ESTUDIOS PREVIOS –
CONTRATACIÓN DIRECTA

FECHA: 2022-ABRIL

ÁREA SOLICITANTE: OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

RESPONSABLE DE LA DIRECCIÓN O GRUPO: JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN JUAN MANUEL PALACIO.

1. INFORMACIÓN GENERAL

1.1. DESCRIPCIÓN DE LA NECESIDAD QUE EL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS – INVIMA, PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos, de conformidad con las funciones asignadas por Ley, es un establecimiento público del orden nacional, de carácter científico y tecnológico, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Salud y Protección Social y perteneciente al Sistema de Salud.[1]

Su objetivo consiste en actuar como institución de referencia nacional en materia sanitaria y ejecutar las políticas formuladas por el Ministerio de Salud y Protección Social en materia de vigilancia sanitaria y de control de calidad de los medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva de conformidad con lo señalado en el artículo 245 de la Ley 100 de 1993 y en las demás normas que la modifiquen, adicionen o sustituyan. [2] Siendo así, el Invima cuenta con jurisdicción a nivel nacional.

Para el cumplimiento y logro de su objetivo, a la Entidad se le asignaron las siguientes funciones:

> *"1. Ejercer las funciones de inspección, vigilancia y control a los establecimientos productores y comercializadores de los productos a que hace referencia el artículo 245 de la Ley 100 de 1993 y en las demás normas que lo modifiquen o adicionen, sin perjuicio de las que en estas materias deban adelantar las entidades territoriales, durante las actividades asociadas con su producción, importación, exportación y disposición para consumo.*
> *2. Certificar en buenas prácticas y condiciones sanitarias a los establecimientos productores de los productos mencionados en el artículo 245 de la Ley 100 de 1993 y expedir los registros*

[1] Artículo 1 del Decreto 2078 de 2012 – *"Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), y se determinan las funciones de sus dependencias"*
[2] Artículo 2, ibídem

sanitarios, así como la renovación, ampliación, modificación y cancelación de los mismos, de conformidad con la reglamentación que expida el Gobierno Nacional.
3. Identificar y evaluar las infracciones a las normas sanitarias y a los procedimientos establecidos, adelantar las investigaciones a que haya lugar y aplicar las medidas sanitarias y las sanciones que sean de su competencia, de conformidad con la Ley 9ª de 1979 y demás normas reglamentarias.
(...)
5. Establecer las directrices técnicas y los procedimientos de operación a ejecutarse por parte de los entes territoriales, en los asuntos competencia del Invima.
6. Liderar, en coordinación con entidades especializadas en la materia, la elaboración de normas técnicas de calidad en los temas de competencia de la entidad.
(...)
8. Actuar como laboratorio nacional de referencia en relación a los productos de su competencia y ejercer la coordinación de la Red de Laboratorios a su cargo.
(...)
10. Dirigir y hacer cumplir en todo el país las funciones de control de calidad y vigilancia sanitaria de los productos de su competencia.
11. Proponer medidas de carácter general para la aplicación de las buenas prácticas o mejores estándares técnicos para la producción, transporte, almacenamiento y las demás actividades dirigidas al consumo de los productos objeto de vigilancia de la entidad.
(...)
15. Adelantar campañas de educación sanitaria con los consumidores, sobre cuidados en el manejo y uso de los productos cuya vigilancia le otorga la ley al Instituto.
17. Desarrollar el sistema de autorización y verificación internacional para productos objeto de vigilancia, de acuerdo con la normatividad vigente.
(...)
19. Otorgar visto bueno sanitario a la importación y exportación de los productos de su competencia, previo el cumplimiento de los requisitos establecidos en las normas vigentes.
(...)" [3]

En tal sentido, el Invima cuenta con diferentes grupos de trabajo, que, de acuerdo a su especificidad, aportan al logro de las metas y objetivos institucionales desde su competencia; como es el caso de la Oficina de Tecnologías de la Información, a la cual se asignaron funciones específicas, dentro de las que se destacan las siguientes:

"1. Asesorar a la Dirección General en la definición de las políticas, planes, programas y procedimientos relacionados con el uso de las tecnologías de información y comunicaciones, que contribuyan a incrementar la eficiencia y eficacia en las diferentes dependencias del Instituto, así como garantizar la calidad en la prestación de los servicios.
3. Promover e intervenir en todas las actividades y programas que tiendan a incorporar el uso de las tecnologías de la información y las comunicaciones en el desarrollo de las actividades relacionadas con los objetivos estratégicos del Invima, como estrategia fundamental en la administración de indicadores de resultado, alertas de gestión del riesgo y calidad en la operación.
(...)

[3] Artículo 4, ibidem

6. Gestionar y consolidar la información estadística a través de los diferentes sistemas de información que soportan la operación de las dependencias del Instituto, como mecanismo de gestión y control de las mismas.
7. Definir las necesidades que en materia de sistemas de información requiera el Invima, para el desarrollo de sus funciones y coordinar su adquisición con la Secretaría General.
8. Desarrollar e implementar las diferentes estrategias y líneas de política relacionadas con la optimización de servicios y acceso en línea a la información entre entidades del Estado y por parte de los ciudadanos, atendiendo las directrices que para el efecto imparta el Gobierno Nacional.
9. Consolidar, desarrollar e implementar las diferentes estrategias, estándares de datos e integración de procesos y líneas de políticas gubernamentales sobre el uso y alcance de las tecnologías de la información y las comunicaciones.
(...)
11. Atender, proponer e implementar las políticas y acciones relativas a la seguridad de la información y de la plataforma tecnológica del Instituto.
(..)
13. Garantizar la aplicación a nivel institucional de los estándares, buenas prácticas y principios para la información estatal.
(...)
16. Apoyar el desarrollo y sostenimiento del Sistema Integrado de Gestión Institucional y la observancia de sus recomendaciones en el ámbito de su competencia.
(...)"

En concordancia con lo anterior, se cuenta con el Grupo de Soporte Tecnológico[4] adscrito a la Secretaria General, al cual le fueron asignadas funciones dentro de las cuales, se destacan las siguientes:

"1. Asegurar la disponibilidad de la infraestructura tecnológica y de comunicaciones basado en los niveles de servicio acordados ante el Instituto.
(...)
3. Administrar y mantener las herramientas y soluciones de seguridad para la plataforma tecnológica y de comunicaciones del Instituto, acorde a los lineamientos de la dirección general, recomendaciones del Gobierno Colombiano y normas internacionales.
(...)
8. Respaldar y asegurar la disponibilidad de los datos informáticos del Instituto bajo el lineamiento de estándares generados por organismos y/o indicaciones del Gobierno Colombiano
(...)
10. Administrar y mantener la seguridad tecnológica y de comunicaciones basada en las políticas establecidas, atendiendo los niveles de permisibilidad de los sistemas, las medidas de protección lógica (software) y los procedimientos que deben seguir los usuarios del Instituto.
(...)".

Así mismo, la Oficina de Tecnologías de la Información cuenta con el Grupo de Informática, cuyas funciones principales se enuncian a continuación:

[4] Resolución No. 2019003641 de 2019, artículo 5, numeral 14, punto 14.5.

"(...)

5. *Proponer las políticas, planes, programas y procedimientos relacionados con la definición, desarrollos, pruebas y mantenimiento de los sistemas de información.*
6. *Diseñar, desarrollar, implementar y mantener soluciones informáticas innovadoras y estables que apoyen la operación del instituto.*

(...)

8. *Definir y adoptar los lineamientos de arquitectura para los sistemas de información y soluciones informáticas en función del riesgo.*
9. *Determinar y delimitar la viabilidad de los requerimientos solicitados por el usuario.*

(...)

12. *Cumplir y generar propuestas para el mantenimiento y mejoramiento continuo de los sistemas de gestión del INVIMA a partir de procesos a cargo de la oficina de Tecnologías de la Información.*

(...)

14. *Aplicar los estándares, buenas prácticas, principios y seguridades definidas por la ley para el trato de la información estatal.*
15. *Atender solicitudes de control de cambios en los sistemas de información dentro de los acuerdos de servicio establecidos por el área.*
16. *Proponer y desarrollar proyectos que permitan la mejora continua de los sistemas de información."*

De otra parte y de acuerdo con el Artículo 14 del Decreto 2078 de 2012 el INVIMA, como entidad encargada de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar, a través de los Grupos de Laboratorio de la Oficina de Laboratorios y Control de Calidad (OLCC), funciones de gran importancia, entre otras, las siguientes:

"(...)

2.Establecer mecanismos para organizar y controlar el funcionamiento de los laboratorios del Invima.

(...)

3. Apoyar a las direcciones misionales del Instituto en la formulación de programas de inspección, vigilancia y control con enfoque de riesgo.

(...)

4. Mantener actualizado el diagnóstico de oferta técnica de los Laboratorios del Invima y de la Red de Laboratorios a su cargo.

(...).

6.Desarrollar las acciones que garanticen la eficiente operación de los laboratorios de acuerdo con los lineamientos de la Dirección General del Instituto.

(...)

7. Atender y gestionar las diferentes solicitudes de análisis de los productos competencia del Invima, requeridas por las direcciones misionales y reportar sus resultados.

(...)

8.Diseñar e implementar los lineamientos de reporte de información para los Laboratorios del Invima y diseñar los lineamientos de reporte de información para la Red de Laboratorios a su cargo

9.Diseñar, validar e implementar un sistema de monitoreo y evaluación que garantice un control eficiente y eficaz de la gestión de los Laboratorios del Invima y de la Red de Laboratorios a su cargo.

(...)
13.Desarrollar las acciones que faciliten la participación de los laboratorios del Invima en programas de evaluación externa del desempeño con instituciones nacionales e internacionales.
(...)
18. Apoyar el desarrollo y sostenimiento del Sistema Integrado de Gestión Institucional y la observancia de sus recomendaciones en el ámbito de su competencia.
(...)".

Es preciso indicar que los laboratorios del Instituto Nacional de Vigilancia de Medicamentos y Alimentos- Invima, se encuentran certificados por entes nacionales e internacionales, convirtiéndose en laboratorio nacional de referencia, por lo que la calidad y seguridad de la información objeto de reporte debe guardar integralidad y generar confianza respecto a los analitos y gestiones desarrolladas.

En atención a los lineamientos descritos, la gestión de la información de la Oficina de Laboratorios y Control de Calidad (desde la entrada de las muestras hasta la generación del informe) se viene realizando en la entidad, a través del Sistema de Información para Laboratorios de Ensayos SILab (SAMPLER); herramienta desarrollada por la empresa Caudales y Muestreos S.A.S., casa matriz del sistema SAMPLER, el cual fue adquirido por el Invima en el año 2017 por medio del contrato número 599, contando con 108 usuarios concurrentes y licenciamiento para instalación, configuración y uso local (On Premise), es decir, que las bases de datos y los ejecutables de la aplicación, fueron instalados en los servidores locales y en los equipos de escritorio de los funcionarios del Invima.

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[5] que comprometió la disponibilidad de los sistemas de información, plataformas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware[6] llamado Blackbyte el cual encriptó[7] la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto, en los que se encontraba el Sistema de Información para Laboratorios de Ensayos (SILab).

Así las cosas, frente a la afectación del sistema de información mencionado en el presente estudio, se pudo comprobar que se comprometió la configuración y acceso a los aplicativos y bases de datos de dicho sistema, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros.

---

[5] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion.

[6] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com

[7] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

Teniendo en cuenta lo anterior y de conformidad con las recomendaciones emitidas por el Comité Técnico de Seguimiento a la Contingencia a través de acta No. 1250072022 de 16 de marzo de 2022, para la mitigación de la crisis presentada en la entidad se precisa en el numeral 2:

> *"2. Restablecimiento de Servicios y Sistemas:*
> *• Sistema de Información para laboratorios SILAB (SAMPLER): este es el sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), y que permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad. Este sistema y toda su información se encuentra encriptada y se requiere de la instalación, configuración, parametrización, pruebas y salida a producción de este por parte del proveedor exclusivo del sistema y dueño del código fuente la empresa Caudales y Muestreos SAS.".*

Así mismo, para ejecutar las actividades definidas en el Plan de Acción[8], dentro de los recursos establecidos para los posibles efectos denominado "*Disminución o pérdida de productividad*", en aras de restablecer los demás servicios del Instituto, se han realizado actividades de manera manual que han permitido llevar a cabo las operaciones de la Oficina de Laboratorios y Control de Calidad, en lo concerniente a la recepción, análisis, analítica y generación de informes y reportes, no obstante se requiere de forma inminente el restablecimiento de este aplicativo toda vez que en el mismo se lleva la trazabilidad y gestión de la información, desde la recepción de la muestra hasta la generación del informe.

Es de advertir que para el 26 de enero de 2022, el Invima suscribió contrato No. 469, con la firma Caudales y Muestreos S.A.S., cuyo objeto consiste en: "*RENOVAR EL SERVICIO DE SOPORTE TÉCNICO PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER*", estableciendo como plazo de ejecución y vigencia lo contemplado en la cláusula octava del citado contrato:

> ***"OCTAVA. PLAZO DE EJECUCIÓN Y VIGENCIA:*** *La vigencia del soporte técnico y servicios conexos serán por un año (1), a partir del día 7 de abril de 2022. La entrega del certificado de renovación del soporte técnico y los Acuerdos de Niveles de Servicios (ANS) deberá realizarse 10 días calendarios siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. El certificado de renovación debe especificar la fecha de inicio y finalización del soporte técnico."*

Bajo este entendido, es menester mencionar que a la fecha de la ocurrencia del incidente cibernético el contrato aún no había iniciado, por lo que se procedió con la resciliación del mismo, para constituir un nuevo negocio jurídico adecuado a las condiciones técnicas requeridas para la mitigación de las consecuencias generadas por la encriptación de la información contenida en el multicitado sistema de información, como quiera que no se puede iniciar las actividades de soporte sobre los sistemas encriptados.

Además de lo anterior, teniendo en cuenta la interoperabilidad que debe tener este sistema de información con los proyectos en actual ejecución por parte del Instituto (Nueva Plataforma y Sivicos III), es necesario restablecerlo, para dar continuidad con las actividades de diseño, desarrollo, implementación y pruebas contempladas en los proyectos mencionados, en aras de procurar la integración entre los aludidos sistemas.

[8] Plan de acción- incidente de seguridad de la información del 6 de febrero de 2022 (actualización del 25 de febrero de 2022)

En tal sentido, es necesario que el proveedor del código fuente y dueño de los derechos patrimoniales de autor de la obra en uso (SAMPLER[9]), realice la instalación, configuración, parametrización, pruebas y validación en producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor, garantizando de este modo la instalación y puesta en marcha óptima para la Oficina de Laboratorios de Control y Calidad del Invima, recuperando la estabilidad del sistema de información y permitiendo la gestión oportuna, recepción, análisis y generación de informes de todas las muestras que se radican en los laboratorios de medicamentos y alimentos del Instituto.

Por lo antes expuesto, se encuentra justificada la necesidad para que el contratista Caudales y Muestreos S.A.S., realice: la instalación de la base de datos de (SILab) Sampler, la configuración y parametrización de los aplicativos, en el nuevo ambiente y el acompañamiento durante la fase de pruebas y validación, previa al inicio de la fase de producción en la nueva plataforma, la cual se detalla en el numeral 2.2. Especificaciones Técnicas del presente documento, actividades que deberán ser validadas por la Oficina de Tecnologías de la Información del Instituto.

De conformidad con lo dispuesto en el artículo 3° de la Ley 80 de 1993 en cuanto a los fines de la contratación estatal, *"Los* servidores *públicos tendrán en consideración que al celebrar contratos y con la ejecución de los mismos, las entidades buscan el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con ella en la consecución de dichos fines.*

Los particulares, por su parte, tendrán en cuenta al celebrar y ejecutar contratos con las entidades estatales que, colaboran con ellas en el logro de sus fines y cumplen una función social que, como tal, implica obligaciones."

Por su parte, el artículo 2° de la Constitución Política indica que son fines esenciales del Estado: *"servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución".* Y es en atención a los mismos, que se requiere de la presente contratación, con el fin de garantizar el interés general en coordinación y articulación con los planes, programas y proyectos del sector salud.

- **CONSECUENCIAS DE NO REALIZAR LA CONTRATACIÓN:**

La no contratación de la instalación, configuración, parametrización, pruebas, puesta en producción y el servicio de soporte técnico, retrasaría la ejecución del plan de acción propuesto para mitigar los efectos de la contingencia generada por el incidente de seguridad.

En consecuencia, de no contar con el funcionamiento del sistema de información de Laboratorios (SILab) basado en el software Sampler, se impactarían las actividades relacionadas con la atención y trazabilidad de los tramites, y correcta operación de los procesos a cargo de la Oficina de Laboratorios y Control de Calidad del Invima, toda vez que, este es el sistema de información que les permite gestionar los análisis y trazabilidad de muestras.

[9] Certificado de Registro de Soporte Lógico de 5 de diciembre de 2012, Libro 13, Tomo 35, Partida 325", expedido por la Dirección Nacional de Derecho de Autor del Ministerio del Interior.

Finalmente, de no contar con el multicitado sistema no se podría continuar con las actividades de diseño, desarrollo, implementación y pruebas que apuntan a la interoperabilidad del mismo con los proyectos de Nueva Plataforma y Sivicos III.

- **CONCORDANCIA DE LA CONTRATACIÓN CON LOS PLANES, PROGRAMAS Y/O PROYECTOS DEL INVIMA:**

La presente contratación se encuentra encaminada al cumplimiento de la misión, visión, objetivos y metas contenidas en la plataforma estratégica del Instituto, de igual manera es importante mencionar que este contrato tiene impacto no solo de carácter operacional, sino de índole estratégico, conforme a los objetivos de la entidad, como se indica a continuación:

Línea Estratégica	Objetivo Estratégico
Objetivo Plan Nacional de Desarrollo.	Buen gobierno.
Objetivo de la estrategia sectorial PND.	Buen gobierno.
Objetivo específico sectorial.	Optimización de la gestión de la información.
Estrategia del objetivo específico sectorial.	Consolidar el Sistema Integral de Información de la Protección Social (SISPRO). Información Estadística (SISPRO).
Objetivo estratégico Invima.	Implementar modernas tecnologías de información y de comunicación de acuerdo con las necesidades de los usuarios, directrices del Gobierno y estándares internacionales.
Estrategias Invima.	1.- Modernización de las tecnologías de la información. 2.- Seguridad de la información. 3.- Interoperabilidad con los demás sistemas de información (Nueva plataforma; Sivicos)
MIPG.	Eficiencia administrativa.
Producto.	Programa modernización de los sistemas de información actuales del Invima.
Proyecto.	Fortalecimientos de los sistemas de información.
Actividades.	Implantar un sistema de soporte a la operación de los laboratorios - Actividades de acompañamiento de la Oficina de Tecnologías de la Información (OTI).
Dependencia.	Oficina de Laboratorios y Control de Calidad de Producto (OLCC).
4 líneas.	Competitividad.
15 acciones.	Análisis de más productos regulados.
Apoyo a la iniciativa de Gobierno en Línea (GEL).	1. Provisión de Servicios en Línea. 2. Datos abiertos. 3. Gobierno de TI.

A su vez, de conformidad con lo previsto en la Ley 152 de 1994, el Estatuto Orgánico de Presupuesto y el Decreto 1082 de 2015, la entidad cuenta con un banco de proyectos de inversión registrado en el Banco Nacional de Programas y Proyectos de Inversión Nacional (BPIN) el cual es administrado por el Departamento Nacional de Planeación.

En consecuencia, de lo anterior, la contratación objeto del presente estudio se encuentra enmarcada dentro del proyecto de inversión, tal y como se describe a continuación:

CÓDIGO BPIN: 2017011000467
NOMBRE DEL PROYECTO DE INVERSIÓN: Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones nacional
OBJETIVO ESPECÍFICO DEL BPIN: Modernizar la arquitectura tecnológica y los sistemas de información del instituto
ACTIVIDAD DEL BPIN A DESARROLLAR: Realizar el proceso de implementación de software e implantación de soluciones, desarrollos, soporte y actualización para los sistemas de información.

2. OBJETO A CONTRATAR CON SUS ESPECIFICACIONES, AUTORIZACIONES, PERMISOS, Y LICENCIAS REQUERIDOS PARA SU EJECUCIÓN.

2.1. OBJETO:

INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER, AFECTADO POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE.

2.2. ESPECIFICACIONES TÉCNICAS:

En el contrato a celebrar, son requeridas las siguientes especificaciones técnicas, las cuales deberán entregarse y garantizarse por parte del contratista, durante todo el término de ejecución de este.

- **Instalación, configuración y parametrización de base de datos:** El personal del contratista hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log.

  Luego de la finalización de la misma, los funcionarios de la Oficina de Tecnologías de la Información podrán validar la instalación, configuración y parametrización en los servidores.

- **Instalación, configuración y parametrización de aplicativos Web:**

  - **Instalación, configuración y parametrización de los servicios WCF de Sampler y los Aplicativos Web:** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor de Muestras, tanto los aplicativos como los servicios web que los alimentan, asegurándose además de documentar el Checklist de control de cambios.

    Teniendo en cuenta que la infraestructura de servidores, bases de datos, balanceadores y elementos de seguridad es provista por el Instituto, se requiere un trabajo conjunto con la Oficina de Tecnologías de la Información, con el objetivo de garantizar que las configuraciones que se realizan sobre esta infraestructura permitan un óptimo funcionamiento del sistema de información de los Laboratorios (SILab) a fin de garantizar

que el sistema quede con tolerancia a fallos y la carga de los servidores se mantenga balanceada.

- **Instalación, configuración y parametrización de los servicios Windows:** El servicio de Sampler notificaciones, se configurará sobre el servidor de base de datos y también se configurará una cuenta de correo del dominio Invima, para que envíe los correos de notificaciones hacia los buzones de correo de los funcionarios de la entidad. La mencionada actividad incluye los tres ambientes Invima[10]: Producción, pruebas y pre-producción.

  Luego de su finalización, los líderes funcionales y los analistas de Laboratorio deberán informar que el sistema de Información de los Laboratorios (SILab) funciona correctamente. Así mismo, el Grupo de Soporte Tecnológico validará el proceso de configuración en los servidores.

- **Instalación, configuración y parametrización de Aplicativos Win:** Los módulos impresor de etiquetas, instrumental, visor BI, sampler tools y lanzador, serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte del proveedor en forma presencial.

- **Pruebas y puesta en marcha del sistema:** El contratista brindará acompañamiento a los líderes funcionales, analistas y/o funcionarios de TI durante el proceso de revisión/validación/pruebas de usuario, que buscan confirmar que el sistema de información de Laboratorios (SILab) funciona de acuerdo con lo esperado.

- **Validaciones:** El Invima validará a través de sus funcionarios, lo cual será certificado por parte del supervisor del contrato y la Jefe de Oficina de los Laboratorios de Control y Calidad, que el Sistema de Información de Laboratorios (SILab), se encuentra debidamente instalado en los servidores, el desempeño es el establecido y no se presentan fallas o bloqueos al momento de la instalación, configuración, parametrización, pruebas y puesta en producción del mismo.

- **Soporte técnico**: Se activa por parte del proveedor Caudales y Muestreos S.A.S., luego que se culmine la instalación, migración, parametrización, pruebas y puesta en producción del aplicativo Sistema de Información de los Laboratorios (SILab) tal como se evidencia en el siguiente cronograma.

Nota 1: De acuerdo al cronograma contenido en la propuesta allegada por el proveedor, el proceso consiste en la instalación de la base de datos de Sampler (SILab), la configuración y parametrización de los aplicativos en el nuevo ambiente y el acompañamiento durante la fase de pruebas y validación previa al inicio de la fase de producción en la nueva plataforma.

Nota 2: El proceso de Instalación en los servidores de los aplicativos web y volver a tener el sistema en alta disponibilidad se toma un máximo de cuatro (4) días hábiles. Instalar los aplicativos

[10] Se entiende por ambiente, como aquellos recursos disponibles para la generación de los procesos productivos que se usan para el desarrollo del ciclo del software; en el caso del Invima, se cuentan con los ambientes de producción, pruebas y pre-producción, propendiendo por las mejores prácticas que el desarrollo de software indica, encaminadas a contar con diferentes ambientes, con el objetivo de garantizar que los elementos que se colocan en operación cumplan con los requerimientos de usuario, performance y que dichos cambios no afectarán el rendimiento y la experiencia de usuario.

Windows en 120 PCs en los siete laboratorios (dos sedes) toma un máximo de cinco (5) días hábiles. La tarea más compleja es asegurar que todos los scripts de instrumental (la conexión con los equipos de laboratorio) funcionen y ello requiere trabajar de la mano con los analistas. Dado que son más de 80 scripts, esta tarea consume la mayor parte del tiempo de la propuesta, alrededor de tres (3) semanas.

Una vez puesto en producción el sistema de información de Laboratorios (SILab) y teniendo en cuenta el uso y las incidencias que se presentan como parte de la dinámica natural del aplicativo, es necesario contar con soporte técnico por parte del proveedor. Para la vigencia 2021 se identificaron las siguientes incidencias, que requirieron atención y soporte por parte del proveedor:

TIPO DE INCIDENCIA	%
Gestión de Inventarios	13%
Gestión de muestras	24%
Gestión de informes	12%
Gestión de equipos	17%
Gestión de base de datos	22%
Gestión de análisis	12%
Total	100%

Gestión de inventarios: Son las incidencias relacionadas con el manejo de inventarios de los diferentes materiales de laboratorios, consumos y preparación de soluciones y medios de cultivo.

Gestión de muestras: Son las incidencias relacionadas con eventos de solicitud de análisis, recepción y radicación de muestras de todo tipo, incluyendo las consultas asociadas a esta información.

Gestión de informes: Son las incidencias relacionadas con eventos asociados a la generación y elaboración de múltiples modelos de informes de resultados, de acuerdo a todas las exigencias normativas que cumplen los laboratorios.

Gestión de equipos: Son las incidencias relacionadas con eventos de creación, modificación y pruebas de scripts (código que permite la transmisión de los datos de un equipo analítico al software Sampler LIMS) en equipos analíticos, como también la generación de modelos de etiquetas para la identificación de muestras y diversos materiales usados en los laboratorios.

Gestión de base de datos: Son las incidencias relacionadas con eventos del manejo de la información de base de datos, como por ejemplo inclusión de nuevos parámetros o variables analíticas

Gestión de análisis: Son las incidencias relacionadas con el manejo del proceso analítico de las muestras Multilaboratorio, procesos de aprobación de mediciones, entre otros eventos.

Por lo anterior, para la vigencia 2022 se requiere contar con un contrato que contemple la instalación, configuración, parametrización, pruebas y puesta a producción y el soporte que permita atender las incidencias relacionadas con el uso del software, garantizando así su correcto funcionamiento y debida documentación de las funciones de la OLCC, ya que el aplicativo soporta el registro de todas las actividades analíticas de los laboratorios, y así se contribuye a su eficacia y su eficiencia.

Así mismo, se garantizará con dicha contratación el cumplimiento de los requisitos exigidos por organizaciones internacionales como: la Organización Mundial de la Salud (OMS), Organización Panamericana de la Salud (OPS) y las normas de calidad (Informe 44 y 45 de OMS, ISO 17025, 2017) y demás normas aplicables a los laboratorios.

La mencionada necesidad de soporte para el sistema de información de laboratorios SILab basado en el Software Sampler, requiere la ejecución de las siguientes actividades de soporte para el año 2022:

- Soporte técnico del Sistema de Información de Laboratorios SILab, para la OLCC, ante las incidencias que se presentan en el desarrollo de las actividades de rutina. Esto con el fin de garantizar el óptimo funcionamiento del aplicativo.

- Mantener la interoperabilidad del Sistema de Información SILab, conforme a las nuevas tecnologías que se están implementando por la OTI, como parte de la transformación digital del Invima.

- Mantener las consultas de reportes de acuerdo con las exigencias normativas vigentes que apliquen para la OLCC.

- Mantener las condiciones de funcionamiento del aplicativo, en relación a consultas, reportes y funcionalidades disponibles.

- Atender las Incidencias, y documentarlas en aras del correcto funcionamiento de la herramienta.

Soporte Funcional: El soporte funcional a los aplicativos Sampler (SILab) es el proceso a través del cual Caudales y Muestreos S.A.S. resuelve las Incidencias reportadas por el personal de los laboratorios de la OLCC en cuanto al funcionamiento de los aplicativos.

NECESIDADES	DESCRIPCIÓN	ENTREGABLES
Instalar, configurar, parametrizar, pruebas y salida a producción	• Etapa I: Instalación, configuración y parametrización de Base de Datos. • Etapa II: Instalación, configuración y parametrización de Aplicativos Web. - Instalación, configuración y parametrización de los servicios WCF de Sampler y los Aplicativos Web. - Instalación, configuración y parametrización de los servicios Windows. • Etapa III: Instalación, configuración y parametrización de Aplicativos Win. • Etapa IV: Pruebas y puesta en marcha del sistema.	Informe de actividades final, con la certificación de los laboratorios del sistema operando en fase de producción
Mantener el servicio de soporte Técnico requerido para el Sistema de Información de Laboratorios (SILab) basado en el Software Sampler, para la Oficina de Laboratorios de Control y Calidad (OLCC)	• Renovar el servicio de soporte técnico de la plataforma SILab, de acuerdo a las especificas técnicas, estipuladas en el numeral 2.2. de este documento.	Certificado de renovación del soporte técnico del Sistema de Información de los Laboratorios SILab. Entregar los Acuerdos de Niveles de Servicio (ANS) para soporte.

ACUERDOS DE NIVELES DE SERVICIO PARA EL SOPORTE DEL SISTEMA DE INFORMACIÓN SILAB.	
El Invima requiere contratar el soporte técnico para el Sistema de Información de los Laboratorios "SILab", para la vigencia 2022 (por el término de un año), el cual está basado en la necesidad de atender las incidencias reportadas por los 150 usuarios activos en los siete (7) laboratorios de la Oficina de Laboratorios de Control y Calidad (OLCC). Dichas incidencias, se reportarán a través de tickets en la plataforma que designe el proveedor y se atenderán de la siguiente forma:	
Soporte de nivel 1 (N1)	Este soporte técnico se basa en la asistencia en primera línea o soporte *Front-End*, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a la gestión de la solución por parte del proveedor. Este tipo de soporte suele tratar con problemas de fácil solución y que están principalmente relacionados con: - Incidencias relativas a usuarios y contraseñas. - Incidencias relativas a olvidos en la ejecución de una parte de los procesos. El personal asignado por el proveedor para la solución de este tipo de incidencias, son técnicos o tecnólogos de sistemas que se encargan de resolverlas en este nivel de soporte. En caso de no poder hacerlo, lo escalarán al nivel correspondiente según la complejidad.
Soporte de nivel 2 (N2)	En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de *Help Desk*, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas, y suelen enfrentarse a incidencias como: - Ajustes a la configuración - Ajustes a los queries (consultas) en la base de datos. - Ajustes en reportes, consolas, etiquetas o scripts de instrumental El personal asignado por el proveedor para la solución de soporte de nivel 2 son tecnólogos / ingenieros de sistemas que se caracterizan por disponer de competencia técnica en el área TI proporcionando un soporte más completo que el N1, pues disponen de un mayor conocimiento del software.
Soporte de nivel 3 (N3)	Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. Entre las principales funciones de este nivel de soporte se encuentran: - Investigación de incidencias complejas. - Rastreo de Logs para entender cuáles fueron los pasos que siguió el usuario. - Ajustes (tuning) de base de datos para asegurar performance. El personal asignado por el proveedor para la solución de soporte de nivel 3 son ingenieros de sistemas que se caracterizan por un alto conocimiento en SILab.

Soporte de nivel 4 (N4)	Este nivel de soporte este asignado a personal de desarrollo de la plataforma SILab y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado son ingenieros de sistemas desarrolladores.
Soporte Excepcional:	El Invima podrá contar con servicio de soporte por fuera del horario establecido 5x8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

Gestión de incidencias en TI: Los funcionarios designados por Invima para el reporte de incidencias deben: Reportar la incidencia en la plataforma www.sampler.com.co que lleva a un registro y clasificación de cada una de ellas. Luego se realiza un diagnóstico que lleva a la resolución y cierre de la incidencia.

Una vez reportada la incidencia, se enviará una comunicación vía email con el fin de informar que la incidencia fue recibida y se encuentra en la etapa de la clasificación y asignación de un técnico N1 o N2 según el tipo. Estos técnicos diagnostican el problema identificando la causa que lo produce, e intentan resolverlo. En caso de conseguirlo se cierra la incidencia como solucionada. Si el problema no se puede resolver se pasa al siguiente nivel de soporte que se encargará de dicha incidencia, contando con la información aportada por el nivel inferior.

El cierre de la incidencia implica que se han llevado a cabo los procedimientos o acciones necesarias para que el problema que sea solucionado. Todo el personal de soporte está enfocado en buscar una resolución rápida y efectiva de los incidentes reportados

Con el objetivo de garantizar una atención de las incidencias de manera oportuna y eficaz se tendrán en cuenta los siguientes aspectos, para determinar el impacto y la criticidad, permitiendo determinar la priorización de la atención de las incidencias, en virtud del diagnóstico requerido y su posterior solución. Se evaluará la criticidad de acuerdo a:

CRITICIDAD

CRITICIDAD	EVALUACIÓN
Impide la Operación del Laboratorio	Alta
Impide parcialmente la Operación del Laboratorio	Media
Genera demoras en la operación	Baja

IMPACTO

IMPACTO	EVALUACIÓN
Afecta transversalmente los laboratorios de la OLCC	Alta
Afecta a uno o mas laboratorios en su operación de diaria	Media
Afecta a uno o más usuarios, pero no impide no impide la operación del Laboratorio.	Baja

Se determinará la relación entre criticidad e impacto, así:

- IMPACTO +	- CRITICIDAD + BAJA	MEDIA	ALTA
ALTO	MEDIA	MEDIA	ALTA
MEDIO	MEDIA	MEDIA	ALTA
BAJO	BAJA	MEDIA	ALTA

De acuerdo a la evaluación anterior se establecerá la priorización, de la siguiente forma:	**EVALUACION** / **Tiempo para diagnóstico** [redacted] / 2 (dos) horas hábiles para hacer el diagnóstico, contadas a partir de que Soporte se entera de la existencia del ticket Alta / El diagnóstico se entrega el mismo día hábil Media / El diagnóstico se entrega al día hábil siguiente a la llegada del ticket Baja / El diagnóstico se entrega al día hábil siguiente a la llegada del ticket En el marco del diagnóstico, el proveedor establecerá e informará los tiempos de solución. Los mismos serán determinados previo análisis para cada una de las incidencias. No obstante, éstos pueden variar en virtud de la complejidad de las investigaciones que se deriven del diagnóstico mencionado.
CONDICIONES DEL SOPORTE TÉCNICO	- Atención de los siete (7) laboratorios y la jefatura de la Oficina de Laboratorios de Control y Calidad (OLCC), a través de hasta máximo un funcionario por cada área para el reporte de incidencias. - Atención hasta de un máximo de 350 incidencias anuales. - Una reunión semanal de una hora con la presentación del estado de los tickets por laboratorio. - Entrega de un informe mensual de los soportes realizados por laboratorio.

