PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 1a

CARTA PROTESTA DE NO IMPEDIMENTOS PARA CONTRATAR (Personas morales) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre del representante legal de la empresa participante) actuando a nombre y representación de (Nombre de la empresa participante), por medio del presente manifiesto bajo protesta de decir verdad y apercibido de las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial, que conocemos el Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil diecinueve, por el que se regulan los procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos por la Suprema Corte de Justicia de la Nación, y no nos encontramos en ninguno de los supuestos a que se refieren los artículos 62, fracciones XV y XVI y 193, fracciones I, II, III, IV, V, VI, VII, VIII y X, del instrumento normativo antes referido.

Sin otro particular, reitero la veracidad de lo manifestado en el presente escrito.

ATENTAMENTE

Nombre de la empresa participante
Nombre y firma de la persona representante legal de la persona moral

---

CARTA PROTESTA DE NO IMPEDIMENTOS PARA CONTRATAR (Personas físicas) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre de la persona física) por mi propio derecho, por medio del presente manifiesto bajo protesta de decir verdad y apercibido de las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial, que conozco Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil diecinueve, por el que se regulan los procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos por la Suprema Corte de Justicia de la Nación, y no me encuentro en ninguno de los supuestos a que se refieren los artículos 62, fracciones XV y XVI y 193, fracciones I, II, III, IV, V, VI, VII, VIII y X, del instrumento normativo antes referido.

Sin otro particular, reitero la veracidad de lo manifestado en el presente escrito.

ATENTAMENTE

Nombre y firma de la persona participante
(Persona física)

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 1b

MANIFESTACIÓN DE DOMICILIO LEGAL
(Personas morales) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre del representante legal de la persona moral) actuando en nombre y representación de (nombre de la persona moral), por medio del presente escrito señalo como domicilio legal para recibir y oír las notificaciones relacionadas con el presente procedimiento de contratación número LPN/SCJN/DGRM/005/2023, mediante (especificar e incluir copia simple y original para cotejo de predial, agua o CFE), así como las relacionadas con la contratación que llegare a celebrar con los órganos del Poder Judicial de la Federación, el ubicado en calle _____ número exterior _____, número interior_____, colonia _____, Alcaldía o Municipio _____, código postal _____, Ciudad _____.

Asimismo, manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que el comprobante de domicilio presentado y obtenido por medios electrónicos es fidedigno.

Sin otro particular, reitero la veracidad de lo manifestado en el presente escrito.

ATENTAMENTE

Nombre de la empresa participante
Nombre y firma de la persona representante legal de la persona moral

---

MANIFESTACIÓN DE DOMICILIO LEGAL
(Personas físicas) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre de la persona física), por mi propio derecho, por medio del presente escrito señalo como domicilio legal para recibir y oír las notificaciones relacionadas con el presente procedimiento de contratación número LPN/SCJN/DGRM/005/2023, mediante (especificar e incluir copia simple y original para cotejo de predial, agua o CFE), así como las relacionadas con la contratación que llegare a celebrar con los órganos del Poder Judicial de la Federación, el ubicado en calle _____ número exterior _____, número interior_____, colonia _____, Alcaldía o Municipio _____, código postal _____, Ciudad _____.

Asimismo, manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que el comprobante de domicilio presentado y obtenido por medios electrónicos es fidedigno.

Sin otro particular, reitero la veracidad de lo manifestado en el presente escrito.

ATENTAMENTE

Nombre y firma de la persona participante
(Persona física)

ANEXO 1c

MANIFESTACIÓN DE VERSIÓN ELECTRÓNICA FIDEDIGNA (Personas morales) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES DE LA SUPREMA
CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre del representante legal de la empresa participante) actuando a nombre y representación de (Nombre de la empresa participante). Manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que la **cédula de identificación fiscal/ registro patronal**, presentada y obtenida por medios electrónicos es fidedigna.

ATENTAMENTE

Nombre de la empresa participante
Nombre y firma de la persona representante legal de la persona moral

---

MANIFESTACIÓN DE VERSIÓN ELECTRÓNICA FIDEDIGNA (Personas físicas) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES DE LA SUPREMA
CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre de la persona física), por mi propio derecho, por medio de la presente manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que la **cédula de cédula de identificación fiscal/ registro patronal**, presentada y obtenida por medios electrónicos es fidedigna.

ATENTAMENTE

Nombre y firma de la persona participante
(Persona física)

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 1d

MANIFESTACIÓN DE CAPACIDAD PROFESIONAL Y/O TÉCNICA
(Personas físicas) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES DE LA SUPREMA
CORTE DE JUSTICIA DE LA NACIÓN
P R E S E N T E

(Nombre de la persona física), por mi propio derecho, declaro bajo protesta de decir verdad y apercibido de las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial, que cuento con la infraestructura instalada, personal, material, equipo y demás requerimientos mínimos necesarios para la contratación del Servicio Administrado Centro de Operaciones de Ciberseguridad

ATENTAMENTE

Nombre y firma del participante
(Persona física)

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 1e

FORMATO ORIENTATIVO DE CONTRATO DE PARTICIPACIÓN CONJUNTA

CONTRATO DE PARTICIPACIÓN CONJUNTA QUE CELEBRAN POR UN LADO [PERSONA A], A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO _____ Y POR OTRA PARTE [PERSONA B] A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO _____, A QUIENES DE FORMA CONJUNTA SE LES DENOMINARÁ COMO LAS "PARTES" AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

DECLARACIONES

I. DECLARA POR CONDUCTO DE SU REPRESENTANTE LEGAL, QUE: ***(DECLARACIÓN PARA PERSONAS MORALES)***

I.1. Que acredita la existencia de la persona moral denominada con el testimonio de la escritura pública Número. _____, de fecha_____, pasada ante la fe del Notario Público número _____ de la ciudad de _____, el Licenciado _____, misma que fue inscrita en el Registro Público de la Propiedad y del Comercio de_____, bajo el folio _____.
I.2. Que el (la) Señor(a) _____, acredita su personalidad y facultades como representante legal de dicha sociedad, mediante el testimonio de la escritura pública Número. _____, de fecha_____, pasada ante la fe del Notario Público número _____ de la ciudad de _____, el Licenciado _____, facultades que a la fecha no le han sido revocadas, y en este acto señala como domicilio del representante legal _____.
I.3. Cuenta con la clave de inscripción en el Registro Federal de Contribuyentes _____ expedida a nombre de la empresa, por el Servicio de Administración Tributaria.
I.4. Para todo lo relacionado con el presente contrato señala como su domicilio el ubicado en _____.

II. DECLARA _____, POR SU PROPIO DERECHO, QUE: ***(DECLARACIÓN PARA PERSONAS FÍSICAS)***
II.1. Que acredita la existencia y nacionalidad mediante_____.
II.2. Cuenta con la clave de inscripción en el Registro Federal de Contribuyentes _____ expedida a su nombre, por el Servicio de Administración Tributaria.
II.3. Para todo lo relacionado con el presente contrato señala como su domicilio el ubicado en adquisición de equipo diverso para la DGJTV.

