Anexo 1 Especificaciones Técnicas.

1. INTRODUCCION

El presente documento tiene como finalidad dar a conocer las especificaciones técnicas del proceso contractual con objeto “Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC).ID455”.

La Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES dentro del marco de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI que ha definido el Ministerio de Tecnología de Información y Comunicaciones - MinTIC requiere contratar el centro de operaciones de seguridad en la modalidad monitoreo y operaciones, que incluya el ejercicio de ataques simulados sobre la infraestructura, sistemas de Información y servicios de tecnología en donde se contemple además de la intrusión clásica, el escalado de privilegios en las plataformas, sistemas de información o páginas Web de la Entidad, llegando incluso al alertamiento frente a posible alteración, robo de información o denegación de servicios sobre la Infraestructura de la ADRES.

2. ALCANCE

Se requiere contratar los servicios de centro de operaciones de seguridad en la modalidad de monitoreo y operaciones, que incluye: i) servicios de prevención como el análisis de vulnerabilidades, análisis de vulnerabilidades sobre aplicaciones web, Ethical Hacking, ingeniería social y revisión y análisis del plan de recuperación de desastres, ii) servicios de detección como monitoreo y correlación de eventos de seguridad, monitoreo y supervisión de la actividad de bases de datos iii) servicios de respuesta como gestión de incidentes y gestión de Infraestructura de seguridad.

El Contratista deberá contar con sus propias instalaciones, equipos tecnológicos y enlaces de conectividad para la operación del Centro de Operaciones de Seguridad y para el desarrollo de las pruebas que se realicen a nivel externo de la ADRES. Para el desarrollo de las pruebas a nivel interno, la ADRES facilitará un puesto de trabajo.

2.1. Análisis de vulnerabilidades

2.1.1. Objetivo

Evaluar las debilidades o brechas de seguridad que puedan existir sobre la infraestructura de TI que la ADRES requiera, incluyendo sistemas operativos, equipos de red, equipos de seguridad, servidores web, entre otros, que al ser explotado puede afectar el normal desarrollo de los procesos de la Entidad.

2.1.2. Actividades

Se debe contemplar como mínimo las siguientes actividades las cuales deberán ser coordinadas directamente con la Entidad:

- Identificación de IPs objeto de la auditoría.
- Presentación de plan de escaneo indicando la herramienta o herramientas que serán utilizadas.
- Programación y ejecución del escaneo de vulnerabilidades.
- Elaboración o generación de los informes y plan de mitigación

- Socialización de los resultados del análisis de vulnerabilidades

2.1.3. Características

El análisis de vulnerabilidades **se hará por demanda una vez por año,** bajo un entendido de pruebas de caja gris que comprende:

- **Un análisis de vulnerabilidades interno[1] para las dos 255 IPs discriminadas por ubicaciones de la siguiente manera:**
  1. **Infraestructura de Nube Privada que corresponde al centro de datos principal de la Entidad. *Para un máximo de 128 IPs.***
  2. **Infraestructura On Premise alojada en la sede de la Entidad. *Para un máximo de 72 IPs.***
  3. **Infraestructura de la Nube pública Microsoft Azure. *Para un máximo de 55 IPs.***
- **Previo a la ejecución del análisis de vulnerabilidades, las cantidades de IPs relacionadas en el punto anterior podrán ser redistribuidas entre las ubicaciones para cubrir las necesidades cambiantes de la Entidad**.
- **Las IPs objeto del análisis de vulnerabilidades son fijas (no dinámicas), las cuales corresponde a los tipos de activos como servidores, aplicaciones, equipos de red, equipos de seguridad.**
- **El proveedor debe prestar el servicio mediante el uso de una solución o herramienta de análisis de vulnerabilidades del tipo empresarial, licenciada no OPEN SOURCE. El proveedor debe aportar documento que acredite la condición de uso del software con licenciamiento otorgado a su nombre por el fabricante en modalidad de pago.**
- Las herramientas de análisis de vulnerabilidades deben hacer uso del Sistema de Puntaje para Vulnerabilidades Comunes (CVSS), el cual es un estándar reconocido para la estimación de severidad en vulnerabilidades de seguridad.
- **Para las aplicaciones que lo requieran, se debe realizar auditorías basada en APIs y Socket con mecanismos de autenticación avanzados (JWT, Bearer Token).**
- **En los informes se debe incluir la entrega de reportes relacionados con la metodología OWASP Top 10 con el objetivo de proveer un estado de los riesgos cibernéticos en las capas superiores de las aplicaciones.**
- **Socialización de resultados de manera remota a través de Microsoft Teams. La invitación abierta a los grupos de interés de la Entidad será coordinada con el supervisor del Contrato.**
- La facturación del servicio se hará por unidad de IP

2.1.4. Entregables

Por cada análisis de vulnerabilidades realizado, el proveedor debe entregar los siguientes documentos:

Informe directivo. Presentación en Microsoft Power Point usando la plantilla definida por la ADRES, sin información comercial del proveedor, cuyo contenido contemple de manera general los resultados encontrados en la ejecución de este servicio indicando los aspectos más relevantes a nivel de las vulnerabilidades encontradas.

Informe de vulnerabilidades. Informe con el resultado del análisis de vulnerabilidades realizado a los diferentes objetivos tanto a nivel interno como externo incluyendo como mínimo:

- Descripción general de las pruebas realizadas

[1] Se coordinará entre la ADRES y el proveedor la manera más adecuada para poder realizar el respectivo análisis teniendo en cuenta aspectos logísticos para el acceso a los diferentes escenarios de análisis.

- Descripción y licenciamiento de las soluciones o herramientas utilizadas
- Metodología de ejecución de las pruebas.
- Plan de escaneo de vulnerabilidades
- Programación y duración de las pruebas
- Conclusiones

Matriz general de vulnerabilidades. En esta matriz se consolidará de manera general el resultado del análisis de vulnerabilidades realizado a los diferentes objetivos tanto a nivel interno como externo incluyendo como mínimo:

- Nivel de Riesgo: Crítico, Alto, Medio, Bajo
- Nombre de la vulnerabilidad
- Vulnerabilidad encontrada
- Descripción de la vulnerabilidad
- Activo analizado
- Ubicación del activo: Centro de datos Principal, Sede, Nube
- Sistema operativo del activo cuando aplique
- Puertos abiertos
- Herramienta usada.
- Indicador de prueba interna o externa.
- Las vulnerabilidades agrupadas según su nivel de criticidad alta, media y baja
- Estadísticas de vulnerabilidades por ubicación y nivel de riesgo

Plan de recomendaciones. Este documento debe consignar para cada IP como mínimo con los siguientes datos:

- Nivel de Riesgo: Crítico, Alto, Medio, Bajo
- Nombre de la vulnerabilidad
- Activos afectados
- Recomendaciones para realizar la ejecución de la mitigación
- Tipo de recomendación: Instalación, Configuración, Actualización, entre otros
- Descripción del riesgo
- Impacto de la vulnerabilidad

2.2. Análisis de vulnerabilidades sobre aplicaciones web

2.2.1. Objetivo

Evaluar las debilidades o brechas de seguridad que puedan existir sobre las aplicaciones web internas o externas, basado en vulnerabilidades públicas y análisis de las capas de aplicaciones, que al ser explotado puede afectar el normal desarrollo de los procesos de la Entidad.

2.2.2. Actividades

Se debe contemplar como mínimo las siguientes actividades las cuales deberán ser coordinadas directamente con la Entidad:

- Identificación de dominios objeto de la auditoría.

- Presentación de plan de escaneo de los subdominios
- Programación y ejecución del escaneo de vulnerabilidades.
- Elaboración o generación de los informes y plan de mitigación.
- Socialización de los resultados del análisis de vulnerabilidades

2.2.3. Características

El análisis de vulnerabilidades **se hará por demanda una vez por año**, bajo un entendido de pruebas de caja gris que comprende:

- **Un análisis de vulnerabilidades sobre las URLs de las aplicaciones, para un máximo de 20 subdominios[2] de la ADRES:**

No.	Subdominio / Aplicación	Protocolo	Ambiente	Tipo
1	https://www.adres.gov.co	HTTP	Producción	Consulta
2	https://aplicaciones.adres.gov.co	HTTP	Producción	Transaccional
3	https://servicios.adres.gov.co	HTTP	Producción	Transaccional
4	https://iservicios.adres.gov.co	HTTP	Producción	Transaccional
5	http://test.adres.gov.co	HTTP	Pruebas	Transaccional
6	https://rentasterritoriales.adres.gov.co	HTTP	Producción	Transaccional
7	https://rex.adres.gov.co	HTTP	Producción	Transaccional
8	https://mesadeservicios.adres.gov.co	HTTP	Producción	Transaccional
9	https://orfeo.adres.gov.co	HTTP	Producción	Transaccional
10	https://moodle.adres.gov.co	HTTP	Producción	Transaccional
11	https://mui.adres.gov.co/	HTTP	Producción	Transaccional
12	https://reclamaciones.adres.gov.co/	HTTP	Producción	Transaccional
13	https://iaplicaciones.adres.gov.co/	HTTP	Producción	Transaccional
14	https://canastas.adres.gov.co/Account/Login	HTTP	Producción	Transaccional
15	https://docscrm.adres.gov.co	HTTP	Producción	Repositorio Archivos
16	https://orfeo-des.adres.gov.co/login.php	HTTP	Pruebas	Transaccional
17	https://testsite.adres.gov.co/	HTTP	Pruebas	Transaccional
18	tmft.adres.gov.co	SFTP	Pruebas	Servicio SFTP
19	ftp.adres.gov.co	FTP	Producción	Servicio FTP
20	mft.adres.gov.co	SFTP	Producción	Servicio SFTP

- **Previo a la ejecución del análisis de vulnerabilidades, l**as aplicaciones objeto del escaneo de vulnerabilidades podrán ser reemplazadas por otras aplicaciones para cubrir las necesidades cambiantes de la Entidad.
- El servicio se debe ofrecer mediante el uso de herramientas de análisis de vulnerabilidades avanzado sobre aplicaciones y no sobre infraestructura.

