**Control de versiones del documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** | **Responsable** |
| Ver 0.1 | 05/01/2026 | Actualización del Documento | Ing. Abraham Gutiérrez Castillo  Mtra. Azucena Villadozola Cortes |
| Ver 0.2 | 05/01/2026 | Revisión del Documento | Ing. Abraham Gutiérrez Castillo  Mtra. Azucena Villadozola Cortes |
| Ver 1.0 | 05/01/2026 | Aprobación del Documento | Ing. Javier Cortes López |

**Contenido**

[a) Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados. 3](#_Toc219370726)

[I. Características y especificaciones. 3](#_Toc219370727)

[i. Objetivo 3](#_Toc219370728)

[ii. Alcance 4](#_Toc219370729)

[iii. Requerimientos técnicos 5](#_Toc219370730)

[iv. Especificaciones técnicas 5](#_Toc219370731)

[iv.1 Servicios de Seguridad – Continuidad Operativa 5](#_Toc219370732)

[iv.1.1 Servicios de Firewall 5](#_Toc219370733)

[iv.1.2 Servicios de Prevención de Intrusos (IPS) 7](#_Toc219370734)

[iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS) 8](#_Toc219370735)

[iv.1.4 Servicios de Redes Privadas Virtuales (VPN) 10](#_Toc219370736)

[iv.1.5 Servicios de Filtrado de Contenido Web 12](#_Toc219370737)

[iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam) 14](#_Toc219370738)

[iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF) 15](#_Toc219370739)

[iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF) 17](#_Toc219370740)

[iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM) 19](#_Toc219370741)

[iv.1.10 Servicio de Correlación de Eventos 20](#_Toc219370742)

[iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT) 22](#_Toc219370743)

[iv.2 Servicios de Seguridad – Verificación y Calidad 23](#_Toc219370744)

[iv.2.1 Servicios de Borrado Seguro de Información 23](#_Toc219370745)

[iv.2.2 Servicio de Gestión de Dominios 25](#_Toc219370746)

[iv.2.3 Servicio de Certificados Digitales SSL 26](#_Toc219370747)

[iv.2.4 Servicios de Protección de Riesgos Digitales 26](#_Toc219370748)

[iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles. 29](#_Toc219370749)

[iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA). 30](#_Toc219370750)

[iv.2.7 Servicio de Antivirus 32](#_Toc219370751)

[iv.2.8 Servicios de Prevención de Pérdida de Información 33](#_Toc219370752)

[iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) 36](#_Toc219370753)

[iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información 39](#_Toc219370754)

[iv.3 Servicios del Centro de Operaciones de Seguridad (SOC) 40](#_Toc219370755)

[iv.4 Servicios de Seguridad – Análisis y Pruebas de Seguridad 44](#_Toc219370756)

[iv.4.1 Servicios de Análisis de Vulnerabilidades Dinámico 44](#_Toc219370757)

[iv.4.2 Servicios de Análisis de Vulnerabilidades Estático 44](#_Toc219370758)

[iv.4.3 Servicios de Pruebas de Penetración 45](#_Toc219370759)

[iv.4.4 Servicios de Análisis Forense 47](#_Toc219370760)

[iv.5 Servicios de Transferencia de Conocimiento 47](#_Toc219370761)

[v. Perfil del Proveedor 48](#_Toc219370762)

[vi. Condiciones técnicas de aceptación de entregable 52](#_Toc219370763)

[vii. Cronograma de actividades 65](#_Toc219370764)

[viii. Niveles de servicio acordados que deberán cumplirse 65](#_Toc219370765)

[ix. Requerimientos de arquitectura tecnológica 67](#_Toc219370766)

[x. Restricciones e interfaces con otros elementos 67](#_Toc219370767)

[b) Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas. 67](#_Toc219370768)

[c) Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud. 67](#_Toc219370769)

[d) Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior. 67](#_Toc219370770)

[e) Firmas de elaboración, revisión y aprobación 70](#_Toc219370771)

[f) Relación de Anexos 70](#_Toc219370772)

# Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados.

La clave del Clasificador Único de las Contrataciones Públicas (CUCOP) de los bienes a adquirir o arrendar o servicios solicitados se identifica en la siguiente tabla:

|  |  |
| --- | --- |
| **Clave CUCOP** | 31900004 |
| **Descripción** | Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros |
| **Unidad de Medida** | Servicio |
| **Partida Específica (COG)** | 31904 “Servicios Integrales de Infraestructura de Computo” |
| **Objetivo del contrato** | Servicios Administrados de Seguridad Informática |

# Características y especificaciones.

# Objetivo

Para garantizar la continuidad operativa y la seguridad de la información del IMSS, se implementarán dos partidas que operarán de manera integrada y unificada.

Estos servicios se adjudicarán por partida a un único licitante, cuya propuesta cumpla con todos los requisitos obligatorios y obtenga la mayor puntuación en la evaluación combinada de puntos o porcentajes. Debido a la naturaleza técnica de los servicios del SASI 2026, los licitantes solo podrán participar en una de las dos partidas. Esta restricción se establece para evitar conflictos de interés técnico que pudieran afectar al IMSS.

Estas partidas incluirán:

1. **Toma en Operación y Transición:** Esto incluirá la implementación de procesos de cambio, gestión de riesgos y capacitación del personal para asegurar una transición eficiente.
2. **Servicios de Infraestructura:** Abarcará la operación, soporte y mantenimiento de la infraestructura existente, así como la implementación y gestión de infraestructura para los centros de datos. Además, proporcionará atención a los servicios y aplicaciones del instituto. Se asegurará que la infraestructura sea confiable, segura y capaz de satisfacer las necesidades operativas del IMSS.
3. **Protección Integral de Servidores, Aplicaciones y Bases de Datos:** Se brindará un servicio completo de protección para los servidores, aplicaciones y bases de datos del IMSS. Esto incluirá medidas preventivas y reactivas para garantizar la integridad y disponibilidad de los datos críticos. Se implementarán soluciones avanzadas de seguridad para hacer frente a las amenazas actuales y emergentes.
4. **Servicios de Seguridad de la Información Especializados:** Este servicio se centrará en asp**ecto**s específicos relacionados con las tecnologías de la información, comunicaciones y seguridad de la información.

**Objetivos específicos**

* Salvaguardar y proteger la información institucional.
* Garantizar la continuidad operativa, de negocio y la seguridad de la información durante la vigencia del presente contrato, especialmente durante la transición del contrato anterior a los servicios de SASI 2026.
* Reforzar la seguridad de la información contra posibles amenazas, reduciendo el riesgo de incidentes de seguridad mediante la aplicación de tecnología de vanguardia para la supervisión, detección, aseguramiento, contención y respuesta ante posibles ataques a la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
* Contar con servicios de infraestructura regulados por niveles de servicio que incluyan la implementación de componentes necesarios en los centros de datos y servicios del IMSS, así como la gestión integral de la infraestructura para satisfacer las necesidades de conectividad, comunicación, protección, control y filtrado de la institución, asegurando que la plataforma tecnológica opere en óptimas condiciones.
* Disponer de servicios de protección de manera unificada e integrada, abarcando la prevención de pérdida de información, protección de sistemas físicos o virtuales, protección del correo electrónico interno y externo, herramientas de colaboración y trazabilidad, así como el filtrado e inspección del acceso a internet e intranet mediante una solución integral que permita la gestión consolidada de funcionalidades y servicios, con el fin de mantener, asegurar y fortalecer el esquema de seguridad del IMSS.
* Contar con servicios de seguridad de la información que complementen de manera consistente y robusta el esquema de seguridad institucional, incluyendo el control, aseguramiento, diagnóstico, pruebas, metodologías, acceso a cuentas privilegiadas, bases de datos, aplicaciones, correlación y trazabilidad de eventos, investigación forense y otros servicios especializados en seguridad y tecnologías de la información.

# Alcance

El alcance del SASI 2026 abarca los siguientes aspectos:

* + - 1. Un esquema de servicios para la implementación, gestión y monitoreo de la infraestructura física y de seguridad necesaria para la integración de los centros de datos. Este esquema se caracteriza por una arquitectura flexible que se adapta a las necesidades de migración. Incluye la operación, soporte y mantenimiento de la infraestructura existente, así como la posibilidad de su sustitución para mantener una plataforma tecnológicamente moderna y uniforme, garantizando la continuidad operativa, empresarial y la seguridad de la información del IMSS.
      2. Un esquema de servicios de protección que ofrece una solución integral, cubriendo la protección de los servicios de colaboración internos, el correo electrónico externo y la navegación web. Este esquema detecta y protege contra amenazas avanzadas, previene la fuga de información y se gestiona de manera consolidada.
      3. Un esquema de servicios de seguridad que complementa el esquema de protección. Incluye servicios orientados a firewalls, sistemas de prevención de intrusiones (IPS), filtrado de contenido, protección contra ataques de denegación de servicio distribuido (DDoS), antispam, firewall de aplicaciones web (WAF), protección de bases de datos (DBF), redes privadas virtuales (VPN) y la implementación y administración de nuevos servicios requeridos por el instituto. Además, se ofrece análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, servicios de protección de riesgos digitales, servicios de protección para redes inalámbricas y dispositivos móviles, gestión y control de acceso para usuarios privilegiados, correlación de eventos, protección contra amenazas persistentes avanzadas (APT), gestión de procesos de seguridad y servicios especializados en seguridad de la información. Este esquema proporciona una cobertura completa de seguridad.

Principio del formulario

# Requerimientos técnicos

Los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A, B y C.

1. **Funcionales**

Los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A, B y C.

1. **No funcionales**

Los requerimientos no funcionales se encuentran integrados en los Términos y Condiciones.

# Especificaciones técnicas

**Partida 1.**

# iv.1 Servicios de Seguridad – Continuidad Operativa

# iv.1.1 Servicios de Firewall

**Descripción del servicio:** El instituto requiere garantizar la continuidad operativa del servicio que proporciona seguridad y protección, incluyendo el control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones, así como la inspección de paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. Por consiguiente, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actualmente en uso por el Instituto, así como de aquellos que sea necesario implementar, mediante el suministro de soporte técnico, licenciamiento y otros recursos necesarios. Esto asegurará cumplir con los niveles de servicio establecidos los apéndices B y C.

• Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda para mantener la continuidad operativa del Instituto, conforme a lo especificado en el Apéndice A.

• Desarrollar en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas del Instituto.

• Realizar las acciones requeridas para la instalación del equipo en los Centros de Datos correspondientes o en cualquier otra ubicación designada por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.

• Continuar con la integración de cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand alone o para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto para este propósito.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

•Mantener el acceso a los servicios alojados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido y respetando la segmentación entre las diferentes zonas de seguridad.

•Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

•Atender todos los requerimientos de cambio, incidencias/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para tal fin.

•Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura del servicio.

•Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas a través de funcionalidades habilitadas en la solución.

•Informar sobre fallas relacionadas con el hardware de los activos de infraestructura provistos a través del servicio.

•Gestionar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones requeridas durante la vigencia de los servicios.

•Realizar evaluaciones operativas de los servicios (herramientas de software y activos de infraestructura) y análisis de vulnerabilidades cada seis meses desde el inicio de operaciones y hasta seis meses antes del término de los servicios. Estas evaluaciones deben identificar mejoras en el rendimiento de los activos, gestión de configuraciones y nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.

•Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos, como componentes de comunicación entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

•Proporcionar al Instituto cuentas de acceso a las consolas de administración correspondientes al servicio, así como herramientas en software para acceder a las mismas, garantizando que sean de solo lectura y que los atributos de consulta se definan según las mesas correspondientes.

•Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento, licenciamiento adquirido y otros datos relevantes para la toma de decisiones sobre el uso del servicio.

•Implementar un servicio de auditoría de reglas de acceso en los dispositivos firewall para el análisis y depuración de estas, mejorando así el control de acceso y la seguridad. Esta solución se ubicará en las instalaciones del centro de datos primario y no generará costos adicionales para el Instituto.

• Garantizar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.2 Servicios de Prevención de Intrusos (IPS)

**Descripción del servicio**: El Instituto requiere garantizar la continuidad operativa del servicio que proporciona protección perimetral basada en firmas y que identifica vulnerabilidades. Este servicio tiene como objetivo contener intentos de acceso no autorizado a los recursos o servicios publicados en Internet o Intranet que podrían afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actuales del Instituto o los que sean necesarios implementar, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para asegurar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos, según lo establecido en el Apéndice B.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.

• Permitir únicamente el tráfico definido por el Instituto, tanto interno como externo, entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que componen el servicio.

•Notificar cualquier actividad sospechosa relacionada con la violación de políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.

• Informar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas de los servicios y análisis de vulnerabilidades cada seis meses, desde el inicio de operaciones y hasta seis meses antes del término de estos, para identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el presente Anexo Técnico, incluyendo componentes que faciliten la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles), las cuales deberán ser de solo lectura y cuyos atributos de consulta se definirán en las mesas establecidas para este propósito.

• Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del presente servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos IPS para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución se implementará en las instalaciones del centro de datos primario y no generará costos adicionales para el instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS)

**Descripción del servicio**: El Instituto requiere mantener la continuidad operativa del servicio que brinda protección contra los ataques de denegación de servicio distribuido, basado en firmas y altos volúmenes de conexión. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Asegurar la continuidad operativa de los activos de infraestructura actuales del Instituto, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para garantizar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos para este propósito, según lo establecido en el Apéndice B.

• Integrar una solución híbrida con activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, junto con una solución de nube para mantener la continuidad operativa del Instituto, conforme a lo dispuesto en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los necesarios para cubrir las necesidades operativas.

• Realizar las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. En ningún momento se podrán realizar cambios en los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, pudiendo ser en modo stand-alone para la administración de todos los dispositivos, y asegurar que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicación (firmware) y otros componentes necesarios.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Continuar con el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

• Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para dicho propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, incluyendo:

* Notificar actividades sospechosas relacionadas con la violación de las políticas, así como las identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura), así como análisis de vulnerabilidades, para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de estos.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, como componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles). Estas cuentas serán de solo lectura, y sus atributos de consulta se definirán en las mesas establecidas para este propósito.

• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DDoS para el análisis, depuración y mejor control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.4 Servicios de Redes Privadas Virtuales (VPN)

**Descripción del servicio**: El Instituto requiere garantizar la continuidad operativa del servicio de interconexión a través de Internet, el cual posibilita establecer comunicaciones desde localidades remotas para la transferencia de información mediante un canal cifrado. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como implementar los recursos necesarios para mantener esta continuidad, incluyendo soporte técnico, licenciamiento y cualquier otro requerimiento para cumplir con los niveles de servicio establecidos en el Apéndice B.