- **Atención de incidentes del sistema de información de laboratorios.**

Con el objetivo de garantizar una atención oportuna de los incidentes se tendrán en cuenta los siguientes aspectos, para determinar los niveles de atención; los incidentes que se reporte por el Invima o que el proveedor de manera proactiva identifique cuentan con unos tiempos de respuesta y solución de acuerdo con la severidad que se le asigne a cada uno de estos incidentes, analizando su gravedad y el impacto que tiene sobre el servicio.

Criticidad/ Impacto	Un laboratorio	Dos o mas laboratorios
Impide la Operación del Laboratorio	Alta	Urgente
Impide parcialmente la Operación del Laboratorio	Media	Alta
Genera demoras en la operación	Baja	Media
Tiempo para diagnóstico:		
Urgente	2h hábiles para hacer el diagnóstico, contadas a partir de que Soporte se entera de la existencia del ticket	
Alta	El diagnóstico se entrega el mismo día hábil	
Media	El diagnóstico se entrega al día hábil siguiente a la llegada del ticket	
Baja	El diagnóstico se entrega al día hábil siguiente a la llegada del ticket	

Tiempo de Solución:		
los tiempos establecidos para la solución de incidencias serán determinados previo análisis caso por caso. No obstante, estos pueden variar en virtud de la complejidad de las investigaciones que se deriven del diagnóstico mencionado.		

Nota 3:

- El servicio de soporte Invima es 5x8, de 8 am a 5 pm.
- Las incidencias priorizadas como urgentes requieren un correo de confirmación de parte la Jefatura de la Oficina de Laboratorios de Control y Calidad.
- Los tiempos se establecen siempre en horas hábiles

2.2.1. ENTORNO TECNOLÓGICO

Para asegurar el correcto desarrollo de las actividades de instalación, configuración, parametrización, pruebas y puesta en producción por parte del contratista, se necesita que Invima asegure/provea/cumpla con las siguientes condiciones:

- Invima deberá proveer el conjunto de servidores de aplicación que la Oficina de Tecnologías de la Información aprovisione, al menos dos para poder configurar la característica de tolerancia a fallos mediante balanceo.
- Invima deberá proveer el cluster de SQL Server donde se instalará, configurará y parametrizará la base de datos, a partir del backup que para tal efecto suministre la Oficina de Tecnologías de la Información, correspondientes a cada uno de los ambientes existentes a febrero 04 de 2022 (Producción, Pruebas y Pre-Producción).
- Las máquinas de los funcionarios del laboratorio deberán tener completa disponibilidad para la configuración y parametrización de los aplicativos.
- Disponibilidad de los funcionarios del laboratorio para que desarrollen las pruebas de la plataforma nueva en los tiempos establecidos en el cronograma de actividades.
- En el caso del módulo Instrumental, se requiere disponibilidad de los directorios de red normalmente usados para la descarga de los archivos desde los equipos del laboratorio. Sin la disponibilidad de estas rutas en la red, el proceso del módulo Instrumental tendría que modificarse.
- Las tareas de acompañamiento en la verificación de la plataforma la desarrollaran los funcionarios de la entidad.

- El módulo de Notificaciones envía a través de correo electrónico mensajes alertando a los usuarios de diferentes eventos que acontecen durante la operación del software. Se requiere que el Invima cuente con buzones de correo operativos para que se pueda evidenciar el envío/recepción de tales mensajes.

- Las integraciones con Directorio Activo, Registro Sanitario y el Sistema de Correspondencia que se implementaron principalmente desde la ventana de tres pasos (radicación de muestras) deberán configurarse en los servicios que se encuentran operativos para el momento en que se desarrollen las tareas de parametrización/configuración. Si los servicios no están operativos, esta configuración será solicitada en el futuro a Caudales y Muestreos S.A.S.

- El Invima dispondrá de los siguientes requerimientos técnicos de infraestructura tecnológica:

  - Servidores de aplicación:

Item	Descripción
Tipo Servidor	Virtual
Cantidad	2 (recomendados 3 en producción)
Sistema Operativo	Windows Server 2012 o superior
Espacio en disco	120 Gb – Paginación 20 Gb
Memoria RAM	24Gb (recomendado 32Gb)
Cores	16
Tarjetas de Red	2
IPs	2
Puertos	Según configuración
Protocolos	TCP, HTTP
.Net Framework	4.6
Internet Information Services	Versión 8 o superior

  - Cluster de base de datos:

Item	Descripción
Tipo Servidor	Virtual PROD LOCAL 2 Nodos

Sistema Operativo	Windows Server 2012 R2 Enterprise o superior
Espacio en disco	80 Gb – Paginación 20 Gb
Memoria RAM	64Gb (recomendado 128Gb)
Cores	24
Tarjetas de Red	1
IPs	1
Puertos	1433
Protocolos	TCP
Version de SQL Server	2017 Enterprise Edition SP3
Unidad de almacenamiento	Agregar 1

2.3. CLASIFICACIÓN UNSPSC:

Clasificador de Bienes y Servicios de las Naciones Unidas	
Código	**Descripción**
43231511	Software de Sistemas de Expertos
43232304	Software de sistemas de manejo de base de datos
43232605	Software Analítico y Científico
81102700	Servicio de Diseño e Ingeniería de Sistemas Instrumentados de Control
81111811	Servicios de Soporte técnico y mesa de ayuda
81112202	Actualizaciones o Parches de Software.
81112205	Mantenimiento de Software de sistemas de gestión de base de datos.
81112210	Mantenimiento de software de gestión de sistemas.

2.4. IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:

El artículo 40 de la Ley 80 de 1993, consagra que, *"las estipulaciones de los contratos serán las que de acuerdo con las normas civiles, comerciales y las previstas en esta ley, corresponden a su esencia y naturaleza. (...) Las entidades podrán celebrar los contratos y acuerdos que permitan la autonomía de la voluntad y requieran el cumplimiento de los fines estatales. En los contratos que celebren las entidades estatales podrán incluirse las modalidades, condiciones y, en general, las cláusulas o estipulaciones que las partes consideren necesarias y convenientes, siempre que no sean contrarias a la Constitución, la ley, el orden público y a los principios y finalidades de esta ley y a los de buena administración".*

Teniendo en cuenta lo anterior, la necesidad indicada en el presente documento se satisface con la celebración de un contrato que, de acuerdo a sus elementos esenciales y naturales corresponde a:

Obra	
Consultoría	
Prestación de servicios	X
Concesión	
Compraventa	
Suministro	
Arrendamiento	
Comodato	
Mandato	
Convenio de asociación	
Donación	
Otro	

AUTORIZACIONES, PERMISOS Y LICENCIAS:

Para la suscripción del contrato y su óptima ejecución, se requieren los siguientes documentos:

Autorización / Permiso / Licencia	Requiere	No requiere	Expide
Recomendación del Comité Asesor de Contratación.	X		Comité de Contratación.
Certificado de inclusión en el Plan Anual de Adquisiciones.	X		Coordinador del Grupo de Gestión Contractual.
Acto administrativo que justifica la contratación directa – Artículo 2.2.1.2.1.4.1 del Decreto 1082 de 2015.	X		Ordenador del Gasto.
Certificado de antecedentes disciplinarios, fiscales, judiciales y de medidas correctivas. En caso de que se trate de persona jurídica deben verificarse los del representante legal y los de la persona jurídica como tal.	X		https://www.procuraduria.gov.co/CertWEB/Certificado.aspx?tpo=2 https://www.contraloria.gov.co/control-fiscal/responsabilidad-fiscal/certificado-de-antecedentes-fiscales https://antecedentes.policia.gov.co:7005/WebJudicial/index.xhtml https://srvcnpc.policia.gov.co/PSC/frm_cnp_consulta.aspx
Autorización para contratar del representante legal de la persona jurídica.	X		Cámara de Comercio – Certificado de Existencia y Representación Legal
Certificado de Derechos de Autor	X		Dirección Nacional de Derechos de Autor del Ministerio del Interior.

2.5. OBLIGACIONES DE LAS PARTES:

2.5.1. DEL CONTRATISTA:

2.5.1.1. OBLIGACIONES GENERALES:

1. Realizar las actividades para el óptimo cumplimiento contractual.
2. Actuar con suma diligencia, responsabilidad e idoneidad en la ejecución de las actividades contratadas.
3. Suscribir el acta de inicio, junto con quien ejerza la supervisión del contrato, una vez se cuente con el lleno de los requisitos legales para ellos.
4. Presentar mensualmente o cuando el Supervisor lo requiera, el informe de actividades de acuerdo a los parámetros señalados por el Supervisor.
5. Responder por la integridad, autenticidad, veracidad y fidelidad de la información a su cargo.
6. Guardar la confidencialidad y la reserva de toda la documentación que le haya sido asignadas en desarrollo de sus obligaciones contractuales.
7. Informar oportunamente al supervisor asignado, los inconvenientes que afecten el normal desarrollo del objeto contractual.
8. Cumplir como contratista con las obligaciones del sistema de seguridad social integral contenidas en las normas legales vigentes y parafiscales, según se requiera.
9. Portar el carné que lo identifica como contratista del Instituto en lugar visible o la identificación que corresponda.
10. Dar cumplimiento a las directrices impartidas por la entidad respecto al MECI, gestión de calidad y ambiental, Códigos de Buen Gobierno y Ética de la Entidad.
11. Recibir, custodiar y cuidar la documentación que por razón de su actividad conserve bajo su cuidado o a la cual tenga acceso, sin que pueda reproducirla, divulgarla o publicarla en cualquier medio.
12. Recibir, custodiar y cuidar los bienes y/o elementos que la entidad le proporciona para el desempeño de sus actividades.
13. Responder por sus actos u omisiones en ejecución del contrato, cuando con ello cause perjuicios a la administración o a terceros.
14. Acatar las instrucciones y recomendaciones que, dentro del marco del objeto y obligaciones contractuales, se realicen por parte del Invima a través del supervisor designado.
15. Prestar los servicios contratados con plena autonomía técnica y administrativa.
16. No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley, con el fin de obligarlos a realizar u omitir un hecho o un acto en el ejercicio de sus obligaciones. En caso de que ello presente, informar inmediatamente al Invima.
17. Al finalizar el contrato, deberá devolver todos los elementos entregados por el Invima para su ejecución, soportando por escrito dicha entrega. De igual forma deberá quedar al día con el aplicativo de correspondencia.
18. Cumplir a cabalidad con la normativa vigente que regula su profesión y el objeto contractual.
19. Registrar y actualizar su información y documentos en el Sistema de Información y Gestión del Empleo Público, SIGEP.
20. Las demás que sean necesarias y requeridas para el óptimo cumplimiento contractual.
21. Actualizar conforme a las reglas previstas en la Ley 2013 de 2019 su declaración de rentas y registro de conflictos de intereses.
22. Cargar y actualizar en su usuario del Secop II, sus cuentas de cobro e informes de actividades de conformidad con lo desarrollado durante la ejecución del contrato.
23. Las demás que sean necesarias y requeridas para el óptimo cumplimiento del objeto contractual.

2.5.1.2. OBLIGACIONES ESPECÍFICAS:

1. Instalar, configurar y parametrizar la base de datos SQL Server.
2. Instalar, configurar y parametrizar los Servicios Windows.
3. Instalar, configurar y parametrizar los aplicativos win.
4. Acompañar en las pruebas de los usuarios para la certificación del sistema en ambiente productivo y su posterior puesta en producción.
5. Entregar el certificado de renovación del soporte técnico del Sistema de Información de los Laboratorios (SILab) y los Acuerdos de Niveles de Servicios (ANS) conforme a la propuesta presentada. Dicho documento será entregado dentro de los cinco (5) días calendario siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato al supervisor.
6. Prestar el servicio de soporte técnico para el Sistema de Información de los Laboratorios SILab (Sampler) durante el plazo de la ejecución del contrato.
7. Disponer para el Invima el servicio de soporte telefónico, correo electrónico y Tickets, a fin de atender y dar solución a dudas, consultas, asesoramiento y/o notificación de problemas sobre cualquier aspecto del software.
8. Prestar servicio de soporte técnico de manera remota y en el caso que la actividad lo amerite desplazarse a las sedes de la entidad de la ciudad de Bogotá D.C., para realizar la evaluación de las posibles fallas que puedan presentarse, sin que represente costo adicional para el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima).
9. Atender hasta un máximo de 350 incidencias anuales teniendo en cuenta los acuerdos de niveles de servicio (ANS) señalados el numeral 2.2. del presente documento.
10. Entregar las nuevas versiones o parches disponibles para la licencia (cuando aplique), de acuerdo con los cambios que por soporte técnico haya sufrido el software, sin ningún costo adicional para la entidad, en cuyo caso se debe realizar el respectivo control de cambios con la Oficina de Tecnologías de la información.
11. Realizar un comité funcional semanal de una (1) hora con el fin de hacer seguimiento a las incidencias reportadas por los usuarios del Sistema de Información de los Laboratorios SILab.
12. Entregar un informe mensual que contenga las actividades realizadas durante el soporte técnico del software SILab, las incidencias, acciones y resultado de éstas.
13. Entregar un reporte de los controles de cambios que por ocasión del soporte técnico se realizaron para la atención de incidencias, los cuales deben ser validados por parte de la Oficina de Laboratorios y control de Calidad y la Oficina de tecnologías de la Información.
14. Asistir a reuniones técnicas con el personal que determine el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), durante la ejecución del objeto contractual.
15. Asumir el costo del recurso humano y logístico para la realización de las actividades contratadas, sin que represente costo adicional para el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima).
16. Las demás que se deriven de la ejecución del contrato.

NOTA. Serán propiedad de la Entidad estatal los resultados de los estudios, investigaciones y en general los informes y trabajos realizados para cumplir el objeto de este contrato. El contratista no podrá hacer uso de los mismos para fines diferentes a los del trabajo mismo, sin autorización previa, expresa y escrita de la Entidad Estatal. El contratista puede hacer uso y difusión, de los resultados, informes y documentos, en general de los productos que se generen en desarrollo y ejecución del presente contrato, siempre y cuando con ello no se afecte la confidencialidad de que trata el contrato y se haya obtenido previamente autorización del contratante.

2.5.1.3. DEL CONTRATANTE

1. Ejercer la supervisión del contrato acorde con las normas vigentes y los manuales adoptados por La Entidad.
2. Exigir al contratista la ejecución idónea y oportuna del objeto contratado.
3. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias y garantías a que hubiere lugar.
4. Solicitar la actualización o revisión de los precios cuando se produzcan fenómenos que en alteren en su contra, el equilibrio económico o financiero del contrato.
5. Adelantar las revisiones periódicas de las obras ejecutadas, servicios prestados o bienes suministrados, para verificar que se cumplan con las condiciones de calidad ofrecidas.
6. Exigir que la calidad de los bienes y servicios adquiridos se ajuste a los requisitos mínimos previstos en las normas técnicas obligatorias, las normas técnicas colombianas o internacionales.
7. Actuar de tal modo que no sobrevenga una mayor onerosidad en el cumplimiento de las obligaciones a cargo del contratista.
8. Corregir los desajustes que puedan presentarse y acordar los mecanismos y procedimientos pertinentes para solucionar rápida y eficazmente las diferencias o situaciones litigiosas que se presenten
9. Efectuar el registro presupuestal correspondiente.
10. Pagar el valor de los honorarios pactados, una vez se cumplan los requisitos para ello.
11. Brindar el acompañamiento, la información y la documentación que el contratista requiera para el adecuado cumplimiento de sus obligaciones.
12. Adelantar todas las gestiones necesarias para la correcta ejecución del contrato, incluyendo las suspensiones y reinicios a que haya lugar.
13. Proveer la infraestructura tecnológica necesaria para instalar, configurar, parametrizar, probar y poner en producción el Sistema de Información de Laboratorios (SILab).
14. Proveer el backup al contratista para instalar configurar, parametrizar, probar y poner en producción el Sistema de Información de Laboratorios (SILab)
15. Garantizar la disponibilidad de los directorios de red (Directorio Activo, Repositorio de Archivos, Internet) normalmente usados para la descarga de los archivos desde los equipos del laboratorio.

2.6. PLAZO DE EJECUCIÓN:

El plazo de ejecución del presente contrato se encuentra establecido como se relaciona a continuación:

PLAZO DE EJECUCIÓN		
1	La instalación, configuración, parametrización, pruebas, puesta en marcha del Sistema de Información SILab para la OLCC.	Treinta (30) días previo el cumplimiento de los requisitos

		legales de perfeccionamiento del presente contrato.
2	La vigencia del soporte técnico y servicios conexos.	Un (1) año a partir de la puesta en producción y recibo a satisfacción por parte de la OTI y la OLCC del Sistema de Información de laboratorios (SILAB).

Nota: La entrega del certificado de renovación del soporte técnico y los Acuerdos de Niveles de Servicios (ANS) deberá realizarse 3 días calendarios siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. El certificado de renovación debe especificar la fecha de inicio y finalización del soporte técnico.

2.7. LUGAR DE EJECUCIÓN O ENTREGA:

El objeto del contrato será ejecutado en las instalaciones de la sede principal del INVIMA ubicada en la Carrera 10 N° 64 - 60, en la sede CAN, Av. Calle 26 # 51 – 20, en la sede Montevideo Carrera 68 D No 17-11 y/o en donde la Entidad lo designe en la Ciudad de Bogotá D.C., de acuerdo con las condiciones estipuladas en el contrato suscrito; así mismo por la características actuales de la emergencia decretada por el gobierno nacional como efecto de la pandemia del Covid – 19, se realizarán actividades y/o reuniones de manera virtual que permitan el cumplimento del objeto contractual.

- **ACCESO REMOTO (VPN):**
  El instituto facilitará para el desarrollo del proyecto, un acceso VPN al contratista al mapa de procesos y los servidores con el fin de que pueda acceder y consultar la información que se solicite y se autorice por parte del supervisor del contrato. El Invima no proveerá puestos de trabajo permanentes para el personal contratista que esté a cargo de la prestación del servicio.

- **SALAS DE REUNIONES VIRTUALES**

  Se podrá disponer de recursos virtuales a través de herramientas tecnológicas con las que cuenta el Instituto como Office 365 (Microsoft Teams), para el desarrollo de reuniones previa solicitud y programación con el supervisor del contrato o responsable de la sede donde se requiera desarrollar actividades de revisión, discusión y/o presentación.

2.8. SUPERVISIÓN CONTRACTUAL

De conformidad con el Manual de Supervisión e Interventoría adoptado por el Invima, la supervisión de la ejecución de las obligaciones contractuales estará a cargo de quien ejerza la Coordinación del Grupo de Informática de la Oficina de Tecnologías de la Información (OTI).

El supervisor asume la responsabilidad por el seguimiento y control del contrato, así como la correcta y cabal ejecución del mismo, de acuerdo a los mecanismos consagrados en el Ordenamiento Jurídico.

El supervisor del contrato deberá verificar, entre otros aspectos, como requisito para el pago de los honorarios a que haya lugar, que el contratista se encuentre al día con sus obligaciones relativas al Sistema de Seguridad Social Integral y parafiscales en caso de que así corresponda.

3. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS.

En virtud de lo dispuesto en el articulo 42 de la Ley 80 de 1993, el cual dispone:

> ARTÍCULO 42. DE LA URGENCIA MANIFIESTA. <Aparte tachado derogado por el artículo 32 de la Ley 1150 de 2007> Existe urgencia manifiesta cuando la continuidad del servicio exige el suministro de bienes, o la prestación de servicios, o la ejecución de obras en el inmediato futuro; cuando se presenten situaciones relacionadas con los estados de excepción; cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, en general, cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o ~~concurso~~ públicos (...).

A su vez, el literal a) del numeral 4° del artículo 2 de la Ley 1150 de 2007 consagra que la **contratación directa** procede para los casos cuando se emita acto administrativo que declara la ***urgencia manifiesta.***

La entidad declaró a través de acto administrativo: *"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte"*, el cual hace parte integral del presente estudio previo.

Sobre el particular, la Corte Constitucional[11] indicó que:

> *"La "urgencia manifiesta" es una situación que puede decretar directamente por cualquier autoridad administrativa sin autorización previa, a través de acto debidamente motivado. Que ella existe o se configura cuando se acredite la existencia de uno de los siguientes presupuestos: - Cuando la continuidad del servicio exija el suministro de bienes, o la prestación de servicios o la ejecución de obras en el inmediato futuro. - Cuando se presenten situaciones relacionadas con los estados de excepción. - Cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, - en general cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o concursos públicos".*

El Consejo de Estado[12], mediante pronunciamiento del 27 de abril de 2006, manifestó:

> *"Se observa entonces cómo la normatividad que regula el tema de la urgencia en la contratación estatal, se refiere a aquellos eventos en los cuales pueden suscitarse hechos que reclamen una actuación inmediata de la Administración, con el fin de remediar o evitar males presentes o futuros pero inminentes, provocados bien sea en virtud de los estados de excepción, o por la paralización de*

[11] Corte Constitucional, Sentencia C-772 de 1998, 10 de diciembre de 1998. Magistrado Ponente: Fabio Morón Díaz.
[12] Consejo de Estado, Sentencia del 27 de abril de 2006, Expediente número 14275. Consejero Ponente: Ramiro Becerra Saavedra.

los servicios públicos, o provenientes de situaciones de calamidad o hechos constitutivos de fuerza mayor o desastres, o cualquier otra circunstancia similar que tampoco dé espera en su solución, de tal manera que resulte inconveniente el trámite del proceso licitatorio de selección de contratistas reglado en el estatuto contractual, por cuanto implica el agotamiento de una serie de etapas que se toman su tiempo y hacen más o menos largo el lapso para adjudicar el respectivo contrato, circunstancia que, frente a una situación de urgencia obviamente resulta entorpecedora, porque la solución en estas condiciones, puede llegar tardíamente, cuando ya se haya producido o agravado el daño. En estas estipulaciones, se hace evidente el principio de la prevalencia del interés general, en este caso, por encima de las formalidades de las actuaciones administrativas, puesto que si aquel se halla afectado o en peligro de serlo, el régimen jurídico debe ceder y permitir que las soluciones se den en la mayor brevedad posible, así ello implique la celebración de contratos sin el cumplimiento de los requisitos legales de selección del contratista y aún, la ejecución de los mismos, sin que medie la formalidad del contrato escrito, si la gravedad de las circunstancias así lo exige".

En virtud de la obligación del Instituto de garantizar el derecho a la salud a través de la salvaguarda de la seguridad sanitaria del país, se requiere mantener la continua prestación del servicio de la entidad y, en atención a la imposibilidad, por razones de tiempo, de seleccionar a los contratistas mediante los procesos ordinarios de selección dispuestos por la Ley 80 de 1993 y demás normas reglamentarias, se requiere declarar la Urgencia Manifiesta, en aras de dar cumplimiento a la Constitución y la Ley, teniendo en cuenta los recursos asignados para tal fin.

4. VALOR ESTIMADO DEL CONTRATO, JUSTIFICACIÓN Y FORMA DE PAGO:

El valor del contrato a celebrar será hasta por la suma de **CUATROCIENTOS SETENTA Y SIETE MILLONES CIENTO NOVENTA MIL PESOS M/CTE ($477.190.000)** incluido IVA y demás impuestos, tasas y contribuciones de ley a que haya lugar.

Para estimar el presupuesto oficial del presente proceso el Instituto solicitó cotización mediante correo electrónico al proveedor Caudales & Muestreos S.A.S., teniendo en cuenta que es el dueño de los derechos de autor, como consta en la certificación de soporte lógico expedido por el Ministerio del Interior, obteniéndose la siguiente información:

NECESIDADES	DESCRIPCIÓN	ENTREGABLES	VALOR SEGÚN OFERTA SIN IVA
Instalar, configurar, parametrizar, pruebas y salida a producción	• Etapa I: Instalación, configuración y parametrización de Base de Datos. • Etapa II: Instalación, configuración y parametrización de Aplicativos Web. - Instalación, configuración y parametrización de los servicios WCF de Sampler y los Aplicativos Web. - Instalación, configuración y parametrización de los servicios Windows. • Etapa III: Instalación, configuración y parametrización de Aplicativos Win. • Etapa IV: Pruebas y puesta en marcha del sistema.	Informe de actividades final, con la certificación de los laboratorios del sistema operando en fase de producción	$ 120.000.000
Garantía de Servicio de soporte Técnico requerido para el Sistema de Información de Laboratorios (SILab) basado en el Software Sampler, para la Oficina de Laboratorios de Control y Calidad (OLCC)	• Garantizar el servicio de soporte técnico de la plataforma SILab, de acuerdo a las especificas, técnicas estipuladas en el numeral 2.2 de este documento.	Certificado de renovación del soporte técnico del Sistema de Información de los Laboratorios SILab. Entregar los Acuerdos de Niveles de Servicio (ANS) para soporte.	**$ 281.000.000**
	SUBTOTAL SIN IVA $ 401.000.000		
TOTAL CON IVA $ 477.190.000			

4.1. FORMA DE PAGO:

El Invima efectuará al proveedor un único pago, una vez se entreguen y reciban a satisfacción por parte del supervisor del contrato la instalación, configuración, parametrización, pruebas y salida a producción del sistema de información de los Laboratorios (SILab); así como la entrega del certificado de activación del servicio de soporte técnico.

Lo anterior, de acuerdo con el programa anual mensualizado PAC, previa presentación del informe de actividades y sus anexos en debida forma, certificación de cumplimiento expedida por el

supervisor y pago de las cotizaciones al sistema general de seguridad social en salud, pensiones y riesgos laborales correspondiente.

NOTA 1: Se recibirán facturas los primeros quince (15) días del mes.

NOTA 2: Generar facturación electrónica en caso de encontrarse dentro de los sujetos obligados para tal efecto de acuerdo al artículo 1.6.1.4.2. del Decreto 1625 de 2016.

4.2. APROPIACIÓN PRESUPUESTAL

El valor anteriormente indicado se cancelará con base a la siguiente información:

Presupuesto	Inversión
CDP N°.	Ver anexo.
Valor del CDP	$ 477.190.000.
Nombre proyecto de inversión	Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones nacional
Código del producto SIIF	C-1903-0300-6-0-1903045
Actividad SUIFP	Realizar el proceso de implementación de software e implantación de soluciones, desarrollos, soporte y actualización para los sistemas de información.
Código actividad interna	42-6-1.
Nombre de la actividad	1. Fortalecimiento Tecnológico-software-IVC.

5. CRITERIOS DE SELECCIÓN MÁS FAVORABLES PARA LA ENTIDAD:

De conformidad con el artículo 5° de la Ley 1150 de 2007, *"es objetiva la selección en la cual la escogencia se haga al ofrecimiento más favorables la entidad y a los fines que ella busca, sin tener en consideración factores de afecto o de interés y, en general, cualquier clase de motivación subjetiva (...)"*

En consecuencia, el contratista que se requiere debe reunir los siguientes criterios de capacidad jurídica, idoneidad y experiencia que a continuación se indican:

Requisitos de capacidad Jurídica	Requisitos de idoneidad	Requisitos de experiencia
• Certificado de existencia o representación Legal emitido por la Cámara de Comercio a enero 2022. • Propuesta de servicios dirigida al Invima. • Copia legible del documento de identidad del representante legal de la persona jurídica. • Copia del documento que soporte la definición de la situación militar, del representante legal de la persona jurídica. • Certificado de estar a paz y salvo con las obligaciones relativas al sistema de seguridad social integral y parafiscales. • Copia del Registro Único Tributario actualizado. • Formato de declaración de bienes y rentas y registro de conflictos de interés. (Ley 2013 de 2019). • Certificación cuenta bancaria. • Certificados de antecedentes disciplinarios, fiscales, judiciales y de medidas correctivas del representante legal de la persona jurídica. • Formato de declaración de imparcialidad y conflicto de interés. • Formato de compromiso de confidencialidad de la información. • Hoja de Vida de la Función Pública debidamente diligenciada, por parte del representante legal.	Certificado de Derechos de Autor, expedido por la Oficina de Registro del Ministerio del Interior (Dirección Nacional de Derecho de Autor, Unidad Administrativa Especial Oficina de Registro).	Entregar a la entidad, cuatro (4) certificaciones de contratos ejecutados cuyos objetos estén encaminados a la implementación, instalación, configuración de software y prestación de servicios de soporte técnico del mismo.

6. ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

De conformidad con lo establecido en el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015 que contiene: *"**Evaluación del Riesgo**. La Entidad Estatal debe evaluar el riesgo que el Proceso de Contratación representa para el cumplimiento de sus metas y objetivos, de acuerdo con los manuales y guías que para el efecto expida Colombia Compra Eficiente."* Y acorde con lo los dispuesto en el Manual para la Identificación y Cobertura del Riesgo en los procesos de contratación. Donde se establecen los parámetros y los elementos a tener en cuenta a la hora de hacer el análisis del riesgo:

IDENTIFICACIÓN Y COBERTURA DEL RIESGO

1. CONTEXTO DEL PROCESO DE CONTRATACIÓN:

OBJETO	"Instalar, configurar, parametrizar, realizar pruebas y puesta en producción, garantizando el soporte funcional para el sistema de información de laboratorios (silab) basado en el software sampler, afectado por el incidente de seguridad de la información generado por el ataque de un ransomware.
PRESUPUESTO OFICIAL:	**$477.190.000**
LUGAR DE EJECUCIÓN DEL CONTRATO:	El objeto del contrato será ejecutado en las instalaciones de la sede principal del INVIMA ubicada en la Carrera 10 N° 64 - 60, en la sede CAN, Av. Calle 26 # 51 – 20, en la sede Montevideo Carrera 68 D No 17-11 y/o en donde la Entidad lo designe en la Ciudad de Bogotá D.C., de acuerdo con las condiciones estipuladas en el contrato suscrito; así mismo por la características actuales de la emergencia decretada por el gobierno nacional como efecto de la pandemia del Covid -- 19, se realizarán actividades y/o reuniones de manera virtual que permitan el cumplimento del objeto contractual.

2. IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS RIESGOS

Para la identificación de Riesgos se tuvo en cuenta la clasificación de clase, fuente, etapa del proceso y tipo de riesgo definido en el *"Manual para la identificación y Cobertura del riesgo en los Procesos de Contratación"* expedido por Colombia Compra Eficiente, en los siguientes aspectos: a) los eventos que pueden afectar la adjudicación y firma del contrato, como resultado del proceso de contratación, b) los eventos que pueden alterar la ejecución del contrato, c) eventos que pueden afectar el equilibrio económico del contrato, d) eventos previsibles que pueden impedir que la Entidad satisfaga la necesidad motivo de la contratación.

3. EVALUACIÓN Y CALIFICACIÓN DEL RIESGO

3.1. PROBABILIDAD DEL RIESGO

	CATEGORIA	VALORACIÓN
PROBABILIDAD	Raro (puede ocurrir excepcionalmente)	1
	Improbable (puede ocurrir en cualquier momento futuro)	2
	Posible (puede ocurrir en cualquier momento)	3
	Probable (probablemente pueda ocurrir)	4
	casi cierto (ocurre en la mayoría de las circunstancias)	5

3.2. IMPACTO DEL RIESGO

		IMPACTO				
CALIFICACIÓN CUALITATIVA		Obstruye la ejecución del contrato de manera intrascendente	Dificulta la ejecución del contrato de manera baja. Aplicando medidas mínimas se puede lograr el objeto contractual	Afecta la ejecución del contrato sin alterar el beneficio para las partes	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual
CALIFICACIÓN MONETARIA		Los sobrecostos no representan más del uno por ciento (1%) el valor del contrato	Los sobrecostos no representan más del cinco por ciento (5 %) del valor del contrato	Genera un impacto sobre el valor del contrato entre el cinco por ciento (5%) y el quince por ciento (15%) del valor del contrato	Incrementa el valor del contrato entre quince por ciento (15%) y el treinta por ciento (20%)	Impacto sobre el valor del contrato en más de treinta por ciento (15%) del valor del contrato
CATEGORIA	VALORACIÓN	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO

		1	2	3	4	5

3.2. VALORACIÓN DEL RIESGO

			IMPACTO				
		CALIFICACIÓN CUALITATIVA	Obstruye la ejecución del contrato de manera intrascendente	Dificulta la ejecución del contrato de manera baja. Aplicando medidas mínimas se puede lograr el objeto contractual	Afecta la ejecución del contrato sin alterar el beneficio para las partes	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual
		CALIFICACIÓN MONETARIA	$25,410	$127,052	$381,157	$762,313	$787,724
	CATEGORIA	VALORACIÓN	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO
			1	2	3	4	5
PROBABILIDAD:	Raro	1	2	3	4	5	6
	Improbable	2	3	4	5	6	7
	Posible	3	4	5	6	7	8
	Probable	4	5	6	7	8	9
	casi cierto	5	6	7	8	9	10

3.4. CATEGORIA DEL RIESGO

VALORACIÓN	CATEGORIA
10, 9 Y 8	Riesgo Extremo
6 Y 7	Riesgo Alto
5	Riesgo Medio
3, 2 Y 1	Riesgo Bajo

4. ASIGNACION Y TRATAMIENTO DE LOS RIESGOS

N°	Clase	Fuente	Etapa	Tipo	Descripción (que Puede Pasar Y Como Puede Ocurrir)	Consecuencia de la ocurrencia del riesgo	Probabilidad	Impacto	Valoración Del Riesgo (n°)	Categoría	¿a quién se le asigna?
1	Especifico	Externo	Ejecución	Operacional	Falta de correcciones o imperfectos detectados durante el uso y/o apropiación por parte del usuario funcional del software "Silab".	Fallas en el desarrollo de las funcionalidades y actualizaciones del software "Silab".	1	4	5	Medio	Contratista
2	Especifico	Externo	Ejecución	Operacional	Bajo rendimiento en las formulaciones empleadas para el desarrollo de las metodologías y funcionalidades de acuerdo a las necesidades identificadas por los analistas de la oficina de laboratorios y control de calidad.	Retrasos y/o reprocesos en la operación de actividades relacionadas con la funcionalidad del software Silab"	2	4	6	Alto	Contratista
3	Especifico	Externo	Ejecución	Operacional	Falta de conocimiento y/o actualización en el desarrollo tecnológico del software, respecto a los cambios técnicos, normativos y procedimentales que se requieran por parte de la oficina de laboratorio y control y calidad.	Retrasos y/o reprocesos en la operación de actividades por falta de actualización relacionadas con la funcionalidad del software " SILab"	2	4	6	Alto	Invima – Contratista
4	Especifico	Externo	Ejecución	Operacional	Pérdida de la confidencialidad, integridad y disponibilidad de la Información Institucional	Uso, modificación o eliminación no autorizada de la información Institucional	3	2	5	Medio	Contratista
5	Especifico	Externo	Ejecución	Operacional	Demora en proveer las actualizaciones durante la ejecución del contrato	Retrasos y/o reprocesos en la operación de actividades relacionadas con la funcionalidad del software	3	4	7	Alto	Contratista

6	Específico	Externo	Ejecución	Operacional	Ausencia o demora en el soporte técnico y operativo de acuerdo a la necesidad requerida por la entidad al contratista	Retrasos y/o reprocesos en la operación de actividades relacionadas con la funcionalidad del software y en las actividades de los funcionarios de la entidad	3	4	7	Alto	Contratista
7	General	Externo	Ejecución	Financiero	Cambio en la legislación laboral y/o tributaria durante la vigencia del contrato	Alteración en las condiciones iniciales del contrato, respecto a los cambios tributarios o normativos del objeto del contrato.	1	2	3	Bajo	Invima -- Contratista
8	GENERAL	EXTERNO	EJECUCIÓN	OPERACIONAL	ATAQUE CIBERNÉTICO A LA INFRAESTRUCTURA TECNOLÓGICA DE LA ENTIDAD O REINCIDENCIA	ENCRIPTACIÓN Y/O PERDIDA DE LA INFORMACIÓN; INDISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS A USUARIOS INTERNOS Y EXTERNOS	3	5	8	RIESGO EXTREMO	CONTRATISTA Y CONTRATANTE

N°	Tratamiento / Controles A Seguir Implementando	Impacto Después Del Tratamiento				Persona Responsable Por Implementar El Tratamiento	Fecha (Inicio del Tratamiento)	Fecha (Tratamiento Completo)	Monitoreo Y Revisión	
		Probabilidad	Impacto	Valoración	Categoría				¿Cómo se realiza el Monitoreo?	Periodicidad ¿cuándo?
1	Desarrollar pruebas de funcionamiento luego de detectar imperfecciones durante el soporte y mantenimiento que sea prestado por parte del contratista de las funcionalidades del software, "Silab" Silab" para garantizar la ejecución del mismo.	1	2	3	Bajo	Contratista	Durante la etapa de ejecución	Al finalizar el contrato	Verificando que el contratista realice las pruebas necesarias para garantizar el correcto funcionamiento del software.	Durante la vigencia del contrato.