III. DECLARAN LAS "PARTES" QUE:
III.1. Se reconocen mutuamente la personalidad y capacidad jurídica con la que comparecen para la celebración del presente instrumento contractual, sin mediar vicio del consentimiento y manifiestan que todas las comunicaciones que se realicen entre ellas se dirigirán a los domicilios indicados en las declaraciones antes indicadas de este instrumento contractual.
III.2. Es su voluntad suscribir el presente instrumento en términos del numeral 7 de las Bases de contratación de la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, cuyo objeto es la contratación del servicio administrado del centro de operaciones de ciberseguridad.
III.3. Conocen el alcance y contenido de este contrato, por lo que están de acuerdo en someterse a las siguientes:

CLÁUSULAS

PRIMERA. OBJETO.
El objeto del presente Contrato es establecer las bases para que las **"PARTES"** se agrupen con el fin de presentar una propuesta conjunta para participar en la Licitación Pública Nacional número L LPN/SCJN/DGRM/005/2023, cuyo objeto es la contratación del servicio administrado del centro de operaciones de ciberseguridad.

SEGUNDA.- DOMICILIO COMUN.
Las **"PARTES"** señalan como su domicilio común para oír y recibir notificaciones el ubicado en _____.

TERCERA.- REPRESENTANTE COMUN.
Las **"PARTES"** convienen que (nombre del representante común), será el Representante Común, otorgándole poder amplio, suficiente y necesario para que actúe ante la Suprema Corte de Justicia de la Nación en nombre y representación de las **"PARTES"** en todo lo relacionado con la proposición y todos y cada uno de los actos de la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, cuyo objeto es la contratación del servicio administrado del centro de operaciones de ciberseguridad.

CUARTA.- DISTRIBUCIÓN DE ACTIVIDADES.
En caso de resultar adjudicada la proposición conjunta de las **"PARTES"**, en la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, cuyo objeto es la contratación del servicio administrado del centro de operaciones de ciberseguridad.

Se obligan a llevar las actividades que a continuación se señalan para dar cumplimiento al objeto del contrato que se derive de dicho procedimiento de contratación:

I. La **[PERSONA A]** se obliga a ejecutar las actividades derivadas del objeto de la contratación de la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, siguientes:
- **a.** [Indicar las actividades conforme al objeto del contrato]
- **b.** [Indicar las actividades conforme al objeto del contrato]
- **c.** [Indicar las actividades conforme al objeto del contrato]
- **d.** [Indicar las actividades conforme al objeto del contrato]

II. La **[PERSONA B]** se obliga a ejecutar las actividades derivadas del objeto de la contratación de la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, siguientes:
- **a.** [Indicar las actividades conforme al objeto del contrato]
- **b.** [Indicar las actividades conforme al objeto del contrato]
- **c.** [Indicar las actividades conforme al objeto del contrato]
- **d.** [Indicar las actividades conforme al objeto del contrato]

QUINTA.- OBLIGACIÓN SOLIDARIA.
Las **"PARTES"**, se obligan en forma conjunta y solidaria entre si y ante la Suprema Corte de Justicia de la Nación, para comprometerse por cualquier responsabilidad derivada del contrato que se firme producto de la Licitación Pública Nacional número LPN/SCJN/DGRM/005/2023, cuyo objeto es la adquisición de equipo diverso para transmisión de señal televisiva.
SEXTA.- EMISIÓN DE COMPROBANTES FISCALES DIGITALES POR INTERNET.
De común acuerdo las "PARTES" convienen en que en caso de ser adjudicados en la Licitación Pública Nacional LPN/SCJN/DGRM/005/2023, cuyo objeto es la contratación del Servicio Administrado de Centro de Operaciones de Ciberseguridad. [**PERSONA A y/o B (en caso de ser conjunta señalar la forma de distribución)]**, será la persona que emitirá los Comprobantes Fiscales Digitales por Internet (CFDI) por la adquisición de los servicios y a quien la Suprema Corte de Justicia de la Nación deberá realizar el pago correspondiente.
Las "PARTES" acuerdan que la empresa o persona física que actúe como Representante Común, será quien presente los Comprobantes Fiscales Digitales por Internet (CFDI) de todos y cada uno de los pagos derivados del contrato.
SÉPTIMA.- LEYES APLICABLES Y TRIBUNALES COMPETENTES. Para todo lo relacionado con la interpretación y ejecución con este instrumento son aplicables las Leyes correspondientes a su objeto y, en caso de controversia, serán competentes los tribunales de [Indicar entidad federativa], renunciando las partes expresamente a cualquier otra jurisdicción que pudiera corresponderles por virtud de sus domicilios presentes o futuros o por cualquier otro motivo.
Leído y entendido el alcance del presente contrato, las "Partes" lo firman de conformidad por duplicado en la Ciudad de México, el **[ ]** de **[ ]** de **[ ].**

FIRMAS

[PERSONA A]	**[PERSONA B]**
Nombre y firma de la persona física o la persona representante legal de la persona moral	**Nombre y firma de la persona física o la persona representante legal de la persona moral**

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 2a

PROPUESTA TÉCNICA

1. Objetivo general

Contar con un servicio administrado que incluya los servicios de un Centro de Operaciones Especializado y Certificado en Procesos de Ciberseguridad (COC), con el objeto de monitorear, detectar, mitigar y gestionar los incidentes de seguridad informática que se presenten en la red LAN de la Suprema Corte de Justicia de la Nación (SCJN) y el ciberespacio, fortaleciendo la protección y continuidad de la operación de los sistemas informáticos jurídicos y administrativos, a fin de coadyuvar a la SCJN cumplir con sus funciones como Máximo Tribunal Constitucional del país.

2. Objetivos específicos

El servicio administrado COC deberá contar con personal y herramientas especializados en seguridad informática que permitan el alcance de lo siguiente:

- **Diagnosticar** eficazmente, recolectando las evidencias necesarias que permitan la **detección oportuna** de amenazas avanzadas o ataques cibernéticos.
- **Clasificar y priorizar incidentes** de seguridad y amenazas avanzadas.
- **Generar planes y aplicar acciones de contención y mitigación** a incidentes de seguridad informática.
- **Obtener información** y generar reportes que permitan al personal técnico de seguridad informática de la SCJN **realizar ciberinteligencia,** así como una mejor toma de decisiones.
- **Determinar y establecer** planes de remediación de riesgos informáticos de la infraestructura crítica de la SCJN.
- **Determinar y cuantificar el nivel de riesgo** de la infraestructura tecnológica de la SCJN.
- **Instalar** y poner en operación servicios de seguridad informática para fortalecer las actividades en la materia.
- Fortalecer las habilidades y conocimientos de seguridad informática, así como promover hábitos en esta materia entre el personal de la SCJN, con la finalidad de generar una **cultura de ciberseguridad**.
- Mantener actualizado y operando el **Modelo Institucional de Gobierno de Seguridad de la Información de la Suprema Corte de Justicia de la Nación (SCJN)** para la mejora continua de la gestión del riesgo y la resiliencia ante amenazas y vulnerabilidades de ciberseguridad, permitiendo la seguridad de los activos informáticos de la Dirección General de Tecnologías de la Información de este Alto Tribunal.