• Integrar activos de infraestructura específicos (Appliances) con capacidad de expansión según demanda, con el fin de asegurar la continuidad operativa del Instituto, conforme a lo especificado en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para asegurar la continuidad operativa de los activos de infraestructura actuales y futuros, de acuerdo con las necesidades operativas.

• Realizar las tareas necesarias para la instalación del equipo en los centros de datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.

• Coordinar con el personal del Instituto, mediante el administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.

• Proseguir con la integración de cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente o stand alone, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios para su funcionamiento.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Continuar proporcionando acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido y respetando la segmentación definida entre las diversas zonas de seguridad.

• Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Atender todas las solicitudes de cambio, incidentes, fallos y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para tales fines.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que conforman el servicio, cumpliendo al menos con lo siguiente:

* Notificar cualquier actividad sospechosa relacionada con la violación de las políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.
* Informar sobre las fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

Principio del formulario

•Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, incluyendo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas de los servicios, herramientas de software y activos de infraestructura, así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de la operación de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, incluyendo componentes que faciliten las comunicaciones entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles), las cuales serán de solo lectura. Los atributos de consulta se definirán en las mesas integradas para este propósito.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, entre otros aspectos relevantes para la toma de decisiones sobre el uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos VPN para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución deberá implementarse en las instalaciones del centro de datos primario sin generar costos adicionales para el instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.5 Servicios de Filtrado de Contenido Web

**Descripción del servicio:** El Instituto requiere garantizar la continuidad operativa del servicio de filtrado de contenido web, el cual permite controlar y filtrar el acceso a Internet según roles y perfiles definidos. En este sentido, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actualmente en posesión del Instituto, así como la implementación de nuevos activos si fuera necesario. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para asegurar dicha continuidad operativa, todo de acuerdo con los niveles de servicio establecidos en el Apéndice B.

• Integrar activos de infraestructura específicos (Appliances) con capacidades de expansión bajo demanda para mantener la continuidad operativa del Instituto, conforme a lo establecido en el Apéndice A.

• Colaborar con el Instituto en la definición de la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los que se necesiten según los requisitos operativos.

• Realizar la instalación del equipo necesario en los Centros de Datos designados o en cualquier otra localidad requerida por el Instituto.

• Coordinar con el personal del Instituto, ya sea a través del administrador del contrato o el cuerpo de gobierno designado, las ventanas de mantenimiento necesarias para asegurar el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software que integran el servicio sin la autorización correspondiente.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, permitiendo la administración independiente (stand-alone) de los dispositivos, y asegurando que la bitácora de cada activo se integre adecuadamente en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Asegurar que los activos de infraestructura estén actualizados tecnológicamente, con un sistema operativo, aplicación (firmware) u otro componente necesario, estable y validado.

• Limitar el tráfico de datos únicamente al definido por el Instituto, tanto interno como externo, entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionándolos de acuerdo con el esquema de seguridad establecido y respetando la segmentación definida entre las diferentes zonas de seguridad.

• Evitar la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Gestionar todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para dicho propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que integran el servicio, cumpliendo al menos con:

* Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas mediante las funcionalidades habilitadas en la solución.
* Notificar sobre fallos relacionados con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener en funcionamiento los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas a los servicios (herramientas de software y activos de infraestructura), así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones, y detectar nuevas funcionalidades operativas derivadas de actualizaciones en las versiones de hardware y/o software. Estas evaluaciones se ejecutarán cada 6 meses, desde el inicio de las operaciones de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el presente Anexo Técnico, como componentes que permitan la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otras disponibles). Estas cuentas serán de solo lectura, y los atributos de consulta se definirán en las mesas integradas para este propósito.

• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, y otros recursos que ayuden en la toma de decisiones sobre el uso del presente servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos de Filtrado de Contenido Web para realizar análisis y depuración de estas, y mejorar el control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin incurrir en costos adicionales para el instituto.

• Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

# iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam)

**Descripción del servicio**: El Instituto busca garantizar la continuidad operativa de un servicio destinado al análisis de correos electrónicos de entrada y salida. Este servicio tiene como finalidad bloquear aquellos correos que sean identificados como spam, *malware*, *phishing*, o que contengan contenido malicioso, entre otros. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

•Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como implementar nuevos recursos si es necesario. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para mantener la operatividad, de acuerdo con los niveles de servicio establecidos en el Apéndice B.

• Incorporar activos de infraestructura específicos (Appliances) con capacidad de expansión bajo demanda, según lo definido en el Apéndice A, para asegurar la continuidad operativa del Instituto.

• Trabajar en conjunto con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y futuros, según las necesidades operativas.

• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, atendiendo las solicitudes del Instituto.

• Implementar un servicio de protección para el correo electrónico entrante y saliente, así como salvaguardar la reputación de las direcciones IP utilizadas para la comunicación en Internet, mediante un mecanismo de sanitización en la nube que brinde una doble capa de verificación sobre correos anómalos o no deseados.

• Establecer, en coordinación con el personal del Instituto, las ventanas de mantenimiento necesarias para la correcta operación del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado.

• Mantener la integración de cada activo de infraestructura hacia su consola de administración centralizada, garantizando la integración de la bitácora de cada activo en la solución de correlación de eventos designada por el Instituto.

•Asegurar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) u otros componentes necesarios para su correcto funcionamiento.

• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y otros puntos de interconexión con redes externas.

• Continuar permitiendo el acceso a servicios ubicados en la capa de servidores de los centros de datos, gestionándolos según el esquema de seguridad establecido y respetando la segmentación entre las zonas de seguridad.

• Implementar medidas proactivas para evitar la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Brindar atención a todos los requerimientos de cambio, incidentes, fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Supervisar todos los eventos registrados en la solución y enviar alertas sobre incidentes generados por los activos de infraestructura del servicio, incluyendo notificaciones sobre actividades sospechosas y fallas de hardware.

* Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• Incluir el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, así como realizar renovaciones durante la vigencia del contrato.

• Realizar evaluaciones periódicas de los servicios y activos de infraestructura para identificar mejoras y detectar nuevas funcionalidades operativas, así como analizar vulnerabilidades cada 6 meses.

• Implementar integraciones de conectividad física y lógica para habilitar los servicios descritos, incluyendo componentes como cableado, montaje en racks, entre otros.

• Facilitar al Instituto cuentas de acceso a las consolas de administración del servicio y a las bases de conocimiento de las tecnologías integradas, con información relevante para la toma de decisiones.

• Implementar un servicio de auditoría de reglas de acceso en dispositivos Antispam para mejorar el control de acceso y seguridad, sin costo adicional para el Instituto.

• Asegurar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF)

**Descripción del servicio**. El Instituto requiere garantizar la continuidad del servicio de protección, prevención y control de ataques dirigidos a los aplicativos *web* expuestos en Internet/Intranet. Por ende, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como la implementación de cualquier recurso adicional necesario para mantener esta continuidad, lo que incluye soporte técnico, licenciamiento y cualquier otro requisito necesario para asegurar el servicio de acuerdo con lo estipulado en el Apéndice B.

• Integrar activos de infraestructura específicamente diseñados (Appliances) con capacidad de expansión bajo demanda, asegurando la continuidad operativa del Instituto según lo especificado en el Apéndice A.

• Colaborar con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y aquellos que sean necesarios para satisfacer las necesidades operativas.

• Realizar las tareas requeridas para instalar el equipo en los Centros de Datos correspondientes o en cualquier otra ubicación solicitada por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea de forma independiente o en modo stand alone, asegurando que la bitácora de cada activo se integre en la solución de correlación de eventos designada por el Instituto.

• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Mantener el acceso a los servicios en la capa de servidores de los centros de datos (DMZ), gestionándolos de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

• Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso en las redes del Instituto.

• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos para este propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con la violación de políticas o fallas en el hardware de los activos de infraestructura provistos a través del servicio.

* Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.
* Realizar evaluaciones operativas y análisis de vulnerabilidades de los servicios y activos de infraestructura para identificar mejoras en el desempeño, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software, ejecutándose cada 6 meses desde el inicio de operaciones hasta 6 meses antes del término de estos.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, como componentes de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software para acceder a las mismas, las cuales deben ser de solo lectura y cuyos atributos de consulta deben ser definidos en las mesas que se integren para este propósito.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, entre otros aspectos relevantes para la toma de decisiones respecto al uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos WAF para analizar y depurar las mismas, mejorando el control de acceso y seguridad, con la solución implementada en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF)

**Descripción del servicio**: El Instituto requiere mantener la operatividad continua del servicio de protección para las instancias de bases de datos en tiempo real, así como supervisar el tráfico de la base de datos para detectar ataques avanzados. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

•Garantizar la continuidad operativa de los activos de infraestructura del Instituto, ya sea los existentes o los que se necesiten implementar, proporcionando soporte técnico, licenciamiento y otros recursos necesarios para asegurar dicha continuidad, conforme a lo establecido en el Apéndice B.

• Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, según lo dispuesto en el Apéndice A, para mantener la continuidad operativa del Instituto.

• Definir en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas.

• Realizar la instalación del equipo en los Centros de Datos correspondientes o en otras ubicaciones solicitadas por el Instituto.

• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, y abstenerse de realizar cambios en los componentes de hardware o software sin una autorización de cambio previa.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos o mediante otras configuraciones requeridas, garantizando la integración de las bitácoras de cada activo en la solución de correlación de eventos definida por el Instituto.

• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, aplicación (firmware) y otros componentes necesarios.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (Base de datos), gestionando según el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.

• Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando sobre actividades sospechosas relacionadas con la violación de las políticas y fallas relacionadas con el hardware de los activos de infraestructura.

* Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada 6 meses, desde el inicio de operaciones hasta 6 meses antes del término de estos, identificando mejoras en el desempeño, gestión de configuraciones y nuevas funcionalidades operativas.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, como componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio, así como herramientas en software que permitan acceder a las mismas, garantizando que sean de solo lectura y definiendo los atributos de consulta en las mesas correspondientes.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento vigentes, licenciamiento adquirido, y otras que faciliten la toma de decisiones.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DBF para mejorar el control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.8 iv.1.8 iv.1.8 iv.1.8 iv.1.8 iv.1.8 iv.1.8 iv.1.8 iv.1.8 Principio del formulario

# iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM)

**Descripción del servicio**: El Instituto busca asegurar la continuidad operativa del servicio de protección perimetral especializado en control de acceso, prevención de intrusos, filtrado de contenido web y VPN, con el fin de controlar el tráfico y detectar actividades anómalas. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto o implementar nuevos activos según sea necesario. Esto incluye proporcionar soporte técnico, licenciamiento y cualquier otro requisito para garantizar esta continuidad operativa, en conformidad con lo establecido en el Apéndice B.

• Integrar activos de infraestructura específicos (Appliances) con capacidad de expansión bajo demanda para mantener la continuidad operativa del Instituto, de acuerdo con lo estipulado en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los nuevos requeridos para satisfacer las necesidades operativas.

• Realizar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Acordar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software del servicio sea autorizado mediante un control de cambios.

• Continuar integrando cada activo de infraestructura en su consola de administración centralizada respectiva, ya sea en modo independiente o en conjunto, y asegurar que el registro de cada activo esté integrado en la solución de correlación de eventos especificada por el Instituto.

• Garantizar que los activos de infraestructura estén actualizados tecnológicamente, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.

• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con violaciones de políticas y fallas en hardware.

* Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, incluyendo todas las renovaciones requeridas durante la vigencia de los servicios.

• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada seis meses, identificando mejoras en el desempeño, la gestión de configuraciones y la detección de nuevas funcionalidades operativas.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, como componentes de comunicación entre redes, cableado eléctrico y de datos, y montaje en racks.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software para acceder a las mismas, con atributos de consulta definidos en mesas de trabajo específicas.

• Proporcionar al Instituto acceso a bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido para cada servicio proporcionado.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos UTM para análisis, depuración y mejor control de acceso y seguridad, sin generar costo adicional para el Instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.10 Servicio de Correlación de Eventos

**Descripción del servicio:** El Instituto requiere un servicio de seguridad que gestione, analice, explote, utilice y aproveche los registros de actividad de los dispositivos de seguridad para comprender completamente lo que sucede en varios puntos de la red de manera centralizada y eliminar los falsos positivos generados. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

• Proveer activos de infraestructura de última generación, exclusivamente dedicados a satisfacer las necesidades del Instituto.

• Habilitar los activos de infraestructura en esquemas de Alta Disponibilidad (HA).

• Integrar activos de infraestructura de propósito específico (appliances o servidores físicos) con capacidades de expansión bajo demanda, pudiendo estas últimas ser instancias virtuales, según lo dispuesto en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la correlación de eventos en la arquitectura de seguridad y comunicaciones.

• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se realizarán cambios a los componentes de hardware/software sin un control de cambios autorizado por el Instituto.

• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente (stand alone) para la administración de todos los dispositivos, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.

• Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión vía syslog con otras redes o nubes.

• Atender los requerimientos de cambio, atención de fallas y solicitudes de información generadas por el Instituto, según los Niveles de Servicio definidos.

• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.

* Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.

• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.

• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.

• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.

• Incluir un servicio de auditoría de reglas de acceso en los dispositivos del Correlacionador de Eventos para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

**Descripción del servicio:** El Instituto busca implementar un servicio que le brinde la capacidad de protegerse contra amenazas avanzadas que puedan estar activas dentro de la organización y que hayan eludido los controles de seguridad existentes. En este sentido, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

• Proveer activos de infraestructura de última generación, dedicados exclusivamente a las necesidades del Instituto.

• Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA).

• Integrar activos de infraestructura de propósito específico (appliances) con capacidades de expansión bajo demanda, pudiendo estas últimas ser instancias virtuales, según lo dispuesto en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la detección de Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.

• Ejecutar las tareas necesarias para la instalación del equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o el cuerpo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, sin realizar cambios a los componentes de hardware/software sin autorización.

• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, asegurando que la bitácora de cada activo quede integrada en la solución de correlación de eventos designada por el Instituto.

• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.

• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes o nubes, previniendo la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Atender los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generadas por el Instituto, apegado a los Niveles de Servicio definidos.

• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.

* Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
* Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.

• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.

• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.

• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

# iv.2 Servicios de Seguridad – Verificación y Calidad

El Instituto requiere mantener la prestación de servicios bajo demanda durante la vigencia del contrato, con el objetivo de definir, identificar, clasificar y priorizar las debilidades de las aplicaciones que proporcionan una evaluación de las amenazas previsibles. Esto permitirá reaccionar de manera adecuada y fortalecer la confidencialidad, integridad y disponibilidad de la información, en línea con las necesidades operativas del IMSS.

# iv.2.1 Servicios de Borrado Seguro de Información

**Descripción del servicio:** Se busca mantener la solución de borrado seguro de información para una variedad de dispositivos, incluyendo computadoras personales, laptops, servidores, unidades de almacenamiento fijas y removibles, así como cualquier otro dispositivo determinado por el Instituto. El objetivo es evitar la pérdida y dispersión de información propiedad del Instituto cuando estos dispositivos sean retirados debido a razones como la conclusión de contratos, obsolescencia, fallas, bajas o reasignaciones, entre otros motivos. Para lograrlo, es necesario renovar el derecho de uso y soporte técnico de los productos de software de borrado seguro, así como actualizar el licenciamiento correspondiente. Estas actualizaciones (updates y upgrades) deben garantizar la confidencialidad de la información del Instituto, cumpliendo con la legislación vigente sobre derechos de autor.

El proveedor de servicios deberá cumplir con las siguientes especificaciones funcionales mínimas y asegurar que los servicios y entregas de información estén de conformidad con la normativa aplicable para dichas soluciones y servicios.

• Integrar todas las renovaciones necesarias durante la vigencia de los servicios.

• Garantizar que las herramientas de borrado seguro cuenten con la última versión liberada, estable y validada por parte del fabricante, así como para otros componentes necesarios del servicio correspondiente.

• Permitir la realización de borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como equipos de cómputo (de escritorio y portátiles), equipos de propósito específico (appliance), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.

• Asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales.

* + HMG Infosec Standard 5 (baseline and enhanced)
  + Opnavinst 5239.1A
  + Extended NIST 800-88
  + DoD 5220.22-M
  + ISO-IEC 15408
  + ECE y BSI/VSITR

• Borrado de discos duros IDE/ATA, SCSI, SAS, USB, SATA, SSD, Fiber Channel y FireWire, tanto de estado sólido como mecánicos, independientemente de su tamaño.

• Destrucción local y/o remota en múltiples dispositivos de almacenamiento.

• Capacidades para desmontar RAID (SCSI) cuando sea necesario.

• Facilitación del proceso de borrado y detección de zonas bloqueadas/ocultas (DCO, HPA).

• Generación de certificados de borrado infalsificables, incluyendo el resultado del proceso de borrado, fecha, hora, detalles del equipo y del dispositivo de almacenamiento borrado, con el fin de ofrecer protección legal.

• Emisión de una firma electrónica para autenticar la integridad del reporte de sanitización emitido por el software de borrado.

• Ejecución de la solución sin importar el sistema operativo utilizado.

• Exportación del reporte generado por la solución a un medio de almacenamiento como USB o disco duro.

• El servicio de borrado seguro se proporciona a través de un proceso operativo que incluye:

* Solicitud de borrado.
* Identificación del medio a borrar.
* Definición de fecha para el borrado.
* Flujos operativos para autorización de borrado o destrucción.
* Se muestran los insumos a ser atendidos como referencia.

| **DISPOSITIVOS** |
| --- |
| **Derecho Uso de Licencias y Soporte Técnico** | |
| PC y Laptops |
| Servidores |
| Máquinas Virtuales y Unidades Lógicas |
| Archivos, carpetas, bases de datos |
| Console Management |
| **Servicio de Soporte Técnico Especializado** | |
| Disco Duro, PC, Laptops, Disco Duro Servidor y Disco Duro Storage |
| Borrado de Bases de Datos, LUN's y Contenedores |
| Borrado de Máquinas Virtuales |
| Degaussing Discos Duros, SSD y Cintas LTO |

• Es fundamental que la continuidad del servicio garantice que los usuarios tengan acceso a las consolas de administración de la solución. Esto les permitirá gestionar, administrar, supervisar y operar, con el objetivo de habilitar las funcionalidades necesarias para llevar a cabo el borrado seguro de manera descentralizada, incluso en oficinas remotas.

# iv.2.2 Servicio de Gestión de Dominios

**Descripción del servicio:** Garantizar la continuidad operativa para el registro y gestión de dominios conforme a los requisitos establecidos por el NIC. El proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Registro:

* Seguimiento ante las instancias certificadoras.
* Coordinación con el personal designado por el Instituto para el nombre de dominio acordado.
* Verificación de la no duplicación o uso por terceros del nombre de dominio.

• Alojamiento:

* Supervisión del alojamiento del dominio.
* Actualización de las directivas de seguridad.
* Mantenimiento continuo según sea necesario.

El proveedor de servicios deberá encargarse de la gestión y los pagos relacionados con el registro, cambio de dominio o proveedor, sin costos adicionales para el Instituto.

# iv.2.3 Servicio de Certificados Digitales SSL

**Descripción del Servicio:** Se busca garantizar la continuidad del servicio para obtener certificados SSL destinados a proteger las páginas web del Instituto durante la duración del contrato. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Validación de dominios.

• Encripción SSL de al menos 256 bits.

• Los certificados no deben ser auto firmados, sino emitidos por instancias certificadoras válidas (terceros de confianza).

• El tiempo de emisión debe cumplir con los niveles de servicio establecidos para su entrega al personal del Instituto vía correo electrónico.

• El proveedor se encargará de la gestión de los pagos de derechos y cualquier otro cargo asociado a la obtención y mantenimiento de los certificados.

• Los certificados deberán ser, al menos, de los siguientes tipos:

* Certificados SSL con validación de dominio (DV SSL):
* Certificado para un solo dominio.
* Certificado para múltiples dominios (SAN).
* Certificados comodines (wildcard).
* Certificados para código.

# iv.2.4 Servicios de Protección de Riesgos Digitales

**Descripción del servicio:** El Instituto busca un servicio de inteligencia con capacidad de acción que le permita responder de manera oportuna ante amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, así como realizar investigaciones según sus necesidades. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Detección de posible venta de información confidencial del Instituto en mercado negro.

• Generación de reportes de perfilamiento técnico de actores de amenaza (Actor Profiling) basados en evidencia digital y TTPs, sin interacción directa ni uso de engaños..

• Monitoreo automatizado y pasivo de fuentes abiertas, canales públicos y espacios de acceso restringido (Deep/Dark Web) para la detección temprana de amenazas.

• Monitoreo de foros y comunidades en redes abiertas y en la Red Onion/Tor donde se perpetren y difundan campañas de ataques informáticos que representen un riesgo para el Instituto.

• Inteligencia de fuentes abiertas (OSINT) enfocada exclusivamente en la detección de fugas de información y vulnerabilidades expuestas, excluyendo monitoreo de opinión pública.

• Recopilación de información a través de un cuestionario especializado para realizar el análisis de la situación global del Instituto y generar perfiles de investigación para los servicios permanentes.

* + Páginas publicadas.
  + Historial de amenazas de seguridad experimentadas por el Instituto.
  + Sistemas críticos consultados por usuarios externos.
  + Lista de activos críticos y su atracción o valor para el ciber-crimen.
  + Contactos para la elaboración de la matriz de escalación.
  + Datos para la elaboración de la declaración de trabajo (SOW por sus siglas en inglés).

• Análisis de la situación global del Instituto teniendo en cuenta el contexto del entorno y la identificación de exposiciones y amenazas que podrían impactarle, tanto a nivel local como global.

• Generación de reportes de perfilamiento técnico de actores de amenaza (Actor Profiling) basados en evidencia digital y TTPs, sin interacción directa ni uso de engaños..

• Establecimiento de umbrales para eventos que desencadenarán alertas hacia la matriz de notificación definida en conjunto con el Instituto para los servicios de "Vigilancia Permanente".

• Mantenimiento de supervisión de correos/sitios de phishing y direcciones IP sospechosas proporcionadas por el Instituto para su análisis. Además, se llevará a cabo vigilancia continua en el ciberespacio las 24 horas del día, los 365 días del año, incluyendo redes sociales, Darknet y buscadores de Internet de las cosas. Se utilizarán técnicas de OSINT (Inteligencia de Fuentes Abiertas) como líneas de tiempo y mapas de conexiones, así como Virtual HUMINT para la infiltración de perfiles virtuales.

• Identificación de campañas para ataques específicos, venta de información y exposición de infraestructura vulnerable en Internet, así como relaciones entre perfiles y grupos privados de Facebook, entre otros.

• Búsqueda continua de credenciales corporativas (@imss.gob.mx), documentos oficiales, bases de datos de derechohabientes y código fuente en paste sites, foros criminales y repositorios públicos.

• Detección de dominios apócrifos (typosquatting) utilizados para campañas de phishing contra derechohabientes o empleados.

• Alertas sobre vulnerabilidades críticas que afectan la tecnología específica utilizada por el IMSS, antes de que sean explotadas masivamente (Patch Management Intelligence)

• Realización de evaluaciones en los siguientes casos:

* Durante la vigilancia de Riesgos Digitales al identificar una amenaza real para el Instituto.
* Cuando se solicite análisis de sitios o correos de phishing, o direcciones IP.
* Durante análisis de grupos hacktivistas.
* Durante análisis de direcciones IP de ataques de denegación de servicio experimentados por el Instituto.

• Realizar un análisis correlacionando información recolectada con eventos específicos y emisión de dictámenes con inteligencia accionable hacia el Instituto en un plazo máximo de 24 horas después de la detección de eventos críticos, como ataques de denegación de servicio, defacements, fuga de información, phishing, entre otros.

* Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
* Defacements.
* Fuga de información confidencial del Instituto hacia sitios públicos.
* Malware dirigido.
* Phishing detectado en parking domains.
* Indicios de amenazas o ataques informáticos sobre el Instituto.
* Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
* Venta o publicación de información sensible del Instituto en la Darknet.
* Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
* Nuevos esquemas de fraude detectados en otros organismos del sector.

• Generación de procesos de inteligencia accionable en casos donde se haya detectado un ataque con impacto en el Instituto o en análisis a petición del Instituto sobre phishing y direcciones IP, proporcionando recomendaciones pertinentes.

* Cuando se detecte que un ataque ya sucedió y tuvo un impacto en el Instituto, para lo cual se emitirán recomendaciones hacia el Instituto.
* En los casos donde se realice el análisis a petición del Instituto de sitios o correos relacionados con phishing así como direcciones IP, se deberá generar a partir de los hallazgos identificados inteligencia accionable donde deberán incluirse detalles sobre los sitios, direcciones IP, artefactos maliciosos, entre otros, al igual que sobre los reportes generados como parte de los servicios.

• Análisis mensual de direcciones IP sospechosas para identificar posibles actividades de ataque, intrusiones a otros organismos similares, participación en botnets, defacements u otras campañas específicas.

• Análisis del hacktivismo en México, incluyendo operaciones actuales, objetivos e impacto, proporcionando recomendaciones de protección.

• Análisis de correos electrónicos o sitios web sospechosos, incluyendo identificación de encabezados, análisis de *malware*, extracción de datos y evaluación de riesgo en una plataforma de Inteligencia sobre Amenazas.

* Identificación de los encabezados y análisis del *malware* en el contenido.
* Extracción de datos como dominios y direcciones IP, mismas que deberán ser analizadas en una plataforma de “Inteligencia sobre Amenazas” para determinar el riesgo que representa el Phishing para el Instituto.

• Todas las actividades de mapeo de actividades, reportes, hallazgos relevantes y demás información recopilada y generada para el presente servicio deberá estar referenciada al uso del framework de MITRE ATT&CK.

# iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.

**Descripción del servicio:** El Instituto busca un servicio especializado en protección de redes inalámbricas, dirigido a segmentos específicos, que permita implementar controles efectivos para garantizar la seguridad y protección de la información generada internamente y recibida a través de los recursos de redes inalámbricas (WLAN), así como la protección para dispositivos móviles que garantice la prevención del robo o la sustracción de información. El objetivo es prevenir ataques comunes que intentan aprovechar estas redes para infiltrarse en la infraestructura de comunicaciones del Instituto. Para cumplir con estos requisitos, el proveedor debe satisfacer las siguientes especificaciones funcionales mínimas.

De igual manera el Instituto requiere una plataforma de movilidad que permita el acceso seguro a aplicaciones y datos institucionales desde dispositivos propiedad de los empleados (BYOD), internos y externos, garantizando la separación total entre la información personal del usuario y la información corporativa, bajo un modelo de arquitectura Zero Trust.

• La solución no debe procesar ni almacenar datos en el dispositivo físico del usuario. La interacción debe realizarse mediante la transmisión de píxeles cifrados desde un entorno virtual seguro centralizado (nube o centro de datos).

• Garantizar que ninguna caché, archivo temporal, base de datos o credencial institucional persista en el dispositivo móvil físico tras finalizar la sesión (Zero Data at Rest).

• La solución no deberá requerir permisos de administrador sobre el dispositivo personal, ni tener capacidad para visualizar, inventariar o borrar aplicaciones personales, fotos o datos privados del trabajador, eliminando la necesidad de borrado remoto del dispositivo físico completo.

• Capacidad de realizar una atestación de seguridad del dispositivo físico antes de permitir la conexión (detección de root, jailbreak o malware) sin invadir la privacidad.

• Bloqueo técnico que impida copiar/pegar datos desde el entorno virtual hacia el entorno personal del dispositivo, así como bloqueo de capturas de pantalla en el entorno seguro.

• Cliente ligero compatible con sistemas operativos iOS, Android y Windows, desplegable mediante tiendas de aplicaciones públicas.

• Asegurar que las herramientas propuestas para el servicio estén respaldadas por la última versión estable y validada por el fabricante, así como también para otros componentes necesarios del servicio correspondiente.

• Incluir el licenciamiento del software necesario para activar los servicios y recursos de infraestructura pertinentes, así como gestionar todas las renovaciones requeridas durante el período de vigencia de los servicios.

• Proteger contra ataques informáticos comunes dirigidos a la red inalámbrica (WLAN).

• Mejorar y actualizar los procesos de autenticación de usuarios internos, integrando autenticación de usuarios de forma local y/o por un gestor de identidad, que de manera enunciativa puede ser directorio activo, ldap, radius, entre otros.

• Implementar cifrado TKIP y/o AES basado en hardware (WPA-PSK, WPA2-PSK, WPA2-EAP, WPA/WPA2-PSK, WPA3).

• Contar con funcionalidades de WIPS en tiempo real (prevención de intrusiones inalámbricas).

