Superintendencia Financiera de Colombia

# ANEXO 1

# FICHA TÉCNICA

- **OBJETO:**

  Adquirir la suscripción al servicio de software en línea (Software as a Service) que permita identificar, en tiempo real, la postura de ciberseguridad de las entidades vigiladas, de conformidad con las especificaciones técnicas señaladas

Conforme lo establecido en el numeral 1 del artículo 2.2.1.2.1.2.1 del Decreto 1082 de 2015, la presente ficha técnica incluye lo siguiente: a) la clasificación del bien o servicio de acuerdo con el Clasificador de Bienes y Servicios; b) la identificación adicional requerida; e) la unidad de medida; d) la calidad mínima, y e) los patrones de desempeño mínimos, así:

- **CLASIFICACIÓN UNSPSC:**

De acuerdo con la codificación de Bienes y Servicios del Código Estándar de Productos y Servicios de Naciones Unidas, el bien y/o servicio requerido se encuentra codificado de la siguiente manera:

**Tabla.** Códigos UNSPSC relacionados con el proceso.

| SEGMENTO | FAMILIA | CLASE |
|---|---|---|
| 81000000 | 81110000 | 81112200 |
| Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios Informáticos | Mantenimiento y soporte de software |
| 83000000 | 83120000 | 83121700 |
| Servicios públicos y servicios relacionados con el sector público | Servicios de Información | Servicio de comunicación masiva |
| 81000000 | 81110000 | 81111500 |
| Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios Informáticos | Ingeniería de software o hardware |
| 4300000000 | 43230000 | 43232300 |
| Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de consultas y gestión de datos |

Uso Interno

| SEGMENTO | FAMILIA | CLASE |
|---|---|---|
| 4300000000 | 43230000 | 43232900 |
| Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software para trabajo en redes |
| 4300000000 | 43230000 | 43231500 |
| Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software funcional específico de la empresa |
| 4300000000 | 43220000 | 43222500 |
| Difusión de Tecnologías de Información y Telecomunicaciones | Equipos o plataformas y accesorios de redes multimedia o de voz y datos | Equipos de seguridad de red |
| 4300000000 | 43230000 | 43232700 |
| Difusión de Tecnologías de Información y Telecomunicaciones | software | Software de aplicaciones en red |

**Fuente:** https://operaciones.colombiacompra.gov.co/clasificador-de-bienes-y-servicios

Los demás aspectos de la ficha técnica se encuentran incluidos en los siguientes requerimientos y características técnicas:

- **CONDICIONES TÉCNICAS GENERALES:**

1. Proveer una suscripción a un servicio de software en línea (Software as a Service) que incluya 150 licencias para recopilar, atribuir, calificar y monitorear en tiempo real la postura de ciberseguridad organizacional. El servicio deberá evaluar la salud general de la ciberseguridad de las entidades vigiladas[1], analizando los dominios web reportados por estas y proporcionando una evaluación detallada conforme a la ficha técnica.

2. Asimismo, deberá contar con un módulo que permita la incorporación ilimitada de dominios web de entidades adicionales, brindando su respectiva calificación general.

3. La suscripción tendrá una vigencia de un (1) año y deberá ofrecer flexibilidad para intercambiar licencias entre módulos o asignarlas a nuevos dominios web de entidades y organizaciones, según lo requiera la Superintendencia Financiera, con el fin de garantizar una cobertura óptima para las necesidades de la entidad.

[1] Entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia bajo la circular externa 007 de 2018

Uso Interno

4. Gestionar junto con el supervisor de contrato, dentro del día hábil siguiente a la firma del acta de inicio, una reunión para la presentación de los responsables tanto de la Entidad como del contratista, con el fin de acotar y contemplar el desarrollo de las siguientes etapas:

   - **Alistamiento:** implementación de requerimientos técnicos. (numeral I - REQUERIMIENTOS TÉCNICOS - ALISTAMIENTO de este documento).
   - **Parametrización inicial:** creación de usuarios, entidades, alertas, transferencias de conocimiento al personal de la SUPERINTENDENCIA y puesta en funcionamiento. (numeral II de este documento – TRANSFERENCIA DEL CONOCIMIENTO).
   - Durante la vigencia del licenciamiento, se podrán acordar las sesiones adicionales que sean requeridas por esta SUPERINTENDENCIA para realizar ajustes y parametrizaciones en la herramienta que sean necesarias, sin que esto genere un costo adicional para la entidad.