3. Alcance del servicio

El servicio administrado de Centro de Operaciones de Ciberseguridad (COC), deberá ser provisto en el marco de un contrato abierto plurianual, con apego a estándares nacionales e internacionales, así como alineación a las mejores prácticas en materia de seguridad informática y ciberseguridad.

El servicio del COC, deberá administrar y operar los servicios de seguridad informática solicitados en el presente anexo, así como gestionar, atender, solucionar y documentar los eventos de seguridad informática que se generen dentro de la red interna de la SCJN, así como los eventos que se presenten en el ciberespacio. Además, deberá incluir la consultoría necesaria para la actualización del SGSI y la mejora del Modelo Institucional de Gobierno de Seguridad de la Información (MIGSI) de la SCJN, aplicado a los activos informáticos de la DGTI.

Partida Única. Servicio Administrado de un Centro de Operaciones en Ciberseguridad para la Suprema Corte de Justicia de la Nación.

4. Descripción de los servicios

La SCJN requiere mantener y fortalecer la seguridad informática de sus activos de información a través de una solución que incluya los servicios de un Centro de Operaciones Especializado y Certificado en Procesos de Ciberseguridad (COC) que integre a la infraestructura de la SCJN nuevas soluciones tecnológicas para la detección y contención de amenazas informáticas, que permitan la detección temprana de amenazas y ataques cibernéticos, contemplando la generación y aplicación de planes, esquemas y acciones de mitigación y respuesta a incidentes.

Al ser un servicio integral administrado, se deberán incluir todos aquellos componentes de hardware, accesorios, software y de servicios especializados necesarios para la puesta en operación, administración y gestión de los servicios requeridos de seguridad informática en las instalaciones de la SCJN, tales como:

- **Hardware**: Equipos especializados/appliances de seguridad informática, equipos servidores físicos y equipos de comunicación (switches).
- **Accesorios**: Patchs Cord (categoría 6/6a o superior), fibras ópticas (velocidades de 1,10, 40 Gbps), Gbics (velocidades de 1,10, 40 Gbps), organizador de cables, rieles, soportes/montajes, tornillos, cables de alimentación eléctrica y PDU.
- **Software**: licenciamiento de appliances, suscripciones a servicios en la nube, licenciamiento de software especializado, licenciamiento de servicios de seguridad informática y máquinas virtuales.
- **Servicios especializados**: instalación, puesta en operación, administración y gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas, soporte en sitio y a distancia; así como consultoría especializada.

En cada servicio de seguridad del presente anexo se detallan los componentes hardware, accesorios, software y de servicios especializados a considerar para la operación de cada solución, sin embargo, el prestador de servicios adjudicado de acuerdo con su solución y arquitectura propuesta por servicio será el responsable de determinar todos los componentes e insumos que requerirá para la operación de ellos.

Cabe señalar que los costos de todos aquellos componentes de hardware, accesorios, software y de servicios especializados para el presente proyecto deberán estar incluidos dentro del costo mensual por servicio.

A continuación, se describen los servicios de seguridad informática requeridos en el presente proyecto:

Servicio de protección para portales web: Este servicio permitirá el monitoreo y la protección de los portales web de la SCJN y de sus registros en internet (DNS) contra ataques provenientes del ciberespacio, que tienen como objetivo afectar la reputación de la SCJN, al realizar actos maliciosos que atentan contra el contenido o acceso a los portales de la SCJN.

Servicio de protección de correo electrónico: Este servicio permitirá la protección de los buzones de correo electrónico de usuarios y de servicios de la SCJN contra ataques de correo electrónico como son: spam (correo no deseado), phishing (extorsión, estafas, suplantación de identidad, entre otros), malware (virus contenidos en el cuerpo del correo, ya sea virus adjuntos o ligas web), además de proteger el proceso de entrega y envió de correo electrónico de la SCJN.

Servicio de detección y protección de amenazas avanzadas con base en comportamiento: Este servicio permitirá el monitoreo integral de la seguridad informática de la red LAN de la SCJN (tráfico interno); y de los puntos finales (equipos de cómputo de usuarios y equipos servidores) independientemente si se encuentran en la red LAN o en internet, con el objetivo de contar con una visibilidad amplia y análisis sobre el tráfico institucional que pudiera ser identificado como malicioso o anómalo y que pueda poner en riesgo los activos críticos, activos esenciales, usuarios finales o representen un riesgo a la confidencialidad, integridad y disponibilidad de la información de la SCJN y sus servicios informáticos. El servicio debe ser capaz de identificar y dar seguimiento a las posibles ciber amenazas con base en el análisis de los patrones de comportamiento de usuarios y entidades en la red LAN de la SCJN o en internet, mediante el uso de algoritmos inteligentes y aprendizaje automático.

Servicio de Protección para puntos finales: El servicio se encargará de la protección de los equipos de cómputo de la SCJN (equipos de usuarios y equipos servidores) contra cualquier amenaza malware, permitiendo detectar, investigar y mitigar cualquier actividad sospechosa con base en comportamiento (Solución XDR) en cada equipo de cómputo protegido, independientemente si se encuentran en la red LAN de la SCJN o en internet. Este servicio se prestará en la modalidad bajo demanda considerando montos variables (mínimos y máximos) durante la prestación del contrato.

El **Servicio de Centro de Operaciones de Ciberseguridad (COC):** Deberá brindar servicio 7x24 los 365 días del año realizando con propias herramientas y personal especializado, las actividades de monitoreo, identificación, análisis, registro y apoyo en la resolución de cualquier incidente en materia de ciberseguridad que pudieran llegar a comprometer la confidencialidad, disponibilidad e integridad de los servicios informáticos de la SCJN.

Servicio de actualización y mejora del MIGSI - Modelo Institucional de Gobierno de Seguridad de la Información para la SCJN aplicado a los activos informáticos de la Dirección General de Tecnologías de la Información (DGTI) bajo el marco del estándar ISO/IEC 27001, en función a lo establecido en el **ISO/IEC 27014 – Gobernanza de seguridad de la información;** en su **versión vigente**; así dicho modelo debe considerar como mínimo los siguientes ejes:

- **Alineación estratégica**: demostrando que la dirección en la postura de seguridad informática coadyuva al logro de los objetivos de la SCJN
- **Gestión de riesgos:** mitigando los riesgos y reducir el posible impacto sobre los activos informáticos a un nivel aceptable, mediante la propuesta e implementación de mecanismos o controles aplicables.
- **Entrega de valor:** optimizando la seguridad informática con base a los objetivos institucionales.
- **Optimización de recursos:** utilizando el conocimiento y la infraestructura de seguridad informática y ciberseguridad con eficacia.
- **Medición del desempeño:** monitoreando y reportando el estado de los procesos de seguridad cuidando que estos alcancen sus objetivos.