• Integrar un tercer radio de banda dual específico sin comprometer el rendimiento del punto de acceso.

• Integrar autenticación basada en certificados con EAP-TLS para WPA2/WPA3-Enterprise.

• Permitir la implementación de políticas de control sobre las aplicaciones en los dispositivos.

• Facilitar la instalación de aplicaciones y la ejecución de actualizaciones en múltiples dispositivos de manera remota, controlando el tipo de conexión y la programación de ejecución.

• Posibilitar la modificación de contraseñas de bloqueo, permitiendo configurar aspectos como longitud, tipo (alfanumérica o numérica) y número de intentos, entre otros.

• Permitir a los administradores del sistema mantener y controlar los dispositivos de forma centralizada.

• Realizar análisis en los dispositivos para asegurar el cumplimiento de las políticas institucionales.

• Recuperar toda la información relevante de los dispositivos, incluyendo detalles del dispositivo, certificados y aplicaciones instaladas.

• Regular el acceso a cuentas institucionales, como correos electrónicos, redes Wi-Fi y VPN.

• Bloquear dispositivos de manera remota para prevenir robos o pérdida de información.

• Deberá ser compatible con la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto, el cual debe ser compatible con al menos las siguientes plataformas operativas: macOS, iOS, Android y Windows desde la versión 10 en adelante.

# iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).

**Descripción del servicio:** El Instituto requiere de un servicio de control de acceso para usuarios privilegiados con el objetivo de brindar funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados en sus servidores, así como implementar un sistema de Autenticación, Autorización y Contabilización (AAA, por sus siglas en inglés: Authentication, Authorization and Accounting). Por lo tanto, el proveedor seleccionado deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Implementar una solución tecnológica que permita un control detallado del acceso a los activos de infraestructura que respaldan las aplicaciones, mediante la administración del ciclo de vida de las identidades.

• Integrar procesos que identifiquen los roles y perfiles de cada usuario por aplicación, junto con la capacidad de rastrear los accesos realizados, incluyendo la captura de imágenes de pantalla y la grabación de video de las sesiones de acceso.

• Considerar, entre otras, las siguientes plataformas operativas:

* Microsoft Windows
* Unix
* Linux

• Revisar y validar junto con el Instituto los requisitos para proteger las claves privilegiadas en los servidores donde se implementará el servicio.

• Implementar los agentes proporcionados por la solución en los sistemas operativos respaldados por los fabricantes correspondientes.

• Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centros de Datos designados por el Instituto.

• Acordar con el personal del Instituto las ventanas de mantenimiento necesarias según el tiempo de implementación requerido.

• Integrar el dispositivo con la consola de administración de la solución y garantizar la integración de la bitácora del dispositivo con la solución de Correlación del proyecto.

• Ofrecer servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e identidad en la red del Instituto.

• Habilitar los activos de infraestructura necesarios en esquemas de Alta Disponibilidad (HA).

• Capacidad para generar políticas basadas en reglas y atributos.

• Integración con bases de datos externas como Active Directory y LDAP.

• Capacidad de integrarse con un dominio de Directorio Activo.

• Integración con soluciones de contraseña única.

• Integración con dispositivos de red para aplicar políticas de seguridad basadas en identidad.

• Utilización de los siguientes protocolos de autenticación:

* CHAP/MSCHAP
* PAP
* PEAP
* EAP-TLS
* MS-CHAP
* EAP-MD5

• Generación de políticas de restricción por dispositivo y horario.

• Uso de listas de acceso descargables.

• Capacidad para operar en esquemas de clúster con más de 3 dispositivos funcionando como un solo sistema.

• Funcionalidad para operar en esquemas de procesamiento físico (appliance) o virtualizados.

• Interfaz de administración gráfica basada en web.

• Interfaz de programación para operaciones de actualización, creación, lectura y eliminación de dispositivos, terminales y usuarios en la base de datos interna.

• Funcionalidades de reporte y auditoría.

• Capacidades de monitoreo y diagnóstico de problemas.

• Administración de eventos (logs) exportables.

# iv.2.7 Servicio de Antivirus

El proveedor deberá proveer el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución diseñada para proteger contra amenazas de código malicioso que puedan afectar a los dispositivos de trabajo, servidores, correos electrónicos externos e internos, así como la navegación web hacia Internet. Además, se aplicarán políticas de seguridad con el objetivo de fortalecer los controles para mitigar riesgos, proteger la infraestructura institucional y garantizar la continuidad operativa de las actividades de los usuarios.

La protección antivirus se llevará a cabo mediante un agente distribuido a los activos de infraestructura requeridos por el Instituto. El proveedor será responsable de asegurar la entrega de dicho agente a los activos de infraestructura especificados por el Instituto. La distribución y administración del agente puede llevarse a cabo tanto en entornos locales (on-premise) como en la nube.

El proveedor deberá tener en cuenta que las actividades de remediación de infecciones por virus serán de su responsabilidad. Por lo tanto, deberá brindar el apoyo necesario mediante la utilización de las funcionalidades proporcionadas por la solución antivirus propuesta como parte del servicio actual. Además, el proveedor deberá notificar al personal designado por el Instituto sobre cualquier actividad sospechosa detectada, ya sea a través de correo electrónico u otro medio acordado por ambas partes. Asimismo, deberá ocuparse de atender los incidentes de *malware* según lo estipulado en los Acuerdos de Nivel de Servicio o los Acuerdos de Nivel Operativo.

En el caso de que la instalación requerida por el Instituto supere los 200 agentes, el proveedor, en colaboración con el Instituto, deberá establecer una estrategia para implementar el agente antivirus y garantizar la actualización de este en todos los activos de infraestructura solicitados, sin que ello afecte el funcionamiento del Instituto. Es importante considerar que estos activos y consolas de administración podrán estar distribuidos en diferentes localidades del Instituto.

El proveedor deberá configurar las políticas de seguridad base en la solución antivirus propuesta, las cuales se definirán en conjunto con el Instituto como parte de las reglas que regirán el servicio. Estas políticas deberán ser desplegadas en los activos de infraestructura correspondientes a través de la consola de administración de la solución. Además, el proveedor deberá ajustar estas políticas según sea necesario, basándose en el monitoreo continuo de la solución y en los requerimientos del Instituto.

Se requerirá que el proveedor y el Instituto definan una estrategia para la entrega de actualizaciones de antivirus en todos los activos de infraestructura, asegurando que no se vean afectadas las operaciones de los servicios internos, los cuales están distribuidos en diferentes localidades a nivel nacional. El proveedor será responsable de mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus proporcionada por el fabricante.

Además, el proveedor, en colaboración con el Instituto, determinará la cantidad de activos de infraestructura que constituirán la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio, se llevará a cabo una redefinición de esta línea base para el próximo año.

El proveedor deberá suministrar al personal del Instituto la última versión del agente de antivirus para su integración en la imagen de software de los Puestos de Servicio.

Como parte de la operación del presente servicio, el proveedor deberá:

•Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antivirus.

•Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.

•Notificar sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.

•Notificar sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de estas a través de la solución propuesta.

•Resolver las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.

•Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y el proveedor.

•Desarrollar la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

# iv.2.8 Servicios de Prevención de Pérdida de Información

**Descripción del servicio:** El Instituto requiere una solución para detectar y prevenir la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS ubicados en los Centros de Datos. Esta solución debe estar integrada con los activos de infraestructura, el servicio de correo electrónico externo, el correo electrónico interno, la navegación web y los portales de colaboración, lo que permitirá una visión completa y una prevención efectiva en múltiples capas de seguridad.

El módulo debe tener la capacidad de establecer políticas mediante el uso de palabras clave o expresiones regulares que identifiquen información sensible, bloqueando su transmisión a través de diferentes canales de comunicación.

El servicio se enfocará en prevenir la fuga de información sensible desde los puestos de servicio.

El proveedor deberá configurar en la solución propuesta las políticas base de seguridad definidas en colaboración con el Instituto, adaptándolas a los activos de infraestructura y creando los perfiles correspondientes.

Estas políticas se desplegarán a través de la consola de administración de la solución, y el proveedor será responsable de ajustarlas mediante un proceso de puesta a punto continuo, basado en su monitoreo constante y los requisitos específicos del Instituto. Para este fin, el Instituto requiere que se tomen en consideración, al menos, las siguientes premisas:

• **Tipos de documentos:** Este apartado abarca las diversas formas en que se pueden estructurar los activos de información relevantes para los procesos del Instituto. Incluyen, entre otros, reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos y otros documentos similares.

• **Medios de almacenamiento de la información:** Este apartado hace referencia a los diferentes medios disponibles para resguardar los activos de información con el propósito de manipularlos en el futuro.

El proveedor deberá garantizar que las funcionalidades de la Solución de Prevención de Pérdida de Información se cumplan incluso si el activo de infraestructura no está asociado a ningún Directorio Activo o a la red del Instituto.

En el marco de la operación del servicio, el proveedor deberá:

• Emitir alertas de incidentes y vigilar los eventos generados por los componentes tecnológicos de la solución de Prevención de Pérdida de Información.

• Supervisar el cumplimiento de las políticas de uso de la información establecidas en la solución.

• Informar al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas de fuga de información configuradas en los activos de infraestructura.

• Implementar medidas de contención ante actividades sospechosas.

• Atender las solicitudes de soporte técnico especializado para prevenir fugas de información en los equipos donde esté habilitada la solución.

• Recopilar e integrar, al menos, la información de eventos de seguridad o registros generados por la solución de Prevención de Pérdida de Información en la solución de correlación de eventos, cuyo alcance será definido entre el Instituto y el proveedor.

• Gestionar los componentes tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones según los requisitos del Instituto.

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

•Presentar un registro de auditoría que contenga todas las actividades realizadas por los usuarios.

• Ofrecer reportes predefinidos y personalizados que puedan ser programados o generados de manera puntual.

• Disponer de un mecanismo de alertas y notificaciones.

• Tecnología de Detección:

* Capacidad para extraer texto de diversos tipos de documentos para llevar a cabo análisis de contenido.
* Habilidad para realizar detecciones basadas en palabras clave o frases clave personalizadas, con la capacidad de combinar múltiples palabras en una sola regla de detección.

• Capacidad para realizar análisis de contenido en varios canales de información (correo electrónico, HTTPS/HTTP, FTP, entre otros).

• Permitir la creación de reglas de políticas basadas en los identificadores de hardware (Vendor ID - VID y Product ID - PID) y clases de dispositivos para permitir, bloquear o restringir su uso dentro de la sesión virtual.

• Perfiles de Acceso a Medios de Almacenamiento: Se requiere la capacidad técnica para configurar el comportamiento de los puertos USB de almacenamiento masivo en tres niveles diferenciados según el perfil del usuario o del equipo:

1. Bloqueo Total: Denegación de montaje de unidades USB.

2. Acceso de Solo Lectura: Permitir la lectura de archivos desde el USB hacia el entorno virtual, pero bloqueando técnicamente cualquier intento de escritura o exfiltración de datos hacia el dispositivo USB.

3. Acceso de Lectura y Escritura: Habilitado exclusivamente para personal autorizado mediante excepción y doble factor de autenticación.

• Soporte para Dispositivos Médicos y de Digitalización: Capacidad de redirección optimizada (canales virtuales dedicados) y genérica (redirección USB a bajo nivel) para periféricos especializados como escáneres documentales, impresoras térmicas, lectores de tarjetas inteligentes y dispositivos de diagnóstico médico conectados vía USB, garantizando su funcionamiento nativo dentro de la sesión virtual.

• Integrar capacidades de prevención de fuga de datos (DLP) con un sistema avanzado de Grabación y Auditoría de Sesiones (Session Recording) que permita la vigilancia proactiva de vectores de riesgo, específicamente en puertos periféricos:

• Permitir detectar, registrar y alertar en tiempo real sobre la inserción de dispositivos de almacenamiento masivo en los equipos terminales que interactúan con la infraestructura institucional.

• Iniciar automáticamente la grabación visual de la sesión del usuario o marcar el evento en la línea de tiempo de la grabación, permitiendo a los auditores revisar exactamente qué archivos fueron accedidos o transferidos durante el periodo de conexión del dispositivo.

• Generar bitacoras de auditoría detallados que identifiquen el usuario, el dispositivo terminal, el ID del dispositivo USB conectado y los nombres de los archivos transferidos entre el entorno virtual y el medio físico, asegurando la cadena de custodia de la evidencia digital.

• Inspeccionar o sanitizar el tráfico de datos proveniente de dispositivos USB antes de que interactúe con la red central, previniendo la inyección de malware a través de memorias portátiles.

# iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)

El servicio tiene como objetivo asegurar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), el cual debe estar alineado con el estándar ISO/IEC 27001:2022. Este sistema se encargará de emitir directivas relacionadas con la seguridad de la información tanto a las áreas de TI como a los terceros responsables de apoyar la operación de TI. Es fundamental que este servicio sea adaptable a las actualizaciones necesarias para mantener la conformidad con las últimas versiones y requisitos normativos.

El proveedor del servicio deberá garantizar la continuidad operativa del mismo, ofreciendo al menos las siguientes funcionalidades operativas:

El MGSI del IMSS se concibe como un sistema vivo, evolutivo y transversal, habilitador del gobierno digital, el gobierno de datos, la adopción segura de nube e IA, y la interoperabilidad con la ATDT.

**Capacitación de seguimiento**: Se llevará a cabo un curso de "Inducción a la norma NIST y MERT o la versión vigente", con el objetivo de proporcionar a los participantes las habilidades necesarias para:

* Se de generar con base en todo lo que sea aplicable al IMSS
* Se contempla la participación de al menos 8 personas, con una duración mínima de 8 horas y máxima de 40 horas.

**Seguimiento y actualización en la aplicación de las directivas en materia de seguridad:**

Revisión y actualización de la Política de Seguridad de la Información que cumplirá con los siguientes criterios:

* Cubrir los dominios establecidos por la norma ISO/IEC 27001:2022., NIST, MERT y verificar que cumpla con la ATDT.
* Incluir los procesos de seguridad aplicables según la normativa actual.
* Generar y desarrollar el catálogo detallado de las Infraestructuras críticas del Instituto
* Estar dirigido tanto a las áreas de TI como a los terceros que prestan servicios de TI al Instituto, abordando al menos 20 directivas relacionadas con el catálogo de infraestructuras críticas del Instituto.