5. Entregar a nombre de la SUPERINTENDENCIA el documento emitido por el fabricante donde se indique la configuración y parametrización de usuarios, de acuerdo con lo indicado en los requerimientos técnicos de alistamiento.

6. Durante la vigencia del licenciamiento, el contratista deberá contar con un sistema de seguimiento de los casos y/o errores que se reporten, de tal manera que la SUPERINTENDENCIA pueda conocer el estado de evolución y la solución de estos. La herramienta que disponga el CONTRATISTA es de administración y gestión de su propiedad y se dispone para el escalamiento de casos que se requieran por parte de esta Superintendencia y no se requiere que se realice una instalación adicional a la indicada en el objeto del contrato.

7. El contratista deberá dar cumplimiento a las normas sobre propiedad intelectual y derechos de autor que ostenta el fabricante y/o titular de los Derechos, y mantener indemne a la SUPERINTENDENCIA ante cualquier reclamación respecto del incumplimiento de estas.

8. Disponibilidad y reportes
   8.1. Los servicios de monitoreo se deberán prestar de forma continua (7x24).
   8.2. El contratista deberá entregar reporte de los mantenimientos programados sobre la plataforma que ejecuta el fabricante indicando el día y la cantidad de horas que estaría intermitente.
   8.3. En caso de presentarse algún tipo de evento que afecte la disponibilidad o prestación del servicio de monitoreo, el Contratista deberá informar al supervisor del contrato, en un tiempo no mayor a treinta (30) minutos, el tipo de evento que se presente a través de los medios definidos para tal fin, como correo electrónico y herramienta de gestión de casos del proveedor.

Uso Interno

9. Confidencialidad
   9.1. La Información de la SUPERINTENDENCIA tiene el carácter de confidencial, por lo tanto, el CONTRATISTA, por el solo hecho de la firma del contrato, se compromete a no revelar, difundir, comentar, analizar, evaluar, copiar, vender o realizar un uso diferente del previsto en este contrato, ni utilizará dicha información para el ejercicio de su propia actividad, ni la duplicará o compartirá con terceras personas, salvo autorización EXPRESA escrita y previa de la SUPERINTENDENCIA, so pena de incumplir el contrato
   9.2. No utilizar en forma alguna, directamente o a través de terceros, en asuntos, negocios, y/o actividades de cualquier tipo, distintas a aquellas autorizadas expresamente por la Entidad, la información de la que tenga conocimiento o acceso por cualquier medio y por cualquier circunstancia en virtud de este proceso.
   9.3. Asumir la responsabilidad por la totalidad de los daños, perjuicios, gastos y costas que genere el mal o inadecuado manejo de la información a que tenga acceso en virtud de este contrato y/o por la violación de las obligaciones de reserva establecidas acá respecto de la guarda de la confidencialidad.
   9.4. Actuar con suma diligencia en la guarda y tratamiento de la información.
   9.5. El Contratista debe garantizar y enviar el acta donde se evidencie el borrado seguro de los datos de configuración y personalización dentro de los 30 días siguientes a la finalización de la vigencia del licenciamiento.

## I. REQUERIMIENTOS TÉCNICOS - ALISTAMIENTO

### 1. Monitoreo de postura de ciberseguridad

El contratista deberá garantizar el acceso a una solución tecnológica en línea, bajo el modelo Software as a Service (SaaS), que permita identificar en tiempo real la postura de ciberseguridad de las entidades vigiladas.

Se entiende por postura de ciberseguridad una solución de tipo Third Party Risk Management (TPRM), o gestión de riesgos de terceros, que habilite el análisis y la supervisión continua del estado de ciberseguridad de dichas entidades.