Además, el modelo deberá considerar lo siguiente:

- La adecuación y operación de los objetivos y procesos de gobernanza establecidos en el marco de referencia **ISO/IEC 27014 – Gobernanza de seguridad de la información** en su versión vigente más reciente; así como los requisitos del cuerpo de gobierno sobre el Sistema de Gestión de Seguridad Informática (SGSI).

- La actualización y mejora del Sistema de Gestión de Seguridad Informática (SGSI) en función a lo establecido en el **estándar internacional ISO/IEC 27001 – Requisitos para la seguridad de la información** y el marco **ISO/IEC 27002 – Código de prácticas para los controles de seguridad de la información**; ambas en **la versión más reciente (mínimo 2022).**

    - Realizar un análisis de riesgos, con base en lo estipulado tanto en el marco **ISO/IEC 27005 – Seguridad de la información, ciberseguridad y protección de la privacidad**: orientación sobre la gestión de los riesgos de seguridad de la información, como en otras guías de nivel internacional o marcos de referencia aplicables, que permitan identificar, de forma oportuna, las brechas de seguridad que pueden afectar la confidencialidad, integridad y disponibilidad de los sistemas informáticos que soportan la operación de la SCJN; esto, a través de un enfoque holístico que considere los resultados derivados de los ejercicios de análisis de vulnerabilidades, pruebas de intrusión, la detección y priorización de amenazas, así como lo derivado de la relación de los procesos, tecnología y personas con la administración, operación y ciclo de vida de los activos informáticos de la DGTI, entre otros.

- Mantener y actualizar el **Programa de Concientización en Seguridad Informática (PCSI),** implementado por la DGTI**,** que impulse la adopción de mejores prácticas y mecanismos de seguridad permitiendo a los usuarios desarrollar las competencias adecuadas que coadyuven a preservar la seguridad de la información, además de

integrar mecanismos que permitan evaluar la evolución de la cultura de seguridad informática, como ejercicios (simulaciones) de correo phishing.

4.1 Especificaciones técnicas de los servicios

Los componentes requeridos para el Servicio Administrado de Centro de Operaciones de Ciberseguridad se describen a continuación:

Descripción
1) Servicio de protección para portales web. 2) Servicio de protección de correo electrónico. 3) Servicio de detección y protección de amenazas avanzadas con base en comportamiento. 4) Servicio de protección para puntos finales (XDR). 5) Servicio de Centro de Operaciones en Ciberseguridad (COC). 6) Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación (SCJN).

A continuación, se desglosan las especificaciones técnicas de los componentes requeridos:

4.1.1.Servicio de protección para portales web.

El prestador de servicios adjudicado deberá proporcionar un servicio de protección para portales web desde una plataforma en línea (nube), considerando lo siguiente:

- La administración y gestión del servicio de protección estará a cargo del prestador de servicios adjudicado, debiendo considerar una cuenta de administrador y cuentas de sólo lectura para el personal técnico autorizado de la SCJN, estableciendo acuerdos de operación.
- El prestador de servicios adjudicado deberá documentar cada uno de los cambios realizados en la solución, tales como: requerimientos, incidentes, problemas de operación o interrupciones del servicio.
- El servicio deberá garantizar una disponibilidad del 99.99% mensual.

Generales:

- Solución tecnológica con una consola de administración, gestión y operación en la nube (internet).
- Solución tecnológica única que permita cubrir todas las funcionalidades de protección requeridas.
- Deberá permitir la protección de todos los portales web de la SCJN publicados en internet, así como de sus registros DNS públicos.
- Generación y envió de alertas de seguridad y de disponibilidad, así como integración con herramienta de correlación de eventos.
- Capacidad en la nube para almacenar eventos de seguridad de los portales web de la SCJN, por al menos 90 días de histórico.
- La solución tecnológica deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución WAF deberá estar posicionado en el cuadrante de líderes de la metodología de investigación denominada “Gartner Magic Quadrant” para soluciones “WAF”.

El servicio de protección de portales web deberá contar en una solución tecnológica en una plataforma en línea única que proporcione las siguientes funcionalidades:

a) Módulo de DNS (Domain Name System), que permita la resolución de nombres de dominio de los portales web de la SCJN, así como la gestión de dominios, zonas y registros considerando como mínimo los siguientes alcances:
   - Manejo ilimitado de registros DNS por dominio o zona tales como: A, CNAME, TXT, NS, entre otros.
   - Manejo de registros de correo electrónico: MX, DMARC, SPF, DKIM.
   - Estadísticas del tráfico de DNS.
   - Protección contra ataques de DNS.
   - Manejo de dominios DNS: se deberá considerar la capacidad de soportar al menos 20 zonas de DNS o dominios públicos.

b) Módulo de protección anti DDoS, que permita la protección contra ataques de denegación de servicio distribuido (DDoS), el cual permita:
   - Identificación y bloqueo de tráfico anómalo hacia los portales web de la SCJN.
   - Contención de los principales tipos de ataques DDoS.
   - Mitigación de ataques DDoS en conexiones SSL
   - Monitoreo de tráfico.
   - Generación de reportes de ataques.

c) Módulo de protección WAF (Web Application Firewall), que permita la protección de portales web de la SCJN contra cualquier intento de modificación o alteración no autorizada, considerando los siguientes puntos:
   - Permitir el monitoreo, filtración y análisis del tráfico desde Internet hacia los portales web, detectando y bloqueando ataques maliciosos hacia los portales/aplicativos webs de la SCJN expuestos en internet.
   - Protección contra bots maliciosos.
   - Protección contra los ataques definidos en el OWASP top 10 más reciente.
   - Soporte para carga, uso y administración de certificados digitales SSL para portales Web.
   - Bloqueo geográfico/regional y por dirección IP.
   - Uso de listas blancas/negras.
   - Configuración de reglas o políticas de acceso globales y por aplicación (granulares).
   - Configuración y uso de los puertos estándar de acceso web TCP 80/443 HTTP/HTTPS, así como puertos particulares que usen los aplicativos de la SCJN.
   - Generación de reportes de ataques.
   - Estadísticas de tráfico hacia los portales web.
   - El módulo de WAF deberá considerar los necesario para gestionar hasta 90 portales o dominios web.

Certificados SSL

- Para la operación del servicio de protección de los portales web se deberán proveer y configurar certificados SSL en el módulo de WAF para los dominios y subdominios de la SCJN, conforme a las siguientes características:
- Se deberá considerar certificados SSL de tipo EV (Extended Validation), OV (Organization Validation) y WildCard.
- Los certificados deberán ser emitidos por una autoridad certificadora reconocida por los principales navegadores web del mercado.
- Debe permitir cifrado SSL para establecer canales seguros de comunicación y como mínimo el uso de algoritmo SHA-256 y llave de 2048 bits.
- Los certificados SSL deberán estar vigentes durante la vigencia del contrato y serán emitidos a nombre de la SCJN conforme las especificaciones técnicas requeridas.