**Identificación y evaluación de activos (relacionados con el catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información.**

La metodología que seguir deberá contemplar los siguientes aspectos:

* Identificación de los activos del proceso.
* Valoración de los activos del proceso.
* Identificación de los requisitos de seguridad.
* Identificación de los controles de seguridad existentes.

**Generación de la Declaración de Aplicabilidad (SoA: Statement of Applicability).**

La metodología deberá abordar los siguientes aspectos:

* Identificación y evaluación de la aplicabilidad de los requerimientos internos y externos.
* Selección de los objetivos de control y los controles para mitigar los riesgos.
* Verificación de los requisitos contractuales y legales.
* Identificación de los requisitos internos y externos pertinentes.
* Validación de la aplicabilidad de los requisitos identificados.
* Elaboración del Formato de Autorización para la implementación y operación del Sistema de Gestión de Seguridad de la Información.
* Preparación de la Declaración de Aplicabilidad.
* Documentación de los objetivos de control, los controles seleccionados y la justificación de su elección.
* Documentación de los controles actualmente implementados.
* Documentación de la exclusión de controles y la justificación de dicha exclusión.

**Operación del Sistema de Gestión de Seguridad de la Información**

* Análisis de Riesgos de Seguridad de la Información
* Análisis de riesgos basado en el servicio definido de gestión de riesgos de seguridad.
* Generación y actualización del plan de tratamiento de riesgos.

La metodología debe considerar los siguientes aspectos:

* Identificación de las acciones a realizar por parte de la institución y su administración.
* Identificación de los recursos necesarios y establecimiento de prioridades.
* Asignación de responsabilidades para la gestión de riesgos de seguridad de la información.

**Aplicación del seguimiento al plan de tratamiento de riesgos.**

La metodología deberá considerar los siguientes aspectos:

* Asignación de roles y responsabilidades para supervisar los controles relacionados con personas, procesos y tecnología involucrados en la mitigación de los riesgos.
* Actualización de la documentación, conforme a los requisitos establecidos en la normativa vigente.

**Detalle y actualización de políticas y procedimientos de seguridad existentes**

**Definición del proceso de reporte y atención de incidentes de seguridad**

**Propuestas de implementación de los controles.**

La metodología deberá abordar los siguientes temas:

* Actualización de los controles de seguridad internos alineados a ISO27000:2022, NIST, MERT y verificar que cumpla con la ATDT
* Implementación de nuevos controles de seguridad para la Inteligencia Artificial, Gobierno de Datos y la nube
* Control de accesos.
* Monitoreo de cuentas.
* Definición del proceso de Continuidad del Negocio.
* Implementación de los roles y responsabilidades definidos para el Sistema de Gestión de Seguridad de la Información.
* Controles de seguridad en la infraestructura tecnológica, conforme a lo establecido en el alcance.

**Gestión del cambio cultural.**

La metodología debe abordar los siguientes aspectos:

* Actualización del Programa de Concientización dirigido a usuarios y operadores del Sistema de Gestión de Seguridad de la Información.
* Seguimiento y apoyo a las necesidades de capacitación del personal encargado de administrar el Sistema de Gestión de Seguridad de la Información y de la seguridad de la información.
* Elaboración o actualización del Manual de Gestión de Seguridad de la Información. Este manual deberá incluir las referencias generadas en esta fase para garantizar la trazabilidad de las cláusulas de la norma.

**Monitoreo y revisión del Sistema de Gestión de Seguridad de la Información.**

La metodología deberá abordar los siguientes aspectos:

* Los responsables del proceso deben realizar una revisión y actualización del Sistema de Gestión de Seguridad de la Información para garantizar que los objetivos de este sistema estén alineados con los objetivos de negocio en materia de seguridad de la información, y que aseguren el manejo adecuado de los riesgos existentes.
* El proveedor debe actualizar el procedimiento de las revisiones gerenciales.
* Asimismo, el proveedor deberá actualizar los formatos necesarios para llevar a cabo las revisiones gerenciales.

**Revisiones internas.**

La metodología deberá abarcar lo siguiente:

Revisión de sistemas institucionales

* Elaboración de formatos de auditoria para los sistemas críticos del Instituto
* Elaboración de plan de revisiones internas.
* Apoyo en la programación de reuniones
* Reporte final

Revisiones internas para el SGSI

* Seguimiento y apoyo en la elaboración del plan de auditorías internas para las áreas de TI y para los terceros que proporcionan servicios de TI al Instituto.
* Actualización o, en su caso, definición de los formatos necesarios para llevar a cabo las auditorías.
* Ejecución de una auditoría interna del Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2022, NIST, MERT y verificar que cumpla con la ATDT o la normativa vigente, así como con los procesos establecidos en la normativa aplicable.

**Actualización del Sistema de Gestión de Seguridad de la Información e Implementación de**

**Mejoras**

Deberá considerar los siguientes aspectos:

* Priorización de las acciones correctivas y de las no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas.
* Identificación de los responsables encargados de llevar a cabo las mejoras.
* El Instituto establecerá fechas de compromiso para la finalización de las mejoras, exclusivamente para seguimiento interno.

**Acciones Correctivas y No Conformidades**

Deberá tener en cuenta lo siguiente:

* Apoyo en la definición y seguimiento del procedimiento para llevar a cabo acciones correctivas y atender no conformidades derivadas de las auditorías.
* Actualización del formato para el registro de acciones correctivas y no conformidades.
* Coordinación de la ejecución de las acciones correctivas ya definidas y, en caso necesario, de las no conformidades identificadas.

**Comunicación de los Resultados de las Acciones Tomadas**

Se deberán considerar los siguientes puntos:

* Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información, con el fin de informar sobre el alcance de las acciones correctivas y las no conformidades abordadas, y verificar su cumplimiento con los requisitos de los propietarios de la información y de los involucrados en los procesos del Instituto.

# iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información

**Descripción del Servicio:** El Instituto requiere la implementación de un programa de gestión del cambio para fortalecer la protección de la información, en consonancia con los requisitos del estándar ISO/IEC 27001:2022, mediante una estrategia cultural.

Este servicio deberá incluir un plan exhaustivo de transferencia de conocimientos al personal del Instituto sobre los principales aspectos de seguridad de la información, abarcando al menos los siguientes ámbitos:

* + Regulación actual en materia de seguridad de la información.
  + Políticas de seguridad específicas del Instituto.
  + Procesos relacionados con la seguridad en el Instituto.
  + Controles de seguridad implementados en el Instituto.

El servicio se estructura en las siguientes etapas:

**Etapa 1: Definición de la Estrategia de Gestión del Cambio**

* Contextualización del Instituto: El proveedor deberá comprender el contexto cultural del Instituto en lo que respecta a la seguridad de la información.
* Diagnóstico del Estado Actual: El proveedor realizará un análisis para evaluar el nivel de conocimiento existente en seguridad de la información, identificando las brechas entre la situación actual y los requisitos establecidos por el Instituto.
* Preparación de la Estrategia: Basándose en los resultados del diagnóstico, el proveedor propondrá una estrategia de gestión del cambio en seguridad de la información para facilitar una transferencia efectiva de conocimientos.

**Etapa 2: Diseño del Programa de Gestión del Cambio**

* Preparación del Programa: El proveedor elaborará un plan de trabajo detallado que incluirá los temas a abordar en la transferencia de conocimientos, el número de personal involucrado y las fechas de implementación.
* Elaboración de Contenidos: El proveedor desarrollará materiales en formato PowerPoint u otros definidos por el Instituto, que serán utilizados para la transferencia de conocimientos en seguridad de la información.
* Creación del Modelo de Evaluación: El proveedor presentará un modelo de evaluación destinado a medir la efectividad de la transferencia de conocimientos en seguridad de la información.
* Preparación del Grupo de "Train the Trainers": El proveedor identificará y preparará a un grupo de 5 facilitadores con el fin de que puedan replicar la transferencia de conocimientos en otras áreas clave dentro del Instituto.

**Etapa 3: Comunicación del Programa de Gestión del Cambio**

* Implementación de la Transferencia: El proveedor ejecutará la transferencia de conocimientos al personal de Tecnologías de la Información del Instituto y a las áreas definidas por este, ubicadas en la Ciudad de México.

**Etapa 4: Medición del Programa de Gestión del Cambio**

* Implementación de Evaluaciones: El proveedor pondrá en marcha una herramienta tecnológica para realizar evaluaciones en línea a los participantes de la transferencia de conocimientos.
* Análisis de Datos: El proveedor analizará la información recopilada para organizar los resultados obtenidos.
* Presentación de Resultados: El proveedor llevará a cabo una presentación ejecutiva ante el personal de Tecnologías de la Información del Instituto, en la que se expondrán los resultados generales obtenidos.

# iv.3 Servicios del Centro de Operaciones de Seguridad (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de Seguridad (SOC) que esté físicamente ubicado en las instalaciones del proveedor. El propósito de este centro deberá ser garantizar la continuidad operativa y gestionar la seguridad, así como encargarse de la administración, operación, monitoreo, soporte y resolución de fallas de los componentes de las soluciones de seguridad. Esto implica llevar a cabo actividades como revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, y establecimiento de acciones para mejorar de manera sostenible.

El servicio del Centro Operaciones de Seguridad (SOC), que respaldará la operación y prestación del servicio requerido por el Instituto debe ofrecer un control continuo, mayor eficiencia y oportunidad de mejora. Para lograr esto, el licitante debe proporcionar servicios de tecnología de la información confiables en lo que respecta a la gestión de servicios de TI. Estos servicios deben estar respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes, en caso de presentar una propuesta de participación individual o conjunta.

El licitante deberá tener en cuenta que el servicio de SOC se refiere a las soluciones propuestas e implementadas actualmente por el instituto. Además, deberá considerar que la correlación de bitácoras se basará en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso deben ser ilimitados. Asimismo, las respuestas a incidentes deben estar alineadas con los niveles de servicio (SLA) establecidos para este servicio, garantizando tiempos de respuesta adecuados.

El Centro de Operaciones de Seguridad (SOC) debe estar ubicado en el territorio nacional, lo cual se puede verificar con una copia simple de las certificaciones ISO/IEC27001:2022 e ISO/IEC20000-1:2018 a nombre del proveedor participante. Este SOC deberá cumplir con las siguientes especificaciones:

* Funcionamiento continuo las 24 horas del día, los 7 días de la semana, los 365 días del año (7x24x365), de acuerdo con lo establecido en el contrato.
* Disponibilidad de personal cualificado para brindar atención tanto en el lugar como de forma remota, con las credenciales necesarias para administrar y monitorear los componentes de la solución.
* Operación en un centro de datos alternativo ubicado en el territorio nacional.
* Mantenimiento de suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información para detectar nuevas vulnerabilidades.
* Infraestructura dedicada para la gestión, operación y monitoreo de los componentes de hardware y software de los servicios de seguridad.
* Ejecución de evaluaciones operativas a los servicios (software y activos de infraestructura) cada 3 meses desde el inicio de operaciones y hasta 3 meses antes de la finalización de estos, con el fin de identificar mejoras en el rendimiento, la gestión de configuraciones y nuevas funcionalidades.
* Implementación de acciones correctivas y preventivas para garantizar la confidencialidad, integridad y disponibilidad de la información manejada en las soluciones de seguridad.
* Envío de notificaciones y alertas personalizadas en caso de desviaciones, anomalías o brechas de seguridad para cada solución de seguridad.
* Revisiones continuas de la operación del SOC para mejorar procesos, procedimientos y controles de seguridad.
* Análisis de eventos de seguridad y registros de administración integrados en los servicios de correlación de información para establecer acciones preventivas mediante modificaciones en las configuraciones de las soluciones de seguridad.
* Integración de un Equipo de Atención y Respuesta a Incidentes de Seguridad.
* Soporte y atención a fallas de los componentes de hardware y software de la solución según lo establecido en los acuerdos de niveles de servicio.
* Monitoreo de la disponibilidad de los componentes hardware y software de la solución, con capacidad para generar alertas y notificaciones en caso de fallos, degradación del rendimiento, intermitencia o pérdida de disponibilidad.
* Mantenimiento preventivo y correctivo de las soluciones de seguridad habilitadas y los activos de infraestructura que respaldan cada servicio.
* Ejecutar procesos operativos para al menos los siguientes rubros:
* Gestión de Riesgos
* Gestión de Continuidad
* Monitoreo y Detección
* Gestión de Seguridad de la información
* Administración de Dispositivos
* Gestión de solicitudes de servicio
* Administración de Cambios Operacionales
* Administración de Configuraciones
* Administración de Vulnerabilidades
* Gestión de Incidentes
* Gestión de Problemas

• Integración de una Mesa de Servicio conforme a las prácticas de ITIL v4, la cual deberá ser compatible con la Mesa de Servicios Tecnológicos del Instituto. Esta integración debe abarcar todas las actividades relacionadas con la configuración, desarrollo de software, ajustes, y otras tareas necesarias para facilitar la comunicación y el intercambio de requerimientos, cambios, incidentes y otros procesos determinados por el Instituto.

• El servicio de gestión de requerimientos, cambios, incidentes y otras solicitudes deberá permitir la creación de eventos (tickets) a través de los mecanismos definidos en las mesas de trabajo correspondientes, los cuales incluyen, de manera ejemplificativa pero no limitativa:

* Un número telefónico directo en las instalaciones del SOC.
* Un número telefónico de diez dígitos.
* Correo electrónico.
* Portal web.

• El Instituto se reserva el derecho de solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento durante la vigencia del contrato, con el fin de asegurar la entrega adecuada del servicio.

• Supervisión de la Base de Datos de la Gestión de la Configuración (CMDB, por sus siglas en inglés), la cual contendrá los detalles pertinentes de cada elemento de configuración (CI) y sus relaciones, abarcando equipos físicos, software, y las interconexiones entre incidencias, problemas, cambios y demás datos del servicio de seguridad.

• Generación de informes de Inteligencia de Negocios y Análisis de Información para obtener estadísticas sobre el uso y rendimiento de los servicios de seguridad. Esto tiene como objetivo respaldar la toma de decisiones estratégicas y operativas, así como determinar el plan de capacidad para cada tecnología implementada. Estos informes pueden incluir, entre otros datos, lo siguiente:

* Estadísticas de utilización de procesamiento por tecnología.
* Estadísticas de rendimiento por tecnología (throughput).
* Estadísticas de ataques informáticos bloqueados.
* Estadísticas de comportamientos típicos esperados por tecnología (líneas base).
* Estadísticas de usuarios concurrentes por servicio.
* Estadísticas de crecimiento diario, mensual y anual para cada servicio.