[2] Entiéndase como URLs donde se encuentran aplicaciones Web o accesos vía SFTP o FTP.

- **El proveedor debe prestar el servicio mediante el uso de una solución o herramienta de análisis de vulnerabilidades del tipo empresarial, licenciada no OPEN SOURCE. El proveedor debe aportar documento que acredite la condición de uso del software con licenciamiento otorgado a su nombre por el fabricante en modalidad de pago.**
- Las herramientas de análisis de vulnerabilidades deben hacer uso del Sistema de Puntaje para Vulnerabilidades Comunes (CVSS), el cual es un estándar reconocido para la estimación de severidad en vulnerabilidades de seguridad.
- **Para máximo dos aplicaciones, se debe realizar auditorías basada en APIs y Socket con mecanismos de autenticación avanzados (JWT, Bearer Token).**
- **En los informes se debe incluir la entrega de reportes relacionados con la metodología OWASP Top 10 con el objetivo de proveer un estado de los riesgos cibernéticos en las capas superiores de las aplicaciones.**
- **Socialización de resultados de manera remota a través de Microsoft Teams. La invitación abierta a los grupos de interés de la Entidad será coordinada con el supervisor del Contrato.**
- La facturación del servicio se hará por unidad de aplicación.

2.2.4. Entregables

Por cada análisis de vulnerabilidades realizado, el proveedor debe entregar los siguientes documentos:

Informe directivo. Presentación en Microsoft Power Point usando la plantilla definida por la ADRES, sin información comercial del proveedor, cuyo contenido presentará de manera general los resultados encontrados en la ejecución de este servicio indicando los aspectos más relevantes a nivel de las vulnerabilidades encontradas.

Informe de vulnerabilidades. En este informe se consolidará el resultado del análisis de vulnerabilidades realizado a los diferentes objetivos tanto a nivel interno como externo incluyendo como mínimo:

- Descripción general de las pruebas realizadas
- Descripción y licenciamiento de las soluciones o herramientas utilizadas
- Metodología de ejecución de las pruebas.
- Plan de escaneo de vulnerabilidades
- Programación y duración de las pruebas
- Conclusiones y recomendaciones

Matriz general de vulnerabilidades. En esta matriz se consolidará de manera general el resultado del análisis de vulnerabilidades realizado a los diferentes objetivos tanto a nivel interno como externo incluyendo como mínimo:

- Nivel de Riesgo: Crítico, Alto, Medio, Bajo
- Nombre de la vulnerabilidad
- Vulnerabilidad encontrada
- Descripción de la vulnerabilidad
- Activo analizado
- Ubicación del activo: Centro de datos Principal, Sede, Nube
- Sistema operativo del activo cuando aplique
- Puertos abiertos
- Ruta del servicio cuando aplique

- Herramienta usada.
- Indicador de prueba interna o externa.
- Las vulnerabilidades agrupadas según su nivel de criticidad alta, media y baja
- Estadísticas de vulnerabilidades por ubicación y nivel de riesgo

Plan de recomendaciones. Este documento debe consignar para cada IP como mínimo con los siguientes datos:

- Nivel de Riesgo: Crítico, Alto, Medio, Bajo
- Nombre de la vulnerabilidad
- Activos afectados
- Recomendaciones para realizar la ejecución de la mitigación
- Tipo de recomendación: Instalación, Configuración, Actualización, entre otros
- Descripción del riesgo
- Impacto de la vulnerabilidad

2.3. Ethical Hacking

2.3.1. Objetivo

Buscar la explotación de manera controlada de una o varias vulnerabilidades encontradas en el análisis de vulnerabilidades sobre la infraestructura y aplicaciones.

2.3.2. Actividades

En estos ejercicios deben ser incluidos como mínimo las siguientes actividades.

a. Identificación de IPs, aplicaciones y vulnerabilidades y/o debilidades evidenciadas en las auditorías técnicas de análisis de vulnerabilidades sobre la infraestructura y análisis de vulnerabilidades sobre aplicaciones web
b. Presentación de plan de ataque para autorización por parte de la Entidad.
c. Programación y ejecución de ataque.
d. Elaboración de informes
e. Socialización de los resultados

2.3.3. Características

El servicio se hará por demanda una vez por año, bajo un entendido de pruebas de caja gris que comprende:

- **Se requiere un ejercicio de Ethical Hacking** de intrusión interna y externa acordes a las metodologías que se encuentran en el mercado tales como OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL – OSSTMM, INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK – ISSAF, OFFENSIVE SECURITY – OS, OPEN WEB APPLICATION SECURITY PROJECT - OWASP, entre otras y teniendo como insumo adicional los hallazgos de los análisis de vulnerabilidades.
- **Los activos objeto del ataque autorizado corresponden a ocho (8) IPs y cinco (5) aplicaciones transaccionales, los cuales serán seleccionadas por parte de la ADRES, teniendo como referencia los resultados de las auditorías técnicas de análisis de vulnerabilidades sobre la infraestructura y**

análisis de vulnerabilidades sobre aplicaciones web. Estos activos podrán ser del tipo servidor, aplicaciones transaccionales, equipos de red o equipos de seguridad.

- La definición de fechas para la ejecución de las actividades será coordinada entre el proveedor seleccionado y el supervisor del contrato, por lo cual, eventualmente se podrá tener actividades a ejecutar en horario no hábil. **Las pruebas internas se deben realizar en sitio y las pruebas externas se pueden realizar de manera presencial o remota.**
- **Socialización de resultados de manera remota a través de Microsoft Teams. La invitación abierta a los grupos de interés de la Entidad será coordinada con el supervisor del Contrato.**
- La facturación del servicio se hará por unidad de IP o de aplicación

2.3.4. Entregables

Por cada ejercicio de Ethical Hacking realizado, el proveedor debe entregar los siguientes documentos:

Informe directivo. Presentación en Microsoft Power Point usando la plantilla definida por la ADRES, sin información comercial del proveedor, cuyo contenido presentará de manera general los resultados encontrados en la ejecución de este servicio indicando los aspectos más relevantes a nivel de las vulnerabilidades explotadas.

Informe consolidado del ejercicio de Ethical Hacking. En este informe se consolidará de manera concreta el resultado para cada una de las pruebas de Ethical Hacking realizadas a nivel técnico, físico y bajo procedimientos de ingeniería social incluyendo como mínimo:

- Descripción de los activos objeto de ataque.
- Fecha y hora de la ejecución
- Duración de las pruebas.
- Listado de vulnerabilidades atacadas
- Evidencia de los ataques ejecutados en cada uno de los activos donde se observe el nivel de acceso logrado.
- Conclusiones

2.4. Ingeniería Social

2.4.1. Objetivo

Realizar ejercicios de entrenamiento para los usuarios de la Entidad, mediante la simulación de ataques de PHISHING con técnicas de ingeniería social, que permitan informar sobre el progreso de preparación de amenazas de los usuarios, así como los pasos siguientes recomendados para preparar mejor a los usuarios para futuros ataques.

2.4.2. Actividades

En esta fase deben ser incluidas como mínimo las siguientes actividades.

a. Definición de ataques de PHISING[3].

[3] **Phishing**: Es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas. A través de técnicas de manipulación emocional genera confianza en las personas para poder robar su información y dinero. El objetivo del phishing

b. Programación y ejecución de ataques de PHISING.
c. Elaboración o generación de informe
d. Socialización de resultados y sensibilización de los resultados de los ejercicios de Ingeniería Social a toda la Entidad.
e. Socialización de resultados y sensibilización de los ejercicios de Ingeniería Social.