- Los certificados SSL tendrán un periodo de vigencia de 12 meses y se podrán integrar o disminuir dominios web durante el periodo de renovación (hasta 4 por renovación).

Como referencia actualmente se cuentan en operación dos certificados EV, dos certificados OV y dos Certificados WildCard.

Sistema de monitoreo portales web.

- El prestador de servicios adjudicado deberá considerar un sistema de monitoreo automático 365X24X7 para la vigilancia de la disponibilidad e integridad de los portales web de la SCJN, considerando:
- Herramienta de monitoreo que permita la vigilancia de la disponibilidad de los portales web, la cual podrá ser una plataforma en la nube, garantizando el monitoreo 24x7.
- El monitoreo de disponibilidad de los portales web de la SCJN se realizará por dominio/IP y monitoreo de su integridad (en caso de alguna modificación no autorizada).
- Permitirá el alertamiento ante errores de comunicación/acceso (400, 401,403,404, 429, 500, 502, 503, 504, entre otros), errores generados en la plataforma del servicio de protección de portales web del presente anexo, o en su caso, que el contenido de algún portal haya sido modificado sustancialmente por un acceso no autorizado.
- Permitirá el envío de notificaciones automáticas de alertas de indisponibilidad o problemas de integridad a correo electrónico y a sistema de mensajería instantánea.
- Ante algún evento de indisponibilidad o cambio de contenido de algún portal web, se deberá generar el ticket correspondiente y alertar al personal de la SCJN de manera inmediata de acuerdo con la matriz de escalamiento correspondiente.

Los componentes mínimos que se deben considerar para la prestación del servicio son:

- Software: suscripción servicio en la nube, suscripción para almacenamiento en la nube (90 días), certificados SSL anuales, licencia/suscripción de software de monitoreo.
- Servicios especializados: instalación, puesta en operación, administración/gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas, soporte a distancia.

4.1.2 Servicio de protección para correo electrónico.

- El prestador de servicios adjudicado deberá proporcionar un servicio de protección para correo electrónico desde una plataforma en línea (nube), considerando lo siguiente:
- La administración y gestión la solución de protección estará a cargo del prestador de servicios adjudicado, debiendo considerar una cuenta de administrador y cuentas de solo lectura para el personal técnico autorizado de la SCJN, estableciendo acuerdos de operación.
- El prestador de servicios adjudicado deberá documentar cada uno de los cambios realizados en la solución, tales como: requerimientos, incidentes, problemas de operación o interrupciones del servicio.
- El servicio deberá garantizar una disponibilidad del 99.99% mensual.

Generales:

- Solución tecnológica única que permita cubrir todas las funcionalidades de protección requeridas.
- Solución tecnológica con una consola de administración, gestión y operación en la nube (internet).
- Deberá permitir la protección de todos los buzones de correo de la SCJN, incluyendo buzones de usuario y de servicios (deberá considerar como máximo 4000 buzones para el servicio requerido).

- Generación y envió de alertas de seguridad y de disponibilidad, así como integración con herramienta de correlación de eventos.
- La solución tecnológica deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución de protección de correo electrónico deberá estar posicionado en la sección de líderes de la metodología de investigación denominada “Forrester Wave” para soluciones “Enterprise Email Security”.

El servicio de protección para correo electrónico deberá contar en una solución tecnológica única que proporcione las siguientes funcionalidades:

a) Comunicación con Correo electrónico:
- Compatible con el servicio de correo de Microsoft Exchange On Premise y con Office 365 (en la nube de Microsoft).
- Permitir la integración con Directorio Activo de Microsoft AD para identificación de cuentas de correo electrónico válidas.
- Capacidad de recibir tráfico con conexiones SMTP/TLS y poder hacer conexiones con otros servidores de SMTP/TLS.
- Permitir el relay o envío de correo electrónico directamente desde equipos servidores en las instalaciones de la SCJN (debiendo considerar lo necesario para establecer esta comunicación, por ejemplo: equipo servidor o algún servicio adicional).
- Se deberá considerar lo necesario para gestionar al menos un mínimo de 3,600 cuentas de correo electrónico.

b) Protección Correo electrónico:
- Capacidad de filtrar correo entrante y/o saliente.
- Permitir la creación de políticas a nivel global por grupos o por usuario.
- Permitir crear listas negras/blancas generales para el bloqueo de dominio, email, y dirección IP.
- Permitir la identificación de cualquier atacante, indicando IP, dominio o datos que permitan realizar el bloqueo proveniente del mismo.
- Contar con un repositorio para cuarentena de correo electrónico, que permita almacenar correos SPAM por un mínimo de 90 días.
- Permitir el cifrado de correo electrónico.
- Permitir la generación de reportes de ataques, spam y flujo de correo.

c) Protección Antispam:
- Contar con un sistema interno de clasificación de correo electrónico, permitiendo la detección y bloqueo de acuerdo con la clasificación seleccionada, i.e. Spam, Marketing, Newsletter, Phishing, entre otros.
- Analizar todos los correos entrantes y salientes en tiempo real por contenido SPAM o no deseado.
- Contar con métodos de filtrado que dependiendo del resultado obtenido rechazarán o marcarán el correo electrónico como SPAM, para su posterior validación.
- Contar con filtros inteligentes de idioma para detectar y bloquear Spam en otros idiomas además del español.
- Enrutar los correos basura (SPAM) a un depósito de cuarentena que pueda ser revisado por usuarios registrados en LDAP y AD.
- Bloqueo automático de IPs debido a alta cantidad de envío de spam.

d) Protección Antivirus:
- Permitir la detección y bloqueo de cualquier malware (virus, gusanos, troyanos, spyware, ransomware, backdoors, rootkit, entre otros.) contenido en correos electrónicos.
- Actualización continua de firmas de amenazas de malware.

- Identificación de archivos o códigos maliciosos en el contenido del correo y adjuntos, eliminando todo archivo malicioso.

e) Protección por identificación de contenido:

- Analizar los correos y sus adjuntos en busca de contenido no deseado.
- Creación de reglas que establezcan que palabras o frases no están permitidas en ningún mensaje o adjunto.
- Permitir la identificación y bloqueo de archivos cifrados.
- Detección y bloqueo de ligas web maliciosas dentro del cuerpo de correo electrónico.

f) Envío de alertas y notificaciones:

- La solución deberá permitir él envió de alertas de seguridad.
- Permitir el envío de notificaciones a usuarios de correos en bandeja de spam.

Certificado SSL TLS

Para la operación del servicio de protección para correo electrónico se deberá proveer y configurar un certificado SSL TLS, para establecer conexiones seguras de correo electrónico, conforme las siguientes características:

- El certificado deberá ser emitido por una autoridad reconocida por los principales navegadores web del mercado.
- Debe permitir cifrado SSL TLS para establecer canales seguros de comunicación para correo electrónico.
- El certificado SSL TLS deberá estar vigente durante la vigencia del contrato, será emitido a nombre de la SCJN conforme las especificaciones técnicas requeridas y será generado por un periodo mínimo de 12 meses, debiendo realizar su renovación correspondiente.