• Facilitar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como proporcionar herramientas de software que permitan acceder a estas consolas (ya sea mediante aplicaciones cliente-servidor, portales web u otros medios disponibles). Estas cuentas deberán tener únicamente permisos de lectura, y los atributos de consulta se definirán en las reuniones establecidas con ese fin.

• Las consolas de administración proporcionadas para los servicios de seguridad deberán permitir visualizar, como mínimo:

* Políticas: Control de Acceso.
* Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas Negras), Líneas Base de Seguridad.
* Objetos: Usuarios, Grupos, Direcciones IP.
* Bitácoras.
* Estadísticas en Tiempo Real: Desempeño, Procesamiento, Usuarios Conectados, Conexiones por Segundo, Ancho de Banda Utilizado.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio. Estas bases de datos deben contener información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licencias adquiridas para cada servicio proporcionado, y cualquier otra información relevante que facilite la toma de decisiones con respecto al uso de los servicios de seguridad.

• Implementar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad, independiente de las consolas de administración y herramientas de monitoreo. Este tablero proporcionará información estratégica en tiempo real y de manera histórica sobre el uso de los servicios, permitiendo al Instituto obtener una visión general del rendimiento de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información pertinente para la toma de decisiones sobre las condiciones operativas de los servicios. El licitante deberá incluir en su oferta económica los costos asociados al desarrollo para cumplir con este requisito.

• Habilitar al personal designado por el administrador del contrato para generar reportes haciendo uso de todas las variables y funcionalidades de la herramienta de monitoreo. Se proporcionará la opción de parametrizar estos reportes y acceder a ellos a través de una interfaz web.

• Habilitar servicios de supervisión a través del Centro de Operaciones del Instituto en el cual se integren los siguientes rubros:

* Pantallas Multiples (Videowall) donde se observen entre otros los siguiente:
  + Monitoreo de estado de salud de las plataformas tecnológicas provistas en el contrato (disponibilidad, desempeño, alertas por falla o malfuncionamiento de aplicaciones, entre otros)
  + Monitoreo de evento e incidentes de seguridad en tiempo real y con manejo de información histórica de al menos 1 año
  + Monitoreo de eventos e incidentes de Riesgos Digitales que muestren posibles tendencias de ataque, así como patrones anómalos de tráfico.
  + Monitore de eventos de hacktivismo, así como de daño reputacional por suplantación de identidad, información comprometida
* Equipos de cómputo de propósito especifico que interactúen con las pantallas múltiples (Videowall) para gestionar las consolas de acceso de las diferentes tecnologías.
* Personal en sitio que coadyuve en la supervisión realizada por el Centro de Operaciones del proveedor y del IMSS, mismo que podrá designarse de los recursos humanos solicitados para la gestión y atención de todas las tecnologías, así como de los operadores de primer nivel.

**Partida 2**

# iv.4 Servicios de Seguridad – Análisis y Pruebas de Seguridad

# iv.4.1 Servicios de Análisis de Vulnerabilidades Dinámico

**Descripción del servicio:** El Instituto requiere asegurar la continuidad operativa de un servicio que permita llevar a cabo análisis técnicos especializados sobre los activos de infraestructura de procesamiento, redes, sistemas y aplicaciones, con el objetivo de identificar vulnerabilidades nuevas o conocidas. Por tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

* Integrar las tareas necesarias para ejecutar análisis de vulnerabilidades en los centros de datos especificados por el Instituto, así como en otras ubicaciones según sea necesario.
* Realizar el seguimiento de los reportes utilizando las herramientas disponibles para complementar los análisis de vulnerabilidades realizados.
* Renovar el licenciamiento del *software* necesario para continuar con los servicios y activos de infraestructura pertinentes.
* Garantizar que las herramientas de análisis de vulnerabilidades cuenten con la última versión liberada, estable y validada por el fabricante, así como otros componentes necesarios para el servicio.
* Identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
* Identificar vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
* Identificar configuraciones por omisión.
* Tener la capacidad para evaluar el grado de vulnerabilidad ante técnicas de ataque como SQL injection, Cross Site Scripting, Cross Site Request Forgery, Sensitive Data Exposure, Security Misconfiguration, y Broken Authentication and Session Management.
* Elaborar un reporte ejecutivo y técnico para cada requerimiento atendido, describiendo los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP denominada "OWASP Risk Rating Methodology", e incluyendo recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
* Implementar un proceso y/o procedimiento para garantizar la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
* Integrar un mecanismo operativo para llevar a cabo el proceso de remediación conforme a las vulnerabilidades reportadas, incluyendo personal especializado para las plataformas operativas y herramientas de software identificadas.
* Integrar un tablero que contenga las vulnerabilidades detectadas, descripción, clasificación de criticidad e impacto de cada vulnerabilidad (CVE, CVSS, u otros marcos de clasificación), que permitan relacionarlo con cada aplicativo, sistemas o activo de información que haya sido sometido verificación de seguridad.

# iv.4.2 Servicios de Análisis de Vulnerabilidades Estático

**Descripción del servicio:** El Instituto busca evaluar el nivel inicial de madurez de sus prácticas de seguridad en el software y requiere un proveedor que cumpla con las siguientes especificaciones funcionales mínimas:

* Implementar una solución tecnológica centralizada que permita realizar pruebas dinámicas y estáticas, con soporte para los lenguajes de programación como HTML, Java, .Net, C#, PHP.
* Integrar el licenciamiento del software necesario, incluyendo renovaciones durante la vigencia de los servicios.
* Garantizar el uso de las últimas versiones estables y validadas de las herramientas propuestas, así como de otros componentes necesarios.
* Incorporar un proceso de evaluación de las prácticas existentes de seguridad de software en el Instituto.
* Desarrollar un programa de evaluación de seguridad de software con iteraciones definidas en conjunto con el Instituto.
* Actualizar y establecer procesos en las diferentes etapas del ciclo de vida de desarrollo de software para garantizar la seguridad de este.
* Asistir en el cumplimiento de estándares y marcos normativos previamente definidos.
* Identificar el nivel inicial de madurez de las prácticas de seguridad en el software del Instituto.
* Comprender el entorno del Instituto, incluyendo personal, normativas y tecnologías relevantes, para diseñar el modelo de operación y flujos de interacción necesarios.
* Integrar las mejores prácticas de seguridad en el software, alineadas con OpenSAMM.
* Transferir las prácticas de seguridad en el software implementadas al personal designado por el Instituto.
* Operar el modelo de madurez establecido, certificando el nivel de cumplimiento del software evaluado en tres etapas: al inicio, durante y posterior al desarrollo de una aplicación.
* Preservar la integridad y confidencialidad de la información recibida durante las pruebas.
* Elaborar un reporte ejecutivo y técnico por cada requerimiento atendido, detallando los riesgos asociados a cada hallazgo o vulnerabilidad identificada, así como recomendaciones y acciones específicas para remediarlas.

# iv.4.3 Servicios de Pruebas de Penetración

**Descripción del servicio:** El Instituto requiere mantener un servicio que asegure un proceso sistemático para verificar las vulnerabilidades de las aplicaciones y la infraestructura que las respaldan, con el objetivo de detectar posibles brechas o fallos en la seguridad. Para cumplir con este propósito, el proveedor deberá atender las siguientes especificaciones funcionales mínimas:

* Integrar todas las actividades necesarias para ejecutar pruebas de penetración en los centros de datos designados por el Instituto, así como en otras ubicaciones según sea necesario.
* Realizar un seguimiento detallado de los servicios o activos de información que se someterán a análisis, incluyendo la cantidad de equipos involucrados y las versiones de las plataformas de los sistemas examinados.
* Identificar vulnerabilidades y configuraciones incorrectas.
* Explotar posibles accesos a los sistemas aprovechando las brechas de seguridad y/o vulnerabilidades detectadas.
* Evaluar vulnerabilidades en áreas como autenticación y autorización, gestión de sesiones, inyección de código, criptografía, ataques lógicos, protección de datos y divulgación de información.
* Evaluación de vulnerabilidades de al menos los siguientes ámbitos:

- Autenticación y Autorización

* Intentos ilimitados de inicio de sesión
* Insuficiente autenticación
* Insuficiente autorización

- Gestión de sesión

* Predicción de sesión
* Secuestro de sesión
* Reproducir sesión
* Expiración de sesión insuficiente

- Inyección de código

* Inyección comando de Sistema Operativo
* Inyección SQL
* Cross-site Scripting
* Inyección LDAP
* Inyección HTML
* Parameters Tampering
* Cookie Poisoning
* Hidden Field Manipulation

- Criptografía

* Fortaleza del algoritmo
* Gestión de llaves

- Ataques Lógicos

* Abuso de funcionalidades
* Input Field Validation Checking

- Protección de Datos

* Transporte
* Almacenamiento

- Divulgación de Información

* Indexado de directorio
* Path Traversal
* Manejo inseguro de errores
* Comentarios HTML
* Elaborar informes ejecutivos y técnicos para cada requisito atendido, utilizando la metodología de cálculo de riesgos de OWASP, detallando los riesgos asociados a cada vulnerabilidad identificada y proporcionando recomendaciones y acciones específicas para su corrección.
* Implementar un proceso o procedimiento para garantizar la continuidad de las medidas de remediación y las recomendaciones derivadas de cada revisión realizada.
* Establecer un mecanismo operativo para llevar a cabo el proceso de remediación de acuerdo con las vulnerabilidades reportadas, incluyendo personal especializado en las plataformas operativas y herramientas de software identificadas.
* Integrar un tablero que contenga las vulnerabilidades detectadas, descripción, clasificación de criticidad e impacto de cada vulnerabilidad (CVE, CVSS, u otros marcos de clasificación), que permitan relacionarlo con cada aplicativo, sistemas o activo de información que haya sido sometido verificación de seguridad.

# iv.4.4 Servicios de Análisis Forense

**Descripción del servicio:** El Instituto requiere la continuidad de un servicio de análisis de incidentes de seguridad para determinar y documentar, mediante la integración de registros o bitácoras, las evidencias o indicios de eventos y su relación temporal. Este análisis debe identificar cuándo ocurrió un incidente, qué infraestructura, servicios tecnológicos o sistemas de información se vieron comprometidos, cómo se llevó a cabo y quién o qué estuvo relacionado con el incidente, así como el impacto del evento. Para cumplir con estos objetivos, el proveedor deberá satisfacer las siguientes especificaciones funcionales mínimas:

* Integrar las tareas necesarias para llevar a cabo análisis forenses en los centros de datos designados por el Instituto, así como en otras ubicaciones según sea necesario.
* Continuar con la definición de objetivos, parámetros y cuestionarios relevantes para cada investigación solicitada.
* Mantener un seguimiento continuo de los casos solicitados y registrar los indicadores correspondientes.
* Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense, asegurando una cadena de custodia adecuada.
* Participar en entrevistas con los principales involucrados para obtener el contexto necesario en las investigaciones digitales.
* Obtener información de fuentes públicas en la red, si es relevante para la investigación realizada.
* Realizar evaluaciones de información en diversos dispositivos y equipos, como computadoras, servidores físicos y virtuales, dispositivos móviles y equipos de comunicaciones, para identificar indicios de compromiso y su evidencia correspondiente.
* Llevar a cabo un proceso de recuperación de información que haya sido borrada previamente.
* Mantener y dar seguimiento a una herramienta colaborativa diseñada para facilitar la visualización de hallazgos a los usuarios finales, así como para generar informes de hallazgos cuando sea necesario.
* Elaborar un dictamen técnico para cada requerimiento atendido, con la información identificada en los procesos de análisis forense, generando y firmando documentos que expresen los resultados de la investigación de manera clara y concisa, para que puedan ser comprendidos por aquellos que no dominan el lenguaje técnico.

# iv.5 Servicios de Transferencia de Conocimiento

Descripción del Servicio: El Instituto busca un servicio de transferencia de conocimiento que fortalezca la comprensión y ejecución de los procesos operativos del proveedor de servicios, capacitando a 10 personas por sesión. El objetivo es facilitar la mejora continua de cada servicio implementado.

Transferencia Tipo Certificación

Se debe incluir en la propuesta técnica la iniciativa de entrenamiento presencial para los usuarios de la Dirección de Innovación y Desarrollo Tecnológico, considerando las unidades de entrenamiento del proyecto. Los cursos de "Entrenamiento Certificado", que incluyen la impartición de cursos con certificación, deben ser ofrecidos al menos una vez al año durante todo el periodo del contrato por instructores certificados del fabricante.

El proveedor deberá proporcionar instalaciones que cumplan con las características necesarias para realizar un entrenamiento cómodo y satisfactorio. Además, se debe garantizar la disponibilidad de infraestructura como proyectores, equipos, material didáctico, facilitadores y todo lo necesario para asegurar que el entrenamiento sea interactivo y completo.

Al finalizar la transferencia, cada participante deberá recibir una certificación oficial emitida por el fabricante del equipo o una empresa certificada, que acredite su asistencia al curso y, según corresponda, la aprobación del examen correspondiente. En esta modalidad, se deben considerar al menos los siguientes puntos:

* Los componentes de infraestructura y seguridad propuestos por el proveedor en cada uno de sus aspectos.
* Las herramientas y metodologías de las diversas soluciones de servicios proporcionadas según lo establecido en este anexo.

Esta certificación garantizará que los participantes adquieran los conocimientos y habilidades necesarios en la implementación y mantenimiento de las soluciones propuestas.

Transferencia Tipo Entrenamiento Especializado

El Instituto también solicita que se incluya entrenamiento especializado para preparar al personal operativo en conocimientos avanzados de seguridad de la información. Por lo tanto, el Proveedor deberá ofrecer un programa de formación certificado que cubra habilidades y conocimientos sobre seguridad de la información, incluyendo, entre otros, los siguientes aspectos:

* Certificación “Security Management ISO 27001:2013”.
* Certificación “CISSP”.
* Certificación “CISA”.
* Métodos de auditoría forense (GCFA o CHFI o CEH).
* Certificación CRISC.
* Certificación CGEIT.
* Certificación CBCP.
* Certificación CISM.

Este entrenamiento deberá ser provisto por personal especializado.

# Perfil del Proveedor

El licitante deberá demostrar la capacidad y competencia técnica certificada para implementar y operar soluciones de seguridad, asegurando su correcto funcionamiento en los sitios requeridos por "EL INSTITUTO". Para cumplir con este requisito, se solicita presentar una copia simple del acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas, de acuerdo con las características y especificaciones establecidas en el presente Anexo Técnico.