2	Verificar el funcionamiento que las formulaciones empleadas en el software para las metodologías de los ensayos cumplan con las condiciones técnicas y regulatorios de acuerdo con la necesidad de la oficina de laboratorios.	1	2	3	Bajo	Supervisor del Contrato / Contratista	Durante la etapa de ejecución	Al finalizar el contrato	Revisar y verificar con las pruebas de funcionamiento que las formulaciones empleadas en el software se desarrollen de acuerdo a lo requerido	Durante la vigencia del contrato.
3	Verificar y revisar que el contratista preste el soporte y mantenimiento de las incidencias reportadas durante la ejecución del contrato, que se realicen bajo los estándares de calidad en actualización técnica, procedimental y normativa, de acuerdo con las necesidades identificadas por la oficina de laboratorio control de calidad.	1	3	4	Bajo	Supervisor del Contrato / Contratista	Inmediatamente, al iniciar la etapa de ejecución del contrato	Durante la etapa de ejecución del contrato	Verificando que el desarrollo de las funcionalidades si se encuentre con los procedimientos y cambios tecnológicos vigentes dentro del software.	Durante la vigencia del contrato.
4	Verificar aplicación de las Políticas de Seguridad de Información de la institución	2	1	3	Medio	Contratista - Oficina de Tecnologías de la Información - Grupo de Soporte Tecnológico	Inmediatamente, al iniciar la etapa de ejecución del contrato	Al finalizar la ejecución del contrato	Permanente revisión de controles informáticos y seguimiento del supervisor del contrato.	Permanente, durante la ejecución del contrato
5	Garantizar la prestación del servicio de actualizaciones durante el tiempo de ejecución del contrato	2	3	4	Bajo	Contratista	Inmediatamente, al iniciar la etapa de ejecución del contrato	Al finalizar la ejecución del contrato	Verificando vía correo electrónico la versión actualizada disponible	Permanente, durante la ejecución del contrato

6	Exigir la responsabilidad del contratista del cumplimiento de los niveles de servicio para el soporte y mantenimiento. En caso de no obtener resultados satisfactorios, se aplicaría el cumplimiento de las garantías del contrato.	2	3	5	Medio	Supervisor del Contrato / Contratista	Inmediatamente, al iniciar la etapa de ejecución del contrato	Al finalizar la ejecución del contrato	Verificación de las soluciones y los tiempos de respuesta de las preguntas, requerimientos o solicitudes realizadas al contratista	Al momento en que se hagan requerimientos de soporte técnico y operativo, durante la ejecución del contrato	
7	Deber de información y actualización por parte del contratista y el contratante sobre cambios en la normatividad que regula el bien y/o servicio durante la vigencia del contrato	1	2	3	Bajo	Supervisor del Contrato / Contratista	Al iniciar la etapa de contratación	Al finalizar el contrato	Actualización sobre la normatividad a través de la verificación de los medios oficiales de los entes estatales y de los medios publicitarios	Cada vez que el gobierno apruebe nuevas leyes, decretos o normas	

NOTA 1. Para estructurar la siguiente Matriz de Riesgos se tuvo en cuenta, los siguientes aspectos: a) los eventos que pueden afectar la adjudicación y firma del contrato como resultado del proceso de contratación, b) los eventos que pueden alterar la ejecución del contrato, c) eventos que pueden afectar el equilibrio económico del contrato, d) eventos previsibles que pueden impedir que la Entidad satisfaga la necesidad motivo de la contratación. **NOTA 2. FUERZA MAYOR O CASO FORTUITO,** Son los eventos naturales previsibles en los cuales no hay intervención humana que puedan tener impacto en la ejecución del contrato, por ejemplo los temblores, inundaciones, lluvias, sequías, entre otros. En caso de llegar a presentarse, la distribución de este se realizará 50% para la entidad y 50% para el contratista.

No obstante, lo anterior, el contratista tendrá la absoluta responsabilidad en la ejecución de todas las actividades necesarias para la total y cabal ejecución del objeto contractual. Por lo tanto, deberá considerar, previo a la suscripción del contrato todos los aspectos técnicos, económicos, financieros, para evitar la ocurrencia de situaciones y materialización de riesgos que afecten la cabal ejecución del contrato, y en tal evento, serán de su cargo y responsabilidad, los gastos que esto conlleve.

7. GARANTÍAS A EXIGIR EN EL PROCESO DE CONTRATACIÓN:

En el presente proceso de selección y, de acuerdo con el análisis del riesgo efectuado, serán exigibles las siguientes garantías:

GARANTÍA SOLICITADA	CUANTÍA DEL AMPARO-SUFICIENCIA DE LA GARANTÍA	VIGENCIA DEL AMPARO
Cumplimiento del contrato.	20%	Vigencia por el termino de ejecución del contrato y cuatro (4) meses más, contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.
Calidad y Correcto Funcionamiento de los Bienes.	20%	Vigencia por el término de ejecución del contrato y seis (6) meses más, contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.
Calidad del servicio prestado.	20%	Vigencia por el término de ejecución del contrato y seis (6) meses más, contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.

Pagos de Salarios, prestaciones legales e indemnizaciones laborales.	5%	Vigencia por el término de ejecución del contrato y tres (3) años más, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.

8. ACUERDOS COMERCIALES APLICABLES AL PROCESO DE SELECCIÓN:

De conformidad con el *Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación* publicado por la Agencia Nacional de Contratación – Colombia Compra Eficiente, las Entidades Estatales que adelantan sus Procesos de Contratación con las Leyes 80 de 1993 y 1150 de 2007, no deben hacer este análisis en las modalidades de selección de contratación directa, mínima cuantía o para la enajenación de bienes del Estado.

Siendo lo anterior así, el presente proceso no se encuentra cobijado por Acuerdo Comercial alguno.

ANÁLISIS DEL SECTOR

1. SECTOR OBJETO DEL ESTUDIO

Dentro de los aspectos generales del mercado se pudo identificar el sector de la actividad económica a la cual pertenece el bien, producto o servicio del objeto contractual.

Sector terciario o sector de servicios: Incluye todas aquellas actividades que no producen una mercancía en sí, pero que son necesarias para el funcionamiento de la economía. Como ejemplos de ello tenemos el comercio, los restaurantes, los hoteles, el transporte, los servicios financieros, las comunicaciones, los servicios de educación, los servicios profesionales, el Gobierno, etc.

Este sector tiene como funciones principales apoyar la dirección, organización y facilitar la actividad productiva de los otros sectores especialmente el primario y el secundario y la realización de actividades de soporte a la vida cotidiana de una población determinada. Aunque se le considera un sector de la producción, propiamente su papel principal se encuentra en los dos pasos siguientes de la actividad económica: la distribución y el consumo.[13]

Los posibles oferentes para esta contratación están ubicados dentro del tercer sector de la economía o sector servicios. Incluye todas aquellas actividades que no producen una mercancía en sí, pero que son necesarias para el funcionamiento de la economía. Es indispensable aclarar que los dos primeros sectores producen bienes tangibles, por lo cual son considerados como sectores productivos. El tercer sector se considera no productivo, puesto que no produce bienes tangibles, pero, sin embargo, contribuye a la formación del ingreso nacional y del producto nacional. La presente contratación hace referencia al sector servicios, específicamente en la actividad económica de Información y Comunicaciones.

1.1. PRODUCTOS INCLUIDOS DENTRO DEL SECTOR

13 Fuente: www.dane.gov.co

De acuerdo con la investigación realizada se evidenció que en el Clasificador de Bienes y Servicios de las Naciones Unidas los servicios relacionados con el presente objeto del proceso contractual son:

Clasificador de Bienes y Servicios de las Naciones Unidas	
Código	**Descripción**
81111811	Servicios de Soporte técnico y mesa de ayuda
81112202	Actualizaciones o Parches de Software.
81112205	Mantenimiento de Software de sistemas de gestión de base de datos.
81112210	Mantenimiento de software de gestión de sistemas.

1.2. AGENTES INCLUIDOS EN EL SECTOR

- Ministerio de las Tecnologías de la Información, MinTIC
- Superintendencia de Industria y Comercio.

1.3. GREMIOS Y ASOCIACIONES QUE PARTICIPAN EN EL SECTOR

Las entidades y organizaciones relacionadas con la ingeniería en Colombia son:

- ANDI. Asociación Nacional de Empresarios de Colombia.
- ISO. International Organization for Standardization.
- FENALCO. Federación Nacional de Comercio.
- ACOPI. Asociación Colombiana de Pequeños Industriales.
- ICONTEC – Instituto Colombiano de Normas Técnicas y Certificación
- SICAL – Subsistema Nacional de la Calidad.
- CCIT. Cámara Colombiana de Informática y Telecomunicaciones.
- FEDESOFT. Federación Colombiana de la Industria de Software y Tecnologías Informáticas.
- Observatorio TI.
- **Asociaciones universitarias y estudiantiles de ingeniería** (Asociación Colombiana de Facultades de Ingeniería ACOFI, la Sociedad Colombiana de Ingenieros, Consejo Profesional de Ingeniería Química CPIQ).
- **Capítulos y redes por titulaciones de ingeniería.**
- Asociaciones regionales de ingenieros.
- **Sociedad Colombiana de Ingenieros,** SCI, Ley 46 de 1904,
- **Consejo Profesional Nacional de Ingeniería,** COPNIA, Ley 842 de 2003.

1.4. VARIABLES ECONÓMICAS QUE AFECTAN EL SECTOR

El Banco Mundial clasifica las economías del mundo en cuatro grupos de ingreso: alto, mediano alto, mediano bajo y bajo. Esta clasificación se basa en el Ingreso Nacional Bruto (INB) per cápita calculado usando el método del Atlas.

Todos los años el 1 de julio se actualiza la clasificación debido a dos razones:

1. En cada país, factores como el crecimiento del ingreso, la inflación, los tipos de cambio y los cambios demográficos influyen en el INB per cápita.
2. Para mantener los umbrales en dólares que separan las clasificaciones fijadas en términos reales, se ajustan según la inflación.

Esta clasificación posiciona a Latinoamérica y a Colombia en una economía de ingresos medios y altos dentro de los 42 países que componen esta categoría.

Existen diversos factores que influyen o determinan el crecimiento o decrecimiento económico del sector económico estudiado, para lo cual se analizarán diferente indicadores y cifras:

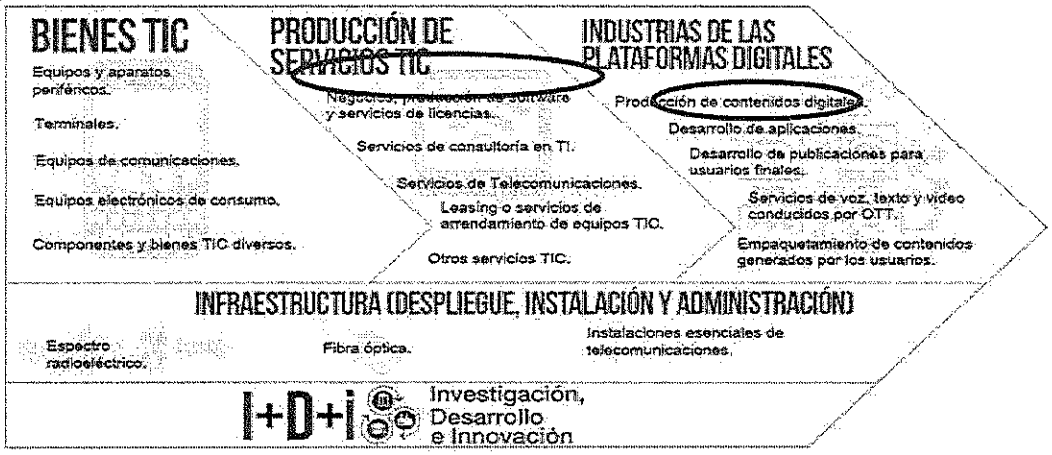
PRODUCTO INTERNO BRUTO: El producto interno bruto es considerado la medida más importante para conocer el bienestar económico de cualquier región en el mundo, aunque en él no se vean reflejados temas como el impacto en el medio ambiente, la distribución de la riqueza y la informalidad, si permite conocer como ha crecido un sector económico en determinado tiempo.

1.5. SECTOR TIC

Los retos de este sector son dominar nuevas tecnologías y adaptarlas al entorno empresarial para alcanzar a desarrollar alternativas que para las empresas sean interesantes. Este es el caso de los servicios de informática, toda vez que su crecimiento en los últimos años ha sido en niveles positivos y el comportamiento de sus ingresos es favorable para la economía del país.

El desempeño del sector y su comportamiento es destacable; en la última década su crecimiento fue similar o superior al crecimiento del producto interno bruto de Colombia. La actividad que más se desarrolló en este sector fue la relacionada con el mantenimiento de redes y la administración de datos, puesto que las empresas con grandes volúmenes de información requieren una manera óptima de administrar estos recursos, así mismo por la facilidad de conectar a nivel nacional la información y archivos de las empresas usuarias.

Para cada subsector de gobierno se analizó la distribución de la inversión según segmento TI



Fuente: Autor, Guide to Measuring the Information Society (2011). OECD; Clasificación Central de Productos – CPC Vers. 2 A.C. DANE; CRC (2010). Análisis del sector TIC en Colombia: Evolución y Desafíos; RAÚL KATZ (2015). El ecosistema y la economía digital en América Latina.

(Aplicaciones y software, Infraestructura y hardware y Servicios TI), con el fin de establecer qué sectores el más importante en cada caso. Debe tenerse en cuenta que este análisis solamente da

cuenta de la prioridad en cada subsector, y no de la magnitud de la inversión. Es decir que un porcentaje muy alto no indica una inversión alta en términos absolutos, sino sólo una alta proporción al interior de su subsector.

En general se evidencia un predominio más frecuente de la inversión en Servicios; se destacan los subsectores de Inteligencia (76%), Salud y protección social (73%), Interior (72%), Comunicaciones (69%) y Cultura (60%). Los subsectores que han dado mayor prioridad a la inversión en Aplicaciones y software son: Ambiente y desarrollo sostenible (100%), Ciencia y tecnología (44%), Educación (41%, Agropecuario y Minas y Energía (31% cada uno).

Dentro del componente de producción de servicios TIC, se destaca el de servicios de consultoría en TI, que se ajusta a nuestra necesidad contractual. Según el mismo informe, entre los servicios de consultoría más contratados en el sector, se destacan los servicios de gestión de procesos empresariales, buenas prácticas, soporte, diseño y desarrollo de TI para aplicaciones.

1.6. MERCADO CAMBIARIO

Durante el tercer trimestre de 2021, el dólar estadounidense se fortaleció frente a la mayoría de las monedas de países desarrollados y monedas de emergentes (de acuerdo con el DXY, el dólar se fortaleció 1,9%). Las monedas de países emergentes y de la región se debilitaron en línea con el fortalecimiento del dólar y se vieron presionadas además por factores idiosincráticos dentro de los que se destaca la incertidumbre política y fiscal, y la disminución de las cotizaciones de algunas materias primas como el cobre, el hierro y la soya. El peso colombiano se deprecio 1,7% durante el trimestre en línea con el fortalecimiento del dólar. Hasta inicios de agosto, el peso acumulo una depreciación de alrededor del 6% y alcanzo su mayor nivel en lo corrido del año, presionado adicionalmente por la caída de los precios del petróleo y el amplio diferencial de tasas de interés entre Colombia y otros países de la región. Sin embargo, a partir de mediados de agosto, la depreciación de la moneda corrigió parcialmente gracias a la recuperación de las cotizaciones del petróleo y las mayores expectativas de monetizaciones por parte del Gobierno.[14]

El mercado cambiario en el 2021 cierra otro año de alta volatilidad que llevó al dólar a alcanzar los $4.000, y a ganar $500 respecto a la TRM del 27 de diciembre de 2020, que fue de $3.493. (TRM para hoy es de $3,994).

En el tercer trimestre de 2021 el Producto Interno Bruto, en su serie original, crece 12,4% respecto al mismo periodo de 2020. Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

- Comercio al por mayor y al por menor; Reparación de vehículos; Transporte y almacenamiento; Alojamiento y servicios de comida crece 26,5% (contribuye 5,3 puntos porcentuales a la variación anual del valor agregado).
- Industrias manufactureras crece 26,2% (contribuye 2,3 puntos porcentuales a la variación anual del valor agregado).
- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 8,7% (contribuye 1,6 puntos porcentuales a la variación anual del valor agregado).

[14] ttps://www.banrep.gov.co/sites/default/files/publicaciones/archivos/reporte_de_mercados_financieros_3trim_2021.pdf

En lo corrido del año 2021, respecto al mismo periodo del año anterior, el Producto Interno Bruto presenta un crecimiento de 9,8%. Esta variación se explica principalmente por:

- Comercio al por mayor y al por menor; Reparación de vehículos; Transporte y almacenamiento; Alojamiento y servicios de comida crece 16,5% (contribuye 3,4 puntos porcentuales a la variación anual del valor agregado).
- Industrias manufactureras crece 22,7% (contribuye 1,9 puntos porcentuales a la variación anual del valor agregado).
- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; Actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 33,4% (contribuye 1,5 puntos porcentuales a la variación anual del valor agregado).

Respecto al trimestre inmediatamente anterior, el Producto Interno Bruto en su serie ajustada por efecto estacional y calendario crece 5,9%. Esta variación se explica principalmente por la siguiente dinámica:

- Comercio al por mayor y al por menor; Reparación de vehículos; Transporte y almacenamiento; Alojamiento y servicios de comida crece 14,4%.
- Industrias manufactureras crece 14,2%.
- Información y comunicaciones crece 5,6%

Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen[1]
Tercer trimestre 2021[pr]

Actividad económica	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2021[pr] - III/ 2020[pr] - III	2021[pr] / 2020[pr]	2021[pr] - III/ 2021[pr] - II
Agricultura, ganadería, caza, silvicultura y pesca	4,2	3,5	-0,5
Explotación de minas y canteras	-5,5	3,6	0,4
Industrias manufactureras	26,2	22,7	14,2
Suministro de electricidad, gas, vapor y aire acondicionado[2]	5,5	2,8	1,7
Construcción	-20,7	-10,6	-2,6
Comercio al por mayor y al por menor[3]	26,5	16,5	14,4
Información y comunicaciones	16,1	10,8	5,6
Actividades financieras y de seguros	2,2	3,4	1,1
Actividades inmobiliarias	1,4	1,3	0,6
Actividades profesionales, científicas y técnicas[4]	10,7	8,3	4,8
Administración pública, defensa, educación y salud[5]	8,7	5,6	2,3
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	23,1	33,4	-3,9
Valor agregado bruto	**11,9**	**9,4**	**5,9**
Total impuestos menos subvenciones sobre los productos	16,6	12,8	4,0
Producto Interno Bruto	**12,4**	**9,8**	**5,9**

Fuente: DANE, Secretaría Distrital de Desarrollo Económico (Convenio 440 de 2021). Cuentas Nacionales

15

[15] https://www.dane.gov.co/files/investigaciones/boletines/pib/Bogota/Bol_PIB_Bta_III_trim_21.pdf

Con la aparición de nuevas variantes del Covid-19, los pronósticos económicos se han venido revisando a la baja. Por ejemplo, ahora la cifra de relativo consenso sobre crecimiento en Estados Unidos está cerca del 6% para el 2021 (un recorte de 1.5%) y 4% en 2022, mientras que en Europa se ha mantenido relativamente inalterada en cerca del 5% para ambos años.

En Colombia, las proyecciones de crecimiento también venían al alza, a pesar del efecto de los paros de abril-junio del 2021. Dado que el primer semestre terminó con una expansión cercana al 9% anual, luce probable que el crecimiento del 2021 (como un todo) se ubique en el rango 6%-7%.

Este es un crecimiento más bien moderado, si tenemos en cuenta la contracción cercana al 7% que experimentó el PIB-real de Colombia durante 2020 por cuenta de la pandemia. Y todo parece indicar que el crecimiento del 2022 estará en el rango 3.5%-4%, considerando el menor dinamismo de los energéticos (antes comentados).

Existen al menos tres factores que deben preocuparnos respecto de la solidez de la recuperación económica del periodo 2022-2026:

1. La alta dependencia exportadora de los commodities energéticos (cercana al 50% de nuestra canasta).
2. El elevado nivel de desempleo (14%) y su persistencia.
3. Las limitadas capacidades para aplicar políticas fiscales y monetarias contra-cíclicas.

Las primeras debidas al frágil paquete tributario (de solo 1% del PIB) que se discutió en el Congreso y las segundas debidas al rebrote inflacionario que está requiriendo que pronto el Banco de la Republica se mueva en la dirección de elevar su tasa repo del 1.75% hacia el 2.5% (+75 pbs) antes de finalizar este 2021.[16]

1.7. ANÁLISIS TÉCNICO

Para el presente proceso, se identifica que los bienes y servicios de tecnologías de la información y las comunicaciones comprenden: (i) infraestructura, soporte en la utilización de los servicios y productos, (ii) la fabricación y/o venta de los bienes TIC, (iii) producción de los servicios de telecomunicaciones, (iv) industria de las plataformas digitales e (v) investigación y hacen parte del sector terciario de la economía, que se refiere al ofrecimiento de servicios en donde se encuentran todas aquellas actividades intangibles que no producen mercancía en sí, como el comercio, el transporte, entre otros.

La infraestructura y soporte es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que necesita la entidad para poder llevar a cabo todas sus actividades. El conjunto de hardware consta de elementos tan diversos como los reguladores de corriente, los sistemas de seguridad, las cámaras, los servidores de aplicaciones, los elementos de red como: routers, repetidores o cortafuegos, las computadoras personales, las impresoras, las tabletas, los teléfonos, copiadoras, proyectores, conmutadores, etc. El conjunto de software va desde los sistemas operativos (licenciamiento), programas de oficina (licenciamiento), plataformas administrativas y operativas (contabilidad, administración, cobranza, calificaciones, etc.).

[16] https://www.larepublica.co/analisis/sergio-clavijo-500041/perspectivas-macro-economicas-colombia-2021-2022-3234467

El 2020 y 2021 fueron años cruciales para la reafirmación de la industria del software, pues la crisis global generada por la pandemia se convirtió en una oportunidad de poner sobre la mesa lo fundamental y necesario que es para la modificación de modelos de negocios y la transición a la digitalización, lo que ha permitido que el software colombiano se afiance más como un producto de calidad para el desarrollo del país.

Cuando analizamos la evolución histórica del mercado de software colombiano, podemos observar que tiene un crecimiento del 17.6% anual, lo que representa un avance acelerado, sumando a la industria la indiscutible generación de empleo, pero también la necesidad de pensar en estrategias de formación de profesionales en el campo tecnológico que reduzca drásticamente el déficit de 60 mil personas, todo con el propósito de seguir progresando en el peldaño de la creación y exportación de tecnología de calidad.

De acuerdo con lo anterior, las empresas del sector TIC en términos generales, se especializan en una actividad general o línea de negocio principal, sin embargo, algunas de ellas desarrollan también líneas de negocio secundarias. Estas empresas están representadas en mayor porcentaje por pequeñas y medianas empresas; en la siguiente tabla se presenta el número de empresas vinculadas a las diversas líneas de negocios del sector teniendo como parámetro de clasificación el tamaño de estas.

Líneas de Negocio	Menos de 10 empleados	Entre 11 y 50 empleados	Entre 51 y 200 empleados	Más de 200 empleados
Cloud computing	26	1	0	0
Consultoría e implementación	122	20	1	0
Desarrollo/Fábrica de Software	607	134	26	5
Gerencia	4	2	0	0
Infraestructura como servicio	224	72	3	1
Manejo de Centro de Datos	565	216	45	25
Mantenimiento de soporte de aplicaciones	104	29	8	2
Mesa de ayudas	327	122	17	11
Otros servicios Ti	85	24	6	0
Plataformas tecnológicas (servicio)	68	15	4	3
Software como servicio	90	22	3	1
Testing de software	241	71	12	6

Fuente: Min Tic.

1.8. PERSPECTIVA LEGAL DEL SECTOR

En el aspecto regulatorio que enmarca este proceso contractual, la entidad más importante es la Dirección Nacional de Derechos de Autor de la Unidad Administrativa Especial del Ministerio del Interior, organismo del Estado Colombiano que se encarga del diseño, dirección, administración y ejecución de las políticas gubernamentales en materia de derechos de autor y derechos conexos, que para los efectos del presente contrato garantiza que el proveedor sea el dueño exclusivo de los derechos de autor del código de fuente del software y que por ende pueda brindar los servicios de soporte requeridos por la Entidad.

Sumado a lo anterior, en materia de derechos de autor se encuentra la siguiente normatividad asociada:

Decreto 1066 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior":

CAPÍTULO 3

Inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor

ARTÍCULO 2.6.1.3.1 Soporte lógico. De conformidad con lo previsto en la Ley 23 de 1982 sobre Derechos de Autor, el soporte lógico (software) se considera como una creación propia del dominio literario.

ARTÍCULO 2.6.1.3.2 Elementos. El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción de programa y el material auxiliar.

ARTÍCULO 2.6.1.3.3 Definiciones. Para los efectos del ARTÍCULO anterior se entiende por:

1. "Programa de computador": La expresión de un conjunto organizado de instrucciones, en lenguaje natural o codificado, independientemente del medio en que se encuentre almacenado, cuyo fin es el de hacer que una máquina capaz de procesar información, indique, realice u obtenga una función, una tarea o un resultado específico.

2. "Descripción de Programa: Una presentación completa de procedimientos en forma idónea, lo suficientemente detallada para determinar un conjunto de instrucciones que constituya el programa de computador correspondiente.

3. "Material auxiliar": Todo material, distinto de un programa de computador o de una descripción de programa, creado para facilitar su comprensión o aplicación, como, por ejemplo, descripción de problemas e instrucciones para el usuario.

ARTÍCULO 2.6.1.3.4 Obra inédita. El soporte lógico (software), será considerado como obra inédita, salvo manifestación en contrario hecha por el titular de los derechos de autor.

ARTÍCULO 2.6.1.3.5 Requisitos. Para la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, deberá diligenciarse una solicitud por escrito que contenga la siguiente información:

1. Nombre, identificación y domicilio del solicitante, debiendo manifestar si habla a nombre propio o como representante de otra en cuyo caso deberá acompañar la prueba de su representación.

2. Nombre e identificación del autor o autores.

3. Nombre del productor.

4. Título de la obra, año de creación, país de origen, breve descripción de sus funciones, y en general, cualquier otra característica que permita diferenciarla de otra obra de su misma naturaleza.

5. Declaración acerca de si se trata de obra original o si, por el contrario, es obra derivada.

6. Declaración acerca de si la obra es individual, en colaboración, colectiva, anónima, seudónima o póstuma.

ARTÍCULO 2.6.1.3.6 Requisitos adicionales. A la solicitud de que trata el ARTÍCULO anterior, deberá acompañarse por lo menos uno de los siguientes elementos: el programa

- Ley 1955 del 25 de mayo de 2019, por el cual se expide el plan nacional de desarrollo 2018-2022. Pacto por colombia, pacto por la equidad.
- Ley 1915 del 12 de julio de 2018 "por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos".
- Ley 1834 de 2017 "por medio de la cual se fomenta la economía creativa ley naranja".
- Ley 1801 del 29 de julio de 2016 por la cual se expide el código nacional de policía y convivencia.
- Ley 232 de 1995 ley derogada por el art. 242 de la ley 1801 de 2016.
- Ley 1680 del 20 de noviembre de 2013, "por la cual se garantiza a las personas ciegas y con baja visión el acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y las comunicaciones"
- Ley 603 de 2000 "por la cual se modifica el artículo 47 de la ley 222 de 1.995".
- Ley 44 de 1993 "por la cual se modifica y adiciona la ley 23 de 1982 y se modifica la ley 29 de 1944".
- Ley 23 del 28 de enero de 1982 ley de derechos de autor.

de computador, la descripción de programa y/o el material auxiliar. ARTÍCULO 2.6.1.3.7 Protección. La protección que otorga el derecho de autor al soporte lógico (software), no excluye otras formas de protección por el derecho común.	

1.9. ESTUDIO DE LA OFERTA:

En el mercado, se encuentran empresas de origen nacional y extranjero que ofertan software de gestión de información de laboratorios (Laboratory Information Management System - LIMS), tales como:

- LABWARE
- SAMPLEMANAGER
- THERMOFISHER
- SAMPLE MASTER
- ABBOT STARLIMS
- ENGINEERING

Sin embargo, el objeto del presente estudio sólo puede ser realizado por la empresa Caudales y Muestreos S.A.S, quienes poseen tanto los derechos de las marcas como los derechos de autor del software empleado en los laboratorios del Invima, así como la exclusividad para la venta, distribución, comercialización y/o soporte para las soluciones ofrecidas, conforme al certificado emitido por el Ministerio del Interior -Dirección Nacional de Derecho de Autor Unidad Administrativa Especial- No. 13-35-325 otorgado el 5 diciembre del 2012.

Una vez claro lo anterior, es importante destacar que la empresa en comento se dedica al desarrollo y comercialización de software para laboratorios[17], contando con más de once (11) años de existencia en el mercado, ejecutando contratos en el sector público y en el privado, con reconocidas empresas y entidades estatales como las que se mencionan a continuación: Colanta, Casa Luker, Alquería, Gloria (Parmalat),Universidad de Medellín, Universidad del Valle, Acueducto Metropolitano de Bucaramanga, Sena, Agrosavia, Gobernación del Quindío, entre otras.

De las contrataciones mencionadas previamente, se destacan los siguientes casos de éxito:

- Colanta: 17 plantas con la recepción de muestras automatizada en Sampler. Laboratorio de calidad de leche 100% automatizado. Más de 2.500.000 muestras procesadas en los últimos 5 años.
- Casa Luker: Laboratorio de calidad de cacao automatizado. Ensayos sensoriales. Operación 24/7 en 7 plantas.
- Servimeters: 11 Laboratorios de Calibración. 100% automatizados.

Así las cosas, dando atención al principio de transparencia establecido en la ley 80 de 1993, para la estimación del presupuesto oficial de esta contratación, la Entidad requirió cotización a la empresa Caudales y Muestreos S.A.S., recibiendo la siguiente información:

[17] Como lo es el software SAMPLER que contiene varios módulos que permiten la gestión integral de los laboratorios.

Caudales y Muestreos S.A.S., le propone a la Oficina de Tecnologías de la Información, instalar, configurar, parametrizar, probar y salir a producción con la plataforma Sampler (SILab) en infraestructura local más el soporte funcional de los aplicativos por un (1) año, con el fin de proporcionar a la Oficina de Laboratorios y Control de Calidad y sus 7 laboratorios continuidad a sus labores y la responsabilidad en el análisis de las muestras y mantener las acreditaciones nacionales e internacionales con las que cuenta dicha oficina del Invima.

Valor: CUATROCIENTOS SETENTA Y SIETE MILLONES CIENTO NOVENTA MIL PESOS MCTE. ($477.190. 000.oo) incluido IVA.

Propuesta Económica:

Instalación de Sampler en Servidores Invima y Soporte.
Funcional por un (1) año.

No.	TAREAS	VALOR	CANTIDAD	VALOR TOTAL
1	INSTALACION, CONFIGURACION, PARAMETRIZACION, PRUEBAS Y SALIDAD EN PRODUCCION	$120.000.000	1	$ 120.000.000
2	SOPORTE FUNCIONAL POR UN (1) AÑO	$ 281.000.000	1	$ 281.000.000
		SUBTOTAL		$ 401.000.000
		IVA		$ 76.190.000
		TOTAL		$ 477.190.000

Victoria Muentes Nieves.
C.C. 37.937.588 de Barrancabermeja
Representante Legal Caudales y Muestreos
SAS

1.9.1 ESTUDIO DE LA DEMANDA.

En virtud del presente proceso, el contratista ha prestado sus servicios al Invima por medio de los siguientes contratos:

Contrato Numero	Objeto	Valor	Modalidad
477 del 2021	ADQUIRIR LA GARANTÍA DE SOPORTE Y MANTENIMIENTO Y PRESTAR LOS SERVICIOS DE DESARROLLO REQUERIDOS PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER	$326.000.000	Contratación Directa
263 de 2018	REALIZAR LA IMPLANTACION DE LA SOLUCION TECNOLOGICA (LIMS LABORATORY INFORMATION MANAGEMENT SYSTEM) PARA LA GESTION DE INFORMACION DE LA OFICINA DE LABORATORIOS Y CONTROL DE CALIDAD	$1.451.086.000	Contratación Directa

Complementario a lo anterior, se revisaron objetos contractuales similares realizados por otras Entidades, regidas por la Ley 80 de 1993, para lo cual se tomó información de la plataforma SECOP II y se seleccionaron procesos para la comparación correspondiente. Se destaca el hecho de que la modalidad de contratación es la contratación directa.

Se pudo constatar en la búsqueda realizada que son pocas Entidades del Estado las cuales cuentan con estos sistemas de información y que las entidades relacionadas en la siguiente tabla son instituciones que dentro de su misionalidad cuentan con laboratorios que realizan actividades de ensayo.