Los componentes mínimos que considerar para la prestación del servicio son:

- **Software:** suscripción de servicio en la nube, suscripción para almacenamiento en la nube y certificado SSL anual.
- **Servicios especializados**: instalación, puesta en operación, administración/gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas y soporte a distancia y en sitio.

En el caso que su solución requiera un equipo servidor en sitio para relay de los servidores internos de la SCJN:

- **Hardware:** equipo(s) servidores físicos.
- **Accesorios:** Patchs Cord (categoría 6/6a o superior), rieles, soportes/montajes, tornillos, cables de alimentación eléctrica.

4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.

El prestador de servicios adjudicado deberá proporcionar un servicio de detección y protección de amenazas avanzadas con base en comportamiento, con una solución tecnológica on premise (en sitio) en alta disponibilidad para dos edificios de la SCJN en la CDMX, considerando lo siguiente:

- La administración y gestión la solución de protección estará a cargo del prestador de servicios adjudicado, debiendo considerar una cuenta de administrador y cuentas de solo lectura para el personal técnico autorizado de la SCJN, estableciendo acuerdos de operación.
- El prestador de servicios adjudicado deberá documentar cada uno de los cambios realizados en la solución, tales como: requerimientos, incidentes, problemas de operación o interrupciones del servicio.

- El servicio deberá garantizar una disponibilidad del 99.99% mensual.

Generales:

- Solución tecnológica única que permita cubrir todas las funcionalidades de protección requeridas.
- Deberá considerar una solución en alta disponibilidad (2 equipos, nuevos y de última generación) para dos sitios de la SCJN en la CDMX (4 equipos en total).
- Contar con una consola de administración, gestión y operación en la nube para los 4 equipos, la cual será un servicio del propio fabricante de los equipos.
- Capacidad en la nube para almacenar y analizar eventos de seguridad de los equipos on premise que serán instalados en las instalaciones de la SCJN, por al menos 3 meses de histórico.
- La solución propuesta para el servicio de detección y protección de amenazas avanzadas con base a comportamiento deberá integrarse con la solución del servicio de protección para puntos finales (XDR), debiendo ser de la misma familia de productos del mismo fabricante e incluir el licenciamiento necesario para su integración en la consola de protección en la nube del fabricante de las soluciones.
- La solución tecnológica deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución NGFW deberá estar posicionado en el cuadrante de líderes de la metodología de investigación denominada “Gartner Magic Quadrant” para soluciones “NGFW”.

El servicio de detección y protección de amenazas avanzadas con base en comportamiento deberá contar en una solución tecnológica única que proporcione las siguientes funcionalidades:

a) Protección en línea en tiempo real:

- Protección en línea de la infraestructura de servidores y de comunicación interna (LAN) de la SCJN.
- Análisis de tráfico de red, paquetes e inteligencia de amenazas por usuarios, aplicaciones, zonas, protocolos, dominios, IPs, entre otros.
- Despliegue de información de la capa de transporte y de protocolos detallados para las amenazas/ataques detectados.
- Búsquedas personalizadas por intervalos de tiempo, IP, amenaza, malware, origen, destinos, puertos, usuarios, entre otros.
- Análisis, detección, contención y bloqueo en tiempo real de amenazas avanzadas, cibercrimen, campañas de ataque, explotación de vulnerabilidades, escaneos de red, malware, malware avanzado, ataques de día zero y contra cualquier comportamiento anómalo en la red de la SCJN.
- Uso de reglas de acceso, parámetros de IPS/IDS, análisis de virus en línea, NAT e inspección SSL.
- Actuación reactiva ante la ocurrencia de un incidente de seguridad mediante indicadores de ataque, con múltiples puntos de visibilidad, detección y mitigación.

b) Servicios de protección:

- Protección de DNS.
- Control de usuarios y de aplicaciones.
- Inspección de tráfico cifrado SSL.
- Detección y mitigación por IPS/IDS.
- Prevención de amenazas avanzadas (threat prevention advanced) que incluya como mínimo: antivirus, anti-spyware y protección contra vulnerabilidades.
- Análisis avanzado de amenazas malware (WildFire/Sandboxing) y protección contra amenazas “zero day”.

- Configuración de políticas de acceso de red (por interfaces, puertos, aplicaciones, IP, Segmentos de red, entre otros).
- Uso de zonas para separación de tráfico y/o segmentos de red.

c) Especificaciones técnicas de los equipos:

- Cuatro equipos nuevos y de última generación de propósito específico para seguridad de la red (Gateway) tipo data center.
- Fuentes de poder redundantes Hot-Swap en cada uno.
- Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente.
- Equipos con interfaces de 40/10/1 Gbps, considerando como mínimo 4 interfaces de 40 Gbps y 6 interfaces de 10 Gbps por equipo (se deberá incluir los conectores Gbics tanto del equipo del servicio y del equipo a conectar para garantizar su correcta conectividad).
- Los equipos se configurarán en alta disponibilidad por edificio (considerar conector HA entre equipos en caso de requerirlo).
- Los equipos deben contar con un sistema operativo propietario o software interno (firmware) desarrollado por el fabricante de los equipos, los equipos contaran con la versión estable más reciente de dicho software.
- Acceso y configuración mediante GUI y CLI a través de comunicaciones cifradas, empleando SSL y SSH respectivamente.
- Integración a directorio activo MS AD.
- Sincronización de reloj.
- Configuración de cuentas de acceso.
- Contarán con el licenciamiento necesario para habilitar todas las funcionalidades de protección y contención de amenazas avanzadas de la solución de seguridad.
- Contarán con acceso a actualizaciones de bases de datos/firmas, así como de firmware para el equipo durante la vigencia del contrato.
- Contarán con garantía con el fabricante ante cualquier falla durante la vigencia del contrato.

Consola de administración:

- Para la administración de los equipos on premise de la solución se deberá contar con una consola que gestione, administre y aplique políticas de acceso, seguridad y/o configuraciones de red.
- La consola de administración será en la nube y deberá comunicarse y operar con los equipos on premise en las instalaciones de la SCJN.

Equipos switches:

Se deberá proporcionar equipos switches en alta disponibilidad (dos) para al menos 2 sitios de la SCJN dentro de la CDMX, los cuales se interconectará con la infraestructura LAN de la SCJN y permitirá la administración y acceso a la infraestructura on premise que ponga en operación el participante en las instalaciones de la SCJN, tal como los equipos del “Servicio de detección y protección de amenazas avanzadas con base en comportamiento” y cualquier otro equipo o servidor que requiera para brindar los servicios de seguridad en alcance el presente proyecto.

Los componentes mínimos que debe considerar para la prestación del servicio son:

- Hardware: Equipos especializados/appliances de seguridad informática y equipos de comunicación (switches).