2.4.3. Características

El servicio se hará por demanda tres (3) simulaciones por año, en paquetes de 593 cuentas de usuario que comprende:

- Ejercicio de Phishing a funcionarios y contratistas de la Entidad.
- Los ejercicios se deben realizar mediante la funcionalidad de entrenamiento de simulación de ataque de la herramienta Microsoft 365 defender **o por medio de otra herramienta, siempre y cuando permita verificar la evolución del usuario frente a los ejercicios de ingeniería social y cuente con diferentes fuentes de plantillas.**
- La ADRES suministrará y asignará los accesos a la herramienta Microsoft 365 Defender
- La ADRES podrá suministrar, logos, plantillas o documentos internos con el propósito de hacer más acertado los ejercicios planeados.
- **Socialización de resultados y sensibilización por cada uno de los ejercicios o simulaciones de Ingeniería Social de manera remota a través de Microsoft Teams. La invitación abierta a la Entidad para la socialización de resultados será coordinada con el supervisor del Contrato.**
- La facturación del servicio se hará por unidad de simulación por usuario.

2.4.4. Entregables

Por cada ejercicio de ingeniería social realizado, el proveedor debe entregar los siguientes documentos:

Memorias de sensibilización. Presentación en Microsoft Power Point usando la plantilla definida por la ADRES, sin información comercial del proveedor, cuyo contenido presentará de manera general los resultados encontrados en la ejecución de este servicio indicando los aspectos más relevantes a nivel de las vulnerabilidades explotadas.

Informe específico de Ejercicios de Ingeniería Social. En este informe se consolidará de manera concreta el resultado de los ejercicios de ingeniería Social incluyendo como mínimo:

- Simulaciones realizadas
- Comparación con datos históricos
- Cobertura de las simulaciones
- Usuarios reincidentes en simulaciones consecutivas
- Eficacia del entrenamiento
- Conclusiones y recomendaciones

2.5. Monitoreo y correlación de eventos de seguridad

es engañar a las personas para obtener datos confidenciales, como contraseñas e información bancaria. Este cibercrimen se comete a través de correos falsos, mensajes o llamadas telefónicas. El estafador utiliza una identidad falsa para obtener los datos que necesita y cometer delitos como el robo de dinero en cuentas bancarias. Tomado de: https://www.pichincha.com/portal/blog/post/que-es-phishing

2.5.1. Objetivo

Reducir los tiempos de respuesta ante amenazas, los falsos positivos y los eventos de seguridad que requieren investigación, que se pueden generar dentro de Azure, Microsoft Office 365, Centro de datos principal y sede, lo cual, define una infraestructura hibrida a ser monitoreada.

2.5.2. Actividades

Se debe adelantar las siguientes etapas para este servicio:

Identificación y preparación del servicio. Se debe realizar el levantamiento de información e identificación de las necesidades del servicio, que incluye la identificación de las tecnologías a utilizar, eventos a ser analizados y presentados, la arquitectura técnica de comunicaciones, ubicación de los sensores de recolección de datos (Logs) en el caso que se requieran, confirmación del inventario de dispositivos a evaluar, identificación del modelo de red y modelo de categorías de activos.

Integración. Se debe realizar la definición del modelo de gestión en donde se crearán los niveles de escalamiento y entrega de información, indicadores de riesgos, condiciones, reglas y filtros que serán aplicados a los eventos dentro de su ciclo de vida.

Plataforma de análisis. Se debe realizar las siguientes actividades sobre el SIEM Microsoft Sentinel suministrado por la ADRES:

- Revisión y ajustes de la configuración de la ingesta de datos de las diferentes fuentes de eventos de los sistemas de ADRES, las cuales incluyen soluciones de seguridad, sistemas operativos, aplicaciones, equipos de red, directorios de identidad, bases de datos, entre otros. Si se hace necesario, la ADRES dispondrá de las máquinas virtuales que sean requeridas para la implementación de colectores de datos desde las fuentes de eventos.
- Configuración, ajustes y monitoreo de los conectores o mecanismos de recopilación de datos con y sin agente o través de servicios API REST
- Revisión de la configuración del periodo de almacenamiento de los eventos recolectados en línea y en reposo. La ADRES aprovisionará el almacenamiento necesario de acuerdo con las fuentes de datos a integrar y correlacionar.
- Configuración de reglas y filtros de correlación
- Creación de técnicas de detección basadas en la agregación y en umbrales

Ejecución. Se debe realizar el monitoreo y análisis de los eventos e indicadores con base en la información recolectada y su presentación formal mediante la generación de informes o matrices según el alcance del servicio. Una vez un evento es confirmado como sospechoso o incidente, este se debe reportar según los niveles de escalamiento definidos en la etapa de integración. Entre las actividades a realizar se encuentran:

- Identificación, análisis, escalamiento, reporte de los casos, acciones de tratamiento e indicadores de compromiso y seguimiento de las alarmas, eventos e incidentes detectados.
- Clasificación y priorización de alarmas, eventos e incidentes detectados y analizarlos con el fin de poder determinar sus causas, origen e impacto.
- Definición y afinación de las reglas de correlación con base en el análisis de la información, los falsos positivos identificados y sobre la evolución de la organización, la infraestructura y las amenazas tecnológicas

- Adición de excepciones y personalización de normas para reducir los falsos positivos
- Exploración y análisis geoespaciales de datos de red.
- Monitorización de datos en tiempo real
- Personalización, definición y programación de nuevos informes
- Supervisión de la geolocalización de usuarios
- Detección avanzada de amenazas usando reglas de correlación para identificar un ataque dirigido o identificar comunicaciones y movimientos internos sospechosos como movimientos laterales, escalamiento de privilegios entre otros.
- Actualización permanentemente y de manera especializada para estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad y por ende repórtalas de manera oportuna.
- Confirmación con los usuarios sobre la realización de alguna actividad identificada como sospechosa, para los tipos de eventos que se definan. La comunicación se hará a través de Microsoft Teams, **para lo cual la Entidad creará las cuentas de usuario en el dominio de ADRES y aprovisionará las licencias necesarias que se acuerden con el supervisor del contrato.**

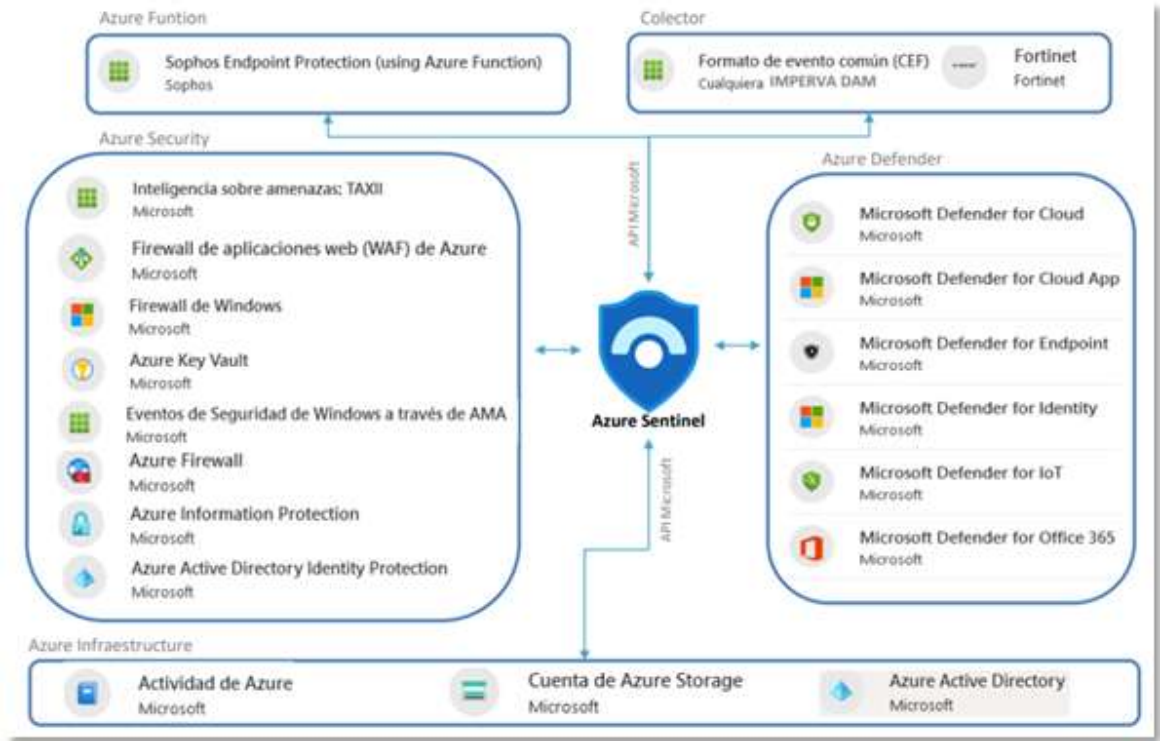
2.5.3. Características

El servicio de monitoreo y correlación de eventos de seguridad se debe prestar en la modalidad 7x24 hasta la fecha de finalización del contrato, el cual incluye la recolección de eventos, correlación de eventos, detección, investigación y respuesta ante eventos de seguridad, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la ADRES.