No obstante, la Oficina de Tecnologías de la Información realizó la búsqueda enfocada a actividades similares al objeto a contratar por el Instituto, como lo es el mantenimiento y soporte de software de otras Entidades públicas que se utilizan como parte de las soluciones tecnológicas para el logro y desarrollo de los objetivos estratégicos de las mismas, encontrando lo siguiente:

CONTRATO No.	ENTIDAD	OBJETO	VALOR	TIEMPO DE EJECUCIÓN	PROVEEDOR
MHCP-SIE-16-2021	MINISTERIO DE HACIENDA Y CREDITO PUBLICO	Actualización del software, soporte y mantenimiento técnico de las soluciones de VPN SSL PULSE SECURE para el SIIF Nación (Presentación de oferta)	$ 218.504.522	8 meses	C&M S.A.S COLOMBIA
148-CENACINTELIGENCIA-2021	CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA CENAC INTELIGENCIA	SERVICIO DE MANTENIMIENTO Y SOPORTE INFRAESTRUCTURA DE BIGDATA HYDRA PARA EL SUBSISTEMA DE INTELIGENCIA DURANTE LA VIGENCIA 2021 Y 2022.	$ 188.273.530,93	240 días	CENACINTELIGENCIA
CO1.PCCNTR.1878536-2021	GOBERNACION DE CALDAS	Prestación de servicios de apoyo a la gestión para el soporte y mantenimiento al licenciamiento de software SAP (SERVICIO ENTERPRISE SUPPORT) licencias de uso del software MySAP de software sap (Licencias usuarios finales) licencias de motor de base de datos (ORACLE) Runtime y software de apoyo	$ 182.610.710	240 días	SAP COLOMBIA S.A.S.
CO1.PCCNTR.320432-2021	INSTITUTO COLOMBIANO PARA LA EVALUACIÓN DE LA EDUCACIÓN - ICFES	Renovar las licencias de los productos ORACLE lo cual incluye proveer la actualización y el soporte técnico (software UpdateLicense & Support) de los productos de ORACLE licenciados por el Instituto de conformidad con lo establecido en el anexo técnico.	$ 337.878.794	300 días	Oracle Colombia LTDA

CONTRATO No.	ENTIDAD	OBJETO	VALOR	TIEMPO DE EJECUCIÓN	PROVEEDOR
CO1.PCCNTR .2486705-2021	FISCALÍA GENERAL DE LA NACIÓN NIVEL CENTRAL.	Contratar los servicios de soporte técnico del sistema de manejo de información de laboratorios (LIMS) con destino al grupo de genética del CTI Bogotá".	$173.319.111	180 días	INNOVACION TECNOLOGICA S.A.S - INNOVATEK S.A.S.
CD-424-2021 / CO1.PCCNTR .2806406	ALCALDÍA MUNICIPIO DE BELLO	Fortalecimiento institucional a través de las actualizaciones tecnológicas del soporte, actualización y mantenimiento del sistema de información SICOF-ERP (presupuesto, contabilidad, tesorería, nomina, talento humano, RNTAS, almacén, compras, cobro coactivo y otros módulos implementados) situ y fondos educativos del municipio de bello	$400.913.768	120 días	ADA S.A

Teniendo en cuenta los contratos presentados en la tabla precedente, se observa que la cotización presentada por parte de Caudales y Muestreos S.A.S, (dueño del soporte lógico) se encuentra dentro del rango de valores a contratar.

CONCLUSIONES

Como se puede observar, se hizo un estudio de las condiciones del sector e incluso se efectuó un estudio de mercado que arrojó la entrega de cotización por parte de la empresa Caudales Y Muestreos S.A.S.; pese a que se debe efectuar contratación directa de la misma por lo tantas veces manifestado acerca de la propiedad del soporte lógico. No obstante, se desplegaron dichas actividades, con el propósito de dar cumplimiento al principio de transparencia establecida en la ley 80 de 1993 y demás normas concordantes por parte del Instituto.

Atentamente,

JUAN MANUEL PALACIO POSADA
Jefe Oficina de Tecnologías de la Información.

INVIMA
Oficina Asesora de Planeación
Visto bueno Inversión
OAP-PS-IN 4652

Área técnica	Grupo de Gestión Contractual	Visto bueno – Jefe de Oficina Asesora de Planeación
Elaboró: Saaibi Arenas Moreno- Contratista de la OTI.	Revisó:	Daladier Medina Niño El suscrito Certifica que: el objeto de la contratación solicitada esta contemplado dentro de las actividades del proyecto de inversion respectivo.
Revisó: María del Pilar Caicedo-Abogada Contratista OTI Aprobó: : Camilo Andrés Guzmán Camacho -Coordinador Grupo de Informática	Aprobó: María Margarita Cárdenas Cortes. Asesora de la Dirección General con Delegación de Funciones del Grupos Gestión Contractual	

invima	GESTIÓN ADMINISTRATIVA		ADQUISICIÓN DE BIENES Y SERVICIOS		
	FORMATO CERTIFICACIÓN DEL PLAN ANUAL DE ADQUISICIONES				
	Código: GAD-ABS-FM021		Versión: 04		Fecha de Emisión: 03/07/2020

CERTIFICACIÓN No 623

LA SUSCRITA ASESORA DE LA DIRECCIÓN GENERAL CON DELEGACIÓN DE FUNCIONES DEL GRUPO DE GESTION CONTRACTUAL

El siguiente bien o servicio solicitado por la Oficina de Tecnologías de la Información

OBJETO CONTRACTUAL	MODALIDAD DE SELECCIÓN	VALOR PLANEADO	VALOR A CONTRATAR SEGÚN ESTUDIO PREVIO	RUBRO O PROYECTO DE INVERSIÓN
INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER, AFECTADO POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE.ID 862	Contratación Directa	477,180,000.00	477,180,000.00	Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones

Se encuentra registrado en el Plan Anual de Adquisiciones de la vigencia del año 2022

Igualmente se realiza la verificación de existencias en el Almacen General de la Entidad NO APLICA

OBSERVACIONES:

Dada en Bogotá D. Abril 5 de 2022

MARIA MARGARITA CARDENAS CORTES

Elaboró: Nancy Rocio Silva Olarte. NRS

Invima	GESTIÓN ADMINISTRATIVA	GESTIÓN CONTRACTUAL	
	SOLICITUD DE DISPONIBILIDAD PRESUPUESTAL		
	Código: GAD-GCT-FM25	Versión: 01	Fecha de Emisión: 2022-02-01

1250 - 020 - 2022

PARA:	MARLON SIMON ORTEGA ORDOSGOITIA Asesor de Dirección General con delegación de funciones del Grupo Financiero y Presupuestal Coordinador Grupo Financiero y Presupuestal
ASUNTO:	Solicitud Disponibilidad Presupuestal
FECHA:	23/03/2022

TIPO DE CDP: INICIAL [ ] ADICIÓN [ ]

Por el presente le solicito expedir certificado de disponibilidad presupuestal por la suma de CUATROCIENTOS SETENTA Y SIETE MILLONES CIENTO NOVENTA MIL PESOS M/CTE ($ 477.190.000) incluido IVA y demás impuestos, tasas y contribuciones de ley a que haya lugar Para respaldar la contratación de INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER, AFECTADO POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE

- **PROYECTOS DE INVERSIÓN:**

PROYECTO	ACTIVIDAD SUIFP	Producto	%	FUENTE	REC	VALOR
Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones nacional	Realizar el proceso de implementación de sotware e implantación de soluciones, desarrollos, soporte y actualización para los sistemas de información	C-1903-0300-6-0-1903045__ Servicios de información para la gestión de la inspección, vigilancia y control sanitario	100	Propios	21	$ 477.190.000,00
		TOTAL :	100			$ 477.190.000,00

- **PRESUPUESTO DE FUNCIONAMIENTO:**

PRESUPUESTO	CONCEPTO	%	VALOR
Funcionamiento			

Atentamente,

NOMBRE	JUAN MANUEL PALACIO POSADA
Cargo	Jefe de Oficina
Dependencia	Oficina de Tecnologías de la Información

NOMBRE	ROY LUIS GALINDO WEHDEKING
	Secretario General

So. 90222.
CDP. 88822.
01 ABR 2022

SIIF Nación

Reporte Certificado de Disponibilidad Presupuestal Comprobante

Usuario Solicitante:	MHhnunez	HERNAN NUNEZ GUIZA
Unidad ó Subunidad Ejecutora Solicitante:	19-12-00	INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA
Fecha y Hora Sistema:	2022-04-01-3:30 p. m.	

CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

El suscrito Jefe de Presupuesto CERTIFICA que existe apropiación presupuestal disponible y libre de afectación en los siguientes "ítems de afectación de gastos"

Numero:	88822	Fecha Registro:	2022-04-01	Unidad / Subunidad ejecutora:	19-12-00 INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA						
Vigencia Presupuestal	Actual	Estado:	Generado		Tipo:	Gasto			Uso Caja Menor	Ninguno	
Valor Inicial:	477.190.000,00	Valor Total Operaciones:	0,00		Valor Actual.:	477.190.000,00	Saldo x Comprometer:	477.190.000,00	Vr. Bloqueado	0,00	

SOLICITUD DE CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL				AUTORIZACION DE ADQUISICION DE BIENES Y SERVICIOS					
Número:	90222	Fecha Registro:	2022-04-01	Número:		Modalidad de contratación:		Tipo de contrato:	

ITEM PARA AFECTACION DE GASTO

DEPENDENCIA	POSICION CATALOGO DE GASTO	FUENTE	RECURSO RECURSO	SITUAC.	FECHA OPERACION	VALOR INICIAL	VALOR OPERACION	VALOR ACTUAL	SALDO X COMPROMETER	VALOR BLOQUEADO
19-12-00 INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA	C-1903-0300-6-0-1903045-02 ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIO DE INFORMACIÓN PARA LA GESTIÓN DE LA INSPECCIÓN, VIGILANCIA Y CONTROL SANITARIO - FORTALECIMIENTO DE LA ARQUITECTURA TECNOLÓGICA Y LOS PROCESOS ASOCIADOS A LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y	Propios	21	CSF						
					Total:	477.190.000,00	0,00	477.190.000,00	477.190.000,00	0,00

Objeto:	RESPALDAR LA INSTALACION, CONFIGURACION, PARAMETRIZACION Y REALIZAR PRUEBAS Y PUESTA EN PRODUCCION, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACION DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER

Firma Responsable

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

EL SECRETARIO GENERAL DEL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS –INVIMA-

En ejercicio de las facultades legales, la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015, el Decreto 2078 de 2012, la Resolución de Delegación de Funciones No. 2012030802 del 19 de octubre de 2012, la Resolución No. 2020006742 del 25 de febrero de 2020, acta de posesión No. 040 del 25 de febrero de 2020 y,

CONSIDERANDO QUE:

La Constitución Política de Colombia en su artículo 2, contempla:

> "ARTICULO 2º—Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares. (Subrayado fuera del texto).

Por medio del artículo 245 de la Ley 100 de 1993 se crea el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA como establecimiento público del orden nacional, adscrito al Ministerio de Salud y Protección Social, con personería jurídica, patrimonio independiente y autonomía administrativa, cuyo objeto es la ejecución de las políticas en materia de vigilancia sanitaria y de control de calidad de medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva.

Para tal fin el Decreto 2078 de octubre de 2012 *"Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos -Invima y se determinan las funciones de sus dependencias"*, en el numeral 1 de su artículo 4, establece las funciones de la entidad entre las cuales se encuentra la siguiente:

> *Ejercer las funciones de inspección, vigilancia y control a los establecimientos productores y comercializadores de los productos a que hace referencia el artículo 245 de la Ley 100 de 1993 y en las demás normas que lo modifiquen o adicionen, sin perjuicio de las que en estas materias deban adelantar las entidades territoriales, durante las actividades asociadas con su producción, importación, exportación y disposición para consumo.*

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En tal sentido, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima como organismo encargado de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar a través del talento humano (contemplando funcionarios y contratistas) que conforman y hacen parte del apoyo de las direcciones, oficinas, coordinaciones y demás grupos internos de trabajo de su estructura orgánica, las actividades necesarias para la efectiva prestación del servicio público que se brinda por la institución.

Así mismo, para realizar las labores misionales y administrativas, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que soporta los múltiples sistemas de información, bases de datos y aplicativos necesarios para la correcta ejecución de sus oficios, administrada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades desarrolladas por la entidad se ejecuten, a través de los distintos aplicativos[1]; situación que se venía cumpliendo efectivamente en las diferentes sedes de la entidad de forma presencial y virtual, garantizando la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso.

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[2] que comprometió la disponibilidad de los sistemas de información, bases de datos, plataformas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad, restringiendo su acceso, afectando la operación de varios de los servidores y estaciones de trabajo cliente, así como los aplicativos y sistemas de información dispuestos para la operación del Instituto, de conformidad al estado situacional[5].

Dicho incidente ocasionó un problema de continuidad del negocio, afectando la ejecución de las actividades diarias del Instituto, toda vez que el mismo es considerado como "*incidente de seguridad de la información*"[6].

En este orden, la entidad implementó medidas, que van desde la contención del incidente hasta la activación de un plan de contingencia, cuyo eje fundamental fue la reactivación de los servicios tecnológicos desde los que se despliega la misionalidad del Instituto, de conformidad a los aplicativos aludidos en el anexo 1- Relación de softwares de este acto administrativo. Estos servicios se

[1] Ver Anexo 1: Relación de softwares.
[2] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion.
[3] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com
[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos
[5] Ver anexo 2: Estado situacional.
[6] Debe precisarse que respecto del incidente, y conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no se evidencian indicios de fuga de la información sin embargo, la entidad se atiene al resultado del análisis forense que fue solicitado a la Superintendencia de Industria y Comercio - SIC, y a lo definido en la investigación penal que adelanta la Fiscalía General de la Nación con apoyo de la Policía Nacional – Dirección de Investigación Criminal e Interpol.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

restauraron de forma paulatina con la gestión de las actividades tecnológicas y jurídicas correspondientes, que a su vez desplegó la entidad, como lo son: la actualización e implementación del plan de acción y medidas de contingencia frente a los posibles efectos o consecuencias del incidente cibernético, la emisión de las medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, emitiendo los siguientes actos administrativos:

- Resolución 2022500000 del 9 de febrero de 2022; la Resolución 2022500001 del 15 de febrero de 2022; 2022500002 del 22 de febrero de 2022; 2022500003 del 25 de febrero de 2022; 2022500005 del 8 de marzo de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites, y la Resolución No. 2022500009 del 16 de marzo de 2022, por medio de la cual se adoptaron decisiones y se actualizaron las medidas administrativas transitorias necesarias para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto.

- Circular 1000-001-22 del 18 de febrero de 2022, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

- Circular 1000-002-22 del 25 de febrero de 2022, a través de la cual se otorga la ampliación de empresas beneficiadas por formato de contingencia para autorización de traslado de alimentos, materias primas, otros alimentos perecederos, desde el sitio de ingreso a otro sitio que cumplan con las condiciones sanitarias para su almacenamiento.

De forma paralela la entidad con las actividades anteriormente descritas, interpuso ante la Fiscalía General de la Nación denuncia penal Expediente CAD N° 110016000050202201569 por el presunto delito de acceso abusivo a un sistema informático, tipificado en el artículo 269 A de la Ley 1263 de 2009, actuación de la que se desprendieron las consecuentes investigaciones, iniciando con las practicas del recaudo del material probatorio y/o evidencia física sobre los servidores y equipos diagnosticados con la transmisión o inoculación del virus ransomware. En consecuencia, la policía judicial realizó las actividades forenses correspondientes, extrayendo las que conformarían el caudal probatorio que soporta la denuncia en cita, actividad que fue desplegada hasta el 15 de marzo de 2022, fecha en la que se emite el acta que autoriza proceder con el uso para formateo de los servidores afectados, en relación con el acta de formateo de servidores del Instituto[7].

El 16 de marzo de 2022, se llevó a cabo Comité Técnico de Seguimiento[8], integrado por los funcionarios y contratistas del Grupo de Soporte Tecnológico como de la Oficina de Tecnologías de la Información del Invima y la Oficial de Seguridad de la Información, quienes recomendaron:

1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción

[7] Ver anexo 3: Acta formateo servidores del Invima.
[8] Ver anexo 4: Comité Técnico de Seguimiento Contingencia.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativos: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.

2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos[9] y la Nueva Plataforma de Trámites y Servicios[10], así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[11]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el

[9] Sivicos es la denominación utilizada para referirse al proyecto que comprende el desarrollo de una solución que consiste en un software que permite la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima.

[10] El proyecto de nueva plataforma es el relacionado con el desarrollo de una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para la ejecución en línea, de las actividades misionales de los procesos: "Registros sanitarios y tramites asociados" y "Auditorías y certificaciones" del instituto.

[11] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.

8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.
10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

Bajo este contexto, y respecto a la importancia del cumplimiento de las labores de la entidad, teniendo en cuenta que la misionalidad del Instituto se basa en proteger y promover la salud de los colombianos, es claro que las actividades que desarrolla no se pueden paralizar; por lo cual se hace necesario activar la causal de contratación directa a través de urgencia manifiesta, de conformidad al plan de acción, en relación con las actividades anteriormente descritas establecidas en el Comité precitado y acogidas por la Entidad como medida conducente en el proceso de mitigación.

Así las cosas y, con el propósito de garantizar la disponibilidad y el acceso total a la información y las comunicaciones del Instituto Nacional de Vigilancia de Medicamentos y Alimentos- Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte, se hace necesaria la contratación de bienes y servicios para conjurar, mitigar los efectos y con ello restablecer

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información de la Entidad..

Corolario, se requiere gestionar los trámites contractuales de forma inmediata, toda vez que no se cuenta con el plazo indispensable para adelantar el procedimiento ordinario de escogencia de contratistas[12], siendo viable acudir al mecanismo idóneo para adelantar las contrataciones, con atención a las situaciones anteriormente expuestas, garantizando una respuesta contigua de la administración.

De igual manera, debe tenerse en cuenta la prohibición establecida en el marco de Ley de garantías, contemplada en el artículo 33 de la Ley 996 de 2005, el cual dispone:

> **Artículo 33. Restricciones a la contratación pública.** Durante los cuatro (4) meses anteriores a la elección presidencial y hasta la realización de la elección en la segunda vuelta, si fuere el caso, queda prohibida la contratación directa por parte de todos los entes del Estado.
>
> Queda exceptuado lo referente a la defensa y seguridad del Estado, los contratos de crédito público, los requeridos para cubrir las emergencias educativas, sanitarias y desastres, así como también los utilizados para la reconstrucción de vías, puentes, carreteras, infraestructura energética y de comunicaciones, en caso de que hayan sido objeto de atentados, acciones terroristas, desastres naturales o casos de fuerza mayor, y los que deban realizar las entidades sanitarias y hospitalarias. Adicionalmente se exceptúan aquellos gastos inaplazables e imprescindibles que afecten el normal funcionamiento de la administración[13].

En atención a la situación expuesta, se encuentra configurada la circunstancia de fuerza mayor contemplada en el artículo 42 de la Ley 80 de 1993[14], el cual refiere la condición de la urgencia manifiesta a partir de situaciones necesarias para conjurar contextos excepcionales relacionadas con la fuerza mayor, para este caso, en concordancia con la excepción dispuesta en el artículo 33 de la citada Ley 996 de 2005.

En tal sentido, la Ley 1150 de 2007 (Literal a, numeral 4 del artículo 2. De las modalidades de selección) refiere:

---

[12] Licitación pública, selección abreviada, concurso de mérito, contratación mínima cuantía.

[13] Texto subrayado declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia C-1153 de 2005; el resto del artículo fue declarado EXEQUIBLE, condicionado a que se entienda que para el Presidente o el Vicepresidente de la República se aplique desde que manifiestan el interés previsto en el artículo 9º.

[14] ARTÍCULO 42. DE LA URGENCIA MANIFIESTA. <Aparte tachado derogado por el artículo 32 de la Ley 1150 de 2007> Existe urgencia manifiesta cuando la continuidad del servicio exige el suministro de bienes, o la prestación de servicios, o la ejecución de obras en el inmediato futuro; cuando se presenten situaciones relacionadas con los estados de excepción; cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, en general, cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o ~~concurso~~ públicos (...).

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

> **4. Contratación directa.** La modalidad de selección de contratación directa solamente procederá en los siguientes casos:
>
> (...)
>
> a) Urgencia manifiesta;

Es preciso indicar que se acude a la excepción contemplada en el citado artículo, en atención a la situación de fuerza mayor descrita en la parte inicial del presente documento, en este orden y conforme a lo indicado en múltiples ocasiones por el Consejo de Estado[15], se entiende que la fuerza mayor debe ser:

> **1) Exterior:** esto es que está dotado de una fuerza destructora abstracta, cuya realización no es determinada, ni aún indirectamente por la actividad del ofensor.
> **2) Irresistible:** esto es que ocurrido el hecho el ofensor se encuentra en tal situación que no puede actuar sino del modo que lo ha hecho.
> **3) imprevisible:** cuando el suceso escapa a las previsiones normales, esto es, que ante la conducta prudente adoptada por quien lo alega, era imposible pronosticarlo o predecirlo.

En línea de lo anterior manifiesta la misma corporación frente a lo dicho por la Corte Suprema de Justicia a este respecto (Sentencia de 15 de junio de 2000, Exp. 12.423):

> (...) La fuerza mayor sólo se demuestra mediante la prueba de un hecho externo concreto (causa extraña). Lo que debe ser imprevisible e irresistible no es el fenómeno como tal, sino sus consecuencias (...) En síntesis, para poder argumentar la fuerza mayor, el efecto del fenómeno no sólo debe ser irresistible sino también imprevisible, sin que importe la previsibilidad o imprevisibilidad de su causa. Además de imprevisible e irresistible debe ser exterior del agente, es decir, no serle imputable desde ningún ámbito.

Teniendo en cuenta la normatividad citada, es claro que no se trata de evadir los procedimientos legales ordinarios para este tipo de procesos sino de simplificarlos, en atención a las circunstancias excepcionales por las que atraviesa la Entidad, dado que no da espera a los tiempos de las modalidades típicas que se aplicarían ordinariamente para resolver este tipo de procesos, toda vez que los tiempos de gestión que implica realizar el procedimiento de selección correspondiente sería superior a 72 días[16].

Sobre el particular, la Corte Constitucional[17] indicó que:

---

[15] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, expediente 13.833, sentencia de 26 de febrero de 2004, C. P. Germán Rodríguez Villamizar.

[16] Circular No. 109 del 1 de octubre de 2020, emitida por el Secretario General del Instituto Nacional de Vigilancia de medicamentos y Alimentos- Invima.
[17] Corte Constitucional, Sentencia C-772 de 1998, 10 de diciembre de 1998. Magistrado Ponente: Fabio Morón Díaz.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

> *"La "urgencia manifiesta" es una situación que puede decretar directamente por cualquier autoridad administrativa sin autorización previa, a través de acto debidamente motivado. Que ella existe o se configura cuando se acredite la existencia de uno de los siguientes presupuestos: - Cuando la continuidad del servicio exija el suministro de bienes, o la prestación de servicios o la ejecución de obras en el inmediato futuro. - Cuando se presenten situaciones relacionadas con los estados de excepción. - Cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, - en general cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o concursos públicos".*

El Consejo de Estado[18], mediante pronunciamiento del 27 de abril de 2006, manifestó:

> *"Se observa entonces cómo la normatividad que regula el tema de la urgencia en la contratación estatal, se refiere a aquellos eventos en los cuales pueden suscitarse hechos que reclamen una actuación inmediata de la Administración, con el fin de remediar o evitar males presentes o futuros pero inminentes, provocados bien sea en virtud de los estados de excepción, o por la paralización de los servicios públicos, o provenientes de situaciones de calamidad o hechos constitutivos de fuerza mayor o desastres, o cualquier otra circunstancia similar que tampoco dé espera en su solución, de tal manera que resulte inconveniente el trámite del proceso licitatorio de selección de contratistas reglado en el estatuto contractual, por cuanto implica el agotamiento de una serie de etapas que se toman su tiempo y hacen más o menos largo el lapso para adjudicar el respectivo contrato, circunstancia que, frente a una situación de urgencia obviamente resulta entorpecedora, porque la solución en estas condiciones, puede llegar tardíamente, cuando ya se haya producido o agravado el daño. En estas estipulaciones, se hace evidente el principio de la prevalencia del interés general, en este caso, por encima de las formalidades de las actuaciones administrativas, puesto que si aquel se halla afectado o en peligro de serlo, el régimen jurídico debe ceder y permitir que las soluciones se den en la mayor brevedad posible, así ello implique la celebración de contratos sin el cumplimiento de los requisitos legales de selección del contratista y aún, la ejecución de los mismos, sin que medie la formalidad del contrato escrito, si la gravedad de las circunstancias así lo exige".*

En virtud de la obligación del Instituto de garantizar el derecho a la salud a través de la salvaguarda de la seguridad sanitaria del país, se requiere mantener la continua prestación del servicio de la entidad y, en atención a la imposibilidad, por razones de tiempo, de seleccionar a los contratistas mediante los procesos ordinarios de selección dispuestos por la Ley 80 de 1993 y demás normas reglamentarias, se requiere declarar la Urgencia Manifiesta, en aras de dar cumplimiento a la Constitución y la Ley, teniendo en cuenta los recursos asignados para tal fin.

[18] Consejo de Estado, Sentencia del 27 de abril de 2006, Expediente número 14275. Consejero Ponente: Ramiro Becerra Saavedra.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 0121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En razón a las causas y finalidades mencionadas y, de conformidad con los componentes técnicos en los que se justifica la necesidad de contratación suscrita por el Grupo de Soporte Tecnológico, la Oficina de Tecnologías de la Información y la Oficina Asesora de Planeación – Oficial de Seguridad de la Información; en este orden, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA MANIFIESTA son los siguientes[19]:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la	• Hacking Ético: Interno de caja blanca para 160 IP[20]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[19] En desarrollo de lo dispuesto en el Plan de Acción Incidente de Seguridad de la Información.
[20] IP: Internet Protocol – Protocolo de comunicaciones de Internet

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓI DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 0021
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		2. Condiciones técnicas del servicio de soporte técnico: **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.	• Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz. **Fase de estabilización** • Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información. **Fase cuatro: Actividad de Salida a producción** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. **Operación en producción** Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores. **Tecnológicos para ambiente de producción** REQUERIMIENTOS / CARACTERISTICAS **Servidor de Aplicaciones** Memoria: 128 Gygas Procesador: 32 cores Disco Duro: 800 Gygas — Dos Discos (1) 300 y (1) 500 Gygas Sistema Operativo: Windows Server 2019 Datacenter **Servidor de Base de datos** Memoria: 64 Gygas Procesador: 24 cores Disco Duro: 1 Tera Engine: SQL Server 2017 Enterprise Edition Bases de Datos: SeSuiteProducción y Utilitario **Servidor de configuración y paso** Memoria: 64 Gygas Procesador: 8 cores Disco Duro: 400 Gygas — Dos Discos: (1) de 150 Gygas (1) de 350 Gygas Sistema Operativo: Windows Server 2019 Datacenter **File server** Sistema de archivos: NTFS Capacidad: 20 Teras

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TECNICA</th><th>CONDICIONES TECNICAS</th></tr>
<tr><td></td><td></td><td>
Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.
Características Especiales
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo
Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log
Respaldo de los archivos nuevos cargados al File Server diario.
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta

Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta.</td></tr>
</table>
</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft®ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.</td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 3121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS			
	contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima. En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad. Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin.				• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas. • Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection • Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans
		2	KF5-00002EAEA SAP	Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP	• Protección de próxima generación que incluye protección antimalware y antivirus robusta. • Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
	Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativos: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnoiógico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
	entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor de Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2171
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramient encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Instalación del Ambiente de Producción: Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TECNICAS
	Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
		Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

Las necesidades anteriormente expuestas respecto a los bienes y servicios, conciernen únicamente a los requerimientos que, de acuerdo con su complejidad y especialidad, deben ser atendidos por proveedores expertos e idóneos, de conformidad con la plataforma, arquitectura, lenguaje de programación, ambiente de pruebas (QA) y producción, así como su calidad de proveedor exclusivo o canal autorizado del fabricante.

La duración de la Urgencia Manifiesta será por un término aproximado de seis (6) meses, plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En desarrollo del proceso de contratación directa, la entidad debe garantizar los principios que rigen la contratación estatal, consagrados en los artículos 24, 25 y 26 de la Ley 80 de 1993, referentes a los principios de transparencia, economía y responsabilidad[21].

En mérito de lo expuesto, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA,

RESUELVE:

ARTÍCULO PRIMERO: Declarar la URGENCIA MANIFIESTA en el **INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA**, para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, y con ello, restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte.

PARÁGRAFO PRIMERO: La duración de la Urgencia Manifiesta será por un término aproximado de seis (6) meses, plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

ARTÍCULO SEGUNDO: Establecer como modalidad a aplicar para la contratación que aquí se trata, la contratación directa conforme a la causal prevista en el artículo 42 de la ley 80 de 1993 de conformidad con lo señalado en el literal a) numeral 4 artículo 2° de la Ley 1150 de 2007, y el artículo 2.2.1.2.1.4.2. Del Decreto 1082 de 2015. Y, en consecuencia, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA, son los siguientes:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de	• Hacking Ético: interno de caja blanca para 160 IP[22]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration

[21] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera. Radicado interno 37.044. marzo 7 de 2011. Magistrado Ponente: Doctor Enrique Gil Botero.
[22] IP: Internet Protocol – Protocolo de comunicaciones de Internet

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
	brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del	**3. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
	Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACION DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **4. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto.	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.	• Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de Insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos. • Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz. **Fase de estabilización** • Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información. **Fase cuatro: Actividad de Salida a producción** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. **Operación en producción** Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores. **Tecnológicos para ambiente de producción** REQUERIMIENTOS | CARACTERISTICAS **Servidor de Aplicaciones** Memoria | 128 Gygas Procesador | 32 cores

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2171
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS		
		Disco Duro	800 Gygas	Dos Discos (1) 300 y (1) 500 Gygas
		Sistema Operativo	Windows Server 2019 Datacenter	
		Servidor de Base de datos		
		Memoria	64 Gygas	
		Procesador	24 cores	
		Disco Duro	1 Tera	
		Engine	SQL Server 2017 Enterprise Edition	
		Bases de Datos	SeSuiteProducción y Utilitario	
		Servidor de configuración y paso		
		Memoria	64 Gygas	
		Procesador	8 cores	
		Disco Duro	400 Gygas	Dos Discos: (1) de 150 Gygas (1) de 350 Gygas
		Sistema Operativo	Windows Server 2019 Datacenter	
		File server		
		Sistema de archivos	NTFS	
		Capacidad	20 Teras	
		Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.		
		Características Especiales		
		Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		
		Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log		
		Respaldo de los archivos nuevos cargados al File Server diario.		
		Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura		
		Configuración de una estrategia de seguridad robusta		

Tecnológicos para ambiente de pruebas

REQUERIMIENTOS	CARACTERISTICAS	
Servidor de Aplicaciones		
Memoria	64 Gygas	
Procesador	8 cores	
Disco Duro	400 Gygas	Dos Discos de 150 y 250 Gygas
Sistema Operativo	Windows Server 2019 Datacenter	
Servidor de Base de datos		
Memoria	16 Gygas	
Procesador	8 cores	
Disco Duro	500 Gygas	
Engine	SQL Server 2017 Enterprise Edition	
Bases de Datos	SeSuiteproduccion y Utilitario	
Características Especiales		
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60X) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>Backup de las bases de datos 1 Diario completo y cada 3 horas
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta.</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft@ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-</td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACION TECNICA</th><th colspan="4">CONDICIONES TECNICAS</th></tr>
<tr><td></td><td>buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad.

Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad.

Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin.

Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y</td><td></td><td></td><td></td><td>365/exchange/compare-microsoft-exchange-online-plans</td></tr>
<tr><td></td><td></td><td></td><td>2</td><td>KF5-00002EAEA SAP</td><td>Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP</td><td>• Protección de próxima generación que incluye protección antimalware y antivirus robusta.
• Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas
• Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales.
• Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager
• Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android
• Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de los servidores que se encuentran en el Datacenter de la entidad.	
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TÉCNICAS
	Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorías y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60X) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 Nº 64 - 28 - Bogotá
Administrativo: Cra 10 Nº 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre si y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades:

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
		de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

ARTÍCULO TERCERO: Ordenar al Grupo de Gestión Contractual y Grupo Financiero y Presupuestal adelantar los trámites precontractuales pertinentes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO CUARTO: Ordenar al Grupo Financiero y Presupuestal que se realicen los traslados presupuestales correspondientes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO QUINTO: Desígnese un comité de seguimiento y acompañamiento respecto de la ejecución de las actividades enunciadas en el artículo segundo del presente acto administrativo a la Oficina de Tecnologías de la Información y al Grupo de Soporte Tecnológico, desde el rol administrativo, jurídico y financiero a:

- La Oficina Asesora de Planeación, representada por el Jefe de Oficina y el Oficial de Seguridad.
- El Grupo Financiero y Presupuestal, representado por el Asesor de la Dirección delegado para el Grupo Financiero y Presupuestal.
- La Oficina Asesora Jurídica, representada por el Jefe de Oficina.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

- Asesor de la Dirección General Delegado para tal fin.

ARTÍCULO SEXTO: Disponer que, por el Grupo de Gestión Contractual, se conformen y organicen los expedientes respectivos, con copia de este acto administrativo, de los contratos originados en la presente urgencia manifiesta, y demás estudios y documentos precontractuales de orden técnico y administrativo, con el fin de que sean remitidos a la Contraloría General de la República, para el ejercicio del control fiscal pertinente, de conformidad con el artículo 43 de la Ley 80 de 1993.

ARTÍCULO SÉPTIMO: La presente resolución rige a partir de la fecha de su publicación.

Dada en Bogotá D.C., el 23 de marzo de 2022.

PUBLÍQUESE Y CÚMPLASE

ROY GALINDO WEHDEKING
Secretario General

Proyectó: María José Amaya López - Abogada contratista Grupo de Gestión Contractual.
María Laura Olivella Dangond – Abogada contratista Grupo de Gestión Contractual.
Leidy Diana García Arevalo – Contratista Oficina de Tecnologías de la Información.

Aprobó: María Margarita Cárdenas – Asesora de la Dirección General con delegación de funciones del Grupo de Gestión Contractual.
María Margarita Jaramillo P- Jefe de la Oficina Asesora Jurídica.
Juan Manuel Palacio Posada- Jefe de Oficina de Tecnologías de la Información.
Eliodoro Rojas Ochoa- Coordinador del Grupo de Soporte Tecnológico.
Camilo Guzmán Camacho- Coordinador del Grupo de Informática.
Miguel Díaz Peña- Coordinador del Grupo de Gestión de la Información.
Nidia Nayibe González Pinzón- Oficial de Seguridad de la Información de la Oficina Asesora de Planeación.

Anexo 1: Relación Software
Anexo 2: Estado situacional
Anexo 3: Acta Formateo Servidores
Anexo 4: Acta Comité Seguimiento Técnico
Anexo 5: Plan de Acción
Anexo 6: Anexo Técnico

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601)(1) 742 2121
www.invima.gov.co

ANEXO 2

ESTADO SITUACIONAL Y DIAGNÓSTICO INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN 06 DE FEBRERO DE 2022

1. INTRODUCCIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos Invima, de conformidad con las funciones asignadas por Ley, es un establecimiento público del orden nacional, de carácter científico y tecnológico, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Salud y Protección Social y perteneciente al Sistema de Salud.[1]

Su objetivo consiste en actuar como institución de referencia nacional en materia sanitaria y ejecutar las políticas formuladas por el Ministerio de Salud y Protección Social en materia de vigilancia sanitaria y de control de calidad de los medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva de conformidad con lo señalado en el artículo 245 de la Ley 100 de 1993 y en las demás normas que la modifiquen, adicionen o sustituyan.