La solución deberá contar con las siguientes capacidades mínimas:

- Identificación de activos y servicios expuestos en internet (huella digital), a partir del dominio de la entidad vigilada.
- La evaluación no debe limitarse a los dominios reportados, sino incluir el descubrimiento constante de activos no declarados en Dark Web, Deep Web y foros de ciberdelincuentes.

Uso Interno

- Análisis de riesgos o vulnerabilidades sobre los activos identificados, mediante técnicas de escaneo pasivo y no intrusivo, sin requerir la instalación de agentes.
- Comparación de las brechas detectadas frente a una base de datos de vulnerabilidades y exposiciones conocidas, como la Common Vulnerabilities and Exposures (CVE).
- Detección de posibles afectaciones o incidentes de ciberseguridad reportados en fuentes de la web profunda, incluyendo la Deep Web y la Dark Web.

La solución debe contar al menos con las siguientes categorías de riesgo para el cálculo del score o puntuación:

- **Seguridad de Red:** identificación de puertos abiertos, cifrado débil, configuraciones por defecto de servicios de red, entre otros.
- **Seguridad de DNS (Domain Name Server):** validación del estado y configuración de los registros DNS, de los servidores de correo que tengan la protección adecuada y verificación de que los servidores DNS se encuentren correctamente configurados.
- **Parcheo de seguridad (Cadencia de parcheo):** revisión del estado actual de parches de seguridad en los servidores y su nivel de exposición y su velocidad de gestión para la mitigación de riesgos asociados a vulnerabilidades.
- **Seguridad de correo electrónico:** identificación de debilidades en la configuración de la plataforma corporativa del correo electrónico.
- **Seguridad del Endpoint:** validación de sistemas operativos, navegador web y complementos activos con el objetivo de identificar versiones obsoletas.
- **Reputación de IP:** identificación de amenazas, malware y verificación en listas negras asociado al direccionamiento IP de la entidad.
- **Seguridad de Aplicaciones:** identificación de aplicaciones vulnerables, versiones obsoletas, código de desfiguración (defacement[2]) y atributos de seguridad en las aplicaciones web expuestas.
- **Filtración de Información:** validación e identificación en la Deep web acerca de filtraciones masivas de datos que tengan que ver con la entidad.
- **Comunicaciones de piratas informáticos:** monitoreo y análisis de conversaciones de piratas informáticos que permitan identificar flujos de información que involucren a las entidades vigiladas.

El contratista será el encargado de habilitar la solución, la cual realiza el análisis de la postura de ciberseguridad de las entidades indicadas por esta SUPERINTENDENCIA, realizar la transferencia de conocimientos a los funcionarios designados por la entidad para la administración de la solución, dar el soporte de la solución, la gestión de escalamiento de casos requeridos por la Superintendencia, brindar el acompañamiento necesario para permitir el acceso a la información del monitoreo de postura de ciberseguridad a través de la

[2] Defacement es un ataque a un sitio web que cambia la apariencia visual de una página web.

Uso Interno

aplicación web y el intercambio de información vía API del software en línea (Software as a Service) sin costo adicional

**2. Huella digital**

El software en línea (Software as a Service) debe permitir la visualización completa de la huella digital (consistente en IPs, Dominios y Subdominios) de todas las entidades monitoreadas sin necesidad de autorización de esta, con evidencias para cada caso.

**3. Scoring o Puntuación**

La metodología, cálculo y algoritmo debe ser público y publicado en internet, así como dado a conocer a cualquier usuario o empresa que lo solicite.

La solución debe tener publicados los detalles de su metodología en un portal de transparencia de acceso público.

Una vez calculadas las puntuaciones para cada una de las categorías de riesgo, indicadas en el numeral anterior, el software en línea (Software as a Service) debe estar en capacidad de generar un score o puntuación global.

La calificación de postura de Ciberseguridad y monitoreo de las entidades debe ser por el total de sus activos en internet sin que esto implique un pago adicional por entidades que tienen miles o millones de activos.