El personal responsable de las operaciones de los servicios de seguridad debe contar con experiencia demostrada en tecnología y seguridad de la información. Para cumplir con este requisito, se solicita la presentación de los currículos vitae de todos los recursos humanos involucrados en el servicio, los cuales deben incluir al menos:

* Experiencia profesional: Se evaluarán todos los puestos anteriores de cada miembro del equipo, detallando las fechas, nombres de los empleadores, títulos de los puestos y las responsabilidades asociadas. Se exigirá una experiencia mínima comprobada de tres años.
* Experiencia en proyectos especializados en Seguridad de la Información: Se deberán mencionar y describir todos los proyectos en los que el personal haya participado, con una experiencia comprobada mínima de tres años en esta área.
* Estudios: Se registrarán todos los estudios relacionados con la seguridad de la información, así como las certificaciones vigentes a la fecha de presentación de la propuesta técnica. Se requerirán certificaciones de tecnología y/o seguridad de tipo "vendor-neutral".
* Estructura del equipo de trabajo: Se proporcionará una descripción de la estructura del grupo de trabajo, detallando las responsabilidades y competencias de cada perfil.
* Los servicios ofrecidos por el o los licitantes deberán estar respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes, en caso de presentar una propuesta de participación individual o conjunta.

El acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas y las certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes serán indispensable y **su ausencia será motivo de desechamiento de la propuesta.**

A continuación, se enumeran las credenciales y capacidades que deben cumplir los recursos asignados al proyecto:

**Partida 1.**

| **Perfil** | **Certificaciones que acreditar** | **Experiencia que demostrar** | **Función** | **Número de recursos** |
| --- | --- | --- | --- | --- |
| Administrador del Centro de Operaciones de Seguridad (SOC) | CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional) | Tres años de experiencia en proyectos relacionados con seguridad de la información. | Responsable de la administración, monitoreo y operación de los servicios provistos por el SOC, además de brindar soporte y atención a fallas e incidentes de seguridad. | Al menos 1 |
| Administración y Operación de soluciones y herramientas tecnológicas | Especialista consultor en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables los certificados vigentes obtenidos directamente del fabricante. | Tres años de experiencia en proyectos relacionados con seguridad de la información. | Administrar, operar y monitorear las soluciones de seguridad propuestas. | Al menos 1 por cada servicio |
| Líder de proyecto | PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master) | Tres años de experiencia en proyectos relacionados con seguridad de la información. | Responsable de administrar y coordinar el proyecto | Al menos 1 |
| Operador de la mesa de servicios SOC | ITIL v4 Foundation Certification | Tres años de experiencia participando en proyectos de seguridad de la información. | Personal encargado de las operaciones de soporte de primer nivel, monitoreo de servicios, registro y seguimiento de solicitudes de ventanas de mantenimiento, reporte de fallas y requerimientos. | Al menos 8 |
| Arquitecto especializado en redes y seguridad. | CCNP (Cisco Certified Network Professional) | Tres años de experiencia en participación en proyectos de redes y seguridad de la información. | Responsable de la administración, monitoreo y operación de los servicios proporcionados por el SOC en lo referente a servicios de interconexión de red, así como del soporte y la atención a fallas e incidentes que surjan en la interoperabilidad con otros proveedores y/o fabricantes. | Al menos 1 |

**Partida 2.**

| **Perfil** | **Certificaciones que acreditar** | **Experiencia que demostrar** | **Función** | **Número de recursos** |
| --- | --- | --- | --- | --- |
| Líder de proyecto | PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master) | Tres años de experiencia participando en proyectos relacionados con seguridad de la información. | Responsable de administrar y coordinar el proyecto. | Al menos 1 |
| Analista de Seguridad | CEH (Certified Ethical Hacker) | Tres años de experiencia participando en proyectos de seguridad de la información. | Responsable de llevar a cabo las revisiones de seguridad en las aplicaciones y la infraestructura, así como de prever, detectar, analizar, contener, erradicar y documentar incidentes de seguridad. | Al menos 2 |
| Consultor de Penetración | GPEN (GIAC Certified  Penetration Tester) o CEH  (Certified Ethical Hacker)  o CICP (Core  Impact Certified  Profesional) | Tres años de experiencia en proyectos relacionados con seguridad de la información. | Llevar a cabo simulacros de ataques a la red de infraestructura o aplicaciones para determinar el alcance de lo que los atacantes pueden acceder y los problemas que podrían ocasionar.  Evaluar la seguridad de la infraestructura de red y las aplicaciones mediante el uso de herramientas y técnicas que un atacante podría emplear. | Al menos 2 |
| Consultor Forense de Cómputo | EnCE (EnCase Certified  Examiner) o CHFI (Certified  Hacker Forensics  Investigator) | Tres años de experiencia participando en proyectos relacionados con seguridad de la información. | Analizar la metodología de ataque en caso de una penetración exitosa a la infraestructura, con el fin de determinar cómo se llevó a cabo y cuál fue el alcance del daño, lo que permitirá identificar las medidas preventivas a implementar. Además, debe poseer la capacidad de llevar a cabo investigaciones forenses si fuese necesario. | Al menos 1 |

# Condiciones técnicas de aceptación de entregable

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir diversos tipos de documentos, informes, artefactos, dictámenes o esquemas que aseguren el buen desempeño y continuidad del servicio. Estos documentos deben proporcionar certeza sobre las actividades diarias que el proveedor llevará a cabo bajo la supervisión de los servidores públicos designados por el Instituto para este propósito.

**Entregables Generales**

**Partida 1.**

| **SERVICIO** | **ENTREGABLE** | **PERIODICIDAD** | **ENTREGA** |
| --- | --- | --- | --- |
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | En un plazo de 15 días naturales después de la emisión del fallo. |
| Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | En un plazo de 15 días naturales después de la emisión del fallo |
| Matriz de Escalación | Única Vez | En un plazo de 15 días naturales después de la emisión del fallo |
| Declaración escrita por parte del proveedor, firmada por su representante legal, en la que se manifiesten las habilidades, competencias y capacidades necesarias para respaldar la prestación de los servicios. | Única Vez | En un plazo de 15 días naturales después de la emisión del fallo |
| Servicios de Seguridad – Continuidad Operativa | Documento que contenga el diseño de alto nivel de las soluciones de seguridad que se implementarán en los centros de datos, o en cualquier ubicación especificada por el Instituto. | Única Vez | En un plazo de 5 días hábiles después de la integración de las mesas de trabajo para cada servicio que se pretenda habilitar. |
| Documento que contenga el diseño detallado de las soluciones de seguridad a implementar en los centros de datos, o en cualquier ubicación especificada por el Instituto. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo para cada servicio que se pretenda habilitar. |
| Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas | Única Vez | En un plazo de 10 días hábiles después de completar la habilitación de todos los componentes en los Centros de Datos, o en cualquier ubicación especificada por el Instituto, y tras la integración de las mesas de trabajo correspondientes a cada solución integrada. |
| Memorias Técnicas Actualizadas de las Servicios de Seguridad | Única Vez | 20 días hábiles antes de la finalización del contrato para los servicios que ya estén habilitados. |
| Servicios de Seguridad – Verificación/Calidad | Documento que contenga el diseño de alto nivel de los servicios de seguridad a implementar en los centros de datos, o en cualquier ubicación especificada por el Instituto, que necesiten integrar activos de infraestructura para su habilitación. | Única Vez | En un plazo de 5 días hábiles después de la integración de las mesas de trabajo para cada servicio que se pretenda habilitar. |
| Documento detallado que describa el diseño específico de las Soluciones de Seguridad a implementar en los centros de datos, o en cualquier ubicación designada por el Instituto. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo correspondientes a cada servicio que se pretenda habilitar. |
| Memorias Técnicas de las Soluciones de Seguridad Implementadas, que necesiten integrar activos de infraestructura para su habilitación. | Única Vez | En un plazo de 10 días hábiles después de finalizar la habilitación de todos los componentes en los Centros de Datos, o en cualquier ubicación designada por el Instituto, y tras la integración de las mesas de trabajo correspondientes a cada solución integrada. |
| Memorias Técnicas Actualizadas de los Servicios de Seguridad que requieran integrar activos de infraestructura para su habilitación. | Única Vez | 20 días hábiles antes de la finalización del contrato para los servicios que ya estén habilitados. |
| Servicios de Borrado Seguro de Información | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicio de Gestión de Dominios | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicio de Certificados Digitales SSL | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicios de Protección de Riesgos Digitales | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA) | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicio de Antivirus | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicios de Prevención de Pérdida de Información | Protocolos de Operación del Servicio. | Única Vez | En un plazo de 10 días hábiles después de la integración de las mesas de trabajo. |
| Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) | Plan de Continuidad de Servicios. | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Gestión del Cambio en Seguridad de la Información | Procedimiento para la implementación de los servicios. | Única Vez | En un plazo de 10 días hábiles luego de la integración de las mesas de trabajo. |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Procesos de operación establecidos para:  - Requerimientos  - Cambios  - Configuraciones  - Incidentes  - Problemas  - Monitoreo | Única Vez | En un plazo de 15 días naturales tras la emisión del fallo. |
| Matriz de Escalación Técnica y Organizacional | Única Vez | 15 días naturales después de la emisión del fallo. |
| Procedimientos de operación de la Mesa de Servicios:  - Gestión de Requerimientos  - Gestión de Cambios  - Gestión de Configuraciones  - Gestión de Incidentes  - Gestión de Problemas  - Monitoreo | Única Vez | 15 días naturales después de la emisión del fallo. |
| Expedientes Curriculares del personal del Centro de Operaciones de Seguridad (SOC). | Única Vez | 15 días naturales después de la emisión del fallo. |
| Tablero de Estadísticas de Servicios de Seguridad (Portal Único) | Creación de cuentas de acceso en un portal único para las soluciones de seguridad. | Única Vez | 10 días hábiles después de la finalización de la habilitación de los componentes en los Centros de Datos o en la ubicación designada por el Instituto, según cada solución integrada y después de la integración de las mesas de trabajo. |

**Partida 2.**

|  |  |  |  |
| --- | --- | --- | --- |
| **SERVICIO** | **ENTREGABLE** | **PERIODICIDAD** | **ENTREGA** |
| Servicios de Habilitación, Operación y Transición | Plan detallado de trabajo de los servicios del proyecto. | Única Vez | Dentro de un plazo de 15 días naturales después de la emisión del fallo. |
| Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | Dentro de un lapso de 15 días naturales tras la emisión del fallo. |
| Matriz de Escalación | Única Vez | Dentro de un lapso de 15 días naturales tras la emisión del fallo. |
| Declaración de habilidades, competencias y capacidades del proveedor, firmada por el representante legal, para respaldar la prestación de los servicios. | Única Vez | Dentro de un lapso de 15 días naturales tras la emisión del fallo. |
| Servicios de Análisis de Vulnerabilidades Dinámico | Procedimientos de Operación del Servicio | Única Vez | 10 días hábiles después de la integración de las mesas de trabajo |
| Servicios de Pruebas de Penetración | Procedimientos de Operación del Servicio | Única Vez | 10 días hábiles después de la integración de las mesas de trabajo |
| Servicios de Análisis Forense | Procedimientos de Operación del Servicio | Única Vez | 10 días hábiles después de la integración de las mesas de trabajo |
| Servicios de Análisis de Vulnerabilidades Estático | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles después de la integración de las mesas de trabajo |

**Entregables bajo demanda**

El proveedor deberá generar entregables para los servicios de seguridad, que incluyan, pero no se limiten a, los siguientes conceptos:

**Partida 1.**

| **SERVICIO** | **ENTREGABLE** | **PERIODICIDAD** | **ENTREGA** |
| --- | --- | --- | --- |
| Servicios de Borrado Seguro de Información | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) detallando las actividades de borrado seguro ejecutadas para cada activo o grupo de activos de infraestructura procesados. Se integrarán el o los certificados de borrado por cada medio de almacenamiento analizado, incluyendo al menos la fecha, hora, datos del activo de infraestructura y dispositivos de almacenamiento borrados. | Evento | En un plazo de 5 días hábiles después de la solicitud emitida por el Instituto. |
| Servicio de Gestión de Dominios | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) que detalla los dominios renovados o adquiridos. | Evento | En un plazo máximo de 5 días hábiles posteriores a la solicitud emitida por parte del Instituto. |
| Servicio de Certificados Digitales SSL | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) detallando los certificados renovados o adquiridos, adjuntando además el archivo comprimido con la llave pública correspondiente, conforme a los requisitos establecidos. | Evento | 1 día hábil después de la solicitud generada por el Instituto. |
| Servicios de Protección de Riesgos Digitales | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) detallando los eventos generados de riesgos digitales. | Evento | En un plazo de 5 días hábiles después de la solicitud emitida por el Instituto. |
| Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las políticas, configuraciones o reportes solicitados por el Instituto | Evento | 1 día hábil posterior a la solicitud generada por parte del Instituto |
| Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA) | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las políticas, configuraciones o reportes solicitados por el Instituto | Evento | 5 días hábiles posterior a la solicitud generada por parte del Instituto |
| Servicios de Antivirus | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las políticas, configuraciones o reportes solicitados por el Instituto. | Evento | 1 día hábil posterior a la solicitud generada por parte del Instituto |
| Servicios de Prevención de Pérdida de Información | Informe Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las políticas, configuraciones o reportes solicitados por el Instituto. | Evento | 1 día hábil posterior a la solicitud generada por parte del Instituto |
| Servicios de Sistema de Gestión de Seguridad de la Información | Plan de Continuidad y Operación de los Servicios, de acuerdo con el alcance definido en las mesas de trabajo. | Evento | 10 días hábiles posteriores a la solicitud realizada por parte del Instituto. |
| Servicios de Gestión del Cambio en Seguridad de la Información | Plan de Trabajo para la continuidad y operación de los servicios, acorde al alcance definido en las mesas de trabajo. | Evento | 10 días hábiles posteriores a la solicitud realizada por parte del Instituto. |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad. | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto. |
| Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad. | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto. |
| Actualización de la matriz de escalación. | Evento | En un plazo de 5 días hábiles después de la incorporación o sustitución de nuevo personal en el Centro de Operaciones de Seguridad y Red. |
| Informes técnicos sobre las ventanas de mantenimiento llevadas a cabo en las soluciones de seguridad y red. | Evento | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento |
| Informe de estadísticas de uso y rendimiento (análisis de datos) de las soluciones de seguridad y redes. | Evento | En un plazo de 5 días hábiles posteriores a la solicitud generada por parte del Instituto. |
| Informe técnico sobre las configuraciones de las soluciones de seguridad y red. | Evento | En un plazo máximo de 5 días hábiles después de la solicitud realizada por parte del Instituto. |
| Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Reporte Técnico de los requerimientos registrados en la mesa de servicios | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Diagramas de Arquitectura de las soluciones de seguridad y red. | Evento | 2 días hábiles posteriores a la solicitud generada por parte del Instituto |