- Accesorios: Patchs Cord (categoría 6/6a o superior), fibras ópticas (velocidades de 1,10, 40 Gbps), Gbics (velocidades de 1,10, 40 Gbps), organizador de cables, rieles, soportes/montajes, tornillos, cables de alimentación eléctrica y PDU.
- Software: licenciamiento de appliances, suscripciones a servicios en la nube, suscripción para almacenamiento en la nube (90 días), licenciamiento de servicios de seguridad informática.
- Servicios especializados: instalación, puesta en operación, administración/gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas, soporte en sitio y a distancia.

4.1.4 Servicio de protección para puntos finales (XDR)

El prestador de servicios adjudicado deberá proporcionar un servicio de protección para puntos finales (XDR) que permita la protección de equipos de cómputo de usuarios e infraestructura de servidores de la SCJN mediante la instalación de agentes XDR y de una consola de administración en la nube, considerando lo siguiente:

- La administración y gestión del servicio de protección estará a cargo del prestador de servicios adjudicado, debiendo considerar una cuenta de administrador y cuentas de sólo lectura para el personal técnico autorizado de la SCJN, estableciendo acuerdos de operación.
- El prestador de servicios adjudicado deberá documentar cada uno de los cambios realizados en la solución, tales como: requerimientos, incidentes, problemas de operación o interrupciones del servicio.
- El servicio deberá garantizar una disponibilidad del 99.99% mensual.

Generales:

- Solución tecnológica con una consola de administración, gestión y operación en la nube (internet).
- Solución tecnológica única que permita cubrir todas las funcionalidades de protección requeridas mediante la instalación y operación de un agente XDR en cada equipo de cómputo y/o servidor de la SCJN.
- Generación y envío de alertas de seguridad y de disponibilidad.
- Capacidad en la nube para almacenar y analizar eventos de seguridad de los puntos finales de usuario de la SCJN, por al menos 90 días de histórico.
- El servicio de XDR para los puntos finales, será en una modalidad abierta bajo demanda, en donde la cantidad facturada mensual podrá aumentar o disminuir por integración, reintegración y/o bajas/cambios de equipos de cómputo y de servidores que sean protegidos por la solución de XDR ofertada.
- La solución propuesta para el servicio de protección de los puntos finales (XDR) deberá integrarse con la solución del servicio de detección y protección de amenazas avanzadas con base a comportamiento, debiendo ser de la misma familia de productos del mismo fabricante, debiendo incluir el licenciamiento necesario para su integración en la consola de protección en la nube del fabricante de las soluciones.

Se proporciona únicamente con fines de referencia presupuestal y de dimensionamiento de la solución, la cantidad mínima de 3,500 y hasta 4,000 puntos finales, sin que éste sea un compromiso de facturación mensual por este componente del servicio.

El servicio de protección para puntos finales (XDR) deberá contar en una solución tecnológica única que proporcione las siguientes funcionalidades:

a) Compatibilidad:

- MS Windows en sus versiones 10, 11 y nuevas versiones liberadas durante la vigencia del servicio.

- Sistemas Operativos Mac OS en sus versiones vigentes y nuevas versiones liberadas durante la vigencia del servicio.
- MS Windows Server en sus versiones 2008, 2012, 2016, 2022 y nuevas versiones liberadas durante la vigencia del servicio.
- Sistemas Operativos Linux x86/x64, tales como Red Hat, Ubuntu, CentOS, CentOS Stream, Debian, entre otros, en sus versiones vigentes y nuevas versiones liberadas durante la vigencia del servicio.

b) Servicio de protección:

- Protección de los puntos de servicio de la SCJN, que incluyen equipos de usuario, equipos servidores y contenedores de aplicaciones, contra cualquier actividad maliciosa o sospechosa que pueda comprometer la correcta operación de los equipos de cómputo y de la información contenida en ellos.
- Análisis, detección, investigación y mitigación de actividad sospechosa con base en comportamiento (XDR), haciendo uso de inteligencia artificial o algoritmos avanzados.
- Análisis, detección, bloqueo de ejecución y eliminación de exploits, ataques sin archivos y malware informático, tales como: Troyanos, Spyware, Gusanos, Ransomware, Botnet, Adware, entre otros.
- Análisis, detección, bloqueo de ejecución de aplicaciones/archivos sospechosos o con comportamientos anómalos o con firmas de amenazas informáticas, teniendo la opción de su envió a una zona de cuarentena o su eliminación completa.
- Prevención, detección y respuesta de amenazas mediante procesos de aprendizaje máquina y automatización inteligente.

c) Funciones del Agente XDR:

- Supervisar y monitorear toda la actividad del punto final, tanto en el kernel como en el espacio del usuario (incluyendo archivos, procesos, memoria, registro, red, unidades de almacenamiento externo entre otros.)
- Inspección inteligente de archivos que permita identificar e impedir la ejecución de amenazas avanzadas (malware, exploits, ataques dirigidos, comportamientos anómalos, entre otros.).
- Eliminación automática de cualquier malware o amenaza informática plenamente identificada, así como limpieza de archivos infectados con malware.
- Seguimiento dinámico de la conducta del usuario final, usando el aprendizaje máquina para construir un contexto completo de comportamiento normal, contra el cual detectará amenazas avanzadas a través de múltiples vectores.
- Contención robusta de los incidentes que se presenten, de tal forma que, tras la detección de amenazas, permita bloquear en el punto final afectado, la ejecución de archivos o procesos involucrados.
- Integrar inteligencia en la nube y datos de servicios de reputación para bloquear proactivamente las amenazas conocidas en internet a nivel mundial, a partir de indicadores de compromiso, tales como hash, direcciones IP, URL, firmas, entre otros.

d) Consola de administración/operación/gestión:

- Consola en la nube (Internet) del fabricante de la solución de XDR que permita la gestión de los puntos finales de la SCJN.
- Proporcione información general sobre las amenazas y la información sobre el estado de salud general de los puntos finales protegidos.
- Gestión de los eventos de seguridad presentados en cada uno de los puntos finales de la SCJN.
- Gestión de las versiones de agentes en los puntos finales de la SCJN, permitiendo la actualización, desinstalación, pausa y restablecimiento de servicios de protección.
- Permita la configuración y aplicación de políticas de mitigación automatizadas o manuales.

- Proporcionar análisis detallados en formatos gráficos y de texto (resumen de ataque, descripción general, historia y datos brutos) de los eventos de seguridad identificados.

e) Funciones complementarias:

- La solución deberá permitir conocer tanto el inventario de aplicaciones dentro de cada punto de servicio, como las vulnerabilidades software dentro de los puntos de servicio.
- La solución deberá permitir obtener el nivel de riesgo de los puntos de servicio de la SCJN, permitiendo identificar y clasificar usuarios y equipos en función de las actividades sospechosas reportadas en la plataforma.