La solución debe demostrar de forma transparente el porcentaje de impacto que una determinada vulnerabilidad tiene en la puntuación de la entidad vigilada que se está monitoreando.

**4. Vulnerabilidades y Hallazgos detectados**

La solución debe permitir identificar de manera instantánea y no intrusiva vulnerabilidades y malas prácticas de Criptografía, certificados digitales, expirados, autoformados, uso de tecnología de cifrado obsoleta, arquitectura de red, como exponer en internet sistemas de control industrial, bases de datos, protocolos de acceso a directorios, protocolos para acceso a escritorios remotos, Cámaras IP, entre otros.

De acuerdo con el scoring o puntuación obtenida, el software en línea (Software as a Service) debe mostrar las vulnerabilidades y hallazgos detectados, discriminados por nivel de criticidad (Alta, Media, Baja). Adicionalmente, la información de las vulnerabilidades se debe suministrar a un nivel detallado para que cualquier entidad pueda ser supervisada, como la dirección IP, la fuente de datos, la descripción de la vulnerabilidad, el riesgo, la recomendación de remedición, los enlaces a fuentes de información de remediación, así como información sobre la fecha de detección, la fecha de la última observación, el impacto en la puntuación, su nivel de riesgo y la recomendación técnica para remediarla.

Uso Interno

Los hallazgos deben detectarse a través de fuentes de datos activas, pasivas y de terceros. Los métodos activos de recopilación de datos deben incluir sensores que exploren Internet en busca de vulnerabilidades y debilidades de seguridad que puedan ser aprovechadas por actores malintencionados. Los métodos de datos pasivos, como los sumideros[3], los honeypots[4] y la recopilación de datos de los intercambios publicitarios, así como las fuentes de terceros, deben completar la recopilación para proporcionar una postura de ciberseguridad de las entidades que se supervisan.

Debe respaldar pruebas de la fuente de los hallazgos en la plataforma y terceros utilizados, utilizando fuentes como WHOIS, certificados SSL, búsqueda DNS, datos publicados, fuentes de datos de terceros para respaldar el proceso de evaluación. Este servicio/plataforma también debe proporcionar una forma de visualizar las posibles brechas existentes, los posibles sistemas comprometidos y los datos que puedan indicar transferencias de archivos peer-to-peer.

La información debe compartirse a un nivel detallado para que cualquier tercero pueda ser supervisado, como la dirección IP, la fuente de datos, la descripción de la vulnerabilidad, el riesgo, la recomendación de reparación, los enlaces a fuentes de información de reparación, así como información sobre la fecha de detección, la fecha de la última observación y el impacto en la puntuación.

## 5. Historial del Scoring o Puntuación

El servicio deberá permitir traza de todo el ciclo de vida del riesgo de ciberseguridad (hallazgos) a lo largo del tiempo, hasta con un año de antigüedad (desde que se identifica, se escala a los terceros, se gestiona y se remedia), así mismo el software en línea (*Software as a Service*) debe permitir mostrar el historial del scoring o puntuación de los últimos 7 días, 30 días, 6 meses y un año, con el objetivo de mostrar la evolución del puntaje de la entidad evaluada y debe permitirse visualizar por cada categoría[5] en la misma condición .

## 6. Resolución o Remediación de Hallazgos

El software en línea (*Software as a Service*) debe permitir la inclusión de la solución de los hallazgos detectados, así como realizar un nuevo cálculo del score o puntuación.

La solución debe permitir invitar a las entidades vigiladas de manera gratuita y con un tiempo indefinido para que estos puedan conocer su huella digital, señales de riesgo detalladas y factores de riesgo y puedan gestionar de forma continua las señales detectadas por el regulador en la propia plataforma.

---

[3] Técnica que se utiliza para bloquear el tráfico malicioso y evitar que llegue a su destino

[4] Sistema trampa o señuelo, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante

[5] Numeral 1. Monitoreo de postura de ciberseguridad

Uso Interno

La solución debe permitir generar planes de acción para que la entidad vigilada y el regulador puedan colaborar en la gestión de un plan de mejora de señales de riesgo. En este se podrá trabajar de manera colaborativa tanto en el plan, como en la resolución independiente de las señales.