El servicio de monitoreo de eventos de seguridad debe utilizar la plataforma dispuesta por ADRES, la cual debe incluir el análisis de las siguientes fuentes de información:

- Azure Active Directory
- Azure Activity
- Azure DDoS Protection
- Azure Firewall
- Azure Information Protection
- Azure Key Vault
- Azure SQL databases
- Azure Sorage Account
- Azure Web Application Firewall
- Microsoft 365 Defender el cual incluye
    - Microsoft Defender for Endpoint
    - Microsoft Defender for Identity
    - Microsoft Defender for Office 365
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender Alert Evidence
    - Microsoft Defender Vulnerability Management
    - Microsoft Purview Data Loss Prevention
    - Azure Active Directory Identity Protection
- Microsoft Defender for Cloud
- Windows Firewall
- Windows Security Events
- DAM IMPERVA Enterprise Edition 14.9.1.10
- Web Application Firewall FortiWeb-1000E 6.11
- Firewall FortiGate-600E en sede y centro de datos
- Antivirus Sophos
- Threat intelligence - TAXII

El servicio se prestará con la herramienta de SIEM (Security Information and Event Management) Microsft Sentinel, cuyo licenciamiento y costos asociados al almacenamiento de los eventos serán asumidos por la ADRES. La solución se encuentra implementada y en producción, conforme al siguiente diagrama de referencia.



Para la integración se utilizarán los conectores de datos de Microsoft Sentinel para SYSLOG, Registros de eventos de Windows, Formato de evento común (CEF), Trusted Automated eXchange of Indicator Information (TAXII) (para la inteligencia sobre amenazas). Los sistemas de seguridad de ADRES proceden de múltiples fabricantes como Microsoft, Fortinet, Sophos, IMPERVA, entre otros.

A través de las capacidades de CYBER THREAT HUNTING de Microsoft SENTINEL, el prestador del servicio deberá realizar la búsqueda periódica y proactiva para la detección y aislamiento de amenazas de ciberseguridad que hayan evadido los controles aplicados en la infraestructura. Se utilizará el modelo de ataque MITRE's ATT&CK el cual constituye una base de datos de las técnicas y tácticas de los ciber atacantes.

El servicio se prestará de manera remota vía web, desde las instalaciones y con la conectividad provista por el proveedor del servicio.

El servicio deberá alertar a la entidad cuando se presenten amenazas de alta criticidad, ataques detectados, comportamientos sospechosos.

El prestador del servicio deberá contar con un grupo de personal calificado para el monitoreo, correlación y la atención de eventos de seguridad.

Suministrar información acerca de advertencias, anuncios, boletines y documentación sobre las mejores

prácticas actuales, listas de verificación, ataques de día cero, Información de desarrollo y distribución de actualizaciones de seguridad, con el fin de generar boletines internos y mantener al día a los usuarios de la Entidad sobre nuevas amenazas.

El servicio debe recibir, registrar y atender los requerimientos, eventos, solicitudes de cambio y actividades sospechosas reportadas por los usuarios de la ADRES y relacionadas con el servicio.

La facturación del servicio se hará por unidad mes.

2.5.4. Entregables

Informe Mensual. Generar un informe mensual del análisis de eventos, alertas, incidentes y problemas de seguridad con estadísticas y tendencias actuales. El informe debe incluir los siguientes reportes:

- Top de dispositivos con eventos de seguridad.
- Top de ataques detectados en la entidad
- Top de usuarios con autenticaciones fallidas.
- Reporte de riesgos
- Reporte de alertas e incidentes recurrentes o de alta criticidad.
- Relación de llamadas realizadas que contenga mínimo el usuario, fecha y evento.

2.6. Monitoreo y supervisión de actividad de bases de datos

2.6.1. Objetivo

Monitorear y supervisar la actividad sobre las bases de datos, con el fin de identificar cualquier atipicidad generada dentro del manejo de los datos, de los accesos concedidos a los usuarios, así como acciones que amenacen la confidencialidad, disponibilidad o integridad de la información.

2.6.2. Actividades

A solicitud de la Entidad o por iniciativa del contratista, se deben realizar las siguientes actividades:

- Implementación y validación de políticas, reglas y configuraciones
- Implementación de casos de uso, con el propósito de controlar los usuarios y mejorar la calidad de uso de la solución instalada.
- Monitoreo y supervisión de la actividad sobre las bases de datos.
- Configuración de la evaluación de vulnerabilidades para las bases de datos que se requieran.
- Descubrimiento de activos de información del tipo bases de datos sobre la red de ADRES. Si la entidad así lo decida, el proveedor deberá agregar estos activos a la protección.
- En el evento de ser necesario, el proveedor deberá instalar y configurar un segundo Gateway. En este caso el servidor será aprovisionado por la ADRES.
- Revisión del estado de salud de la solución IMPERVA.
- Instalación o actualización del certificado SSL para el sitio de IMPERVA. El certificado será aprovisionado por la ADRES.

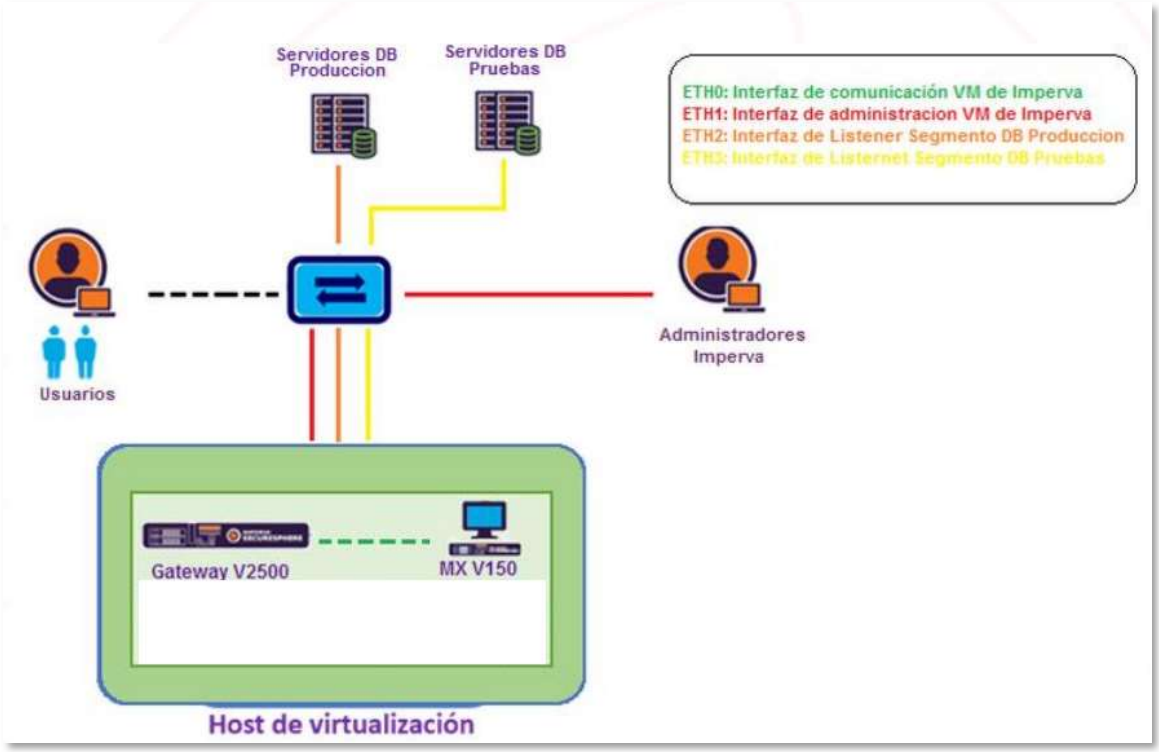
2.6.3. Características

El servicio se debe prestar en la modalidad 5x8 hasta la fecha de finalización del contrato, el cual incluye la implementación de casos de uso, soporte técnico y mantenimiento.

Los motores de bases de datos supervisados corresponden a Microsoft SQL Server 2012, 2016 y 2019. Actualmente no se supervisan bases de datos desplegadas como servicio en la nube pública. A continuación, se relacionan las cantidades de bases de datos supervisadas por ubicación y ambiente:

Ubicación	Producción	Pruebas: MS SQL Server
Nube Pública Microsoft Azure	35	0
Nube Privada	520	32

El IMPERVA se encuentra instalado On Premises con un despliegue por agentes. Para un mejor entendimiento, en la siguiente gráfica se presenta la arquitectura de referencia.