En tal sentido, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima como organismo encargado de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar a través del recurso humano (funcionarios y contratistas) que conforman y hacen parte del apoyo de las direcciones, oficinas, coordinaciones y demás grupos internos de trabajo de su estructura orgánica, las actividades necesarias para la efectiva prestación del servicio público que se brinda por la institución.

Así mismo, para realizar estas labores misionales, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que soporta los múltiples sistemas de información y aplicativos necesarios para la correcta ejecución de sus oficios, administrada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades misionales y administrativas de la entidad se ejecuten, a través de los distintos aplicativos como lo son:

1. SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO.
2. SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA.
3. SOLUCIÓN WEB DE TRÁMITES EN LÍNEA.
4. SISTEMA DE INFORMACIÓN DE CÍVICOS MOVILES -CIS.
5. SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE.

[1] Articulo 1 del Decreto 2078 de 2012 – *"Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), y se determinan las funciones de sus dependencias"*

6. SOLUCIÓN WEB ADMIN.
7. SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA.
8. SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA.
9. SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS.
10. SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM).
11. SOLUCIÓN WEB ACIDOS.
12. SOLUCIÓN WEB FARMACOVIGILANCIA.
13. SOLUCIÓN WEB TRANSPARENCIA.
14. SOLUCIÓN WEB REGISTRO – RECAUDOS.
15. SOLUCIÓN WEB IVC/SOA.
16. SOLUCIÓN WEB REACTIVOVIGILANCIA.
17. SOLUCIÓN WEB TECNOVIGILANCIA.
18. SOLUCIÓN WEB - IVC SOA PUERTOS.
19. SOLUCION WEB PROTOCOLOS DE INVESTIGACIÓN.
20. SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS.
21. SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA.
22. SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB.
23. PORTAL WEB INSTITUCIONAL.
24. SOLUCIÓN WEB KAWAK.
25. SOLUCION WEB ITSM ARANDA.
26. HERRAMIENTA ANTIVIRUS KASPERSKY.
27. SOLUCION WEB OFICINA VIRTUAL.
28. DIRECTORIO ACTIVO.
29. CORREO ELECTRONICO.
30. SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO).
31. SISTEMA DE INFORMACION WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL - SIVICOS (PROYECTO EN DESARROLLO).

De dichos aplicativos se venía haciendo uso de forma efectiva desde las diferentes sedes de la entidad de manera presencial y virtual, conforme a la capacidad diagnosticada y operativamente válida para garantizar la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso. Sin embargo, el 6 de febrero de 2022 el Coordinador (E) del Grupo de Soporte Tecnológico informa a su equipo de trabajo de la caída de la página web de la entidad, generando la indisponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas que soportan las actividades operacionales y administrativas de la Entidad.

En tal sentido, es procedente realizar en desarrollo de las políticas, lineamientos y estándares adoptados por la Entidad el siguiente diagnostico que consta de los puntos que a continuación se tratan, para efectos de tomar las decisiones y acciones procedentes para mitigar los posibles eventos adversos generados como consecuencia de la indisponibilidad.

2. ANTECEDENTES

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[2] que comprometió la disponibilidad de la información del Invima, este se dio por el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

En consecuencia, se procedió a dar paso al Procedimiento Gestión de Incidentes Tecnológicos:

- **Identificar los posibles eventos de seguridad de la información:** El Coordinador (E) del Grupo de Soporte Tecnológico estuvo monitoreando el fin de semana del 5 de febrero de 2022 el funcionamiento de la página web del Instituto, el domingo 6 de febrero de 2022 a las 7:30 de la mañana detectó que la página dejo de funcionar, comunicándose de forma inmediata con el ingeniero Cristian Pinzón para que se realizara la revisión de la infraestructura correspondiente (servidores), indicándose que existía una anomalía, por lo que el funcionario Pinzón se comunica con el ingeniero Jhorbis Ríos, quienes de manera mancomunada proceden a revisar la infraestructura.

  El reporte telefónico indica que se encontró un cambio de contraseña en el administrador, y se percató por parte del Ingeniero Ríos que existían discos encriptados, se observa que uno de los principales servidores Directorio Activo se encontraba encriptado e infectado; de conformidad a lo sucedido y en atención a la experiencia se presumió de forma inmediata que la indisponibilidad obedecía a un ataque.

- **Reportar el evento:** Se procede a informar al oficial de seguridad de la información, al jefe de la Oficina de Tecnologías de la Información y al Coordinador titular del cargo. Quienes tomaron la decisión de comunicarse con el contratista de la entidad Empresa de Recursos Tecnológicos - ERT para que procediera a desconectar los canales de comunicación, de igual forma como medidas de seguridad se comienzan a apagar los servidores de forma gradual y a la elaboración del inventario de los servidores impactados, también se realizó al apagado de suiches de distribución.

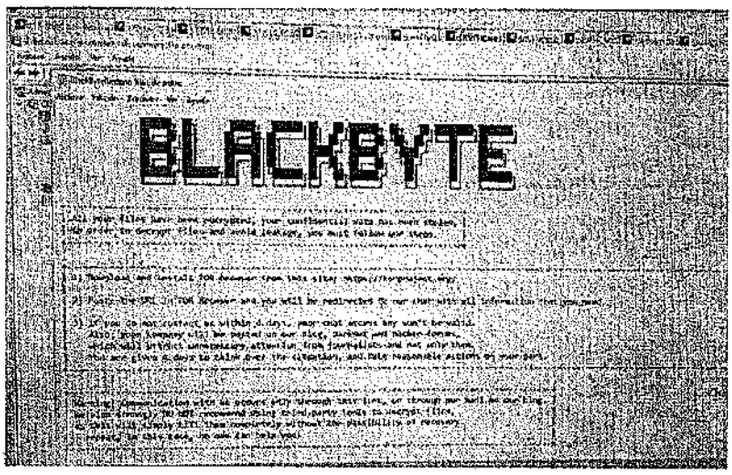
  Según el archivo .txt se observa que es un Ransoware Blackbyte

---

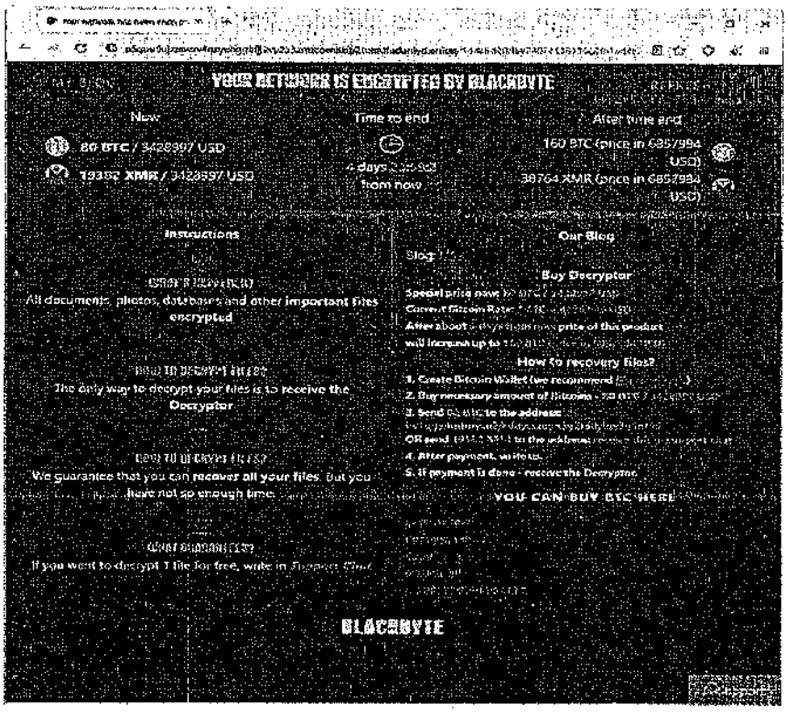
[2] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion

[3] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com

[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos



Finalizado el cifrado del equipo se identificó una nota de rescate que indica:



El incidente se reportó vía telefónica y vía WhatsApp al Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL el día 6 de febrero de 2022 a las 10:07, de conformidad al Instructivo de Relaciones con Autoridades y Grupos de Interés, con el propósito de solicitar apoyo en el manejo de dicha situación.

- **Realizar evaluación preliminar del evento:** Se dispuso la elaboración de la evaluación de los equipos, de la cual se obtuvo el siguiente resultado:

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\AD_DNS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\AD_DNS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\APP	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\APP	1-Sin Acceso	Microsoft Windows Server 2012 Datacenter	Si
INVIMA\APP_BIO_STAR	0-Comprometida	Microsoft® Windows Server® 2008 Standard	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2019 STANDARD	Si
INVIMA\EXCHANGE	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64Bit	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si

Ron	Estado Hoy	OS	Administrada (Si / No)
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\FS_ISS_P_SERVER	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64BIT	Si
INVIMA\FS_ISS_P_SERVER	0-Comprometida	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\IIS	2-Aislada / apagada	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\IIS- ARANDA	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\IIS_RDS_POWER_BI	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Datacenter	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\NPS_RADIUS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Micresoft Windows 7 Professional	Si
INVIMA\OTROS	2-Aislada / apagada	WINDOWS SERVER 2012 R2 STANDARD	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2008 R2 ENTERPRISE - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	Windows Server 2012 R2 estandar	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SFB	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\SQL	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER-SQL	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2008 R2 Enterprise	No
		Microsoft Windows Server 2016 Standard	No
		Microsoft Windows Server 2016 Datacenter	No
		Microsoft Windows Server 2016 Standard	No

- **Evaluar el evento:** De conformidad al procedimiento la oficial de seguridad de la información, junto con la persona que reporta y el equipo de la mesa de ayuda, establecieron que el incidente presentado sobre los sistemas de información y comunicaciones del Instituto se trata de:

Malwares	Ransomware
Disponibilidad:	Sabotaje
Compromiso de Información:	Acceso no autorizado a información
Fraude:	Uso ilegítimo de credenciales
Política de Seguridad:	Acceso a servicios no autorizados
Clasificación de peligrosidad	10 / 10

- **Características más predominantes de BlackByte:**
  - Tiene funcionalidad de gusano en donde realiza consulta de otros posibles equipos objetivo, al conocer el alcance de infección, procede a propagarse a través de la red.

- Paquete Wake-on-LAN en donde se puede controlar de manera remota los equipos afectados al encenderlos cuando están apagados, hibernando o suspendidos. (Ver Anexo: Alerta de Seguridad Ransonware BlackByte).

- **¿Se considera un incidente de Seguridad de la Información?:** Si. (Ver Anexo: Formato de Reporte de Incidentes – CSIRT Gobierno Invima V1).

- **Contener el incidente**: Una vez se presentó el suceso el Invima tomó las siguientes acciones como medida de contención frente a la propagación del programa dañino identificado en los sistemas de información, plataformas tecnológicas y herramientas tecnológicas:

  - Se apagaron de forma gradual los servidores de la entidad, para limitar la expansión del código malicioso en la red que pudiera impactar la información del instituto (servidores de datos compartidos).
  - Se identificó que los computadores de los usuarios estaban afectados, por lo que se desconectó físicamente toda la red.
  - Se desconectaron las interfaces de red y se desactivó toda la red (incluido wifi) para evitar la expansión del virus y afectación de otros servidores.
  - Se procedió a la revisión de los logs y al monitoreo de la herramienta de control de software y antivirus, para efectos de comprobar la finalización de la ejecución del proceso dañino, identificando que los atacantes lograron ganar acceso completo a la infraestructura tecnológica sobre la 1:00 a.m. del 6 de febrero de 2022, con el cambio de la contraseña maestra del Directorio Activo.
  - Se identificó que respecto de las copias de seguridad de la entidad (backup) toda la data e información del Invima se encuentra protegida y no fue objeto de sustracción por parte de los atacantes.
  - Se realizó un levantamiento de información con el propósito de determinar qué información se encontraba encriptada.
  - Como metodología de trabajo se realizó el análisis del comportamiento de este tipo de ataque que se actúa como un virus, respecto de las herramientas de seguridad con la que cuenta la entidad (antivirus, firewall y fireeye). En tal sentido, se estableció como necesidad y dada la clasificación de peligrosidad comportada por este tipo de virus se debe estructurar una estrategia de contención que va desde parchar los servidores, obtener una auditoria forense para delimitar los principales puntos débiles que deben tenerse en cuenta en la evaluación de riesgos por ciberataques atendiendo criterios de razonabilidad, así como mantener actualizadas para posibles nuevas amenazas cibernéticas respecto de los ransomware.
  - Finalmente se instauró denuncia penal bajo el código de noticia criminal No. 110016000050202201569 de fecha 18 de febrero de 2022, por el presunto delito de accedo abusivo a un sistema informático (Artículo 269ª Ley 1273 de 2009).

- **Evaluar el incidente de seguridad:** Al confirmarse que el evento corresponde a un incidente de seguridad de la información se procedió a evaluarlo de acuerdo con el instructivo Gestión de incidentes Tecnológicos lo que conlleva a identificar:

1. Se valida el tipo de incidente, especificando el impacto potencial, la cantidad de usuarios afectados.
2. Se evidencia la indisponibilidad de los servicios tecnológicos del instituto que se encuentran dentro del catálogo de servicios y de los servidores de la entidad

Se procede a categorizar el incidente de seguridad de la información teniendo cuenta la siguiente tabla:

Niveles de prioridad de los incidentes

Prioridad	Descripción
Prioridad 1 (Alta)	Causa una completa pérdida del servicio, sin importar el ambiente en el que se está trabajando (producción, pruebas, desarrollo, etc.). La operación no puede continuar de una manera razonable y no puede ser restablecida inmediatamente.
Prioridad 2 (Media)	Causa una pérdida mínima del servicio. El problema o defecto tiene un impacto menor o no produce inconvenientes. Comprende características importantes inoperables, pero con una solución alterna o características no tan importantes inoperables sin solución alterna.
Prioridad 3 (Baja)	No causa pérdida del servicio. El resultado del problema es un error menor, comportamiento incorrecto o error en la documentación que, de ninguna manera, impide la operación del sistema.

Adicionalmente se identifica una falla masiva es decir en más de 10 usuarios en los siguientes aspectos:

1. Interrupción del servicio en alguna de las aplicaciones o sistemas de información de Invima.
2. Falla al ingresar o realizar alguna operación en aplicativos o sistemas de información del Invima.
3. Falla en alguna de las operaciones o en la generación de reportes
4. Falla es reportada en uno o varios elementos de configuración.
5. Falla de telecomunicaciones o conexión de red o wifi
6. Reducción de la calidad del servicio masiva, no planificada del servicio, determinando si fue producida por la implementación de un cambio.
7. Falla de uno o más servicios que se encuentran activos en el catálogo de servicios

Lo anterior nos lleva a valorar el incidente con un nivel de **Prioridad Alto** y una **Criticidad Alta**, por lo que se procede a aplicar lo establecido en el documento TIC-GTI-IN008 - INSTRUCTIVO GESTIÓN DE PROBLEMAS DE LOS SERVICIOS DE TI (TIC-GTI-IN008).

- **Definir estrategia de atención del incidente:** La estrategia de atención se encuentra registrada en el documento Plan de Acción Riesgo Incidente de Seguridad de la Información

- **Erradicar fallas:** En proceso de análisis
- **Recuperar activos de información:**

  Conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no ha existido fuga de información, sin embargo, la entidad se atiene a lo dispuesto en el análisis forense realizado por la SIC, entidad competente para determinar la perdida de la información.

- **Registrar lecciones aprendidas:** En proceso de análisis
- **Cerrar el incidente:** En proceso

ANEXO 1

INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA

RELACION DE SOFTWARE, SISTEMAS DE INFORMACIÓN Y/O HERRAMIENTAS TECNOLOGICAS INVIMA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

NÚMERO	NOMBRE SOFTWARE, SISTEMA DE INFORMACIÓN, APLICATIVOS TECNOLÓGICOS, PLATAFORMAS TECNOLÓGICAS, HERRAMIENTAS TECNOLÓGICAS Y/O APLICACIONES	DESCRIPCION	ARQUITECTURA	TIPO DE PLATAFORMA	ES MISIONAL?	PROCESO DUEÑO DE LAS DATOS	LENGUAJE DE PROGRAMACIÓN
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	El sistema de información "Registros Sanitarios", se encarga de apoyar las actividades relacionadas con el proceso de expedición de registros sanitarios y trámites asociados de los productos competencia del INVIMA.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	El sistema de información "COMISIÓN REVISORA", se utiliza para relacionar los radicados enviados a la comisión revisora, permite generar un documento que se adiciona al expediente, para informarle a la comisión. Además, permite generar un consolidado con los datos específicos del producto de las actas de la comisión.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	Este sistema web de "TRAMITES EN LÍNEA", permite hacer uso de los siguientes módulos: Consulta estado trámite, Certificado de Venta Libre, Cambio de Clave, Actualizar Datos, Pago Electrónico de Tarifas, Solicitud Certificado de Inspección Sanitaria en Puertos – Alimentos, Solicitud Certificado de Inspección Sanitaria en Puertos - Bebidas Alcohólicas, Adjuntar documentos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-GIS	El sistema de información "SIVICOS", permite realizar la inspección in situ de las inspecciones/exportaciones en puertos, aeropuertos y pasos fronterizos. Así mismo, genera reportes de eventos y reacciones adversas y la consulta de reportes enviados al INVIMA. Inspección PAPF: Solución informática implementada para ser utilizada con tableta en Windows, Android, utilizada como herramienta por los inspectores al momento de realizar la inspección sanitaria de alimentos, materias primas, insumos y bebidas alcohólicas, expide el certificado.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
5	SISTEMA DE INFORMACIÓN CORRESPONDENCIA Y PQRDS - SISQUITE	El sistema de información "CORRESPONDENCIA", permite gestionar y realizar el control de correspondencia interna y externa del INVIMA.	ON PREMISE	ON PREMISE	SI	Transversal a todos los procesos	PHP - JAVA
6	SOLUCIÓN WEB ADMIN	Este sistema web "ADMIN", es interno y permite su gestión diariamente, y genera los reportes diarios y mensuales sobre los siguientes módulos: Certificaciones por Entregar, Notificación por Aviso, Autos por Estado, Registros Cancelados, Registros Negados, Registros o Renovaciones por periodo, Resoluciones Pendientes por Notificar.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTERA	Este sistema web "CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTO", permite consultar los certificados inspección sanitaria en puerto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA	Este sistema web "DOCUMENTOS DE APOSTILLE CANCILLERIA", permite validar los documentos apostillados.	WEB	ON PREMISE	SI	Aseguramiento Sanitario	JAVA - POWER BUILDER
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS	Este sistema web "CONSULTA DE DOCUMENTOS EMITIDOS", permite consultar los documentos con firma digital.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA - POWER BUILDER
10	SOLUCIÓN WEB CODIGO ÚNICO DE MEDICAMENTOS (CUM).	El Servicio Web "CODIGO UNICO DE MEDICAMENTOS (CUM)", le proporciona al Ministerio de Salud la información de los Códigos Únicos de Medicamentos.	SERVICIO WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA - POWER BUILDER
11	SOLUCIÓN WEB ACIDOS.	Este sistema web "ACIDOS", (Decreto 1003/2014) Sistema de información que soporte el registro de control para la comercialización de ácidos, álcalis o sustancias similares o asimilares, quien intervenga en el proceso de comercialización de cualquier sustancia sujeta al registro de control, reportará la información que permita la trazabilidad sobre su procedencia, así como la individualización de cada uno de los actores que intervinieron en la operación de comercialización.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
12	SOLUCIÓN WEB FARMACOVIGILANCIA	Este sistema web "FARMACOVIGILANCIA", permite que usuarios externos reporten información de eventos adversos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
13	SOLUCIÓN WEB TRANSPARENCIA	Este sistema web "TRANSPARENCIA", permite consultar los registros o renovaciones otorgados en una fecha determinada.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
14	SOLUCIÓN WEB REGISTRO - RECAUDOS	Este sistema móvil "Registro - Recaudos", es una solución que permite realizar el cargue manual de los archivos de los pagos recibidos en las ventanillas de Daviviendo a través de la lectura del código de barras.	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	Delphi JAVA
15	SOLUCIÓN WEB IVC/SOA	Este sistema web "IVC/SOA", es una solución Web que permite calcular los índices de severidad, consenso y afectación, desde los grupos de productos por Dirección misional, hasta el consolidado denominado IRA (Índice de Riesgo Asociado), para cada Dirección misional y el Instituto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
16	SOLUCIÓN WEB REACTIVOVIGILANCIA	Este sistema web "REACTIVOVIGILANCIA", permite la notificación, registro y evaluación sistemática de los problemas relacionados con los reactivos de diagnóstico in vitro.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
17	SOLUCIÓN WEB TECNOVIGILANCIA	Este sistema web "TECNOVIGILANCIA", permite el reporte de eventos o incidentes adversos serios e inesperados producidos asociados con los dispositivos médicos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
18	SOLUCIÓN WEB - IVC SOA PUERTOS	Este sistema de IVC SOA Puertos, fue construida como una herramienta para consultar, calcular y/o modificar información relacionada con el Modelo IVC SOA Puertos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
19	SOLUCIÓN WEB PROTOCOLOS DE INVESTIGACIÓN -	Este sistema web "PROTOCOLOS DE INVESTIGACIÓN", herramienta del INVIMA, desde la cual se podrá solicitar el trámite de evaluación inicial de protocolos de investigación con productos en investigación/medicamentos desde la comodidad de su casa u oficina.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	Este sistema web "ESTABLECIMIENTOS", permite el registro de establecimientos nacionales y extranjeros. (conos de establecimientos de alimentos).	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7

21	SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRONICA DEL PROYECTO DE PAISES BAJOS Y COLOMBIA	El proyecto de Paises Bajos y Colombia se divide en dos frentes: 1. La aplicación Sivicos/Visibles: La utilizan los funcionarios en Tablet o Windows para las operaciones que manejan en los puertos. 2. Los microservicios desarrollados en OpenShift: Es la lógica que contiene el desarrollo de los servicios para interactuar con Paises Bajos.	CLIENTE SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	Java JEE7
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS - SILAB	Es una solución tecnológica, para la gestión de la información generada por los laboratorios desde sus procesos analíticos, que permite la gestión integral de las muestras desde el ingreso al laboratorio hasta la generación del informe de resultados, permitiendo la total trazabilidad en custodia, calidad y control de los datos del informe de resultados.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	C#, TSQL, HTML5, CSS, TypeScript
23	PORTAL WEB INSTITUCIONAL	Plataforma que ofrece al ciudadano de forma integrada información del instituto y servicios que este presta de forma virtual o a través del Internet. Principalmente está dirigido para apoyar a resolver las inquietudes y necesidades del ciudadano y los tramites que este requiere.	WEB	ON PREMISE	SI	Servicio Transversal para todos los procesos	CMS LifeRay - Java
24	SOLUCIÓN WEB KAWAK	Plataforma para administrar el Sistema Integrado de Gestión del Instituto	WEB	NUBE	NO	Administración del Sistema de Gestión Integrado	N/A
25	SOLUCIÓN WEB ITSM ARANDA	Aplicativo que agrupa un conjunto de recursos tecnológicos para brindar o prestar servicios con la posibilidad de gestionar y solucionar de manera integral requerimientos relacionados con tecnología y recursos tecnológicos.	WEB	NUBE	NO	Procesos de Apoyo	N/A
26	HERRAMIENTA ANTIVIRUS KASPERSKY	Programa cuyo objetivo es detectar y eliminar virus informáticos, además los bloquea, desinfecta archivos y puede prevenir la infección o daño que los virus puedan ocasionar a la información.	N/A	ON PREMISE	NO	Gestión de Tecnologías de la Información	N/A
27	SOLUCION WEB OFICINA VIRTUAL	Herramienta que permite la interacción del instituto con el ciudadano a través de medios digitales	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	MySQL y PHP
28	DIRECTORIO ACTIVO	Base de datos y conjunto de servicios que conecta a los usuarios de la entidad con los recursos de red que se requieren para realizar su trabajo, esto incluye información crítica sobre el entorno tecnológico instalado los usuarios, los computadores y acceso a la información, así como la definición de permisos.	ON PREMISE Y NUBE		NO	Gestión de Tecnologías de la Información	N/A
29	CORREO ELECTRONICO	Sistema que permite el intercambio de mensajes entre los diferentes usuarios de la entidad y con otros usuarios externos a la misma.	N/A	HIBRIDO	NO	Servicio Transversal para todos los procesos	N/A
30	SISTEMA DE INFORMACION WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo y permitirá ejecutar en línea las actividades misionales de los procesos "Registros Sanitarios Y Tramites Asociados" Y "Auditorias Y Certificaciones" Del Instituto Nacional De Vigilancia De Medicamentos Y Alimentos – Invima. Para este proyecto se encuentra afectada la información de la arquitectura y los ambientes de calidad y producción que ya habían sido implementados en la plataforma OpenShift y la implementación de la tecnología RPA.	WEB	NUBE	SI	Aseguramiento Sanitario	JAVA
31	SISTEMA DE INFORMACION WEB PARA LA INSPECCION, VIGILANCIA Y CONTROL Y SIVICOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo que permitirá la sistematización, automatización, gestión de datos, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de Inspección, Vigilancia y Control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. Para este proyecto se afectó la información de la arquitecaura y los ambientes de calidad donde se habían iniciado pruebas funcionales y el ambiente de producción implementados en la plataforma openshift.	WEB	NUBE	SI	Inspección, Vigilancia y Control	JAVA
32	REQUERIMIENTOS TRANSVERSALES	Requerimientos generales para mantener evidencia del material probatorio y aprovechar la capacidad de almacenamiento: 80 discos de 500 GB Mecánico					

ANEXO 5

PLAN DE ACCIÓN
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN DEL 6 DE FEBRERO DE 2022
Actualización del 25 de Febrero de 2022

1. OBJETIVO

Garantizar la disponibilidad y acceso a la información y las comunicaciones del Instituto Nacional de Vigilancia de Medicamento y Alimentos- Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte.

2. ANÁLISIS DEL RIESGO

A continuación, se presenta el riesgo identificado y gestionado dentro del Sistema de Gestión Integrado del Instituto, en el cual se establece la descripción, causa, efectos y control de este, tal como se observa en la siguiente tabla:

Riesgo	Posibilidad de afectación de la operación de la entidad, por la indisponibilidad del activo de información, debido a las fallas de software y hardware del centro de datos.
Descripción	Imposibilidad de acceso a la información por parte de la entidad cuando se presente una falla en la infraestructura y herramientas tecnológicas del centro de datos (hardware y software).
Causas	Incidente a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio (origen: Externo, factor: Tecnológico
Efectos	• Pérdida de información. • Demoras en los procesos y/u operación • Atención parcial o nula al ciudadano • Pérdida de imagen Institucional • Insatisfacción de los usuarios internos del Invima • Daños irreversibles en equipos y herramientas tecnológicas • Disminución o pérdida de productividad
Control	Monitoreo y mantenimiento de herramientas para control incidentes informáticos
Descripción del control	Se cuenta con un antivirus y herramientas de control de software dañino que son monitoreados periódicamente por los administradores del centro de datos de acuerdo al procedimiento de administración del centro de datos TIC-GTI-PR004, como soporte se cuentan con logs y reportes de eventos de este monitoreo.

Respecto a lo anterior, se relacionan los posibles efectos o consecuencias de la materialización del riesgo antes mencionado, con sus respectivas acciones y medidas de contingencia frente al incidente cibernético para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima.

3. PLAN DE ACCIÓN Y MEDIDAS DE CONTINGENCIA FRENTE A LOS POSIBLES EFECTOS O CONSECUENCIAS DEL INCIDENTE CIBERNÉTICO

Posibles efectos	Acciones y medidas de contingencia
Pérdida de información	A la fecha no se evidencia pérdida de la información, ya que se implementó uno de los controles establecidos frente a este riesgo que consistió en "Disponer de copias de seguridad (backps) para restablecer la plataforma y disponibilidad de la información, así como la aplicación del procedimiento interno "TIC-GSI-PR003- PROCEDIMIENTO GENERACIÓN DE COPIAS DE RESPALDO DE A INFORMACIÓN DE LOS SERVIDORES DEL CENTRO DE COMPUTO" lo que ha permitido la continuidad de la operatividad y la prestación servicios de la entidad.
Demoras en los procesos y/o operación	• Emitir medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto. A la fecha se han emitido las siguientes: ▪ Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites. ▪ Circular - 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.
Atención parcial o nula al ciudadano	• Activar la gestión manual de los trámites sin suspensión de términos (posteriormente estos se incluirán en las bases de datos correspondientes). • Activar la opción de pago de trámites a través de transferencia bancaria. • Activar radicación y atención de PQRDS.
Pérdida de imagen Institucional	• Mantenido la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio. • Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.
Insatisfacción de los usuarios internos del Invima	• Garantizar el uso de equipos de navegación a internet mediante módems y routers a las diferentes dependencias de la entidad, para la continuidad operativa de los funcionarios y contratistas de la entidad.

Posibles efectos	Acciones y medidas de contingencia
	• Restablecer Internet en áreas misionales y críticas de la entidad, puertos (Buenaventura, Cartagena, Barranquilla y Santa Marta) y aeropuerto del dorado.
Daños irreversibles en equipos y herramientas tecnológicas	• A la fecha no se han identificado daños irreversibles en equipos y herramientas tecnológicas
Disminución o pérdida de productividad	• Realizar la priorización del restablecimiento de la plataforma SIVICOS para los trámites de certificados de inspección sanitaria en PAPF. • Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa. • Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones. • Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 • Hacer verificación de los servidores y PC afectados • Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus • Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura • Restaurar copias de seguridad • Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera) • Reactivar el sistema de información de Registros Sanitarios • Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad • Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración. • Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS • Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube • Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad • Restablecer los demás servicios del Instituto

4. RECURSOS

El desarrollo y ejecución de este plan queda sometido a la disponibilidad de recursos humano, tecnológico y presupuestales que deben ser gestionados por el Instituto, entidades aliadas y el gobierno nacional.

El Equipo de Trabajo está conformado por la totalidad de los servidores públicos del Invima.

5. CRONOGRAMA Y RUTA CRITICA

Ítem	Semanas Previas (Febrero)			Semanas (Marzo, Abril y Mayo)										
	1	2	3	1	2	3	4	5	6	7	8	9	10	11
Actividades Administrativas														
Emisión de Resoluciones con medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto	■	■	■											
Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa.	■	■	■											
Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones.	■	■	■											
Mantener la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio.	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.		■	■	■	■	■	■	■	■	■	■	■	■	■
Actividades Operacionales y Técnicas														
Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 (RC)	■	■												
Hacer verificación de los servidores y PC afectados (RC)	■	■	■	■	■	■	■	■						
Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura		■	■	■	■	■	■	■	■	■	■	■	■	■
Restaurar copias de seguridad (RC)			■	■	■	■	■	■	■	■	■	■	■	■
Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera)				■	■									

Item	Semanas Previas (Febrero) 1	2	3	Semanas (Marzo, Abril y Mayo) 1	2	3	4	5	6	7	8	9	10	11
Reactivar el sistema de información de Registros Sanitarios				■	■	■	■	■	■	■	■	■		
Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad			■	■	■	■	■							
Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecanico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración (RC)			■	■	■	■	■	■	■					
Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS				■	■	■	■	■	■	■	■	■	■	■
Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube					■	■	■	■						
Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad				■	■	■	■	■	■	■	■	■	■	■
Restablecer los demás servicios del Instituto								■	■	■	■	■	■	■

Las actividades marcadas con **(RC)** conforman la ruta crítica del plan de acción

ANEXO 6

ANEXO TECNICO

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información que comprometió la disponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware llamado Blackbyte el cual encriptó la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

De conformidad con el Plan de Acción socializado por la entidad para el manejo del incidente, mediante la realización de estos procesos contractuales se da cumplimiento a las siguientes acciones:

- Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad.
- Ampliación de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración.
- Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad.

Es por ello que se deben realizar las siguientes actividades desde la Oficina de Tecnologías de la Información – OTI y el Grupo de Soporte Tecnológico así:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.	• Hacking Ético: interno de caja blanca para 160 IP[1]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[1] IP: Internet Protocol – Protocolo de comunicaciones de Internet

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), Impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **2. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** **Soporte de nivel 1 (N1)** Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la Infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos. • Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz.

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TECNICA</th><th>CONDICIONES TECNICAS</th></tr>
<tr><td></td><td>permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.</td><td>
Fase de estabilización
• Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información.

Fase cuatro: Actividad de Salida a producción
El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado.

Operación en producción
Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores.

Tecnológicos para ambiente de producción
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>128 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>32 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>800 Gygas</td><td>Dos Discos (1) 300 y (1) 500 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>24 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>1 Tera</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteProducción y Utilitario</td><td></td></tr>
<tr><td colspan="3">Servidor de configuración y paso</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos: (1) de 150 Gygas (1) de 350 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td colspan="3">File server</td></tr>
<tr><td>Sistema de archivos</td><td>NTFS</td><td></td></tr>
<tr><td>Capacidad</td><td>20 Teras</td><td></td></tr>
<tr><td colspan="3">Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.</td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log</td></tr>
<tr><td colspan="3">Respaldo de los archivos nuevos cargados al File Server diario.</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta</td></tr>
</table>
Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S</td></tr>
<tr><td>Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td>Configuración de una estrategia de seguridad robusta.</td></tr>
</table>
</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad.

Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEASAP</td><td>Microsoft®ExchangeOnlinePlan2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1,5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans</td></tr>
<tr><td>2</td><td>KF5-00002EAEASAP</td><td>Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP</td><td>• Protección de próxima generación que incluye protección antimalware y antivirus robusta.
• Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o</td></tr>
</table>
</td></tr>
</table>

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS			
	correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima - desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin. Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e Instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en				archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad.	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas.	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorías y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Servicios de conformidad a las condiciones técnicas del proyecto.	desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Despliegue Base de Datos: Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:**

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner ▪ **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: Formateo de Servidores del Invima

Lugar: TEAMS		**Acta No 1250-006-2022**
Fecha: 2022-03-15		
Hora de inicio: 06:00 pm	**Hora de finalización:**	

ASISTENTES

Nombre Completo	Cargo
María Margarita Jaramillo Pineda	**Jefe Oficina Asesora Jurídica**
Juan Manuel Palacio Posada	**Jefe de la Oficina de Tecnologías de la Información**
Eliodoro Rojas Ochoa	**Profesional Especializado - Coordinador Grupo Soporte Tecnológico**
Nidia Nayibe González Pinzón	**Contratista - Oficial de Seguridad de la Información**
Camilo Andrés Guzmán Camacho	**Profesional Especializado – Coordinador Grupo de Informática**
Miguel Fernando Diaz Peña	**Profesional Especializado – Coordinador Grupo Gestión de la Información**

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones

ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC
2. Selección y aprobación de las acciones a seguir con el formateo y reinstalación de los servidores

DESARROLLO ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC

El día 25/02/2022 se realizó la entrega de la información solicitada por la DIJIN, sobre los servidores afectados en el Invima, como parte de las pruebas del proceso penal que se inició ante la Fiscalía General de la Nación con denuncia penal NC_110016000050202201569.

El 28/02/2022 se realizó la entrega de la información solicitada por el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante, "GTIFSD") de la Superintendencia de Industria y Comercio - SIC, para el análisis forense a realizar sobre el incidente de seguridad de la información presentado en el Instituto.