La solución debe proveer un componente para gestión de la huella digital con posibilidad de añadir o eliminar Direcciones IP, Segmentos de Red, o Dominios, y estos podrán tener etiquetas para su gestión.

Si una vulnerabilidad es remediada en la infraestructura de la entidad vigilada y esta resolución es reportada a través del portal de la solución, el impacto debe ser resuelto en un plazo máximo de 72 horas, tras la certificación y confirmación por parte del fabricante de que la vulnerabilidad ya no existe.

Evitar excluir direcciones IP de los datos de las entidades (sin documentación suficiente) para asegurar que no están manipulando la calificación.

## 7. Filtros

El software en línea (Software as a Service) debe permitir la ejecución de filtros que permitan una parametrización inicial con el objetivo de evitar falsos positivos en el análisis, tales como, direcciones IP, rangos de direcciones IP, dominios, subdominios e incluso por país.

## 8. Comparación de resultados

El software en línea (Software as a Service) debe permitir realizar un comparativo entre los scoring o puntuación obtenida por las entidades monitoreadas, indicando, entre otros temas, los factores de riesgo, observaciones generales, los niveles de severidad y el histórico de la puntuación para 7 días, 30 días, 6 meses y 12 meses.

## 9. Reglas y Alertas

El software en línea (Software as a Service) debe permitir la creación de reglas según el comportamiento de las entidades vigiladas que se encuentren monitoreadas.

El software en línea (Software as a Service) debe permitir que, tras la detección de la regla desencadenante, se envíen en forma de correo electrónico o pueden ser capturadas directamente a través de una API[6] para ser capturadas en una fuente central en la SUPERINTENDENCIA, por ejemplo, un canal de teams.

Las reglas y alertas deben como mínimo permitir:

[6] Application Programming Interface

Uso Interno

- Configurarse por cambios porcentuales en la calificación
- Configurarse por cambios en las puntuaciones de los vectores de riesgo
- Configurarse por carteras de terceros

## 10. Arquitectura de la solución

- La solución debe incluir soporte nativo para 2FA.

- La solución debe tener en cuenta las regulaciones de privacidad y no transferir información a entidades externas.

**Integración vía API:** El software en línea (Software as a Service) debe proporcionar una API REST completa. La API debe ser totalmente accesible en la plataforma y estar incluida en las tarifas de suscripción. Algunas de las características mínimas que debe permitir consultar a través de API son:

- Calificación general de la entidad vigilada que está siendo monitoreada.
- Calificación de cada factor de riesgo.
- Señales de vulnerabilidades activas en cada entidad y sus cantidades.
- Nivel de severidad de cada señal activa.
- Al menos la Información de las siguientes alertas:
  - Incidentes de Ransomware.
  - Incidentes de intrusión.
  - Ataques de denegación de servicio (DoS y DDoS) detectados.
  - Intentos de explotación detectados.
  - Dominios objetivos de grupos de actores malintencionados.
  - Fugas de datos
  - Credenciales comprometidas identificadas.
  - Fugas de credenciales.

## 11. Acceso a usuarios

El software en línea (Software as a Service) debe permitir el acceso a la plataforma a un número ilimitado de usuarios, así como su configuración con permisos y roles según lo requiera la SUPERINTENDENCIA.

## CARACTERÍSTICAS TÉCNICAS DEL SERVICIO

### 1. Cambio de URL a monitorear

La plataforma que soporte el servicio de monitoreo debe permitir cambiar las entidades seleccionadas de manera ilimitada para ser evaluadas cada vez que se considere necesario.

Uso Interno

Además, debe contar con la funcionalidad de visualizar entidades vigiladas a nivel general con información sobre su puntuación y su variación en los últimos 30 días sin que esto repercuta en el número de entidades vigiladas a un nivel más profundo. Esta funcionalidad no debe afectar a las entidades a las cuales se les realiza un monitoreo de manera permanente y detallada.