Prestación de soporte técnico sin límite de incidentes y requerimientos sobre la solución IMPERVA.

Cada seis meses, realizar el mantenimiento de la infraestructura que soporta la solución IMPERVA, el cual se ejecutará conforme al plan de trabajo que se acuerde. El mantenimiento incluye:

- **Revisión del rendimiento de los componentes de la solución: MX Server VM150 y DBF V2500**
- **Generación de copias de respaldo**
- **Actualización del sistema operativo**

- **Importación de licenciamiento en el evento que se requiera**
- **Actualización del motor de análisis en el evento que se requiera**

Cada vez que la Entidad realice una solicitud de servicio, por cualquiera de los canales disponibles telefónico, mensajería Instantánea o correo electrónico, el caso debe quedar registrado en la mesa de Servicio o de Ayuda del contratista.

Los servicios serán prestados a través de conferencia telefónica, acceso remoto o servicio en sitio, entregándose prioritariamente a través de conferencia telefónica o acceso remoto.

La facturación del servicio se hará por unidad mes.

2.6.4. Entregables

Informe mensual. El contratista debe entregar mensualmente un informe que contenga:

- Relación de vulnerabilidades encontradas con sus respectivas recomendaciones de mitigación.
- Relación de casos de uso implementados, revisados o ajustados durante el periodo.
- Inventario actualizado de bases de datos monitoreadas, en el evento que se haya realizado alguna modificación
- Relación de incidentes y requerimientos reportados o solicitados en el periodo con sus respectivas soluciones.
- Informe técnico por cada mantenimiento ejecutado, el cual debe incluir las actividades realizadas, los hallazgos encontrados relacionados con el estado de la solución con sus respectivas remediaciones.

2.7. Gestión de incidentes de seguridad

2.7.1. Objetivo

Gestionar los incidentes o hallazgos que sean relevantes dentro del proceso y de conformidad con el procedimiento de respuesta a incidentes de seguridad y los acuerdos de niveles de servicio aprobados, con soporte especializado para casos que requieran de un despliegue con atención de campo.

2.7.2. Actividades

Se deben realizar las siguientes actividades:

- Atención de los eventos e incidentes de seguridad conforme a los procedimientos acordados. Esta gestión incluye acciones de contención por parte del proveedor o de manera compartida con la ADRES.
- Comunicación de ocurrencia del incidente, indicando como mínimo fecha y hora de detección del evento, naturaleza del evento, prioridad y recomendaciones de contención del incidente.
- **Definición del plan de respuestas a incidentes y presentación para la aprobación por parte de la Entidad.**
- Elaboración de los informes por incidente
- Cuando se requiera, realizar el respectivo análisis forense.
- **Acompañamiento a los usuarios en la aplicación de recomendaciones, para los tipos de eventos de seguridad que se definan. La comunicación se hará a través de Microsoft Teams,**

para lo cual la Entidad creará las cuentas de usuario en el dominio de ADRES y aprovisionará las licencias necesarias que se acuerden con el supervisor del contrato.

2.7.3. Características

El servicio de Gestión de Incidentes se debe prestar en la modalidad 7x24 hasta finalizar el contrato, que incluye los procedimientos que permitan reaccionar ante los incidentes de la mejor manera posible minimizando los daños de los sistemas de información, diagnósticos eficaces, recolectando las evidencias necesarias y mitigando las causas de los incidentes.

La gestión de, incidentes deberá contemplar el escalamiento y seguimiento de los casos detectados de acuerdo con el protocolo o procedimiento que se establezca para tal fin.

Se debe detectar, reportar, evaluar y responder a incidentes de seguridad. Para ello, el prestador del servicio deberá establecer un procedimiento apoyado con una metodología CSIRT para la detección, alertamiento, notificación, seguimiento y respuesta de incidentes de seguridad; también para informar puntos débiles de seguridad; definir responsabilidades que se deberían asignar para la gestión de incidentes y proponer mejoras de seguridad de la infraestructura tecnológica.

El prestador del servicio debe contar con un equipo de respuestas a incidentes conformado por personal especializado para la atención a incidentes de seguridad conforme a las metodologías y procedimientos definidos.

Prestar soporte especializado para casos que requieran de un despliegue con atención de campo y realizar el análisis forense ante un incidente de seguridad cuando sea requerido por la ADRES y realizar el levantamiento de la cadena de custodia como apoyo primer respondiente.

Realizar análisis forense cuando al materializarse un incidente de seguridad de la Información se determine que es necesario la ejecución de este tipo de servicios.

El servicio debe recibir, registrar y atender los eventos e incidentes reportadas por los usuarios de la ADRES y relacionadas con el servicio.

Cada vez que la Entidad realice una solicitud de servicio, por cualquiera de los canales disponibles telefónico, mensajería Instantánea o correo electrónico, el caso debe quedar registrado en la mesa de Servicio o de Ayuda del contratista.

La facturación del servicio se hará por unidad mes.

2.7.4. Entregables

Reporte de cada incidente de seguridad ocurrido **o de cada evento de seguridad reportado por los usuarios de la Entidad**, con su debida recomendación de contención de este.

2.8. Gestión de infraestructura de seguridad

2.8.1. Objetivos

Gestionar la infraestructura de seguridad de la ADRES que no se encuentre tercerizada con el fin de mejorar la respuesta ante incidentes y amenazas de seguridad.

2.8.2. Actividades

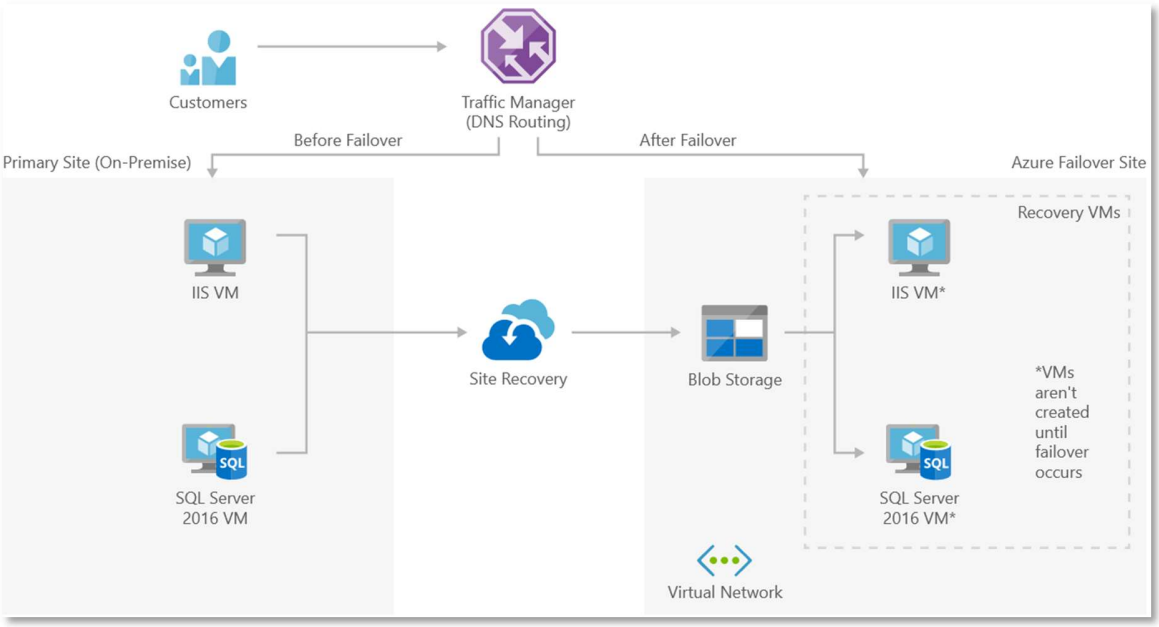
Se deben realizarlas siguientes actividades:

a. Levantamiento de información, que incluye la identificación de las tecnologías a utilizar y las actividades de administración a realizar.
b. Monitoreo y solución de inconvenientes que se presenten en las tecnologías a utilizar
c. Creación y ajustes de reglas utilizando las herramientas dispuestas por la ADRES, con el fin de contener una amenaza u optimizar algún control de seguridad.
d. Proponer los controles de cambio en los casos que se requieran.
e. Monitoreo de cambios realizados para detectar posibles afectaciones en la operación
f. Realizar un plan de aplicación de recomendaciones reportadas por Microsoft Defender for Cloud y Security Center de Azure, con el fin de mejorar la postura de seguridad de las identidades, datos, dispositivos y aplicaciones.