El miércoles 2 de marzo de 2022 a través de correo electrónico el intendente Alejandro González Franco Suboficial Centro Cibernético Policial, en coordinación con el Mayor Félix Daniel Miranda Herrera responsable del despliegue del PMU Ciber Electoral, informa a la oficial de seguridad de la información del Invima que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el centro cibernético policial ya inició el análisis y las actividades investigativas y forenses, por lo que no

van a requerir formación. Por lo anterior se puede disponer de los servidores. Se adjunta imagen del correo electrónico recibido:

RV: Informando requerimiento

Policía Nacional Dios y Patria

Buenas tardes, respetuosamente me permito informar a la señora NIDIA NAYIBE GONZÁLEZ PINZÓN Oficial de Seguridad de la Información de INVIMA, que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el Centro Cibernético Policial ya inicio el análisis y demás actividades investigativas y forenses, por lo anterior ya no se requiere de algún otro requerimiento y ni ninguna interrupción por parte de ustedes en la activación de los servicios de INVIMA.

Por otra parte, esta decisión se toma en coordinación con mi Mayor FELIX DANIEL MIRANDA HERRERA, responsable del despliegue del PMU Ciber electoral.

Quedamos atentos a cualquier solicitud y a la información adicional que nos puedan aportar.

Atentamente,

Intendente
ALEJANDRO GONZÁLEZ FRANCO
Suboficial Centro Cibernético Policial
Teléfono: 5159700 Ext. 30428
www.policia.gov.co/dijin

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

Después de recibir la comunicación se determina esperar hasta el 15/03/2022 para dar inicio al proceso de formateo y reinstalación de los servidores, para dar espacio a cualquier requerimiento adicional por parte de la Superintendencia de Industria y Comercio - SIC.

2. Acciones para seguir con el formateo y reinstalación de los servidores

Luego de realizar un análisis de la información que puede ser vital para determinar hallazgos o recuperar información importante para la gestión de la seguridad y operatividad técnica, se decide seleccionar el servidor AZURE, para los correspondientes a los aplicativos SESUITE y BI, almacenándola de forma segura.

El proceso de formateo se realizará de forma ordenada informando a cada responsable de la información contenida en los servidores que estos se formatearán y reconfigurarán para su uso posterior en el marco de la recuperación de los servicios que presta el Invima. A continuación, se presenta una lista de los servidores físicos y virtuales que se formatearán:

No.	Nombre del Servidor	IP	Descripción
1	SRVVCLUSQL01	172.16.10.21	SERVIDOR SKYPE
2	SRVVCOLOMBIA	172.16.10.128	SERVIDOR JAGUAR
3	SRVVCONOF365	172.16.10.196	CONNECT OFFICE 365
4	SRVVKAS	172.16.10.98	SERVIDOR ANTIVIRUS KASPERSKY Y WSUS
5	SRVVDHCP01	172.16.10.61	SERVIDOR DHCP
6	SRVVMOSCU	172.16.10.102	SERVIDOR DE BASE DE DATOS ACCESS

No.	Nombre del Servidor	IP	Descripción
7	SRVVMYSQLWEB01	172.16.10.218	SERVIDOR WEB BASE DE DATOS – DESARROLLO
8	SRVVNGINXWEB01	172.16.10.52	SERVIDOR LIFERAY DE PRODUCCION
9	SRVVSAPIENS01	172.16.10.198	HV_SAPIENS
10	SRVVSERTRAMI	172.16.10.148	SERVIDOR TRAMITES EN LINEA
11	SRVVWEBDES03	172.16.10.219	SERVIDOR DESARROLLO PAGINA WEB - APP.INVIMA
12	SRVVWFLY01	172.16.10.80	SERVIDOR MASTER WILDFLY 8
13	SRVVWFLY9FV	172.16.10.65	WILDFLY
14	SRVV3MBX	172.16.10.177	SERVIDOR CORREO EXCHANGE MAILBOX
15	SRVVACCESO	172.16.10.79	SERVIDOR PARA EL CONTROL DE ACCESO
16	SRVVRELAY	172.16.80.15	MAQUINA RELAY CORREO LINUX
17	SRVVSESBDPRU	172.16.10.171	SERVIDOR SESUITE BD QA
18	SRVVSOLARW01	172.16.10.152	SERVIDOR MONITOREO SOLARWINDS
19	SRVVWHD	172.16.10.159	SERVIDOR SOLAR WINDS HELP DESK
20	SRVVSAPIENS01	172.16.10.198	SERVIDOR SQL SERVER
21	SRVVAPPEONPROD	172.16.10.55	APP APPEON Productivo
22	SRVV1CAS	172.16.10.175	SERVIDOR CAS DE CORREO EXCHANGE
23	SRVV3SESPRU	172.16.10.82	SERVIDOR DE PRUEBAS DE SESUITE
24	SRVVPAPERCUT	172.16.40.14	Administrador de Impresión – ERT
25	SRVVNAGIOS	172.16.10.197	Monitoreo Nagios Free
26	SRVVAULA	172.16.10.113	SERVIDOR DE SERVICIOS Y APLICACIONES WEB -AULA VIRTUAL
27	SRVVSESAPPRU	172.16.10.172	SERVIDOR DE APLICACIONES SESUITE DE PRUEBAS
28	SRVVMILANFL	172.16.10.194	SERVIDOR DE ARCHIVOS VIEJO
29	SRVVCOLOMBIA_CLON02	172.16.10.127	SERVIDOR JAGUAR
30	SRVV6SENT	172.16.10.36	MOBILE IRON - security.invima.gov.co
31	SVV5CORE	172.16.10.35	MOBILE IRON - mobile.invima.gov.co - CORE
32	SRVVSESAPPRO	172.16.10.181	SERVIDOR SESUITE APLICACIÓN DE PRODUCCION VERSION 2 2017
33	BOG1DMP-WVD-0	172.17.0.16	ESCRITORIOS VIRTUALES
34	BOG1DMP-WVD-1	172.17.0.8	ESCRITORIOS VIRTUALES
35	BOG1DMP-WVD-2	172.17.0.13	ESCRITORIOS VIRTUALES
36	BOG1DMP-WVD-3	172.17.0.6	ESCRITORIOS VIRTUALES
37	BOG1DMP-WVD-4	172.17.0.14	ESCRITORIOS VIRTUALES
38	BOG1DMP-WVD-5	172.17.0.12	ESCRITORIOS VIRTUALES
39	BOG1DMP-WVD-6	172.17.0.11	ESCRITORIOS VIRTUALES
40	BOG1DMP-WVD-7	172.17.0.9	ESCRITORIOS VIRTUALES
41	BOG1DMP-WVD-8	172.17.0.5	ESCRITORIOS VIRTUALES

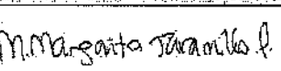
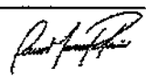
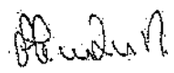
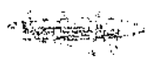
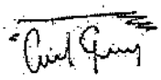
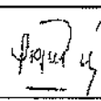
No.	Nombre del Servidor	IP	Descripción
42	BOG1DMP-WVD-9	172.17.0.17	ESCRITORIOS VIRTUALES
43	BOG1DMP-WVD-10	172.17.0.10	ESCRITORIOS VIRTUALES
44	BOG1DMP-WVD-11	172.17.0.7	ESCRITORIOS VIRTUALES
45	BOG1DMP-WVD-12	172.17.0.15	ESCRITORIOS VIRTUALES
46	BOG1DMP-WVD-13	172.17.0.18	ESCRITORIOS VIRTUALES
47	BOG1DMP-WVD-14	172.17.0.4	ESCRITORIOS VIRTUALES
48	ControladorDeDominioAzureInvima	172.17.0.52-52.247.8.221	ESCRITORIOS VIRTUALES

Cada seis (6) meses se realizará una reunión para analizar y verificar la situación de la información resguardada y se tomarán las decisiones sobre mantenerla o eliminarla de acuerdo a la realidad del Instituto en ese momento. Sobre esta revisión periódica se dejarán actas para el respectivo seguimiento.

COMPROMISOS ADQUIRIDOS:

Compromiso	Responsable *(Nombre –Cargo)*	Fecha de Ejecución
Realizar copias de seguridad a los servidores	Grupo de Soporte Tecnológico	25 de marzo del 2022
Formateo y reinstalación de los servidores	Grupo de Soporte Tecnológico	22 de marzo del 2022

SUSCRIBEN EL ACTA

Nombre completo	Firma
María Margarita Jaramillo Pineda	
Juan Manuel Palacio Posada	
Eliodoro Rojas Ochoa	
Nidia Nayibe González Pinzón	
Camilo Andrés Guzmán Camacho	
Miguel Fernando Diaz Peña	
Visto Bueno Asesor Dirección General	*OK DG*

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: COMITÉ TÉCNICO DE SEGUIMIENTO CONTINGENCIA

Lugar: Auditorio Invima	**Acta No 1250-07-2022**
Fecha: 2022-03-16	
Hora de inicio: 9:00 am	**Hora de finalización: 1:00 pm**

ASISTENTES

Nombre Completo	Cargo
Juan Manuel Palacio Posada	Jefe de Oficina de Tecnología (OTI) / INVIMA
Miguel Fernando Díaz Peña	Coordinador del Grupo de Gestión de la Información / OTI /INVIMA
Camilo Andrés Guzmán Camacho	Coordinador del Grupo de Informática / OTI/ INVIMA
Eliodoro Rojas Ochoa	Coordinador del Grupo de Soporte Tecnológico/ Secretaría General (SG)/INVIMA
Cristhian Hernando Pinzón Camacho	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Freddy Holman Pulido Granados	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Jhorbis Ramses Rios Chaves	Contratista OTI/INVIMA
Nidia Nayibe González	Oficial de Seguridad de la Información / Oficina Asesora de Planeación/ INVIMA
Leidy Diana García Arevalo	Contratista OTI/INVIMA

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones
N/A	N/A	N/A

ORDEN DEL DÍA

1. Actividades realizadas para la contención del incidente tecnológico
2. Necesidades de la entidad para restablecer los servicios.

DESARROLLO ORDEN DEL DÍA

Siendo las 9:00 am en el auditorio del Invima, se reúnen los grupos de la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico de la Secretaria General, así como la Oficial de Seguridad de la Información de la Oficina Asesora de Planeación y demás personas que suscriben como intervinientes la presenta acta.

El objetivo de la reunión tiene el fin de evaluar y concluir con las alternativas para que el Jefe de la Oficina de Tecnologías de la Información y la Dirección General avancen en la intervención de las medidas idóneas para conjurar la crisis en la que se encuentran los sistemas de información e infraestructura tecnológica de la Entidad debido al incidente acontecido del pasado domingo 6 de febrero de 2022.

1. Como antecedente se contextualiza, dando lectura al anexo 1. Estado situacional.
2. En el uso de la palabra el Jefe de Tecnologías de la Información, procede a realizar un análisis de avance por cada sistema de información de conformidad al estado anteriormente indicado y en relación con las gestiones que con el recurso técnico y humano desde el Invima se han desarrollado

N.	NOMBRE SOFTWARE SISTEMA DE INFORMACIÓN	TIPO DE PLATAFORMA	LENGUAJE DE PROGRAMACIÓN	SE TIENE EL CODIGO FUENTE?	% AVANCE DE RESTAURACIÓN	RECURSO HUMANO DE LA ENTIDAD
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	ON PREMISE[1]	POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	ON PREMISE	POWER BUILDER	SI	0%	-
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-CIS	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
5	SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE	ON PREMISE	PHP – JAVA	SAAS	0%	-
6	SOLUCIÓN WEB ADMIN	ON PREMISE	JAVA	SI	0%	
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
10	SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM)	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
11	SOLUCIÓN WEB ACIDOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
12	SOLUCIÓN WEB FARMACOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
13	SOLUCIÓN WEB TRANSPARENCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
14	SOLUCIÓN WEB REGISTRO – RECAUDOS	ON PREMISE	Delphi JAVA	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
15	SOLUCIÓN WEB IVCISOA	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
16	SOLUCIÓN WEB REACTIVOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
17	SOLUCIÓN WEB TECNOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico

[1] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

18	SOLUCIÓN WEB – IVC SOA PUERTOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
19	SOLUCIÓN WEB PROTOCOLOS DE INVESTIGACIÓN	ON PREMISE	JAVA JEE7	SI	0%	Grupo de Informática Grupo de Soporte Tecnológico
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
21	SISTEMA DE INFORMACIÓN CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA	ON PREMISE	Java JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB	ON PREMISE	C#, TSQL, HTML5, CSS, TypeScript	NO	0%	-
23	PORTAL WEB INSTITUCIONAL	ON PREMISE	CMS LifeRay – Java	SI	50%	Grupo de Informática Grupo de Soporte Tecnológico
24	SOLUCIÓN WEB KAWAK	NUBE	N/A	NO	100%	Servicio SaaS externo
25	SOLUCIÓN WEB ITSM ARANDA	NUBE	N/A	NO	100%	Servicio SaaS externo
26	HERRAMIENTA ANTIVIRUS KASPERSKY	ON PREMISE	N/A	NO	100%	Servicio Externo
27	SOLUCIÓN WEB OFICINA VIRTUAL	ON PREMISE	MySQL y PHP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
28	DIRECTORIO ACTIVO		N/A	NO	90%	Grupo de Soporte Tecnológico
29	CORREO ELECTRÓNICO	HIBRIDO	N/A	NO	70%	Grupo de Soporte Tecnológico
30	SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-
31	SISTEMA DE INFORMACIÓN WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL – SIVICOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-

3. Destaca el Jefe de Oficina de la Información que las actividades hasta aquí desglosadas están acompañadas de forma paralela con las actuaciones administrativas y jurídicas (de índole judicial) se vienen desarrollando con el apoyo de la Oficina Asesora Jurídica, la Oficial de Seguridad de la Información y la Coordinación del Grupo de Soporte Tecnológico:
   - Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites.
   - Circular 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso – Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

4. Adicionalmente se presenta como punto coyuntural que para efectos de poder continuar las labores de limpieza, formateo y vuelta a la operación de los servidores afectados, se debe tener en cuenta lo consignado en el Acta de Formateo de Servidores del Invima que se realizó el día inmediatamente anterior y que establece el que se puede realizar el formateo de los servidores afectados.

En consonancia, el comité técnico estudia las actividades que deben ser realizadas por terceros de la siguiente manera:

1. **Aseguramiento de la Infraestructura Tecnológica:** La entidad requiere el aseguramiento de la infraestructura para lograr la identificación y mitigación de brechas, minimizando riesgos de incidentes tecnológicos que puedan presentarse en la entidad.

   En este sentido, se encuentra que las actividades de aseguramiento requeridas por la entidad son las siguientes:

   - Hacking Ético: Este servicio va orientado a la identificación y explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.
   - Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.

2. **Restablecimiento de Servicios y Sistemas:**

   - **Sistema de Información para laboratorios SILAB (SAMPLER):** este es el sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), y que permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad. Este sistema y toda su información se encuentra encriptada y se requiere de la instalación, configuración, parametrización, pruebas y salida a producción de este por parte del proveedor exclusivo del sistema y dueño del código fuente la empresa Caudales y Muestreos SAS.
   - **Sistema de Información Gestor Documental Sesuite – Correspondencia y PQRDS:** Este sistema de información contiene los módulos del Gestor Documental de la Entidad y de PQRDS y correspondencia. Es un sistema transversal en el cual reposa la información de los tramites solicitados en la entidad y que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima.
   - **Software Comisión Revisora:** El software de comisión revisora es un software que se integra técnicamente con el software de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de la Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista. Este software fue desarrollado y entregado al Invima por parte de Innpulsa mediante convenio de cooperación 180 de 2021.

3. **Buzones de correo electrónico:** Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. Teniendo en cuenta el incidente

presentado en la entidad, se encuentra comprometida la disponibilidad de recursos como los correos electrónicos configurados On-Premise afectando su funcionamiento, por lo tanto, se requiere que se creen nuevos correos electrónicos para su uso en los aplicativos de la entidad. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.

4. **Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos:** Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados, los servicios tecnológicos de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no hay capacidad de almacenamiento para subir y poner operativos todos los servicios. Por lo anterior se deben adquirir discos de estado sólido y mecánico para el restablecimiento de los servicios.

5. **Aumento (temporal) del ancho de banda para cargue de información y Debido** al incidente se propone por parte del comité técnico cargar en el espacio que brinda Microsoft Sharepoint la información que se encuentra en los servidores comprometidos para poder formatearlos y usarlos para el despliegue de sistemas y servicios en los mismos.

6. **Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión:** Así mismo se requiere del apoyo por parte del contratista ERT en el alistamiento de los computadores y servicios de impresión de la Entidad, en observancia que para cumplir con los cronogramas establecidos no se cuenta con personal suficiente en la entidad.

7. **Instalación de los proyectos de transformación digital en desarrollo y entregados:**

   - **Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo):** El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que una vez desarrollado permitirá ejecutar en línea las actividades misionales de los procesos "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los procedimientos que habían sido entregados por parte del contratista en las fases de desarrollo y codificación del proyecto como se observa en el siguiente cuadro:

PROCEDIMIENTO	% DE EJECUCIÓN DEL PROCEDIMIENTO	% DE EJECUCIÓN FRENTE A PROYECTO
aic-ast- pr001- procedimiento información y atención al ciudadano	100%	33,78%
Ass- ayc- pr001- procedimiento auditorias y certificaciones	100%	
Ass-rsa- pr001- procedimiento registro sanitario nuevo o renovación con estudio previo"	100%	

	Ass-rsa- pr002- procedimiento de expedición de registros sanitarios, permisos sanitarios, notificaciones sanitarias sin estudio previo y control / revisión posterior	100%		
	Ass-rsa- pr003- procedimiento asignación de código de notificaciones sanitarias obligatorias, reconocimientos, renovaciones con firma digital y cambios asociados.	100%		
	Ass-rsa- pr011- procedimiento cancelación de registro sanitario y pérdida de ejecutoriedad	100%		
	Ass-rsa- gu029- guía para la elaboración de certificación de vo.bo. De exclusión de IVA con registro sanitario	100%		
	Ass-rsa-pr005-procedimiento modificación de registros sanitarios	100%		
	Ass-rsa-pr006-procedimiento certificación	100%		
	Ass-rsa-pr007-procedimiento autorización	100%		
	Ass-rsa-pr008-procedimiento visto bueno de importación	100%		
	Ass-rsa-pr010-procedimiento revisión de oficio	100%		
	Ass-rsa- pr013- procedimiento evaluación técnica científica	100%		
	Ass-rsa- pr014- procedimiento de evaluación y seguimiento a protocolos de investigación	100%		
	Ass-rsa- pr015- procedimiento para la aprobación previa de publicidad	100%		
	Ass-rsa- pr016- procedimiento de autorizaciones relacionadas con material es, objetos, envases y equipamientos destinad os a entrar en contacto con alimentos y bebidas para consumo humano	100%		
	Ass-rsa- pr019- procedimiento de autorización, cesión o modificación de uso exclusivo en alimentación y salud humana de organismos vivos modifica dos	100%		
	Ass-rsa- pr021- procedimiento autorización, renovación, modificación y/o cancelación de licencia de fabricación de derivado s de cannabis para uso medicinal y científico	100%		
	Ivc-vig- in043- instructivo para la inscripción de recurso humano que presta servicios de mantenimiento a equipos biomédicos	100%		

Ivc-ins- pr004- procedimiento de inspección para importación y exportación de alimentos, materias primas o ingrediente secundario para la industria de alimentos en sitios de control de primera barrera, zonas francas y depósitos	100%	

- **Sistema de Información SIVICOS III (En desarrollo):** El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista en la fase de Sistematización y Automatización de conformidad con el siguiente cuadro:

MÓDULOS ENTREGADOS SIVICOS	PORCENTAJE HITO
Integración Tramites en línea, Gestión de traza (Reconocimiento de requerimientos, modelado, diseño y simulación, Desarrollo e implementación, Realización de pruebas, Entrega de manual de usuario y técnico, Transferencia de conocimiento, Despliegue en ambiente de pruebas y producción)	11,42%
Módulo para programación, gestión de visitas y otras actividades de IVC	12,81%
Terminar e Integrar Certificado de inspección sanitaria 2 (CIS2), Actas paramétricas, Sincronizador IVC Actas paramétricas, e-Certificates Países Bajos y Traces, Farmacovigilancia	16,49%
Módulo de la Dirección de Operaciones Sanitarias	36,38%
Módulo de la Dirección de Responsabilidad Sanitaria	1,28%
Módulo de la Dirección de Medicamentos y Productos Biológicos	20,24%
Módulo Administrativo y de Gestión del Sistema de Información – Sección para Gestión de Usuarios, Claves, Roles y Permisos de Aplicación, Sección para Diseño y Creación Paramétrica de Reportes, Sección para Gestión de Parámetros de Fuentes IVC SOA e IVC SOA Puertos, Sección para Gestión y Parametrización de la Automatización	10,25%

Conclusiones:

En atención a los análisis realizados, al avance estimado, y a las actividades por desarrollar se concluye en la mesa las siguientes recomendaciones:

1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.
2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos y la Nueva Plataforma de Trámites y Servicios, así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[2]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.
8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.

[2] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

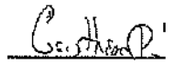
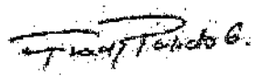
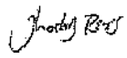
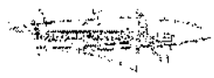
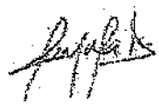
10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

COMPROMISOS ADQUIRIDOS:

Compromiso	Responsable *(Nombre - Cargo)*	Fecha de Ejecución
Asociar estas medidas al Plan de contingencia.	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Reunirse con las diferentes dependencias de la Entidad para la socialización de estas medidas (Grupo de Gestión Contractual, Secretaria General, Oficina Asesora Planeación, Dirección General)	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Solicitar cotizaciones a los proveedores identificados	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022

SUSCRIBEN EL ACTA

Nombre completo	Firma
Juan Manuel Palacio Posada	
Miguel Fernando Díaz Peña	
Camilo Andrés Guzmán Camacho	
Eliodoro Rojas Ochoa	

Cristhian Hernando Pinzón Camacho	
Freddy Holman Pulido Granados	
Jhorbis Ramses Rios Chavez	
Nidia Nayibe González Pinzón	
Leidy Diana García Arevalo	

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

EL SECRETARIO GENERAL DEL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS –INVIMA-

En ejercicio de las facultades legales, la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015, el Decreto 2078 de 2012, la Resolución de Delegación de Funciones No. 2012030802 del 19 de octubre de 2012, la Resolución No. 2020006742 del 25 de febrero de 2020, acta de posesión No. 040 del 25 de febrero de 2020 y,

CONSIDERANDO QUE:

La Constitución Política de Colombia en su artículo 2, contempla:

> "ARTICULO 2º—Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares. (Subrayado fuera del texto).

Por medio del artículo 245 de la Ley 100 de 1993 se crea el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA como establecimiento público del orden nacional, adscrito al Ministerio de Salud y Protección Social, con personería jurídica, patrimonio independiente y autonomía administrativa, cuyo objeto es la ejecución de las políticas en materia de vigilancia sanitaria y de control de calidad de medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva.

Para tal fin el Decreto 2078 de octubre de 2012 *"Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos -Invima y se determinan las funciones de sus dependencias"*, en el numeral 1 de su artículo 4, establece las funciones de la entidad entre las cuales se encuentra la siguiente:

> *Ejercer las funciones de inspección, vigilancia y control a los establecimientos productores y comercializadores de los productos a que hace referencia el artículo 245 de la Ley 100 de 1993 y en las demás normas que lo modifiquen o adicionen, sin perjuicio de las que en estas materias deban adelantar las entidades territoriales, durante las actividades asociadas con su producción, importación, exportación y disposición para consumo.*

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En tal sentido, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima como organismo encargado de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar a través del talento humano (contemplando funcionarios y contratistas) que conforman y hacen parte del apoyo de las direcciones, oficinas, coordinaciones y demás grupos internos de trabajo de su estructura orgánica, las actividades necesarias para la efectiva prestación del servicio público que se brinda por la institución.

Así mismo, para realizar las labores misionales y administrativas, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que soporta los múltiples sistemas de información, bases de datos y aplicativos necesarios para la correcta ejecución de sus oficios, administrada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades desarrolladas por la entidad se ejecuten, a través de los distintos aplicativos[1]; situación que se venía cumpliendo efectivamente en las diferentes sedes de la entidad de forma presencial y virtual, garantizando la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso.

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[2] que comprometió la disponibilidad de los sistemas de información, bases de datos, plataformas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad, restringiendo su acceso, afectando la operación de varios de los servidores y estaciones de trabajo cliente, así como los aplicativos y sistemas de información dispuestos para la operación del Instituto, de conformidad al estado situacional[5].

Dicho incidente ocasionó un problema de continuidad del negocio, afectando la ejecución de las actividades diarias del Instituto, toda vez que el mismo es considerado como "*incidente de seguridad de la información*"[6].

En este orden, la entidad implementó medidas, que van desde la contención del incidente hasta la activación de un plan de contingencia, cuyo eje fundamental fue la reactivación de los servicios tecnológicos desde los que se despliega la misionalidad del Instituto, de conformidad a los aplicativos aludidos en el anexo 1- Relación de softwares de este acto administrativo. Estos servicios se

[1] Ver Anexo 1: Relación de softwares.
[2] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion.
[3] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com
[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos
[5] Ver anexo 2: Estado situacional.
[6] Debe precisarse que respecto del incidente, y conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no se evidencian indicios de fuga de la información sin embargo, la entidad se atiene al resultado del análisis forense que fue solicitado a la Superintendencia de Industria y Comercio - SIC, y a lo definido en la investigación penal que adelanta la Fiscalía General de la Nación con apoyo de la Policía Nacional – Dirección de Investigación Criminal e Interpol.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

restauraron de forma paulatina con la gestión de las actividades tecnológicas y jurídicas correspondientes, que a su vez desplegó la entidad, como lo son: la actualización e implementación del plan de acción y medidas de contingencia frente a los posibles efectos o consecuencias del incidente cibernético, la emisión de las medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, emitiendo los siguientes actos administrativos:

- Resolución 2022500000 del 9 de febrero de 2022; la Resolución 2022500001 del 15 de febrero de 2022; 2022500002 del 22 de febrero de 2022; 2022500003 del 25 de febrero de 2022; 2022500005 del 8 de marzo de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites, y la Resolución No. 2022500009 del 16 de marzo de 2022, por medio de la cual se adoptaron decisiones y se actualizaron las medidas administrativas transitorias necesarias para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto.

- Circular 1000-001-22 del 18 de febrero de 2022, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

- Circular 1000-002-22 del 25 de febrero de 2022, a través de la cual se otorga la ampliación de empresas beneficiadas por formato de contingencia para autorización de traslado de alimentos, materias primas, otros alimentos perecederos, desde el sitio de ingreso a otro sitio que cumplan con las condiciones sanitarias para su almacenamiento.

De forma paralela la entidad con las actividades anteriormente descritas, interpuso ante la Fiscalía General de la Nación denuncia penal Expediente CAD N° 110016000050202201569 por el presunto delito de acceso abusivo a un sistema informático, tipificado en el artículo 269 A de la Ley 1263 de 2009, actuación de la que se desprendieron las consecuentes investigaciones, iniciando con las practicas del recaudo del material probatorio y/o evidencia física sobre los servidores y equipos diagnosticados con la transmisión o inoculación del virus ransomware. En consecuencia, la policía judicial realizó las actividades forenses correspondientes, extrayendo las que conformarían el caudal probatorio que soporta la denuncia en cita, actividad que fue desplegada hasta el 15 de marzo de 2022, fecha en la que se emite el acta que autoriza proceder con el uso para formateo de los servidores afectados, en relación con el acta de formateo de servidores del Instituto[7].

El 16 de marzo de 2022, se llevó a cabo Comité Técnico de Seguimiento[8], integrado por los funcionarios y contratistas del Grupo de Soporte Tecnológico como de la Oficina de Tecnologías de la Información del Invima y la Oficial de Seguridad de la Información, quienes recomendaron:

1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción

[7] Ver anexo 3: Acta formateo servidores del Invima.
[8] Ver anexo 4: Comité Técnico de Seguimiento Contingencia.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativos: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.

2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos[9] y la Nueva Plataforma de Trámites y Servicios[10], así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[11]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el

[9] Sivicos es la denominación utilizada para referirse al proyecto que comprende el desarrollo de una solución que consiste en un software que permite la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima.

[10] El proyecto de nueva plataforma es el relacionado con el desarrollo de una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para la ejecución en línea, de las actividades misionales de los procesos: "Registros sanitarios y tramites asociados" y "Auditorías y certificaciones" del instituto.

[11] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.

8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.
10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

Bajo este contexto, y respecto a la importancia del cumplimiento de las labores de la entidad, teniendo en cuenta que la misionalidad del Instituto se basa en proteger y promover la salud de los colombianos, es claro que las actividades que desarrolla no se pueden paralizar; por lo cual se hace necesario activar la causal de contratación directa a través de urgencia manifiesta, de conformidad al plan de acción, en relación con las actividades anteriormente descritas establecidas en el Comité precitado y acogidas por la Entidad como medida conducente en el proceso de mitigación.

Así las cosas y, con el propósito de garantizar la disponibilidad y el acceso total a la información y las comunicaciones del Instituto Nacional de Vigilancia de Medicamentos y Alimentos- Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte, se hace necesaria la contratación de bienes y servicios para conjurar, mitigar los efectos y con ello restablecer

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información de la Entidad..

Corolario, se requiere gestionar los trámites contractuales de forma inmediata, toda vez que no se cuenta con el plazo indispensable para adelantar el procedimiento ordinario de escogencia de contratistas[12], siendo viable acudir al mecanismo idóneo para adelantar las contrataciones, con atención a las situaciones anteriormente expuestas, garantizando una respuesta contigua de la administración.

De igual manera, debe tenerse en cuenta la prohibición establecida en el marco de Ley de garantías, contemplada en el artículo 33 de la Ley 996 de 2005, el cual dispone:

> **Artículo 33. Restricciones a la contratación pública.** Durante los cuatro (4) meses anteriores a la elección presidencial y hasta la realización de la elección en la segunda vuelta, si fuere el caso, queda prohibida la contratación directa por parte de todos los entes del Estado.
>
> Queda exceptuado lo referente a la defensa y seguridad del Estado, los contratos de crédito público, los requeridos para cubrir las emergencias educativas, sanitarias y desastres, así como también los utilizados para la reconstrucción de vías, puentes, carreteras, infraestructura energética y de comunicaciones, en caso de que hayan sido objeto de atentados, acciones terroristas, desastres naturales o casos de fuerza mayor, y los que deban realizar las entidades sanitarias y hospitalarias. Adicionalmente se exceptúan aquellos gastos inaplazables e imprescindibles que afecten el normal funcionamiento de la administración[13].

En atención a la situación expuesta, se encuentra configurada la circunstancia de fuerza mayor contemplada en el artículo 42 de la Ley 80 de 1993[14], el cual refiere la condición de la urgencia manifiesta a partir de situaciones necesarias para conjurar contextos excepcionales relacionadas con la fuerza mayor, para este caso, en concordancia con la excepción dispuesta en el artículo 33 de la citada Ley 996 de 2005.

En tal sentido, la Ley 1150 de 2007 (Literal a, numeral 4 del artículo 2. De las modalidades de selección) refiere:

---

[12] Licitación pública, selección abreviada, concurso de mérito, contratación mínima cuantía.

[13] Texto subrayado declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia C-1153 de 2005; el resto del artículo fue declarado EXEQUIBLE, condicionado a que se entienda que para el Presidente o el Vicepresidente de la República se aplique desde que manifiestan el interés previsto en el artículo 9º.

[14] ARTÍCULO 42. DE LA URGENCIA MANIFIESTA. <Aparte tachado derogado por el artículo 32 de la Ley 1150 de 2007> Existe urgencia manifiesta cuando la continuidad del servicio exige el suministro de bienes, o la prestación de servicios, o la ejecución de obras en el inmediato futuro; cuando se presenten situaciones relacionadas con los estados de excepción; cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, en general, cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o ~~concurso~~ públicos (...).

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

> **4. Contratación directa.** La modalidad de selección de contratación directa solamente procederá en los siguientes casos:
>
> (...)
>
> a) Urgencia manifiesta;

Es preciso indicar que se acude a la excepción contemplada en el citado artículo, en atención a la situación de fuerza mayor descrita en la parte inicial del presente documento, en este orden y conforme a lo indicado en múltiples ocasiones por el Consejo de Estado[15], se entiende que la fuerza mayor debe ser:

> **1) Exterior:** esto es que está dotado de una fuerza destructora abstracta, cuya realización no es determinada, ni aún indirectamente por la actividad del ofensor.
> **2) Irresistible:** esto es que ocurrido el hecho el ofensor se encuentra en tal situación que no puede actuar sino del modo que lo ha hecho.
> **3) imprevisible:** cuando el suceso escapa a las previsiones normales, esto es, que ante la conducta prudente adoptada por quien lo alega, era imposible pronosticarlo o predecirlo.

En línea de lo anterior manifiesta la misma corporación frente a lo dicho por la Corte Suprema de Justicia a este respecto (Sentencia de 15 de junio de 2000, Exp. 12.423):

> (...) La fuerza mayor sólo se demuestra mediante la prueba de un hecho externo concreto (causa extraña). Lo que debe ser imprevisible e irresistible no es el fenómeno como tal, sino sus consecuencias (...) En síntesis, para poder argumentar la fuerza mayor, el efecto del fenómeno no sólo debe ser irresistible sino también imprevisible, sin que importe la previsibilidad o imprevisibilidad de su causa. Además de imprevisible e irresistible debe ser exterior del agente, es decir, no serle imputable desde ningún ámbito.

Teniendo en cuenta la normatividad citada, es claro que no se trata de evadir los procedimientos legales ordinarios para este tipo de procesos sino de simplificarlos, en atención a las circunstancias excepcionales por las que atraviesa la Entidad, dado que no da espera a los tiempos de las modalidades típicas que se aplicarían ordinariamente para resolver este tipo de procesos, toda vez que los tiempos de gestión que implica realizar el procedimiento de selección correspondiente sería superior a 72 días[16].

Sobre el particular, la Corte Constitucional[17] indicó que:

---

[15] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, expediente 13.833, sentencia de 26 de febrero de 2004, C. P. Germán Rodríguez Villamizar.