**2. Generación de reportes**

El contratista debe permitir el acceso al software en línea (Software as a Service) a 30 usuarios de la SFC para la consulta o generación de al menos los siguientes informes en español e inglés:

1. Resumen detallado del scoring o puntuación con los hallazgos detectados.
2. Resumen ejecutivo del scoring o puntuación.

La Superintendencia Financiera de Colombia debe poder generar los reportes en el momento que lo considere necesario y usando diferentes parámetros para el efecto, como lo son: entidades, periodos y tipo (ejecutivo, resumido y detallado). Los reportes se deben generar de manera individual y comparativa.

La solución debe permitir generar reportes personalizados de Riesgos para áreas específicas de una compañía, ej. Datacenter, Cloud, Canales Digitales, basado en filtros de IP, Georreferencia o Dominios.

Adicionalmente debe permitir la descarga de todos los datos de descubrimiento de las IPs y los dominios mostrados de la entidad vigilada que está siendo monitoreada, esta información debe ser actualizada de forma automática por la herramienta.

**3. Tableros de control**

El contratista deberá poner a disposición de la Superintendencia Financiera de Colombia los tableros de control generados por el software en línea (Software as a Service) que permitan visualizar los resultados de los monitoreos realizados teniendo en cuenta el tipo de entidad y periodo.

**4. Generación de alertas, envío de correos**

El software en línea (Software as a Service) deberá enviar alertas a través del correo electrónico de manera semanal a los usuarios asignados por la Superintendencia, indicando la siguiente información:

- Resumen discriminado por entidad monitoreada indicando su scoring o puntuación y si este ha aumentado o disminuido.
- Posibilidad de establecer acciones automáticas cuando una nueva vulnerabilidad, evento o incidente afecte a una entidad/puntuación, tales

Uso Interno

como envío automático de informes resumidos y detallados a los usuarios del portal y copia de entidades afectadas.

**5. Acceso a la información del monitoreo a través de API o Web Services**

El contratista deberá permitir el acceso a la información del monitoreo de postura de ciberseguridad a través de API del software en línea (Software as a Service) sin costo adicional, por lo tanto, la plataforma debe proveer al menos la siguiente información:

- Calificación general de la entidad vigilada que está siendo monitoreada.
- Calificación de cada factor de riesgo o categoría de riesgo (de acuerdo con lo indicado en el numeral 2.1. Monitoreo de postura de ciberseguridad).
- Señales de vulnerabilidades activas en cada entidad y sus cantidades, las cuales deben estar clasificadas en cada factor de riesgo o categoría.
- Nivel de severidad de cada señal activa o vulnerabilidad.
- Al menos la Información de las siguientes alertas:
    - Incidentes de Ransomware.
    - Incidentes de intrusión.
    - Ataques de denegación de servicio (DoS y DDoS) detectados.
    - Intentos de explotación detectados.
    - Dominios objetivos de grupos de actores malintencionados.
    - Fugas de datos
    - Credenciales comprometidas identificadas.
    - Fugas de credenciales.
- El consumo de servicios a través de API se podrá realizar desde infraestructura on premise o nube perteneciente a esta superintendencia de acuerdo con los requerimientos que se requieran por parte de esta.
- El consumo de las API habilitadas desde la solución deben permitir la integración desde cualquier tipo de nube.
- El resultado del consumo de los servicios API (información) debe ser fácilmente segregada, de tal manera que pueda ser almacenada en las bases de datos de la superintendencia, independientemente del fabricante.
- La disponibilidad de consulta de la herramienta para la obtención de información de los resultados de las evaluaciones realizadas (vía web y API), debe ser 24x7.
- Esta interacción se realizará a demanda por parte de esta superintendencia (en tiempo real, diaria, semanal, mensual, entre otros) y en los horarios que requiera esta.

El contratista dará soporte y acompañamiento en la configuración e integración de los servicios API requeridos por la SUPERINTENDENCIA sin costo adicional.