2.8.3. Características

El servicio de gestión de infraestructura se debe prestar en la modalidad 5x8 hasta finalizar el contrato, mediante la utilización de la plataforma dispuesta por ADRES que no se encuentren tercerizada, que incluye:

a) Herramientas del centro de operaciones de seguridad como son Microsoft Sentinel, Microsoft Azure Monitor, Microsoft Security Center, Microsoft Endpoint (Intune), Azure Defender, Microsoft 365 Defender, Azure Firewall y Azure DDoS.
b) Herramientas adicionales como son las consolas de administración de Microsoft 365, Microsoft Information Protection, Purview y Azure Active Directory. El proveedor del servicio utilizará las herramientas adicionales, solamente para realizar configuraciones de emergencia para una pronta contención de un incidente o amenaza. La administración de estas soluciones seguirá a cargo de los líderes de servicios o del proveedor de servicios que contrate la Entidad.
c) Servicio de Azure Site Recovery y seis (6) servidores entre los cuales se distribuyen los roles de Configuration Server, Process Server, Master Target Server y VMware Center Server. El proveedor del servicio deberá monitorear el estado de la solución de replicación, actualizar de versiones del software de configuración y replicación del servicio, así como de los agentes en cada una de las máquinas virtuales objeto de la replicación. En el evento que se requieran, deberá realizar la instalación y configuración del software en nuevos servidores con el fin de mejorar el rendimiento del servicio de replicación desde el centro de datos principal hacia Azure. **Los servidores serán aprovisionados por la ADRES.**
d) **El servicio de Azure Site Recovery se encuentra desplegado en la nube pública Microsoft Azure y los servidores de replicación se encuentran desplegados en la nube privada. Para un mejor entendimiento, en la siguiente gráfica se presenta la arquitectura de referencia.**



Fuente: Microsoft

e) **La ADRES suministrará las cuentas de usuario necesarias para la administración de las herramientas de seguridad y para acceder a los servidores del servicio de Azure Site Recovery - ASR, exceptuando el VMware Center Server. La actualización de los agentes en cada una de las máquinas virtuales objeto de la replicación del servicio ASR, se realizará desde el portal de Azure.**

f) Para las herramientas de seguridad que se encuentran tercerizadas como Web Application Firewall FortiWeb-1000E 6.11, Firewall FortiGate-600E y Endpoint de Sophos, el prestador del servicio tendrá el rol gestor que facilite las acciones de contención de amenazas por parte de estos terceros.

El servicio debe recibir, registrar y atender los requerimientos, eventos, incidentes y solicitudes de cambio reportadas por los usuarios de la ADRES y relacionadas con el servicio.

La facturación del servicio se hará por unidad mes.

2.8.4. Entregables

Informe mensual sobre el estado y configuraciones realizadas utilizando las herramientas de seguridad

2.9. Revisión y análisis del plan de recuperación de desastres

2.9.1. Objetivos

Realizar ejercicios de entrenamiento para los usuarios técnicos y funcionales, mediante la simulación de ataques o eventos contingentes, que permitan el mejoramiento del plan de recuperación de desastres y la recuperación de los procesos críticos de la Entidad dentro de los tiempos que se definan o se encuentren definidos en el análisis de impacto del negocio.

2.9.2. Actividades

Se deben realizarlas siguientes actividades:

Plan de recuperación de desastres

a. Revisión del actual plan de recuperación de desastres
b. Análisis y mejoramiento del plan de recuperación de desastres. Entre los aspectos a revisar, analizar y mejorar se encuentran:
   - ✓ Determinar las etapas del plan de recuperación de la Entidad
   - ✓ Identificar las estrategias de recuperación previas a la declaración de una contingencia.
   - ✓ Identificación de los roles y responsabilidades ante un evento de recuperación de desastres de TI.
   - ✓ Establecimiento de directrices, mecanismos y guías para la activación de la contingencia, recuperación, restablecimiento y retorno a la operación normal, de los servicios y sistemas de información que soportan los procesos declarados como críticos del negocio.
   - ✓ Socialización y pruebas periódicas del plan de recuperación de desastres.

Simulaciones

Con respecto a la expectativa de la entidad, con relación al tipo de simulaciones, se espera un plan de pruebas simulando escenarios operativos, administrativos, eventos disruptivos o de recursos humanos para probar a nivel procedimental el DRP actual de la entidad. Las simulaciones comprenden:

a. Definición de las simulaciones por ataques o eventos contingentes
b. Programación y ejecución de las simulaciones, las cuales podrían ejecutarse fuera del horario hábil de trabajo
c. Elaboración o generación del informe de simulación
d. Ajustes del plan de recuperación de desastres por hallazgos encontrados en las simulaciones
e. Socialización de los resultados de la simulación

2.9.3. Características

El servicio deberá realizar una revisión, análisis y actualización del plan de recuperación de desastres por año y un ejercicio de pruebas de recuperación por semestre, que involucre componentes de los procedimientos críticos de la Entidad. Por necesidades de la ADRES, se podrán extender los ejercicios sobre otros procedimientos de la Entidad, sin exceder la cantidad de simulaciones establecidas.

La facturación del servicio se hará por unidad global.

A manera informativa se relaciona a continuación un extracto de la información que a la fecha ha construido la entidad respecto al plan de recuperación de desastres, esta información se debe tomar como referencia para establecer el nivel de madurez del plan, entender la estructura actual del documento y así mismo debe ser de utilidad para las estimaciones de esfuerzo que deben hacer los proponentes con el fin de asegurar el cumplimiento del servicio solicitado:

Objetivo

Recuperar las capacidades de las tecnologías de información y Comunicaciones ante la eventualidad de una falla parcial o total de los servicios y sistemas de información que se encuentran bajo la administración directa de la Dirección de Gestión de Tecnologías de la Información y las Comunicaciones, de manera que se pueda continuar con la operación de los procesos del negocio.

El plan de recuperación de desastres será activado una vez se hayan agotado todas las estrategias de recuperación existentes, apoyadas en los procedimientos operacionales que sean determinados para utilizar en el análisis del incidente presentado y no hayan permitido la contención del incidente.

Alcance

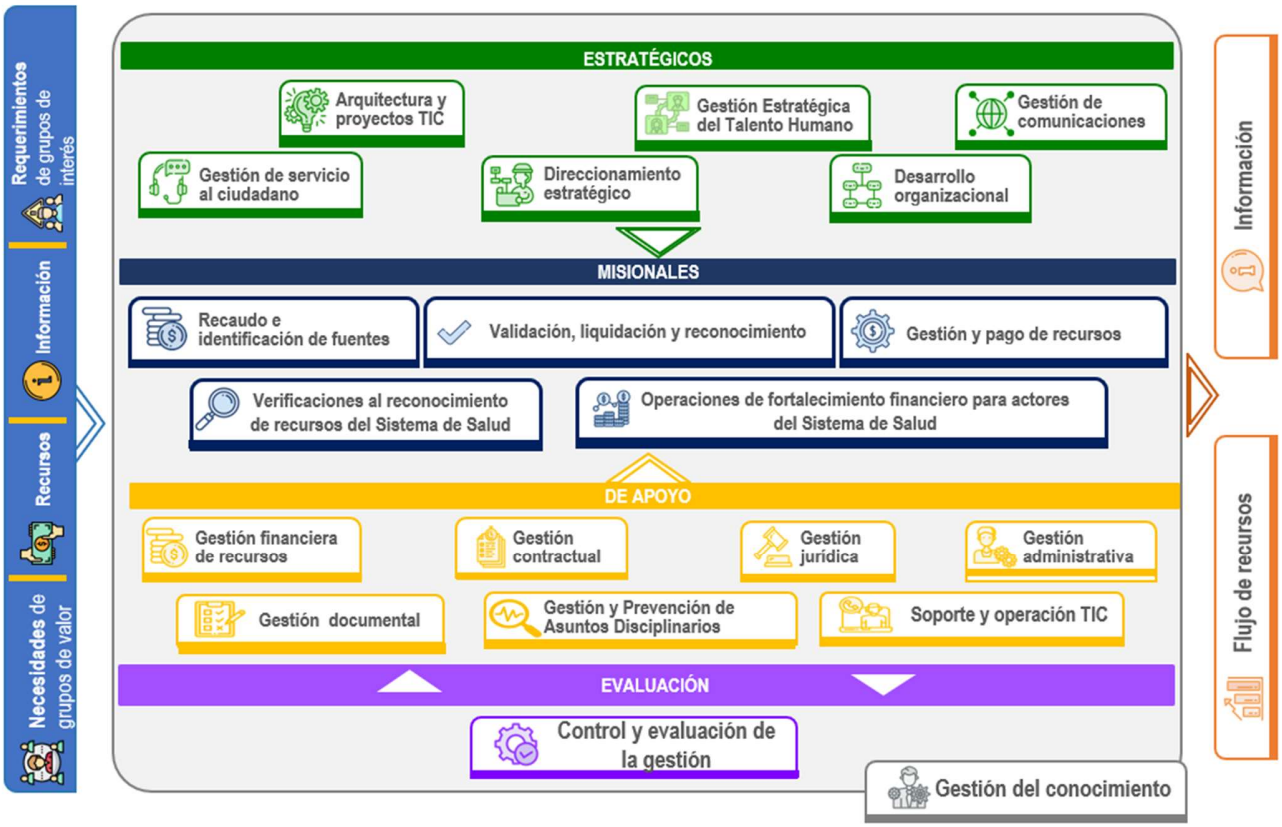
El plan de recuperación de desastres cubre la infraestructura tecnológica de la ADRES que se encuentran bajo la administración directa de la Dirección de Gestión de Tecnologías de la Información y las Comunicaciones, la cual soporta las aplicaciones, sistemas de información o servicios que apalancan los procesos de la ADRES.