[16] Circular No. 109 del 1 de octubre de 2020, emitida por el Secretario General del Instituto Nacional de Vigilancia de medicamentos y Alimentos- Invima.
[17] Corte Constitucional, Sentencia C-772 de 1998, 10 de diciembre de 1998. Magistrado Ponente: Fabio Morón Díaz.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

> *"La "urgencia manifiesta" es una situación que puede decretar directamente por cualquier autoridad administrativa sin autorización previa, a través de acto debidamente motivado. Que ella existe o se configura cuando se acredite la existencia de uno de los siguientes presupuestos: - Cuando la continuidad del servicio exija el suministro de bienes, o la prestación de servicios o la ejecución de obras en el inmediato futuro. - Cuando se presenten situaciones relacionadas con los estados de excepción. - Cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, - en general cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o concursos públicos".*

El Consejo de Estado[18], mediante pronunciamiento del 27 de abril de 2006, manifestó:

> *"Se observa entonces cómo la normatividad que regula el tema de la urgencia en la contratación estatal, se refiere a aquellos eventos en los cuales pueden suscitarse hechos que reclamen una actuación inmediata de la Administración, con el fin de remediar o evitar males presentes o futuros pero inminentes, provocados bien sea en virtud de los estados de excepción, o por la paralización de los servicios públicos, o provenientes de situaciones de calamidad o hechos constitutivos de fuerza mayor o desastres, o cualquier otra circunstancia similar que tampoco dé espera en su solución, de tal manera que resulte inconveniente el trámite del proceso licitatorio de selección de contratistas reglado en el estatuto contractual, por cuanto implica el agotamiento de una serie de etapas que se toman su tiempo y hacen más o menos largo el lapso para adjudicar el respectivo contrato, circunstancia que, frente a una situación de urgencia obviamente resulta entorpecedora, porque la solución en estas condiciones, puede llegar tardíamente, cuando ya se haya producido o agravado el daño. En estas estipulaciones, se hace evidente el principio de la prevalencia del interés general, en este caso, por encima de las formalidades de las actuaciones administrativas, puesto que si aquel se halla afectado o en peligro de serlo, el régimen jurídico debe ceder y permitir que las soluciones se den en la mayor brevedad posible, así ello implique la celebración de contratos sin el cumplimiento de los requisitos legales de selección del contratista y aún, la ejecución de los mismos, sin que medie la formalidad del contrato escrito, si la gravedad de las circunstancias así lo exige".*

En virtud de la obligación del Instituto de garantizar el derecho a la salud a través de la salvaguarda de la seguridad sanitaria del país, se requiere mantener la continua prestación del servicio de la entidad y, en atención a la imposibilidad, por razones de tiempo, de seleccionar a los contratistas mediante los procesos ordinarios de selección dispuestos por la Ley 80 de 1993 y demás normas reglamentarias, se requiere declarar la Urgencia Manifiesta, en aras de dar cumplimiento a la Constitución y la Ley, teniendo en cuenta los recursos asignados para tal fin.

[18] Consejo de Estado, Sentencia del 27 de abril de 2006, Expediente número 14275. Consejero Ponente: Ramiro Becerra Saavedra.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 0121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En razón a las causas y finalidades mencionadas y, de conformidad con los componentes técnicos en los que se justifica la necesidad de contratación suscrita por el Grupo de Soporte Tecnológico, la Oficina de Tecnologías de la Información y la Oficina Asesora de Planeación – Oficial de Seguridad de la Información; en este orden, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA MANIFIESTA son los siguientes[19]:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la	• Hacking Ético: Interno de caja blanca para 160 IP[20]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[19] En desarrollo de lo dispuesto en el Plan de Acción Incidente de Seguridad de la Información.
[20] IP: Internet Protocol – Protocolo de comunicaciones de Internet

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓI DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 0021
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		2. Condiciones técnicas del servicio de soporte técnico: **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.	• Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz. **Fase de estabilización** • Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información. **Fase cuatro: Actividad de Salida a producción** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. **Operación en producción** Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores. **Tecnológicos para ambiente de producción** REQUERIMIENTOS / CARACTERISTICAS **Servidor de Aplicaciones** Memoria: 128 Gygas Procesador: 32 cores Disco Duro: 800 Gygas — Dos Discos (1) 300 y (1) 500 Gygas Sistema Operativo: Windows Server 2019 Datacenter **Servidor de Base de datos** Memoria: 64 Gygas Procesador: 24 cores Disco Duro: 1 Tera Engine: SQL Server 2017 Enterprise Edition Bases de Datos: SeSuiteProducción y Utilitario **Servidor de configuración y paso** Memoria: 64 Gygas Procesador: 8 cores Disco Duro: 400 Gygas — Dos Discos: (1) de 150 Gygas (1) de 350 Gygas Sistema Operativo: Windows Server 2019 Datacenter **File server** Sistema de archivos: NTFS Capacidad: 20 Teras

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TECNICA</th><th>CONDICIONES TECNICAS</th></tr>
<tr><td></td><td></td><td>
Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.
Características Especiales
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo
Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log
Respaldo de los archivos nuevos cargados al File Server diario.
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta

Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta.</td></tr>
</table>
</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft®ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.</td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 3121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS			
	contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima. En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad. Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin.				• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas. • Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection • Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans
		2	KF5-00002EAEA SAP	Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP	• Protección de próxima generación que incluye protección antimalware y antivirus robusta. • Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
	Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativos: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnoiógico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACION TECNICA	CONDICIONES TECNICAS
	entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor de Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2171
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramient encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Instalación del Ambiente de Producción: Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TECNICAS
	Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
		Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

Las necesidades anteriormente expuestas respecto a los bienes y servicios, conciernen únicamente a los requerimientos que, de acuerdo con su complejidad y especialidad, deben ser atendidos por proveedores expertos e idóneos, de conformidad con la plataforma, arquitectura, lenguaje de programación, ambiente de pruebas (QA) y producción, así como su calidad de proveedor exclusivo o canal autorizado del fabricante.

La duración de la Urgencia Manifiesta será por un término aproximado de seis (6) meses, plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

En desarrollo del proceso de contratación directa, la entidad debe garantizar los principios que rigen la contratación estatal, consagrados en los artículos 24, 25 y 26 de la Ley 80 de 1993, referentes a los principios de transparencia, economía y responsabilidad[21].

En mérito de lo expuesto, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA,

RESUELVE:

ARTÍCULO PRIMERO: Declarar la URGENCIA MANIFIESTA en el **INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA**, para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, y con ello, restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte.

PARÁGRAFO PRIMERO: La duración de la Urgencia Manifiesta será por un término aproximado de seis (6) meses, plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

ARTÍCULO SEGUNDO: Establecer como modalidad a aplicar para la contratación que aquí se trata, la contratación directa conforme a la causal prevista en el artículo 42 de la ley 80 de 1993 de conformidad con lo señalado en el literal a) numeral 4 artículo 2° de la Ley 1150 de 2007, y el artículo 2.2.1.2.1.4.2. Del Decreto 1082 de 2015. Y, en consecuencia, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA, son los siguientes:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de	• Hacking Ético: interno de caja blanca para 160 IP[22]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration

[21] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera. Radicado interno 37.044. marzo 7 de 2011. Magistrado Ponente: Doctor Enrique Gil Botero.
[22] IP: Internet Protocol – Protocolo de comunicaciones de Internet

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
	brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del	**3. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
	Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACION DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **4. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto.	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.	• Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de Insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos. • Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz. **Fase de estabilización** • Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información. **Fase cuatro: Actividad de Salida a producción** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. **Operación en producción** Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores. **Tecnológicos para ambiente de producción** REQUERIMIENTOS | CARACTERISTICAS **Servidor de Aplicaciones** Memoria | 128 Gygas Procesador | 32 cores

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2171
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS		
		Disco Duro	800 Gygas	Dos Discos (1) 300 y (1) 500 Gygas
		Sistema Operativo	Windows Server 2019 Datacenter	
		Servidor de Base de datos		
		Memoria	64 Gygas	
		Procesador	24 cores	
		Disco Duro	1 Tera	
		Engine	SQL Server 2017 Enterprise Edition	
		Bases de Datos	SeSuiteProducción y Utilitario	
		Servidor de configuración y paso		
		Memoria	64 Gygas	
		Procesador	8 cores	
		Disco Duro	400 Gygas	Dos Discos: (1) de 150 Gygas (1) de 350 Gygas
		Sistema Operativo	Windows Server 2019 Datacenter	
		File server		
		Sistema de archivos	NTFS	
		Capacidad	20 Teras	
		Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.		
		Características Especiales		
		Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		
		Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log		
		Respaldo de los archivos nuevos cargados al File Server diario.		
		Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura		
		Configuración de una estrategia de seguridad robusta		

Tecnológicos para ambiente de pruebas

REQUERIMIENTOS	CARACTERISTICAS	
Servidor de Aplicaciones		
Memoria	64 Gygas	
Procesador	8 cores	
Disco Duro	400 Gygas	Dos Discos de 150 y 250 Gygas
Sistema Operativo	Windows Server 2019 Datacenter	
Servidor de Base de datos		
Memoria	16 Gygas	
Procesador	8 cores	
Disco Duro	500 Gygas	
Engine	SQL Server 2017 Enterprise Edition	
Bases de Datos	SeSuiteproduccion y Utilitario	
Características Especiales		
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60X) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>Backup de las bases de datos 1 Diario completo y cada 3 horas
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta.</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft@ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-</td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACION TECNICA</th><th colspan="4">CONDICIONES TECNICAS</th></tr>
<tr><td></td><td>buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad.

Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad.

Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin.

Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y</td><td></td><td></td><td></td><td>365/exchange/compare-microsoft-exchange-online-plans</td></tr>
<tr><td></td><td></td><td></td><td>2</td><td>KF5-00002EAEA SAP</td><td>Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP</td><td>• Protección de próxima generación que incluye protección antimalware y antivirus robusta.
• Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas
• Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales.
• Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager
• Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android
• Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de los servidores que se encuentran en el Datacenter de la entidad.	
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TÉCNICAS
	Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorías y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60X) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 Nº 64 - 28 - Bogotá
Administrativo: Cra 10 Nº 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre si y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades:

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(601) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS
		de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

ARTÍCULO TERCERO: Ordenar al Grupo de Gestión Contractual y Grupo Financiero y Presupuestal adelantar los trámites precontractuales pertinentes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO CUARTO: Ordenar al Grupo Financiero y Presupuestal que se realicen los traslados presupuestales correspondientes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO QUINTO: Desígnese un comité de seguimiento y acompañamiento respecto de la ejecución de las actividades enunciadas en el artículo segundo del presente acto administrativo a la Oficina de Tecnologías de la Información y al Grupo de Soporte Tecnológico, desde el rol administrativo, jurídico y financiero a:

- La Oficina Asesora de Planeación, representada por el Jefe de Oficina y el Oficial de Seguridad.
- El Grupo Financiero y Presupuestal, representado por el Asesor de la Dirección delegado para el Grupo Financiero y Presupuestal.
- La Oficina Asesora Jurídica, representada por el Jefe de Oficina.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

- Asesor de la Dirección General Delegado para tal fin.

ARTÍCULO SEXTO: Disponer que, por el Grupo de Gestión Contractual, se conformen y organicen los expedientes respectivos, con copia de este acto administrativo, de los contratos originados en la presente urgencia manifiesta, y demás estudios y documentos precontractuales de orden técnico y administrativo, con el fin de que sean remitidos a la Contraloría General de la República, para el ejercicio del control fiscal pertinente, de conformidad con el artículo 43 de la Ley 80 de 1993.

ARTÍCULO SÉPTIMO: La presente resolución rige a partir de la fecha de su publicación.

Dada en Bogotá D.C., el 23 de marzo de 2022.

PUBLÍQUESE Y CÚMPLASE

ROY GALINDO WEHDEKING
Secretario General

Proyectó: María José Amaya López - Abogada contratista Grupo de Gestión Contractual.
María Laura Olivella Dangond – Abogada contratista Grupo de Gestión Contractual.
Leidy Diana García Arevalo – Contratista Oficina de Tecnologías de la Información.

Aprobó: María Margarita Cárdenas – Asesora de la Dirección General con delegación de funciones del Grupo de Gestión Contractual.
María Margarita Jaramillo P- Jefe de la Oficina Asesora Jurídica.
Juan Manuel Palacio Posada- Jefe de Oficina de Tecnologías de la Información.
Eliodoro Rojas Ochoa- Coordinador del Grupo de Soporte Tecnológico.
Camilo Guzmán Camacho- Coordinador del Grupo de Informática.
Miguel Díaz Peña- Coordinador del Grupo de Gestión de la Información.
Nidia Nayibe González Pinzón- Oficial de Seguridad de la Información de la Oficina Asesora de Planeación.

Anexo 1: Relación Software
Anexo 2: Estado situacional
Anexo 3: Acta Formateo Servidores
Anexo 4: Acta Comité Seguimiento Técnico
Anexo 5: Plan de Acción
Anexo 6: Anexo Técnico

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(601)(1) 742 2121
www.invima.gov.co

ANEXO 2

ESTADO SITUACIONAL Y DIAGNÓSTICO INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN 06 DE FEBRERO DE 2022

1. INTRODUCCIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos Invima, de conformidad con las funciones asignadas por Ley, es un establecimiento público del orden nacional, de carácter científico y tecnológico, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Salud y Protección Social y perteneciente al Sistema de Salud.[1]

Su objetivo consiste en actuar como institución de referencia nacional en materia sanitaria y ejecutar las políticas formuladas por el Ministerio de Salud y Protección Social en materia de vigilancia sanitaria y de control de calidad de los medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva de conformidad con lo señalado en el artículo 245 de la Ley 100 de 1993 y en las demás normas que la modifiquen, adicionen o sustituyan.

En tal sentido, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima como organismo encargado de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar a través del recurso humano (funcionarios y contratistas) que conforman y hacen parte del apoyo de las direcciones, oficinas, coordinaciones y demás grupos internos de trabajo de su estructura orgánica, las actividades necesarias para la efectiva prestación del servicio público que se brinda por la institución.

Así mismo, para realizar estas labores misionales, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que soporta los múltiples sistemas de información y aplicativos necesarios para la correcta ejecución de sus oficios, administrada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades misionales y administrativas de la entidad se ejecuten, a través de los distintos aplicativos como lo son:

1. SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO.
2. SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA.
3. SOLUCIÓN WEB DE TRÁMITES EN LÍNEA.
4. SISTEMA DE INFORMACIÓN DE CÍVICOS MOVILES -CIS.
5. SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE.

[1] Articulo 1 del Decreto 2078 de 2012 – *"Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), y se determinan las funciones de sus dependencias"*

6. SOLUCIÓN WEB ADMIN.
7. SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA.
8. SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA.
9. SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS.
10. SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM).
11. SOLUCIÓN WEB ACIDOS.
12. SOLUCIÓN WEB FARMACOVIGILANCIA.
13. SOLUCIÓN WEB TRANSPARENCIA.
14. SOLUCIÓN WEB REGISTRO – RECAUDOS.
15. SOLUCIÓN WEB IVC/SOA.
16. SOLUCIÓN WEB REACTIVOVIGILANCIA.
17. SOLUCIÓN WEB TECNOVIGILANCIA.
18. SOLUCIÓN WEB - IVC SOA PUERTOS.
19. SOLUCION WEB PROTOCOLOS DE INVESTIGACIÓN.
20. SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS.
21. SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA.
22. SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB.
23. PORTAL WEB INSTITUCIONAL.
24. SOLUCIÓN WEB KAWAK.
25. SOLUCION WEB ITSM ARANDA.
26. HERRAMIENTA ANTIVIRUS KASPERSKY.
27. SOLUCION WEB OFICINA VIRTUAL.
28. DIRECTORIO ACTIVO.
29. CORREO ELECTRONICO.
30. SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO).
31. SISTEMA DE INFORMACION WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL - SIVICOS (PROYECTO EN DESARROLLO).

De dichos aplicativos se venía haciendo uso de forma efectiva desde las diferentes sedes de la entidad de manera presencial y virtual, conforme a la capacidad diagnosticada y operativamente válida para garantizar la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso. Sin embargo, el 6 de febrero de 2022 el Coordinador (E) del Grupo de Soporte Tecnológico informa a su equipo de trabajo de la caída de la página web de la entidad, generando la indisponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas que soportan las actividades operacionales y administrativas de la Entidad.

En tal sentido, es procedente realizar en desarrollo de las políticas, lineamientos y estándares adoptados por la Entidad el siguiente diagnostico que consta de los puntos que a continuación se tratan, para efectos de tomar las decisiones y acciones procedentes para mitigar los posibles eventos adversos generados como consecuencia de la indisponibilidad.

2. ANTECEDENTES

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[2] que comprometió la disponibilidad de la información del Invima, este se dio por el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

En consecuencia, se procedió a dar paso al Procedimiento Gestión de Incidentes Tecnológicos:

- **Identificar los posibles eventos de seguridad de la información:** El Coordinador (E) del Grupo de Soporte Tecnológico estuvo monitoreando el fin de semana del 5 de febrero de 2022 el funcionamiento de la página web del Instituto, el domingo 6 de febrero de 2022 a las 7:30 de la mañana detectó que la página dejo de funcionar, comunicándose de forma inmediata con el ingeniero Cristian Pinzón para que se realizara la revisión de la infraestructura correspondiente (servidores), indicándose que existía una anomalía, por lo que el funcionario Pinzón se comunica con el ingeniero Jhorbis Ríos, quienes de manera mancomunada proceden a revisar la infraestructura.

  El reporte telefónico indica que se encontró un cambio de contraseña en el administrador, y se percató por parte del Ingeniero Ríos que existían discos encriptados, se observa que uno de los principales servidores Directorio Activo se encontraba encriptado e infectado; de conformidad a lo sucedido y en atención a la experiencia se presumió de forma inmediata que la indisponibilidad obedecía a un ataque.

- **Reportar el evento:** Se procede a informar al oficial de seguridad de la información, al jefe de la Oficina de Tecnologías de la Información y al Coordinador titular del cargo. Quienes tomaron la decisión de comunicarse con el contratista de la entidad Empresa de Recursos Tecnológicos - ERT para que procediera a desconectar los canales de comunicación, de igual forma como medidas de seguridad se comienzan a apagar los servidores de forma gradual y a la elaboración del inventario de los servidores impactados, también se realizó al apagado de suiches de distribución.

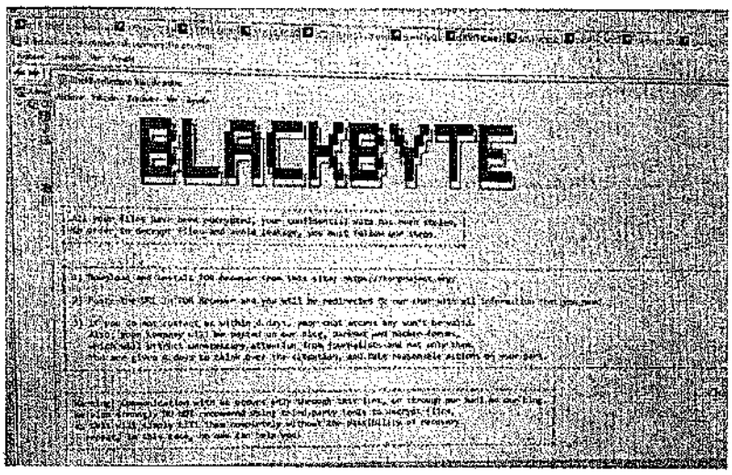
  Según el archivo .txt se observa que es un Ransoware Blackbyte

---

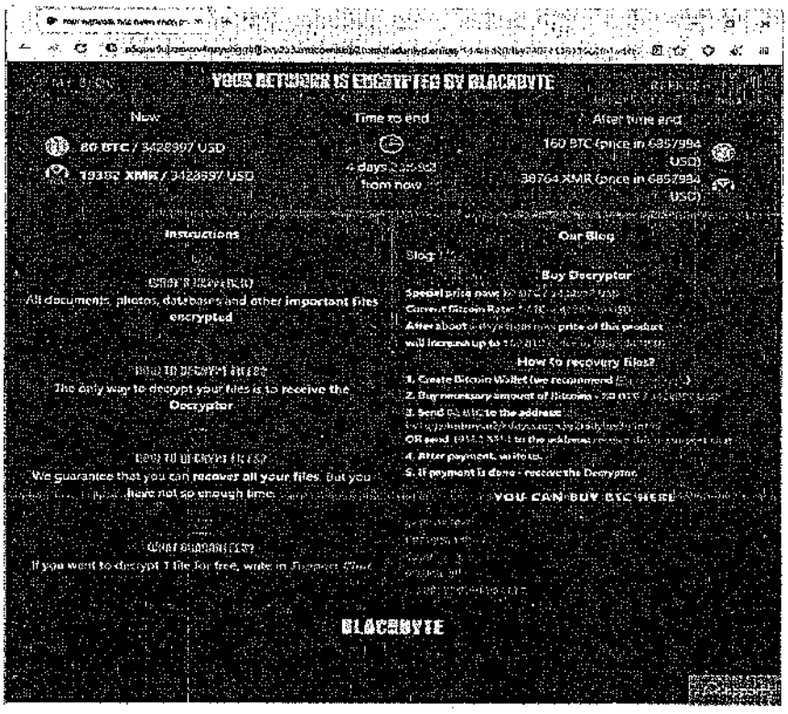
[2] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion

[3] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com

[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos



Finalizado el cifrado del equipo se identificó una nota de rescate que indica:



El incidente se reportó vía telefónica y vía WhatsApp al Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL el día 6 de febrero de 2022 a las 10:07, de conformidad al Instructivo de Relaciones con Autoridades y Grupos de Interés, con el propósito de solicitar apoyo en el manejo de dicha situación.

- **Realizar evaluación preliminar del evento:** Se dispuso la elaboración de la evaluación de los equipos, de la cual se obtuvo el siguiente resultado:

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\AD_DNS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\AD_DNS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\APP	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\APP	1-Sin Acceso	Microsoft Windows Server 2012 Datacenter	Si
INVIMA\APP_BIO_STAR	0-Comprometida	Microsoft® Windows Server® 2008 Standard	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2019 STANDARD	Si
INVIMA\EXCHANGE	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64Bit	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si

Ron	Estado Hoy	OS	Administrada (Si / No)
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\FS_ISS_P_SERVER	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64BIT	Si
INVIMA\FS_ISS_P_SERVER	0-Comprometida	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\IIS	2-Aislada / apagada	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\IIS- ARANDA	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\IIS_RDS_POWER_BI	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Datacenter	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\NPS_RADIUS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Micresoft Windows 7 Professional	Si
INVIMA\OTROS	2-Aislada / apagada	WINDOWS SERVER 2012 R2 STANDARD	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2008 R2 ENTERPRISE - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	Windows Server 2012 R2 estandar	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SFB	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\SQL	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER-SQL	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2008 R2 Enterprise	No
		Microsoft Windows Server 2016 Standard	No
		Microsoft Windows Server 2016 Datacenter	No
		Microsoft Windows Server 2016 Standard	No

- **Evaluar el evento:** De conformidad al procedimiento la oficial de seguridad de la información, junto con la persona que reporta y el equipo de la mesa de ayuda, establecieron que el incidente presentado sobre los sistemas de información y comunicaciones del Instituto se trata de:

Malwares	Ransomware
Disponibilidad:	Sabotaje
Compromiso de Información:	Acceso no autorizado a información
Fraude:	Uso ilegítimo de credenciales
Política de Seguridad:	Acceso a servicios no autorizados
Clasificación de peligrosidad	10 / 10

- **Características más predominantes de BlackByte:**
  - Tiene funcionalidad de gusano en donde realiza consulta de otros posibles equipos objetivo, al conocer el alcance de infección, procede a propagarse a través de la red.

- Paquete Wake-on-LAN en donde se puede controlar de manera remota los equipos afectados al encenderlos cuando están apagados, hibernando o suspendidos. (Ver Anexo: Alerta de Seguridad Ransonware BlackByte).

- **¿Se considera un incidente de Seguridad de la Información?:** Si. (Ver Anexo: Formato de Reporte de Incidentes – CSIRT Gobierno Invima V1).

- **Contener el incidente**: Una vez se presentó el suceso el Invima tomó las siguientes acciones como medida de contención frente a la propagación del programa dañino identificado en los sistemas de información, plataformas tecnológicas y herramientas tecnológicas:

  - Se apagaron de forma gradual los servidores de la entidad, para limitar la expansión del código malicioso en la red que pudiera impactar la información del instituto (servidores de datos compartidos).
  - Se identificó que los computadores de los usuarios estaban afectados, por lo que se desconectó físicamente toda la red.
  - Se desconectaron las interfaces de red y se desactivó toda la red (incluido wifi) para evitar la expansión del virus y afectación de otros servidores.
  - Se procedió a la revisión de los logs y al monitoreo de la herramienta de control de software y antivirus, para efectos de comprobar la finalización de la ejecución del proceso dañino, identificando que los atacantes lograron ganar acceso completo a la infraestructura tecnológica sobre la 1:00 a.m. del 6 de febrero de 2022, con el cambio de la contraseña maestra del Directorio Activo.
  - Se identificó que respecto de las copias de seguridad de la entidad (backup) toda la data e información del Invima se encuentra protegida y no fue objeto de sustracción por parte de los atacantes.
  - Se realizó un levantamiento de información con el propósito de determinar qué información se encontraba encriptada.
  - Como metodología de trabajo se realizó el análisis del comportamiento de este tipo de ataque que se actúa como un virus, respecto de las herramientas de seguridad con la que cuenta la entidad (antivirus, firewall y fireeye). En tal sentido, se estableció como necesidad y dada la clasificación de peligrosidad comportada por este tipo de virus se debe estructurar una estrategia de contención que va desde parchar los servidores, obtener una auditoria forense para delimitar los principales puntos débiles que deben tenerse en cuenta en la evaluación de riesgos por ciberataques atendiendo criterios de razonabilidad, así como mantener actualizadas para posibles nuevas amenazas cibernéticas respecto de los ransomware.
  - Finalmente se instauró denuncia penal bajo el código de noticia criminal No. 110016000050202201569 de fecha 18 de febrero de 2022, por el presunto delito de accedo abusivo a un sistema informático (Artículo 269ª Ley 1273 de 2009).

- **Evaluar el incidente de seguridad:** Al confirmarse que el evento corresponde a un incidente de seguridad de la información se procedió a evaluarlo de acuerdo con el instructivo Gestión de incidentes Tecnológicos lo que conlleva a identificar:

1. Se valida el tipo de incidente, especificando el impacto potencial, la cantidad de usuarios afectados.
2. Se evidencia la indisponibilidad de los servicios tecnológicos del instituto que se encuentran dentro del catálogo de servicios y de los servidores de la entidad

Se procede a categorizar el incidente de seguridad de la información teniendo cuenta la siguiente tabla:

Niveles de prioridad de los incidentes

Prioridad	Descripción
Prioridad 1 (Alta)	Causa una completa pérdida del servicio, sin importar el ambiente en el que se está trabajando (producción, pruebas, desarrollo, etc.). La operación no puede continuar de una manera razonable y no puede ser restablecida inmediatamente.
Prioridad 2 (Media)	Causa una pérdida mínima del servicio. El problema o defecto tiene un impacto menor o no produce inconvenientes. Comprende características importantes inoperables, pero con una solución alterna o características no tan importantes inoperables sin solución alterna.
Prioridad 3 (Baja)	No causa pérdida del servicio. El resultado del problema es un error menor, comportamiento incorrecto o error en la documentación que, de ninguna manera, impide la operación del sistema.

Adicionalmente se identifica una falla masiva es decir en más de 10 usuarios en los siguientes aspectos:

1. Interrupción del servicio en alguna de las aplicaciones o sistemas de información de Invima.
2. Falla al ingresar o realizar alguna operación en aplicativos o sistemas de información del Invima.
3. Falla en alguna de las operaciones o en la generación de reportes
4. Falla es reportada en uno o varios elementos de configuración.
5. Falla de telecomunicaciones o conexión de red o wifi
6. Reducción de la calidad del servicio masiva, no planificada del servicio, determinando si fue producida por la implementación de un cambio.
7. Falla de uno o más servicios que se encuentran activos en el catálogo de servicios

Lo anterior nos lleva a valorar el incidente con un nivel de **Prioridad Alto** y una **Criticidad Alta**, por lo que se procede a aplicar lo establecido en el documento TIC-GTI-IN008 - INSTRUCTIVO GESTIÓN DE PROBLEMAS DE LOS SERVICIOS DE TI (TIC-GTI-IN008).

- **Definir estrategia de atención del incidente:** La estrategia de atención se encuentra registrada en el documento Plan de Acción Riesgo Incidente de Seguridad de la Información

- **Erradicar fallas:** En proceso de análisis
- **Recuperar activos de información:**

  Conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no ha existido fuga de información, sin embargo, la entidad se atiene a lo dispuesto en el análisis forense realizado por la SIC, entidad competente para determinar la perdida de la información.

- **Registrar lecciones aprendidas:** En proceso de análisis
- **Cerrar el incidente:** En proceso

ANEXO 1

INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA

RELACION DE SOFTWARE, SISTEMAS DE INFORMACIÓN Y/O HERRAMIENTAS TECNOLOGICAS INVIMA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

NÚMERO	NOMBRE SOFTWARE, SISTEMA DE INFORMACIÓN, APLICATIVOS TECNOLÓGICOS, PLATAFORMAS TECNOLÓGICAS, HERRAMIENTAS TECNOLÓGICAS Y/O APLICACIONES	DESCRIPCION	ARQUITECTURA	TIPO DE PLATAFORMA	ES MISIONAL?	PROCESO DUEÑO DE LAS DATOS	LENGUAJE DE PROGRAMACIÓN
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	El sistema de información "Registros Sanitarios", se encarga de apoyar las actividades relacionadas con el proceso de expedición de registros sanitarios y trámites asociados de los productos competencia del INVIMA.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	El sistema de información "COMISIÓN REVISORA", se utiliza para relacionar los radicados enviados a la comisión revisora, permite generar un documento que se adiciona al expediente, para informarle a la comisión. Además, permite generar un consolidado con los datos específicos del producto de las actas de la comisión.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	Este sistema web de "TRAMITES EN LÍNEA", permite hacer uso de los siguientes módulos: Consulta estado trámite, Certificado de Venta Libre, Cambio de Clave, Actualizar Datos, Pago Electrónico de Tarifas, Solicitud Certificado de Inspección Sanitaria en Puertos – Alimentos, Solicitud Certificado de Inspección Sanitaria en Puertos - Bebidas Alcohólicas, Adjuntar documentos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-GIS	El sistema de información "SIVICOS", permite realizar la inspección in situ de las inspecciones/exportaciones en puertos, aeropuertos y pasos fronterizos. Así mismo, genera reportes de eventos y reacciones adversas y la consulta de reportes enviados al INVIMA. Inspección PAPF: Solución informática implementada para ser utilizada con tableta en Windows, Android, utilizada como herramienta por los inspectores al momento de realizar la inspección sanitaria de alimentos, materias primas, insumos y bebidas alcohólicas, expide el certificado.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
5	SISTEMA DE INFORMACIÓN CORRESPONDENCIA Y PQRDS - SISQUITE	El sistema de información "CORRESPONDENCIA", permite gestionar y realizar el control de correspondencia interna y externa del INVIMA.	ON PREMISE	ON PREMISE	SI	Transversal a todos los procesos	PHP - JAVA
6	SOLUCIÓN WEB ADMIN	Este sistema web "ADMIN", es interno y permite su gestión diariamente, y genera los reportes diarios y mensuales sobre los siguientes módulos: Certificaciones por Entregar, Notificación por Aviso, Autos por Estado, Registros Cancelados, Registros Negados, Registros o Renovaciones por periodo, Resoluciones Pendientes por Notificar.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTERA	Este sistema web "CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTO", permite consultar los certificados inspección sanitaria en puerto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA	Este sistema web "DOCUMENTOS DE APOSTILLE CANCILLERIA", permite validar los documentos apostillados.	WEB	ON PREMISE	SI	Aseguramiento Sanitario	JAVA - POWER BUILDER
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS	Este sistema web "CONSULTA DE DOCUMENTOS EMITIDOS", permite consultar los documentos con firma digital.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA - POWER BUILDER
10	SOLUCIÓN WEB CODIGO ÚNICO DE MEDICAMENTOS (CUM).	El Servicio Web "CODIGO UNICO DE MEDICAMENTOS (CUM)", le proporciona al Ministerio de Salud la información de los Códigos Únicos de Medicamentos.	SERVICIO WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA - POWER BUILDER
11	SOLUCIÓN WEB ACIDOS.	Este sistema web "ACIDOS", (Decreto 1003/2014) Sistema de información que soporte el registro de control para la comercialización de ácidos, álcalis o sustancias similares o asimilares, quien intervenga en el proceso de comercialización de cualquier sustancia sujeta al registro de control, reportará la información que permita la trazabilidad sobre su procedencia, así como la individualización de cada uno de los actores que intervinieron en la operación de comercialización.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
12	SOLUCIÓN WEB FARMACOVIGILANCIA	Este sistema web "FARMACOVIGILANCIA", permite que usuarios externos reporten información de eventos adversos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
13	SOLUCIÓN WEB TRANSPARENCIA	Este sistema web "TRANSPARENCIA", permite consultar los registros o renovaciones otorgados en una fecha determinada.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
14	SOLUCIÓN WEB REGISTRO - RECAUDOS	Este sistema móvil "Registro - Recaudos", es una solución que permite realizar el cargue manual de los archivos de los pagos recibidos en las ventanillas de Daviviendo a través de la lectura del código de barras.	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	Delphi JAVA
15	SOLUCIÓN WEB IVC/SOA	Este sistema web "IVC/SOA", es una solución Web que permite calcular los índices de severidad, consenso y afectación, desde los grupos de productos por Dirección misional, hasta el consolidado denominado IRA (Índice de Riesgo Asociado), para cada Dirección misional y el Instituto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
16	SOLUCIÓN WEB REACTIVOVIGILANCIA	Este sistema web "REACTIVOVIGILANCIA", permite la notificación, registro y evaluación sistemática de los problemas relacionados con los reactivos de diagnóstico in vitro.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
17	SOLUCIÓN WEB TECNOVIGILANCIA	Este sistema web "TECNOVIGILANCIA", permite el reporte de eventos o incidentes adversos serios e inesperados producidos asociados con los dispositivos médicos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
18	SOLUCIÓN WEB - IVC SOA PUERTOS	Este sistema de IVC SOA Puertos, fue construida como una herramienta para consultar, calcular y/o modificar información relacionada con el Modelo IVC SOA Puertos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
19	SOLUCIÓN WEB PROTOCOLOS DE INVESTIGACIÓN -	Este sistema web "PROTOCOLOS DE INVESTIGACIÓN", herramienta del INVIMA, desde la cual se podrá solicitar el trámite de evaluación inicial de protocolos de investigación con productos en investigación/medicamentos desde la comodidad de su casa u oficina.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	Este sistema web "ESTABLECIMIENTOS", permite el registro de establecimientos nacionales y extranjeros. (conos de establecimientos de alimentos).	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7

21	SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRONICA DEL PROYECTO DE PAISES BAJOS Y COLOMBIA	El proyecto de Paises Bajos y Colombia se divide en dos frentes: 1. La aplicación Sivicos/Visibles: La utilizan los funcionarios en Tablet o Windows para las operaciones que manejan en los puertos. 2. Los microservicios desarrollados en OpenShift: Es la lógica que contiene el desarrollo de los servicios para interactuar con Paises Bajos.	CLIENTE SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	Java JEE7
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS - SILAB	Es una solución tecnológica, para la gestión de la información generada por los laboratorios desde sus procesos analíticos, que permite la gestión integral de las muestras desde el ingreso al laboratorio hasta la generación del informe de resultados, permitiendo la total trazabilidad en custodia, calidad y control de los datos del informe de resultados.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	C#, TSQL, HTML5, CSS, TypeScript
23	PORTAL WEB INSTITUCIONAL	Plataforma que ofrece al ciudadano de forma integrada información del instituto y servicios que este presta de forma virtual o a través del Internet. Principalmente está dirigido para apoyar a resolver las inquietudes y necesidades del ciudadano y los tramites que este requiere.	WEB	ON PREMISE	SI	Servicio Transversal para todos los procesos	CMS LifeRay - Java
24	SOLUCIÓN WEB KAWAK	Plataforma para administrar el Sistema Integrado de Gestión del Instituto	WEB	NUBE	NO	Administración del Sistema de Gestión Integrado	N/A
25	SOLUCIÓN WEB ITSM ARANDA	Aplicativo que agrupa un conjunto de recursos tecnológicos para brindar o prestar servicios con la posibilidad de gestionar y solucionar de manera integral requerimientos relacionados con tecnología y recursos tecnológicos.	WEB	NUBE	NO	Procesos de Apoyo	N/A
26	HERRAMIENTA ANTIVIRUS KASPERSKY	Programa cuyo objetivo es detectar y eliminar virus informáticos, además los bloquea, desinfecta archivos y puede prevenir la infección o daño que los virus puedan ocasionar a la información.	N/A	ON PREMISE	NO	Gestión de Tecnologías de la Información	N/A
27	SOLUCION WEB OFICINA VIRTUAL	Herramienta que permite la interacción del instituto con el ciudadano a través de medios digitales	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	MySQL y PHP
28	DIRECTORIO ACTIVO	Base de datos y conjunto de servicios que conecta a los usuarios de la entidad con los recursos de red que se requieren para realizar su trabajo, esto incluye información crítica sobre el entorno tecnológico instalado los usuarios, los computadores y acceso a la información, así como la definición de permisos.	ON PREMISE Y NUBE		NO	Gestión de Tecnologías de la Información	N/A
29	CORREO ELECTRONICO	Sistema que permite el intercambio de mensajes entre los diferentes usuarios de la entidad y con otros usuarios externos a la misma.	N/A	HIBRIDO	NO	Servicio Transversal para todos los procesos	N/A
30	SISTEMA DE INFORMACION WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo y permitirá ejecutar en línea las actividades misionales de los procesos "Registros Sanitarios Y Tramites Asociados" Y "Auditorias Y Certificaciones" Del Instituto Nacional De Vigilancia De Medicamentos Y Alimentos – Invima. Para este proyecto se encuentra afectada la información de la arquitectura y los ambientes de calidad y producción que ya habían sido implementados en la plataforma OpenShift y la implementación de la tecnología RPA.	WEB	NUBE	SI	Aseguramiento Sanitario	JAVA
31	SISTEMA DE INFORMACION WEB PARA LA INSPECCION, VIGILANCIA Y CONTROL Y SIVICOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo que permitirá la sistematización, automatización, gestión de datos, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de Inspección, Vigilancia y Control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. Para este proyecto se afectó la información de la arquitecaura y los ambientes de calidad donde se habían iniciado pruebas funcionales y el ambiente de producción implementados en la plataforma openshift.	WEB	NUBE	SI	Inspección, Vigilancia y Control	JAVA
32	REQUERIMIENTOS TRANSVERSALES	Requerimientos generales para mantener evidencia del material probatorio y aprovechar la capacidad de almacenamiento: 80 discos de 500 GB Mecánico					

ANEXO 5

PLAN DE ACCIÓN
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN DEL 6 DE FEBRERO DE 2022
Actualización del 25 de Febrero de 2022

1. OBJETIVO

Garantizar la disponibilidad y acceso a la información y las comunicaciones del Instituto Nacional de Vigilancia de Medicamento y Alimentos- Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte.