**6. Servicio, soporte y mantenimiento:**

- El contratista deberá proveer sobre el servicio soporte telefónico, vía correo electrónico y/o vía Web en la modalidad de 7x24.

Uso Interno

- El software como servicio debe contar con una disponibilidad mínima del servicio del 99,95% mensual.
- La respuesta para el soporte, corrección de problemas o corrección de datos debe ser de máximo 24 horas laborables.
- Soporte para análisis de casos que sean escalados por esta Superintendencia sobre los hallazgos identificados a las entidades vigiladas que requieran mayor detalle técnico.
- Escalamiento de casos ante el fabricante de la solución que pueden derivar en falsos positivos y requieran su eliminación.
- Acompañamiento en sesiones técnicas con las entidades vigiladas.
- Soporte y acompañamiento en la integración de las API provistas por el fabricante de la solución para la obtención de información en línea.
- El acompañamiento se realizará a demanda por parte de esta Superintendencia y no cuenta con un límite de tiempo.
- El mantenimiento programado no debe afectar la recolección continua de datos, garantizando que el almacenamiento de hallazgos no se detenga.

**7. Acuerdos de Niveles de Servicios (ANS)**

- Garantizar una disponibilidad mínima del servicio del 99,95%[7]mensual.

- La respuesta para el soporte, corrección de problemas o corrección de datos debe ser de máximo 24 horas laborables.

**8. Acceso de usuarios**

El contratista deberá realizar la configuración de, como mínimo 40 usuarios de la SUPERINTENDENCIA en el software en línea (Software as a Service) que permita la consulta sobre la plataforma de monitoreo. Estos usuarios deben ser configurados con permisos y roles según lo indique el supervisor de contrato. Así mismo, deberá proporcionar soporte en la configuración y actualización de usuarios de la SUPERINTENDENCIA cuando esta lo requiera.

La solución/plataforma debe permitir el acceso a la plataforma a un número ilimitado de usuarios.

**II.TRANSFERENCIA DEL CONOCIMIENTO**

Con ocasión del contrato el contratista deberá realizar dos tipos de transferencias de conocimiento:

1. **Transferencia Inicial:** Esta jornada podrá desarrollarse de forma virtual, presencial o híbrida, según lo determine la supervisión del contrato y se deberá realizar dentro del plazo de ejecución del contrato. Tendrá una duración de hasta ocho (8) horas, o el tiempo que la supervisión considere pertinente.

[7] CE 005 de 2019

Uso Interno

- Se llevará a cabo en días hábiles (lunes a viernes), en el horario comprendido entre las 8:00 a. m. y las 5:00 p. m.
- Estará dirigida a un grupo aproximado de cincuenta (50) funcionarios adscritos a la Delegatura para Riesgo Operacional y Ciberseguridad. Este número podrá incrementarse sin que ello genere costos adicionales para la entidad.

2. **Transferencias Adicionales:** durante la vigencia del licenciamiento el contratista deberá estar disponible para realizar transferencias de conocimiento adicionales, siempre que la SUPERINTENDENCIA lo requiera, ya sea por novedades o particularidades relacionadas con el uso y manejo de la herramienta.
   - Estas sesiones estarán dirigidas a los funcionarios que designe la supervisión del contrato.
   - Estas transferencias deberán realizarse sin que ello genere costos adicionales para la entidad.

En constancia de lo anterior se firma por:

JOSE LUIS CASTAÑEDA MONTES

Firmado digitalmente por JOSE LUIS CASTAÑEDA MONTES
Fecha: 2026.07.27 17:09:00 -05'00'

José LuisCastañeda Montes
Asesor
Grupo Riesgos de Seguridad de Información Ciberseguridad Fraude
Delegatura para Riesgo Operacional y Ciberseguridad

SILVA CUADRADO ROSELIS

Firmado digitalmente por SILVA CUADRADO ROSELIS
Fecha: 2026.07.28 07:14:39 -05'00'

Roselis Silva Cuadrado
Profesional Universitario
Grupo de Ciberseguridad Institucional y Continuidad Tecnológica
Subdirección de Operaciones

Uso Interno