El plan de recuperación de desastres comprende el siguiente alcance:

- Determinar las etapas del plan de recuperación de la Entidad
- Identificar las estrategias de recuperación previas a la declaración de una contingencia.
- Identificación de los roles y responsabilidades ante un evento de recuperación de desastres de TI.
- Establecimiento de directrices, mecanismos y guías para la activación de la contingencia, recuperación, restablecimiento y retorno a la operación normal, de los servicios y sistemas de información que soportan los procesos declarados como críticos del negocio.
- Socialización y pruebas periódicas del plan de recuperación de desastres.

Procesos

Actualmente la ADRES cuenta con 20 procesos, los cuales están divididos según su tipo en procesos estratégicos, misionales, de apoyo y evaluación, a continuación, se presenta el mapa de procesos vigente de la Entidad.



Estrategias de recuperación

Cualquier situación que afecte la disponibilidad de los servicios prestados por la Dirección de Gestión de Tecnologías de Información y Comunicaciones DGTIC inicialmente, será identificada y registrada como un incidente conforme al procedimiento OSTI-PR02 -Gestión de incidentes. Una vez conocido el detalle del incidente reportado y si así se requiere, se activa el procedimiento de OSTI-PR03 Gestión de incidentes de Seguridad, el cual permitirá posteriormente la activación del OSTI- PR14 procedimiento de recuperación de desastres tecnológicos al reportar el informe de incidente ocurrido.

En este sentido, es preciso indicar que según el tipo de indisponibilidad que pueda presentarse, deberán ser implementadas las siguientes estrategias:

Tipo de indisponibilidad	Estrategias de recuperación
Indisponibilidad de la Aplicación	Soporte de Aplicaciones
Indisponibilidad de Servidor Físico	Restauración del servidor
Indisponibilidad de Servidor Virtual	Recuperación de la imagen del Servidor a partir de las copias de respaldo o de la replicación geográfica de datos
Indisponibilidad de base de datos	Recuperación de bases de datos a partir de las copias de respaldo o de la replicación geográfica de datos
Indisponibilidad del Firewall	Activación del Firewall de respaldo en centro de datos principal o sede de ADRES Reemplazo de parte o del equipo a cargo de los proveedores de servicios

Tipo de indisponibilidad	Estrategias de recuperación
Indisponibilidad de equipos activos	Reemplazo de parte o del equipo a cargo de los proveedores de servicios
Indisponibilidad de los enlaces de datos	Conexión VPN con el Firewall dispuesto en el centro de datos principal o la sede
Indisponibilidad centro de datos principal	Operación en centro de datos alterno

Por lo cual, la única opción que activará el plan de recuperación de desastres será la indisponibilidad del centro de datos principal. Las demás indisponibilidades, serán evaluadas como incidentes y se tendrán estrategias puntuales de recuperación. Dicha indisponibilidad podrá obedecer a situaciones o motivos tales como:

- *Agentes Naturales*. Deslizamientos de tierra y/o otros elementos, avalanchas, fallas geológicas, terremoto, temblor, asentamientos, inconsistencias del suelo, inundaciones, erupción volcánica, vientos o cualquier otra convulsión de la naturaleza.
- *Agentes Humanos*. Guerras internacionales o civiles, actos perpetuados por terroristas y/o grupos armados ilegales, rebelión, sedición, usurpación o retención ilegal del mando, asonada, motín, o conmoción popular, huelgas, conflictos colectivos de trabajo o suspensión de hecho de labores y por movimientos subversivos y/o acciones terroristas y/o de grupos armados ilegales que conlleven a daños materiales en las instalaciones.
- *Agentes externos*. Reacción o radiaciones nucleares o contaminación radioactiva.
- *Agentes tecnológicos*. Ataques cibernéticos.

Equipo de Mando Unificado del DRP

Su función principal es la de supervisar y coordinar las diferentes actividades internas de recuperación, restauración y retorno, monitoreando el avance de las acciones realizadas por el personal implicado en la activación de la contingencia tecnológica en los diferentes escenarios de desastre que se activen. Su composición es la siguiente:



Equipo técnicos operativos

Su responsabilidad es velar por el funcionamiento de los Servicios y Sistema de Información que se activen, recuperen, restauren, y retornen dentro del Escenario de Recuperación de Desastres de TI. Este equipo técnico se encuentra dividido en tres:

- Grupo Interno de Soporte a la Tecnologías. El cual tiene un líder o Coordinador, con preventivas y reactivas

- Mesa de servicios. Orgánicamente se encuentra dentro del grupo interno de soporte a las tecnologías, sin embargo, dentro del plan de recuperación de desastres tiene responsabilidades reactivas.

- Grupo Interno de Gestión de Operaciones de Sistemas de Información. El cual tiene un líder o Coordinador, con responsabilidades preventivas y reactivas:

Líderes funcionales
Personal clave dentro de cada proceso de la Entidad, los cuales eventualmente serán el canal directo de comunicaciones entre el comité de crisis y los usuarios El cual tiene un líder o Coordinador con responsabilidades preventivas y reactivas

2.9.4. Entregables

Informe por cada ejercicio de recuperación de desastre realizado, con su respectiva presentación en Microsoft Power Point

Plan de recuperación de desastres actualizado, con su respectiva presentación en Microsoft Power Point.

3. PLAN DE TRABAJO

El adjudicatario deberá elaborar, entregar y socializar previa aprobación del supervisor, el plan de trabajo con su cronograma de actividades, modelo de operación del centro de operaciones de seguridad con procedimientos y metodologías para el desarrollo del objeto contractual dentro de los diez (10) días hábiles siguientes a la fecha de firma del acta de inicio.

La gestión de requerimientos, eventos, incidentes, solicitudes de cambio y de actividades sospechosas del SOC deberá contemplar el escalamiento y seguimiento de los casos detectados de acuerdo con el protocolo o procedimiento que se establezca para tal fin.

4. EQUIPO DE TRABAJO

El adjudicatario deberá presentar el equipo de trabajo conforme al modelo de operación del SOC del proponente, dentro de los cinco (5) días hábiles siguientes a la fecha de firma del acta de inicio.

Si el Contratista durante la ejecución del contrato requiere realizar cambios en el equipo de trabajo, deberá notificar a la ADRES con la debida antelación y presentar el nuevo perfil profesional.

Los cambios de personal no deberán superar los cinco (5) días hábiles.

En el evento en que la supervisión del contrato evidencie que el personal que integra el equipo de trabajo no tiene las competencias para el rol asignado por el proponente o compromete o pone en riesgo la seguridad de la información objeto del contrato y de la ADRES con sus actuaciones o no disponibilidad recurrente, la entidad solicitará el cambio inmediato del personal.

El equipo de trabajo mínimo requerido será presentado por el contratista y verificado por el supervisor del contrato durante la ejecución del contrato. Para ello se deben tener en cuenta las siguientes consideraciones:

- Para la formación académica de cada uno de los perfiles, se tendrán en cuenta las profesiones que integran el Núcleo Básico de Conocimiento (NBC). Para ello se debe aportar copia del diploma o copia del acta de grado.
- Para la acreditación de la experiencia especifica del equipo de trabajo mínimo requerido, se deberá allegar certificaciones donde conste los objetos, funciones, obligaciones y/o actividades relacionadas con la experiencia solicitada.
- La experiencia se contabilizará a partir de la fecha de expedición de la matrícula profesional o del certificado de inscripción profesional de conformidad con lo establecido en el artículo 12 de la Ley 842 de 2003, norma especial que regula el ejercicio de la ingeniería o de alguna de sus profesiones afines o auxiliares.

El contratista deberá contemplar el personal técnico adicional para prestar el objeto del presente proceso de contratación y su alcance conforme al documento de especificaciones técnicas.