2. ANÁLISIS DEL RIESGO

A continuación, se presenta el riesgo identificado y gestionado dentro del Sistema de Gestión Integrado del Instituto, en el cual se establece la descripción, causa, efectos y control de este, tal como se observa en la siguiente tabla:

Riesgo	Posibilidad de afectación de la operación de la entidad, por la indisponibilidad del activo de información, debido a las fallas de software y hardware del centro de datos.
Descripción	Imposibilidad de acceso a la información por parte de la entidad cuando se presente una falla en la infraestructura y herramientas tecnológicas del centro de datos (hardware y software).
Causas	Incidente a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio (origen: Externo, factor: Tecnológico
Efectos	• Pérdida de información. • Demoras en los procesos y/u operación • Atención parcial o nula al ciudadano • Pérdida de imagen Institucional • Insatisfacción de los usuarios internos del Invima • Daños irreversibles en equipos y herramientas tecnológicas • Disminución o pérdida de productividad
Control	Monitoreo y mantenimiento de herramientas para control incidentes informáticos
Descripción del control	Se cuenta con un antivirus y herramientas de control de software dañino que son monitoreados periódicamente por los administradores del centro de datos de acuerdo al procedimiento de administración del centro de datos TIC-GTI-PR004, como soporte se cuentan con logs y reportes de eventos de este monitoreo.

Respecto a lo anterior, se relacionan los posibles efectos o consecuencias de la materialización del riesgo antes mencionado, con sus respectivas acciones y medidas de contingencia frente al incidente cibernético para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima.

3. PLAN DE ACCIÓN Y MEDIDAS DE CONTINGENCIA FRENTE A LOS POSIBLES EFECTOS O CONSECUENCIAS DEL INCIDENTE CIBERNÉTICO

Posibles efectos	Acciones y medidas de contingencia
Pérdida de información	A la fecha no se evidencia pérdida de la información, ya que se implementó uno de los controles establecidos frente a este riesgo que consistió en "Disponer de copias de seguridad (backps) para restablecer la plataforma y disponibilidad de la información, así como la aplicación del procedimiento interno "TIC-GSI-PR003- PROCEDIMIENTO GENERACIÓN DE COPIAS DE RESPALDO DE A INFORMACIÓN DE LOS SERVIDORES DEL CENTRO DE COMPUTO" lo que ha permitido la continuidad de la operatividad y la prestación servicios de la entidad.
Demoras en los procesos y/o operación	• Emitir medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto. A la fecha se han emitido las siguientes: ▪ Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites. ▪ Circular - 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.
Atención parcial o nula al ciudadano	• Activar la gestión manual de los trámites sin suspensión de términos (posteriormente estos se incluirán en las bases de datos correspondientes). • Activar la opción de pago de trámites a través de transferencia bancaria. • Activar radicación y atención de PQRDS.
Pérdida de imagen Institucional	• Mantenido la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio. • Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.
Insatisfacción de los usuarios internos del Invima	• Garantizar el uso de equipos de navegación a internet mediante módems y routers a las diferentes dependencias de la entidad, para la continuidad operativa de los funcionarios y contratistas de la entidad.

Posibles efectos	Acciones y medidas de contingencia
	• Restablecer Internet en áreas misionales y críticas de la entidad, puertos (Buenaventura, Cartagena, Barranquilla y Santa Marta) y aeropuerto del dorado.
Daños irreversibles en equipos y herramientas tecnológicas	• A la fecha no se han identificado daños irreversibles en equipos y herramientas tecnológicas
Disminución o pérdida de productividad	• Realizar la priorización del restablecimiento de la plataforma SIVICOS para los trámites de certificados de inspección sanitaria en PAPF. • Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa. • Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones. • Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 • Hacer verificación de los servidores y PC afectados • Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus • Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura • Restaurar copias de seguridad • Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera) • Reactivar el sistema de información de Registros Sanitarios • Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad • Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración. • Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS • Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube • Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad • Restablecer los demás servicios del Instituto

4. RECURSOS

El desarrollo y ejecución de este plan queda sometido a la disponibilidad de recursos humano, tecnológico y presupuestales que deben ser gestionados por el Instituto, entidades aliadas y el gobierno nacional.

El Equipo de Trabajo está conformado por la totalidad de los servidores públicos del Invima.

5. CRONOGRAMA Y RUTA CRITICA

Ítem	Semanas Previas (Febrero)			Semanas (Marzo, Abril y Mayo)										
	1	2	3	1	2	3	4	5	6	7	8	9	10	11
Actividades Administrativas														
Emisión de Resoluciones con medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto	■	■	■											
Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa.	■	■	■											
Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones.	■	■	■											
Mantener la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio.	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.		■	■	■	■	■	■	■	■	■	■	■	■	■
Actividades Operacionales y Técnicas														
Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 (RC)	■	■												
Hacer verificación de los servidores y PC afectados (RC)	■	■	■	■	■	■	■	■						
Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura		■	■	■	■	■	■	■	■	■	■	■	■	■
Restaurar copias de seguridad (RC)			■	■	■	■	■	■	■	■	■	■	■	■
Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera)				■	■									

Item	Semanas Previas (Febrero) 1	2	3	Semanas (Marzo, Abril y Mayo) 1	2	3	4	5	6	7	8	9	10	11
Reactivar el sistema de información de Registros Sanitarios				■	■	■	■	■	■	■	■	■		
Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad			■	■	■	■	■							
Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecanico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración (RC)			■	■	■	■	■	■	■					
Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS				■	■	■	■	■	■	■	■	■	■	■
Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube					■	■	■	■						
Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad				■	■	■	■	■	■	■	■	■	■	■
Restablecer los demás servicios del Instituto								■	■	■	■	■	■	■

Las actividades marcadas con **(RC)** conforman la ruta crítica del plan de acción

ANEXO 6

ANEXO TECNICO

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información que comprometió la disponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware llamado Blackbyte el cual encriptó la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

De conformidad con el Plan de Acción socializado por la entidad para el manejo del incidente, mediante la realización de estos procesos contractuales se da cumplimiento a las siguientes acciones:

- Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad.
- Ampliación de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración.
- Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad.

Es por ello que se deben realizar las siguientes actividades desde la Oficina de Tecnologías de la Información – OTI y el Grupo de Soporte Tecnológico así:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.	• Hacking Ético: interno de caja blanca para 160 IP[1]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[1] IP: Internet Protocol – Protocolo de comunicaciones de Internet

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), Impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **2. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** **Soporte de nivel 1 (N1)** Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la Infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos. • Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz.

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TECNICA</th><th>CONDICIONES TECNICAS</th></tr>
<tr><td></td><td>permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.</td><td>
Fase de estabilización
• Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información.

Fase cuatro: Actividad de Salida a producción
El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado.

Operación en producción
Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores.

Tecnológicos para ambiente de producción
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>128 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>32 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>800 Gygas</td><td>Dos Discos (1) 300 y (1) 500 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>24 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>1 Tera</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteProducción y Utilitario</td><td></td></tr>
<tr><td colspan="3">Servidor de configuración y paso</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos: (1) de 150 Gygas (1) de 350 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td colspan="3">File server</td></tr>
<tr><td>Sistema de archivos</td><td>NTFS</td><td></td></tr>
<tr><td>Capacidad</td><td>20 Teras</td><td></td></tr>
<tr><td colspan="3">Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.</td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log</td></tr>
<tr><td colspan="3">Respaldo de los archivos nuevos cargados al File Server diario.</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta</td></tr>
</table>
Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S</td></tr>
<tr><td>Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td>Configuración de una estrategia de seguridad robusta.</td></tr>
</table>
</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad.

Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEASAP</td><td>Microsoft®ExchangeOnlinePlan2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1,5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans</td></tr>
<tr><td>2</td><td>KF5-00002EAEASAP</td><td>Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP</td><td>• Protección de próxima generación que incluye protección antimalware y antivirus robusta.
• Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o</td></tr>
</table>
</td></tr>
</table>

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TECNICA	CONDICIONES TECNICAS			
	correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima - desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin. Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e Instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en				archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad.	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas.	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorías y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Servicios de conformidad a las condiciones técnicas del proyecto.	desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Despliegue Base de Datos: Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:**

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner ▪ **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: Formateo de Servidores del Invima

Lugar: TEAMS		**Acta No 1250-006-2022**
Fecha: 2022-03-15		
Hora de inicio: 06:00 pm	**Hora de finalización:**	

ASISTENTES

Nombre Completo	Cargo
María Margarita Jaramillo Pineda	**Jefe Oficina Asesora Jurídica**
Juan Manuel Palacio Posada	**Jefe de la Oficina de Tecnologías de la Información**
Eliodoro Rojas Ochoa	**Profesional Especializado - Coordinador Grupo Soporte Tecnológico**
Nidia Nayibe González Pinzón	**Contratista - Oficial de Seguridad de la Información**
Camilo Andrés Guzmán Camacho	**Profesional Especializado – Coordinador Grupo de Informática**
Miguel Fernando Diaz Peña	**Profesional Especializado – Coordinador Grupo Gestión de la Información**

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones

ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC
2. Selección y aprobación de las acciones a seguir con el formateo y reinstalación de los servidores

DESARROLLO ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC

El día 25/02/2022 se realizó la entrega de la información solicitada por la DIJIN, sobre los servidores afectados en el Invima, como parte de las pruebas del proceso penal que se inició ante la Fiscalía General de la Nación con denuncia penal NC_110016000050202201569.

El 28/02/2022 se realizó la entrega de la información solicitada por el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante, "GTIFSD") de la Superintendencia de Industria y Comercio - SIC, para el análisis forense a realizar sobre el incidente de seguridad de la información presentado en el Instituto.

El miércoles 2 de marzo de 2022 a través de correo electrónico el intendente Alejandro González Franco Suboficial Centro Cibernético Policial, en coordinación con el Mayor Félix Daniel Miranda Herrera responsable del despliegue del PMU Ciber Electoral, informa a la oficial de seguridad de la información del Invima que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el centro cibernético policial ya inició el análisis y las actividades investigativas y forenses, por lo que no

van a requerir formación. Por lo anterior se puede disponer de los servidores. Se adjunta imagen del correo electrónico recibido:

RV: Informando requerimiento

Policía Nacional Dios y Patria

Buenas tardes, respetuosamente me permito informar a la señora NIDIA NAYIBE GONZÁLEZ PINZÓN Oficial de Seguridad de la Información de INVIMA, que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el Centro Cibernético Policial ya inicio el análisis y demás actividades investigativas y forenses, por lo anterior ya no se requiere de algún otro requerimiento y ni ninguna interrupción por parte de ustedes en la activación de los servicios de INVIMA.

Por otra parte, esta decisión se toma en coordinación con mi Mayor FELIX DANIEL MIRANDA HERRERA, responsable del despliegue del PMU Ciber electoral.

Quedamos atentos a cualquier solicitud y a la información adicional que nos puedan aportar.

Atentamente,

Intendente
ALEJANDRO GONZÁLEZ FRANCO
Suboficial Centro Cibernético Policial
Teléfono: 5159700 Ext. 30428
www.policia.gov.co/dijin

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

Después de recibir la comunicación se determina esperar hasta el 15/03/2022 para dar inicio al proceso de formateo y reinstalación de los servidores, para dar espacio a cualquier requerimiento adicional por parte de la Superintendencia de Industria y Comercio - SIC.

2. Acciones para seguir con el formateo y reinstalación de los servidores

Luego de realizar un análisis de la información que puede ser vital para determinar hallazgos o recuperar información importante para la gestión de la seguridad y operatividad técnica, se decide seleccionar el servidor AZURE, para los correspondientes a los aplicativos SESUITE y BI, almacenándola de forma segura.

El proceso de formateo se realizará de forma ordenada informando a cada responsable de la información contenida en los servidores que estos se formatearán y reconfigurarán para su uso posterior en el marco de la recuperación de los servicios que presta el Invima. A continuación, se presenta una lista de los servidores físicos y virtuales que se formatearán:

No.	Nombre del Servidor	IP	Descripción
1	SRVVCLUSQL01	172.16.10.21	SERVIDOR SKYPE
2	SRVVCOLOMBIA	172.16.10.128	SERVIDOR JAGUAR
3	SRVVCONOF365	172.16.10.196	CONNECT OFFICE 365
4	SRVVKAS	172.16.10.98	SERVIDOR ANTIVIRUS KASPERSKY Y WSUS
5	SRVVDHCP01	172.16.10.61	SERVIDOR DHCP
6	SRVVMOSCU	172.16.10.102	SERVIDOR DE BASE DE DATOS ACCESS

No.	Nombre del Servidor	IP	Descripción
7	SRVVMYSQLWEB01	172.16.10.218	SERVIDOR WEB BASE DE DATOS – DESARROLLO
8	SRVVNGINXWEB01	172.16.10.52	SERVIDOR LIFERAY DE PRODUCCION
9	SRVVSAPIENS01	172.16.10.198	HV_SAPIENS
10	SRVVSERTRAMI	172.16.10.148	SERVIDOR TRAMITES EN LINEA
11	SRVVWEBDES03	172.16.10.219	SERVIDOR DESARROLLO PAGINA WEB - APP.INVIMA
12	SRVVWFLY01	172.16.10.80	SERVIDOR MASTER WILDFLY 8
13	SRVVWFLY9FV	172.16.10.65	WILDFLY
14	SRVV3MBX	172.16.10.177	SERVIDOR CORREO EXCHANGE MAILBOX
15	SRVVACCESO	172.16.10.79	SERVIDOR PARA EL CONTROL DE ACCESO
16	SRVVRELAY	172.16.80.15	MAQUINA RELAY CORREO LINUX
17	SRVVSESBDPRU	172.16.10.171	SERVIDOR SESUITE BD QA
18	SRVVSOLARW01	172.16.10.152	SERVIDOR MONITOREO SOLARWINDS
19	SRVVWHD	172.16.10.159	SERVIDOR SOLAR WINDS HELP DESK
20	SRVVSAPIENS01	172.16.10.198	SERVIDOR SQL SERVER
21	SRVVAPPEONPROD	172.16.10.55	APP APPEON Productivo
22	SRVV1CAS	172.16.10.175	SERVIDOR CAS DE CORREO EXCHANGE
23	SRVV3SESPRU	172.16.10.82	SERVIDOR DE PRUEBAS DE SESUITE
24	SRVVPAPERCUT	172.16.40.14	Administrador de Impresión – ERT
25	SRVVNAGIOS	172.16.10.197	Monitoreo Nagios Free
26	SRVVAULA	172.16.10.113	SERVIDOR DE SERVICIOS Y APLICACIONES WEB -AULA VIRTUAL
27	SRVVSESAPPRU	172.16.10.172	SERVIDOR DE APLICACIONES SESUITE DE PRUEBAS
28	SRVVMILANFL	172.16.10.194	SERVIDOR DE ARCHIVOS VIEJO
29	SRVVCOLOMBIA_CLON02	172.16.10.127	SERVIDOR JAGUAR
30	SRVV6SENT	172.16.10.36	MOBILE IRON - security.invima.gov.co
31	SVV5CORE	172.16.10.35	MOBILE IRON - mobile.invima.gov.co - CORE
32	SRVVSESAPPRO	172.16.10.181	SERVIDOR SESUITE APLICACIÓN DE PRODUCCION VERSION 2 2017
33	BOG1DMP-WVD-0	172.17.0.16	ESCRITORIOS VIRTUALES
34	BOG1DMP-WVD-1	172.17.0.8	ESCRITORIOS VIRTUALES
35	BOG1DMP-WVD-2	172.17.0.13	ESCRITORIOS VIRTUALES
36	BOG1DMP-WVD-3	172.17.0.6	ESCRITORIOS VIRTUALES
37	BOG1DMP-WVD-4	172.17.0.14	ESCRITORIOS VIRTUALES
38	BOG1DMP-WVD-5	172.17.0.12	ESCRITORIOS VIRTUALES
39	BOG1DMP-WVD-6	172.17.0.11	ESCRITORIOS VIRTUALES
40	BOG1DMP-WVD-7	172.17.0.9	ESCRITORIOS VIRTUALES
41	BOG1DMP-WVD-8	172.17.0.5	ESCRITORIOS VIRTUALES

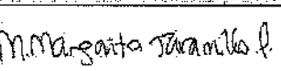
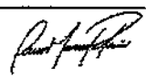
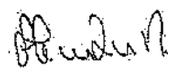
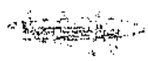
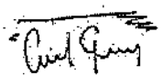
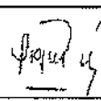
No.	Nombre del Servidor	IP	Descripción
42	BOG1DMP-WVD-9	172.17.0.17	ESCRITORIOS VIRTUALES
43	BOG1DMP-WVD-10	172.17.0.10	ESCRITORIOS VIRTUALES
44	BOG1DMP-WVD-11	172.17.0.7	ESCRITORIOS VIRTUALES
45	BOG1DMP-WVD-12	172.17.0.15	ESCRITORIOS VIRTUALES
46	BOG1DMP-WVD-13	172.17.0.18	ESCRITORIOS VIRTUALES
47	BOG1DMP-WVD-14	172.17.0.4	ESCRITORIOS VIRTUALES
48	ControladorDeDominioAzureInvima	172.17.0.52-52.247.8.221	ESCRITORIOS VIRTUALES

Cada seis (6) meses se realizará una reunión para analizar y verificar la situación de la información resguardada y se tomarán las decisiones sobre mantenerla o eliminarla de acuerdo a la realidad del Instituto en ese momento. Sobre esta revisión periódica se dejarán actas para el respectivo seguimiento.

COMPROMISOS ADQUIRIDOS:

Compromiso	Responsable *(Nombre –Cargo)*	Fecha de Ejecución
Realizar copias de seguridad a los servidores	Grupo de Soporte Tecnológico	25 de marzo del 2022
Formateo y reinstalación de los servidores	Grupo de Soporte Tecnológico	22 de marzo del 2022

SUSCRIBEN EL ACTA

Nombre completo	Firma
María Margarita Jaramillo Pineda	
Juan Manuel Palacio Posada	
Eliodoro Rojas Ochoa	
Nidia Nayibe González Pinzón	
Camilo Andrés Guzmán Camacho	
Miguel Fernando Diaz Peña	
Visto Bueno Asesor Dirección General	*OK DG*

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: COMITÉ TÉCNICO DE SEGUIMIENTO CONTINGENCIA

Lugar: Auditorio Invima	**Acta No 1250-07-2022**
Fecha: 2022-03-16	
Hora de inicio: 9:00 am	**Hora de finalización: 1:00 pm**

ASISTENTES

Nombre Completo	Cargo
Juan Manuel Palacio Posada	Jefe de Oficina de Tecnología (OTI) / INVIMA
Miguel Fernando Díaz Peña	Coordinador del Grupo de Gestión de la Información / OTI /INVIMA
Camilo Andrés Guzmán Camacho	Coordinador del Grupo de Informática / OTI/ INVIMA
Eliodoro Rojas Ochoa	Coordinador del Grupo de Soporte Tecnológico/ Secretaría General (SG)/INVIMA
Cristhian Hernando Pinzón Camacho	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Freddy Holman Pulido Granados	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Jhorbis Ramses Rios Chaves	Contratista OTI/INVIMA
Nidia Nayibe González	Oficial de Seguridad de la Información / Oficina Asesora de Planeación/ INVIMA
Leidy Diana García Arevalo	Contratista OTI/INVIMA

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones
N/A	N/A	N/A

ORDEN DEL DÍA

1. Actividades realizadas para la contención del incidente tecnológico
2. Necesidades de la entidad para restablecer los servicios.

DESARROLLO ORDEN DEL DÍA

Siendo las 9:00 am en el auditorio del Invima, se reúnen los grupos de la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico de la Secretaria General, así como la Oficial de Seguridad de la Información de la Oficina Asesora de Planeación y demás personas que suscriben como intervinientes la presenta acta.

El objetivo de la reunión tiene el fin de evaluar y concluir con las alternativas para que el Jefe de la Oficina de Tecnologías de la Información y la Dirección General avancen en la intervención de las medidas idóneas para conjurar la crisis en la que se encuentran los sistemas de información e infraestructura tecnológica de la Entidad debido al incidente acontecido del pasado domingo 6 de febrero de 2022.

1. Como antecedente se contextualiza, dando lectura al anexo 1. Estado situacional.
2. En el uso de la palabra el Jefe de Tecnologías de la Información, procede a realizar un análisis de avance por cada sistema de información de conformidad al estado anteriormente indicado y en relación con las gestiones que con el recurso técnico y humano desde el Invima se han desarrollado

N.	NOMBRE SOFTWARE SISTEMA DE INFORMACIÓN	TIPO DE PLATAFORMA	LENGUAJE DE PROGRAMACIÓN	SE TIENE EL CODIGO FUENTE?	% AVANCE DE RESTAURACIÓN	RECURSO HUMANO DE LA ENTIDAD
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	ON PREMISE[1]	POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	ON PREMISE	POWER BUILDER	SI	0%	-
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-CIS	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
5	SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE	ON PREMISE	PHP – JAVA	SAAS	0%	-
6	SOLUCIÓN WEB ADMIN	ON PREMISE	JAVA	SI	0%	
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
10	SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM)	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
11	SOLUCIÓN WEB ACIDOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
12	SOLUCIÓN WEB FARMACOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
13	SOLUCIÓN WEB TRANSPARENCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
14	SOLUCIÓN WEB REGISTRO – RECAUDOS	ON PREMISE	Delphi JAVA	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
15	SOLUCIÓN WEB IVCISOA	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
16	SOLUCIÓN WEB REACTIVOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
17	SOLUCIÓN WEB TECNOVIGILANCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico

[1] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

18	SOLUCIÓN WEB – IVC SOA PUERTOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
19	SOLUCIÓN WEB PROTOCOLOS DE INVESTIGACIÓN	ON PREMISE	JAVA JEE7	SI	0%	Grupo de Informática Grupo de Soporte Tecnológico
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
21	SISTEMA DE INFORMACIÓN CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA	ON PREMISE	Java JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB	ON PREMISE	C#, TSQL, HTML5, CSS, TypeScript	NO	0%	-
23	PORTAL WEB INSTITUCIONAL	ON PREMISE	CMS LifeRay – Java	SI	50%	Grupo de Informática Grupo de Soporte Tecnológico
24	SOLUCIÓN WEB KAWAK	NUBE	N/A	NO	100%	Servicio SaaS externo
25	SOLUCIÓN WEB ITSM ARANDA	NUBE	N/A	NO	100%	Servicio SaaS externo
26	HERRAMIENTA ANTIVIRUS KASPERSKY	ON PREMISE	N/A	NO	100%	Servicio Externo
27	SOLUCIÓN WEB OFICINA VIRTUAL	ON PREMISE	MySQL y PHP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
28	DIRECTORIO ACTIVO		N/A	NO	90%	Grupo de Soporte Tecnológico
29	CORREO ELECTRÓNICO	HIBRIDO	N/A	NO	70%	Grupo de Soporte Tecnológico
30	SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-
31	SISTEMA DE INFORMACIÓN WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL – SIVICOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-

3. Destaca el Jefe de Oficina de la Información que las actividades hasta aquí desglosadas están acompañadas de forma paralela con las actuaciones administrativas y jurídicas (de índole judicial) se vienen desarrollando con el apoyo de la Oficina Asesora Jurídica, la Oficial de Seguridad de la Información y la Coordinación del Grupo de Soporte Tecnológico:
   - Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites.
   - Circular 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso – Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

4. Adicionalmente se presenta como punto coyuntural que para efectos de poder continuar las labores de limpieza, formateo y vuelta a la operación de los servidores afectados, se debe tener en cuenta lo consignado en el Acta de Formateo de Servidores del Invima que se realizó el día inmediatamente anterior y que establece el que se puede realizar el formateo de los servidores afectados.

En consonancia, el comité técnico estudia las actividades que deben ser realizadas por terceros de la siguiente manera:

1. **Aseguramiento de la Infraestructura Tecnológica:** La entidad requiere el aseguramiento de la infraestructura para lograr la identificación y mitigación de brechas, minimizando riesgos de incidentes tecnológicos que puedan presentarse en la entidad.

   En este sentido, se encuentra que las actividades de aseguramiento requeridas por la entidad son las siguientes:

   - Hacking Ético: Este servicio va orientado a la identificación y explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.
   - Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.

2. **Restablecimiento de Servicios y Sistemas:**

   - **Sistema de Información para laboratorios SILAB (SAMPLER):** este es el sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), y que permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad. Este sistema y toda su información se encuentra encriptada y se requiere de la instalación, configuración, parametrización, pruebas y salida a producción de este por parte del proveedor exclusivo del sistema y dueño del código fuente la empresa Caudales y Muestreos SAS.
   - **Sistema de Información Gestor Documental Sesuite – Correspondencia y PQRDS:** Este sistema de información contiene los módulos del Gestor Documental de la Entidad y de PQRDS y correspondencia. Es un sistema transversal en el cual reposa la información de los tramites solicitados en la entidad y que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima.
   - **Software Comisión Revisora:** El software de comisión revisora es un software que se integra técnicamente con el software de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de la Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista. Este software fue desarrollado y entregado al Invima por parte de Innpulsa mediante convenio de cooperación 180 de 2021.

3. **Buzones de correo electrónico:** Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. Teniendo en cuenta el incidente

presentado en la entidad, se encuentra comprometida la disponibilidad de recursos como los correos electrónicos configurados On-Premise afectando su funcionamiento, por lo tanto, se requiere que se creen nuevos correos electrónicos para su uso en los aplicativos de la entidad. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.

4. **Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos:** Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados, los servicios tecnológicos de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no hay capacidad de almacenamiento para subir y poner operativos todos los servicios. Por lo anterior se deben adquirir discos de estado sólido y mecánico para el restablecimiento de los servicios.

5. **Aumento (temporal) del ancho de banda para cargue de información y Debido** al incidente se propone por parte del comité técnico cargar en el espacio que brinda Microsoft Sharepoint la información que se encuentra en los servidores comprometidos para poder formatearlos y usarlos para el despliegue de sistemas y servicios en los mismos.

6. **Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión:** Así mismo se requiere del apoyo por parte del contratista ERT en el alistamiento de los computadores y servicios de impresión de la Entidad, en observancia que para cumplir con los cronogramas establecidos no se cuenta con personal suficiente en la entidad.

7. **Instalación de los proyectos de transformación digital en desarrollo y entregados:**

   - **Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo):** El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que una vez desarrollado permitirá ejecutar en línea las actividades misionales de los procesos "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los procedimientos que habían sido entregados por parte del contratista en las fases de desarrollo y codificación del proyecto como se observa en el siguiente cuadro:

PROCEDIMIENTO	% DE EJECUCIÓN DEL PROCEDIMIENTO	% DE EJECUCIÓN FRENTE A PROYECTO
aic-ast- pr001- procedimiento información y atención al ciudadano	100%	33,78%
Ass- ayc- pr001- procedimiento auditorias y certificaciones	100%	
Ass-rsa- pr001- procedimiento registro sanitario nuevo o renovación con estudio previo"	100%	

	Ass-rsa- pr002- procedimiento de expedición de registros sanitarios, permisos sanitarios, notificaciones sanitarias sin estudio previo y control / revisión posterior	100%		
	Ass-rsa- pr003- procedimiento asignación de código de notificaciones sanitarias obligatorias, reconocimientos, renovaciones con firma digital y cambios asociados.	100%		
	Ass-rsa- pr011- procedimiento cancelación de registro sanitario y pérdida de ejecutoriedad	100%		
	Ass-rsa- gu029- guía para la elaboración de certificación de vo.bo. De exclusión de IVA con registro sanitario	100%		
	Ass-rsa-pr005-procedimiento modificación de registros sanitarios	100%		
	Ass-rsa-pr006-procedimiento certificación	100%		
	Ass-rsa-pr007-procedimiento autorización	100%		
	Ass-rsa-pr008-procedimiento visto bueno de importación	100%		
	Ass-rsa-pr010-procedimiento revisión de oficio	100%		
	Ass-rsa- pr013- procedimiento evaluación técnica científica	100%		
	Ass-rsa- pr014- procedimiento de evaluación y seguimiento a protocolos de investigación	100%		
	Ass-rsa- pr015- procedimiento para la aprobación previa de publicidad	100%		
	Ass-rsa- pr016- procedimiento de autorizaciones relacionadas con material es, objetos, envases y equipamientos destinad os a entrar en contacto con alimentos y bebidas para consumo humano	100%		
	Ass-rsa- pr019- procedimiento de autorización, cesión o modificación de uso exclusivo en alimentación y salud humana de organismos vivos modifica dos	100%		
	Ass-rsa- pr021- procedimiento autorización, renovación, modificación y/o cancelación de licencia de fabricación de derivado s de cannabis para uso medicinal y científico	100%		
	Ivc-vig- in043- instructivo para la inscripción de recurso humano que presta servicios de mantenimiento a equipos biomédicos	100%		

Ivc-ins- pr004- procedimiento de inspección para importación y exportación de alimentos, materias primas o ingrediente secundario para la industria de alimentos en sitios de control de primera barrera, zonas francas y depósitos	100%	

- **Sistema de Información SIVICOS III (En desarrollo):** El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista en la fase de Sistematización y Automatización de conformidad con el siguiente cuadro:

MÓDULOS ENTREGADOS SIVICOS	PORCENTAJE HITO
Integración Tramites en línea, Gestión de traza (Reconocimiento de requerimientos, modelado, diseño y simulación, Desarrollo e implementación, Realización de pruebas, Entrega de manual de usuario y técnico, Transferencia de conocimiento, Despliegue en ambiente de pruebas y producción)	11,42%
Módulo para programación, gestión de visitas y otras actividades de IVC	12,81%
Terminar e Integrar Certificado de inspección sanitaria 2 (CIS2), Actas paramétricas, Sincronizador IVC Actas paramétricas, e-Certificates Países Bajos y Traces, Farmacovigilancia	16,49%
Módulo de la Dirección de Operaciones Sanitarias	36,38%
Módulo de la Dirección de Responsabilidad Sanitaria	1,28%
Módulo de la Dirección de Medicamentos y Productos Biológicos	20,24%
Módulo Administrativo y de Gestión del Sistema de Información – Sección para Gestión de Usuarios, Claves, Roles y Permisos de Aplicación, Sección para Diseño y Creación Paramétrica de Reportes, Sección para Gestión de Parámetros de Fuentes IVC SOA e IVC SOA Puertos, Sección para Gestión y Parametrización de la Automatización	10,25%

Conclusiones:

En atención a los análisis realizados, al avance estimado, y a las actividades por desarrollar se concluye en la mesa las siguientes recomendaciones:

1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.
2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos y la Nueva Plataforma de Trámites y Servicios, así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[2]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.
8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.

[2] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

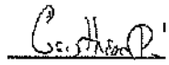
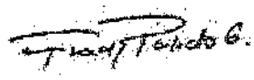
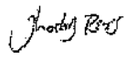
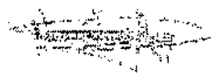
10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

COMPROMISOS ADQUIRIDOS:

Compromiso	Responsable *(Nombre - Cargo)*	Fecha de Ejecución
Asociar estas medidas al Plan de contingencia.	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Reunirse con las diferentes dependencias de la Entidad para la socialización de estas medidas (Grupo de Gestión Contractual, Secretaria General, Oficina Asesora Planeación, Dirección General)	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Solicitar cotizaciones a los proveedores identificados	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022

SUSCRIBEN EL ACTA

Nombre completo	Firma
Juan Manuel Palacio Posada	
Miguel Fernando Díaz Peña	
Camilo Andrés Guzmán Camacho	
Eliodoro Rojas Ochoa	

Cristhian Hernando Pinzón Camacho	
Freddy Holman Pulido Granados	
Jhorbis Ramses Rios Chavez	
Nidia Nayibe González Pinzón	
Leidy Diana García Arevalo	