**Partida 2.**

| **SERVICIO** | **ENTREGABLE** | | **PERIODICIDAD** | | **ENTREGA** | |
| --- | --- | --- | --- | --- | --- | --- |
| Servicios de Análisis de Vulnerabilidades Dinámico | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | Evento | | 7 días hábiles posteriores a la solicitud generada por parte del Instituto | |
| Servicios de Prueba de Penetración | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | Evento | | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | |
| Servicios de Análisis Forense | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados | Evento | | 15 días hábiles posteriores a la solicitud generada por parte del Instituto | |
| Servicios de Análisis de Vulnerabilidades Estático | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | Evento | | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | |

**Entregables Periódicos**

El proveedor deberá generar entregables para los servicios de seguridad, los cuales deben abarcar, entre otros aspectos, los siguientes conceptos mínimos:

**Partida 1.**

| **SERVICIO** | **ENTREGABLE** | **PERIODICIDAD** | **ENTREGA** |
| --- | --- | --- | --- |
| Servicios de Seguridad – Continuidad Operativa | Reportes Técnicos de los activos de infraestructura que contemplen:   * Disponibilidad * Controles de Cambios * Requerimientos * Incidentes/Fallas * Actividad Sospechosa * Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Servicios de Seguridad – Verificación/Calidad | Reportes Técnicos de los activos de infraestructura que contemplen:   * Disponibilidad * Controles de Cambios * Requerimientos * Incidentes/Fallas * Actividad Sospechosa * Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
|  | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

**Partida 2.**

| **SERVICIO** | **ENTREGABLE** | **PERIODICIDAD** | **ENTREGA** |
| --- | --- | --- | --- |
| Servicios de Análisis de Vulnerabilidades Dinámico  Servicios de Análisis de Vulnerabilidades Estático  Servicios de Pruebas de Penetración  Servicios de Análisis Forense | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles siguientes al vencimiento del mes correspondiente. |
| Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

Durante la vigencia del contrato, los entregables requeridos deberán ser presentados en formato electrónico (MS Word, MS Excel, PDF), conforme a los plazos establecidos por el Instituto.

Además, el proveedor deberá establecer y mantener un repositorio digital en el que se almacenarán estos entregables como alternativa. Este repositorio estará disponible para consulta durante todo el periodo del contrato. Los permisos de acceso serán definidos por el Instituto durante las reuniones de trabajo, pudiendo ser otorgados al administrador del contrato, al cuerpo de gobierno designado para este propósito, u otros funcionarios designados por el Instituto.

# Cronograma de actividades



# Niveles de servicio acordados que deberán cumplirse

El propósito de los Niveles de Servicio es proporcionar al Instituto un método para:

* Evaluar de manera efectiva el rendimiento de los servicios proporcionados por el proveedor.
* Garantizar que los servicios sean entregados con la calidad esperada.

Los Niveles de Servicio son indicadores definidos por el IMSS que el proveedor del servicio SASI 2026 deberá cumplir para asegurar la calidad requerida en la prestación del servicio.

En cumplimiento de lo establecido en los artículos 66, fracción XIX, 75 y 76 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en los artículos 131 segundo párrafo, 141, 142 y 143 de su Reglamento, se aplicarán las Penas Convencionales y Deducciones correspondientes por cualquier retraso en las fechas acordadas de entrega o en el inicio de la prestación del servicio, así como por incumplimientos parciales o deficientes en los servicios prestados por el Proveedor del SASI 2026.

La aplicación de los niveles de servicio se regirá de acuerdo con lo establecido en los "Términos y Condiciones”.

**Actualización Tecnológica**

El “IMSS” podrá actualizar en cualquier momento las especificaciones de infraestructura, software y hardware mantenidos por SASI, con el fin de proteger a la organización contra la obsolescencia y mantener la tecnología actualizada de los servicios contratados. Por lo tanto, el “Proveedor” reconoce y acepta que el “IMSS” está en continua evolución tecnológica. En consecuencia, el “IMSS” notificará al “Proveedor” con diez días hábiles de anticipación, a través del “Administrador del Contrato”, para que tome las medidas necesarias y realice las adecuaciones pertinentes, garantizando así la continuidad operativa del servicio y la actualización de la documentación correspondiente (manuales, diagramas, etc.).

A solicitud del “IMSS”, el “Proveedor” deberá facilitar servicios de mejora continua y acceso a nuevas características de los servicios proporcionados mediante la actualización tecnológica de la plataforma informática utilizada. Esto permitirá al “IMSS” utilizar los servicios de acuerdo con los Niveles de Servicio establecidos en este Anexo Técnico. Una vez presentada la propuesta de actualización tecnológica, el Modelo de Gobierno evaluará su conveniencia y beneficios para los entornos del “IMSS”, decidiendo el momento oportuno y el responsable de llevar a cabo la actualización.

Por lo tanto, el “Proveedor” de SASI 2026 deberá incluir en su propuesta actividades relacionadas con la Actualización Tecnológica, que implica la renovación continua de la infraestructura para asegurar que los componentes del sistema se mantengan actualizados conforme a las ofertas del mercado y puedan cumplir satisfactoriamente con los Niveles de Servicio.

Esto incluye, de manera enunciativa:

* Establecimiento, implementación y administración de políticas para actualizar y complementar versiones de software, sistemas operativos, y firmware de equipos.
* Implementación y administración de políticas para actualizar y complementar herramientas de seguridad, monitoreo y gestión con los parches o correcciones necesarias.
* Cumplimiento de las solicitudes de actualización de Componentes Habilitadores requeridas por el “IMSS”, incluyendo la sustitución de equipos activos y actualización de software/firmware según las mejores prácticas.
* Análisis proactivo de alertas de software que puedan afectar la infraestructura administrada.
* Certificación del nuevo sistema operativo en un ambiente controlado antes de su instalación en la red de producción, asegurando soporte para nuevas funcionalidades o administración del ciclo de vida del elemento.

El “Proveedor” de SASI 2026 deberá garantizar que todos los componentes de su solución no se encuentren en situaciones de obsolescencia, como:

* Fin de soporte por parte del fabricante para hardware o software, incluyendo la sustitución o actualización necesaria.
* Falta de acceso a actualizaciones o soporte directo del fabricante, asegurando el acceso continuo a actualizaciones tecnológicas.
* Garantía de cobertura de soporte para equipos y software.

En cumplimiento de este requerimiento, el “Proveedor” de SASI 2026 llevará a cabo las acciones necesarias para la renovación tecnológica de los Componentes Habilitadores del Servicio, incorporando tecnología mejorada que asegure un rendimiento, eficiencia y calidad óptimos.

Adicionalmente, el “Proveedor” de SASI 2026 estará preparado para participar en nuevos proyectos del “IMSS” derivados de la evolución tecnológica, expansión y/o modificación del ambiente operativo, brindando soporte en planificación e implementación según sea necesario.

El “Proveedor” de SASI 2026 garantizará el acceso a la información técnica de las tecnologías y productos utilizados en su solución, proporcionando acceso a boletines, publicaciones periódicas y seminarios pertinentes, todo ello incluido en su propuesta sin costos adicionales para el “IMSS”.

La implementación de activos de infraestructura, como parte de la actualización tecnológica, será consensuada entre el “Proveedor” y el Instituto a través de un plan de trabajo, el cual no podrá exceder 2 meses, una vez que se determine que un servicio debe sufrir adecuaciones.

# Requerimientos de arquitectura tecnológica

Para atender a los requerimientos de Arquitectura Tecnológica, deberá remitirse a lo establecido en el presente Anexo Técnico y sus Apéndices A y B.

# Restricciones e interfaces con otros elementos

No existen restricciones o interfaces con otros elementos para llevar la implementación y/o continuidad operativa de los servicios establecidos en el presente Anexo Técnico y sus Apéndices A, B y C.

# Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas.

No se requiere ejecutar pruebas previas para los servicios solicitados conforme el Anexo Técnico y sus Apéndices A, B y C.

# Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud.

No Aplica

# Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior.

No existen modificaciones técnicas de los servicios conforme las solicitadas en el ejercicio anterior. Sin embargo, el presente Anexo Técnico incluye servicios adicionales conforme las necesidades operativas y en cumplimiento normativo en materia de seguridad de la información.

**Normas:** **Oficial Mexicana, Estándar (antes mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los bienes o servicios requeridos.**

No Aplica.

**Normativa aplicable**

El Proveedor de servicios estará sujeto a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la duración del contrato. Estas políticas aplicables se comunicarán durante las mesas de trabajo; sin embargo, deberán tener en cuenta las siguientes, enunciativas, pero no limitativas:

* Marco normativo de aplicación general y obligatoria en la Administración Pública Federal.
* Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la Información y comunicación, y la seguridad de la información en la Administración Pública Federal.
* Políticas de Seguridad basadas en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
* - ISO/IEC27001:2022 e ISO/IEC20000-1:2018.

**Cumplimiento de Políticas**

El Proveedor de servicios deberá adherirse estrictamente a las políticas de seguridad en vigor en el Instituto y garantizar en todo momento el cumplimiento de los lineamientos establecidos. En caso de que alguno de estos lineamientos cambie durante la vigencia del contrato, el Proveedor deberá ajustar su infraestructura y procesos para cumplir con los nuevos requisitos.

Todos los dispositivos informáticos de propiedad del proveedor de servicios, utilizados en la prestación de los servicios, deben estar equipados con sistemas de detección de intrusos, protección contra virus, así como herramientas para detectar y eliminar programas maliciosos como "backdoors" o "troyanos". Esta medida se aplica tanto a dispositivos móviles (laptops, smartphones, tablets, etc.) como a equipos de escritorio (desktop, deskside, etc.) utilizados por el personal asignado para tareas de administración y gestión.

Si estos dispositivos requieren la instalación de sistemas operativos, aplicaciones, antivirus u otras herramientas necesarias para su correcto funcionamiento, así como la adquisición, instalación, mantenimiento y licenciamiento de estos, todos los costos asociados correrán a cargo del proveedor.

**Consideraciones a la finalización del contrato**

En caso de terminación anticipada del contrato o al finalizar su vigencia, el "proveedor" será responsable de iniciar el proceso de respaldo de la información, realizar el proceso de baja, llevar a cabo los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez concluida la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por el proveedor para la prestación de los servicios se transferirán al IMSS para garantizar la continuidad operativa. Esta transferencia se realizará mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, de manera gratuita y libre de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

El retiro será coordinado con el tercero que resulte adjudicado, es decir al que se entregue el nuevo contrato o la solución que dará continuidad a la operación del IMSS respecto a los servicios de SASI 2026, observando los acuerdos operativos de migración de un contrato a otro, que contemplen aspectos como la migración de la información de usuario actual hacia la nueva solución.

El "proveedor" deberá entregar al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos los elementos necesarios para llevarlo a cabo. Dicho plan debe permitir una transición completa y correcta de los servicios, incluyendo la conformación y actualización de la documentación del proyecto, así como las mesas de trabajo necesarias para dicha transición con los proveedores que den continuidad operativa al proyecto.

La documentación deberá incluir información generada durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, considerando los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite para la transición a un nuevo contrato de servicios, con el fin de continuar prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, minimizando el impacto en la operación.

La fecha límite para la entrega de la documentación final actualizada será 2 meses antes de la finalización del contrato SASI 2026. Además, el "proveedor" implementará un esquema de respaldo de la información en cada uno de los componentes que integran los servicios, incluyendo los relacionados con los Centros de Datos del IMSS. El respaldo de la información se almacenará en cada punto táctico para ser entregado al cuerpo de gobierno del contrato para su resguardo, una vez obtenida la autorización correspondiente.

Asimismo, al término del contrato, el "proveedor" garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor. Dicho período de transición estará sujeto al plan de trabajo previamente presentado por el "proveedor" y aprobado por el IMSS. Durante este período, el "proveedor" proporcionará la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

**Modelo de Gobierno**

El Modelo de Gobierno define la estructura operativa y los lineamientos para el proyecto, así como los criterios para evaluar su desempeño. Surgiendo de la necesidad de implementar una estructura orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática SASI 2026", este modelo facilita la colaboración entre todas las partes involucradas para su implementación y operación eficaz.

Este modelo abarca los aspectos clave para asegurar y supervisar la ejecución del proyecto, incluyendo la organización y los roles del Instituto dentro del mismo. Establece esquemas operativos y procesos para que el administrador del contrato, los líderes del proyecto y el proveedor del servicio (SOC) puedan garantizar los niveles de servicio establecidos en cada etapa de la operación.

Diagrama

Descripción generada automáticamente

La estructura organizacional diseñada para el proyecto de "Servicios Administrados de Seguridad Informática 2026 (SASI)" tiene como objetivo garantizar la eficacia en el trabajo de los responsables, definiendo claramente los roles y responsabilidades en cada nivel. A continuación, se presenta una tabla de manera enunciativa, sin que esto constituya una limitación, que muestra a los responsables y sus roles correspondientes.

# Firmas de elaboración, revisión y aprobación

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró/Revisó** | **Cargo** | **Firma** | **Fecha** |
| Ing. Abraham Gutiérrez Castillo | Titular de la División de Seguridad Informática Física |  | 05/01/2026 |
| Mtra. Azucena Villadozola Cortes | Titular de la División de Seguridad Informática Lógica |  | 05/01/2026 |
| **Aprobó** | **Cargo** | **Firma** | **Fecha** |
| Ing. Javier Cortes López | Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información |  | 05/01/2026 |

# Relación de Anexos

|  |  |  |  |
| --- | --- | --- | --- |
| ***Id.*** | ***Nombre*** | ***Descripción corta*** | ***Fecha de integración al producto*** |
| 1 | Apéndice “A” | Especificaciones técnicas y operativas | 05/01/2026 |
| 2 | Apéndice “B” | Inventario de activos de infraestructura | 05/01/2026 |
| 3 | TyC | Términos y Condiciones | 05/01/2026 |
| 4 | Matriz P1 | Matriz de evaluación SASI Partida 1 | 05/01/2026 |
| 5 | Matriz P2 | Matriz de evaluación SASI Partida 2 | 05/01/2026 |