A continuación, se relaciona el equipo de trabajo mínimo requerido:

Rol	Cantidad	Perfil	Experiencia Específica
Gerente de proyecto	1	Profesional en Ingeniería de Sistemas, industrial, electrónica, telecomunicaciones o afines Tarjeta profesional vigente Especialización en Gerencia de Proyectos o afines. Contar con una (1) de las siguientes certificaciones: • Project Management Professional – PMP • Scrum Master • Scrum Consultant • Scrum Product Owner • **ITIL® 4 Managing Professional Certificate**	Experiencia de mínimo cinco (5) años como gerente o gestor o coordinador o director de proyectos relacionados con: • Seguridad de la información • y/o seguridad informática • y/o seguridad digital • y/o ciberseguridad • y/o centro de operaciones de seguridad • y/o equipos de respuestas de incidentes de seguridad
Director de SOC	1	Profesional en ingeniería de Sistemas o ingeniería Electrónica o afines. Especialización en Seguridad de la información, seguridad informática o **seguridad de redes telemáticas** Tarjeta profesional vigente Contar con dos (2) de las siguientes certificaciones vigentes: • Lead Cybersecurity Professional Certificate – LCSPC. • ITIL® Foundation IT Service Management – ITSM. • Certified Ethical Hacker – CEH. • Certified Penetration Testing Engineer – CPTE. • **Certified Information Systems Security Professional - CISSP** • **Certified Information Security Management - CISM** • **Auditor Líder ISO 27001:2013** • **Certificación NSE4 o superior**	Experiencia de mínimo cuatro (4) años en proyectos relacionados con: • Seguridad de la información • y/o seguridad informática • y/o seguridad digital • y/o ciberseguridad • y/o centro de operaciones de seguridad • y/o equipos de respuesta de incidentes de seguridad
Analista de seguridad líder	1	Profesional en ingeniería de sistemas o ingeniería electrónica o ingeniería de telecomunicaciones o ingeniería telemática o carreras profesionales afines a tecnologías de la información y las comunicaciones Tarjeta profesional vigente. Contar con dos (2) de las siguientes certificaciones vigentes:	Experiencia de mínimo cuatro (4) años relacionada con: • Ejecución de Pruebas de Vulnerabilidad • y/o análisis de vulnerabilidades • y/o gestión de vulnerabilidades

		• Certified Information Systems Security Professional - CISSP • Certified Information Security Management - CISM • Certified Information Systems Auditor - CISA • Certified in Risk and Information Systems Control - CRISC • Auditor interno en ISO 27001:2013 • Auditor líder en ISO 27001:2013 • **Auditor Líder ISO 27032: 2012** • Certified Ethical Hacker - CEH • Ec Council Certified Security Analyst o Licenced Penetration • Tester - ECSA/LPT • Certified Digital Forensics Examiner CDFE • CompTIA Security+ Certified • Computer Hacking Forensic Investigator – CHFI • Offensive security Certified Professional – OSCP • Certified Penetration Testing Engineer – CPTE. • Certified Offensive and Defensive Security Professional – CODSP • Certified Incident Handling Engineer CIHE • Certificado Scrum Máster • **Certificacion ITIL 4** • **Certificación risk manager ISO 31000** • **Certified incident Handler v1 o superior** • **Certificación NSE 4 Network Security Professional** • **Cybersecurity fundamentals certificate**	• y/o pruebas de penetración • y/o pruebas de Ethical hacking • y/o ejercicios de ingeniería social • y/o monitoreo de eventos de seguridad • y/o gestión de incidentes de seguridad.
Analista de seguridad	2	Profesional en Ingeniería de sistemas o ingeniería electrónica o afines Tarjeta profesional vigente Contar con dos (2) de las siguientes certificaciones vigentes: • Auditor interno en ISO 27001:2013 • Auditor líder en ISO 27001:2013 • Certified Ethical Hacker - CEH • Ec Council Certified Security Analyst o Licenced Penetration • Tester - ECSA/LPT • Certified Digital Forensics Examiner CDFE • CompTIA Security+ Certified • Computer Hacking Forensic Investigator – CHFI • Offensive security Certified Professional – OSCP • Certified Penetration Testing Engineer – CPTE. • Certified Offensive and Defensive Security Professional – CODSP • Certified Incident Handling Engineer - CIHE • Certificado Scrum Foundation • **ISO 27032 Manager CiberSecurity**	Experiencia de mínimo tres (3) años relacionada con: • Ejecución de Pruebas de Vulnerabilidad • y/o análisis de vulnerabilidades • y/o gestión de vulnerabilidades • y/o pruebas de penetración • y/o pruebas de Ethical hacking • y/o ejercicio de ingeniería social
Analista de Operaciones de Seguridad	3	Profesional en ingeniería de Sistemas o ingeniería Electrónica o afines. Tarjeta profesional vigente Contar con dos (2) de las siguientes certificaciones vigentes: • Implementador Líder ISO/IEC 27001: 2013. • ISO 31000 Lead Risk Manager. • Certified Penetration Testing Engineer – CPTE. • Certified Incident Handling Engineer – CIHE. • Microsoft Security Operations Analyst • Microsoft Azure Security Technologies • **Auditor Líder ISO/IEC 27001: 2013.** • **ISO 27032 Manager CiberSecurity** • **Certificación NSE4 o superior**	**Experiencia de mínimo dos (2) años relacionada con:** • Monitoreo de eventos de seguridad • y/o correlación de eventos, • y/o contención de incidentes de seguridad • y/o gestión de incidentes de seguridad, • y/o gestión o mitigación de amenazas de seguridad • y/o administración u operación de herramientas de correlación de eventos
Administrador de plataforma	1	Profesional en ingeniería de Sistemas o ingeniería Electrónica o afines. Tarjeta profesional vigente	Experiencia de mínimo tres (3) años relacionada con la Administración, gestión, implementación, operación y/o soporte de infraestructura o plataforma de seguridad.

		Contar con una (1) de las siguientes certificaciones: • Microsoft Security, Compliance, and Identity Fundamentals • Microsoft Azure Security Technologies • Microsoft 365 Security Administration • Microsoft Security Operations Analyst • Microsoft Information Protection Administrator	
Especialista bases de datos SQL SERVER	1	Profesional Ingeniería de Sistemas, o Ingeniería Electrónica, o Ingeniería de telecomunicaciones o afines. Tarjeta profesional vigente **Especialización relacionada en seguridad informática o seguridad de la información o seguridad digital o ciberseguridad.** Contar con una (1) de las siguientes certificaciones: • SQL Database Administration • Administración IMPERVA	Experiencia específica mínimo de cuatro (4) años en implementación, administración, configuración o esquemas de alta disponibilidad para bases de datos SQL Server o en administración de soluciones de monitoreo y supervisión de bases de datos.
Ingeniero de continuidad	1	Profesional en ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines Tarjeta profesional vigente Especialización o Maestría en Gerencia de Servicio o Gerencia de Tecnología o Seguridad de la información o Seguridad informática. Contar con dos (2) de las siguientes certificaciones vigentes: • **Certified Information Security Management - CISM** • **Auditor Líder en Seguridad de la Información, ISO 27001** • **Auditor Interno en Continuidad del Negocio, ISO 22301** • **Auditor interno en ISO 27001** • **Certified Information Systems Auditor - CISA** • **Azure Solutions Architect Expert** • **Certificación risk manager ISO 31000** • **Certified Business Continuity Planning (CBCP)** • **Certified Information Systems Security Professional - CISSP** • **Certified in Risk and Information Systems Control - CRISC**	Experiencia de mínimo de cinco (5) años como líder de procesos en centros de datos, arquitectura de soluciones de contingencia o recuperación ante desastres.

5. CERTIFICACIONES

El Centro de Operaciones de Seguridad desde el cual se prestará el servicio deberá **ser miembro** de mínimo un (1) organismo de respuesta a incidentes de seguridad, como por ejemplo el FIRST, entre otros. El proveedor deberá adjuntar la certificación o membresía o constancia de integración expedida por el organismo.

El adjudicatario deberá mantener la membresía de su centro de operaciones de seguridad con mínimo un (1) organismo de respuesta a incidentes de seguridad durante la ejecución del contrato.

En cuanto la integración con servicios de inteligencia de amenazas provistos por algún proveedor de servicio, asociación o comunidad, esta puede ser ofertada por el proveedor dentro del costo del servicio del SOC, pero no será tenida en cuenta como un organismo de respuesta a incidentes de seguridad.

El proponente deberá garantizar el cumplimiento de estándares de seguridad de la información, para lo cual deberá contar con certificación expedida y vigente ISO27001:2013 o ISO27001:2014 o ISO27001:2017 o ISO27001:2022 aplicable con alguno de los siguientes procesos o servicios:

- Centro de operaciones de Seguridad

- Centro de operaciones de Ciberseguridad
- Monitoreo o correlación de eventos
- Gestión de incidentes de seguridad
- Análisis de vulnerabilidades
- Gestión o administración de infraestructura o de plataformas de seguridad
- Implementación de soluciones de seguridad de la información
- Consultoría de soluciones de seguridad de la información

Las certificaciones serán presentadas por el contratista y verificadas por el supervisor del contrato al inicio de la ejecución del contrato.

SAUL DIAZ OLIVAREZ
DIRECTOR (E) DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Revisó: Guillermo Benítez Rodríguez