Actividades de migración:

- Deberá considerar las actividades necesarias para la desinstalación de la solución de XDR actualmente operando en los equipos de cómputo y de servidores de la SCJN.
- Al completar la desinstalación del agente anterior en cualquier punto final, deberá proceder a la instalación, configuración y alta del nuevo agente XDR de su solución tecnológica, verificando con el personal técnico de la SCJN los cambios realizados sobre cada uno de los equipos protegidos.

Los componentes mínimos que considerar para la prestación del servicio son:

- **Software:** suscripción de servicio en la nube, suscripción para almacenamiento en la nube (90 días), licenciamiento para agentes XDR.
- **Servicios especializados**: instalación, puesta en operación, administración/gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas, soporte en sitio y a distancia.

En el caso que su solución requiera equipo(s) servidor(es) en sitio para análisis de red o exploración de LAN para detección de puntos finales en la red de la SCJN:

- Hardware: equipo(s) servidores físicos.
- Accesorios: Patchs Cord (categoría 6/6a o superior), rieles, soportes/montajes, tornillos, cables de alimentación eléctrica.

4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)

- El prestador de servicios adjudicado deberá proporcionar un servicio de Centro de Operaciones de Ciberseguridad, considerando lo siguiente:
- El Centro de Operaciones de Ciberseguridad deberá proporcionar un servicio 24x7x365, será el encargado de administrar/operar los servicios de seguridad informática, así como gestionar, atender, solucionar y documentar los eventos de seguridad que sean generados en cada servicio administrado.
- Se encargará del monitoreo de los eventos de seguridad de la SCJN, tanto los que se generen dentro de la red interna de la SCJN, así como los eventos que se presenten en el ciberespacio y estén relacionados con la información, personal interno o portales de la SCJN.
- Así mismo, será el encargado de atender, revisar, solucionar, cerrar y documentar cualquier requerimiento (Alta, Baja, Cambio), incidente, problema de operación o interrupciones de los servicios de seguridad.

GENERALES:

- El Centro de Operaciones de Ciberseguridad deberá pertenecer al prestador de servicios adjudicado y ubicarse dentro del territorio nacional.
- El Centro de Operaciones de Ciberseguridad deberá contar con al menos 5 procesos certificados en ISO/IEC 27001 en su versión 2013 o más reciente.
- El Centro de Operaciones de Ciberseguridad deberá contar con certificaciones ISO/IEC 20000 (gestión de servicios de TI) e ISO/IEC 9000 (control y gestión de la calidad).
- El Centro de Operaciones de Ciberseguridad deberá estar afiliado al Foro de Grupos de Seguridad y de Respuesta a Incidentes (FIRST – Forum of Incident Response and Security Teams).

El prestador de servicios adjudicado deberá proveer y administrar durante la vigencia del contrato herramientas especializadas, las cuales integrará junto con los servicios de seguridad informática del presente requerimiento para establecer un monitoreo integral de los eventos de seguridad informática de la SCJN:

- Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD).
  - Se deberá dimensionar para un aproximado de 20 servidores.
- Solución de seguridad informática en la nube (SIEM o solución de análisis superior), la cual permita el análisis, correlación de eventos, clasificación y alertamiento de todos eventos de seguridad informática presentados los servicios de seguridad informática requeridos en el presente anexo, así como directorios activos y servidores críticos de SCJN (equipos con sistemas operativos Linux y Windows).
  - La solución deberá contar con funciones de inteligencia para clasificar, y priorizar y detectar eventos de seguridad críticos, permitiendo la correlación entre las soluciones de seguridad y los puntos de servicio involucrados.
  - Se deberá considerar agentes para envió de logs para los servidores y en caso de requerirlo por su solución, un equipo servidor físico/virtual para funcionar como concentrador de logs.
  - Para el dimensionamiento de la capacidad de la solución, deberá considerar el flujo de logs de las soluciones de seguridad informática, así como un aproximado de 100 servidores, con un periodo de retención de logs de al menos 90 días en la nube.
- Solución de análisis de vulnerabilidades para sistemas operativos a disposición del personal de la SCJN, para dar atención a requerimientos de equipos servidores físicos y virtuales considerando un estimado de 500 servidores. Misma solución a utilizar en el componente de “comprobación técnica” del Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información – MIGSI.

- Finalmente, el prestador de servicios adjudicado debe contar con herramientas de seguridad informática propias para ejecutar las siguientes acciones:
  - Análisis forense.
  - Desinfección de malware en equipos de usuario y servidores.
  - Desinfección de malware en archivos de usuarios.
  - Eliminación de Adware en equipos de usuario.

GESTIÓN DE SERVICIOS DE SEGURIDAD:

El prestador de servicios adjudicado a través de su Centro de Operaciones de Ciberseguridad deberá realizar la gestión, operación y monitoreo de los servicios de seguridad requeridos en el presente proyecto:

- Servicio de protección para portales web.
- Servicio de protección para correo electrónico.
- Servicio de detección y protección de amenazas avanzadas con base en comportamiento.
- Servicio de protección para puntos finales (XDR).

Puesta en operación:

- El Centro de Operaciones de Ciberseguridad deberá realizar la puesta en operación de las soluciones tecnológicas para los servicios de seguridad informática en compañía del fabricante de cada una de ellas. Cada fabricante de cada solución tecnológica a implementar en la SCJN deberá validar la correcta configuración y puesta en operación de su solución tecnológica.

Operación:

- El Centro de Operaciones de Ciberseguridad deberá administrar y operar todos los servicios de seguridad informática contemplados en el presente proyecto, para lo cual se encargará de ejecutar las siguientes tareas:
  - Verificar la correcta operación de cada una de las soluciones tecnológicas.
  - Verificar y realizar las configuraciones necesarias en las soluciones tecnológicas de los servicios de seguridad informática tomando como referencia la norma ISO/IEC 27001 y mejores prácticas del mercado en materia de seguridad informática, así como con las recomendaciones del fabricante.
  - Configurar las soluciones de seguridad informática para que puedan reaccionar de manera proactiva ante eventos de seguridad suscitados en los activos informáticos de la SCJN, configuración que deberá validar con el personal técnico de la SCJN.
  - Atender los diferentes requerimientos de configuración (Altas, Bajas y Cambios) solicitados por el personal autorizado de la SCJN, documentando y registrando cada cambio solicitado, debiéndose atender en un plazo no mayor a 6 horas, excepto aquellos que sean programados en ventanas de mantenimiento.
  - Actualización continua de las soluciones tecnológicas, que incluye la actualización de firmware, software, agentes XDR, así como de todo componente tecnológico que sea susceptible de actualización y sea parte de los servicios de seguridad informática en alcance al presente proyecto.
  - Obtención de información y generación de reportes a demanda de las diferentes soluciones de seguridad informática, ya sea de una solución particular o de la correlación de varias de ellas.

Monitoreo de servicios:

- El Centro de Operaciones de Ciberseguridad deberá implementar un sistema de monitoreo de disponibilidad y desempeño de los servicios de protección implementados en la SCJN, buscando garantizar el nivel de disponibilidad solicitado de 99.99 % mensual.
- Deberá notificar, solucionar y documentar todo evento de indisponibilidad en los servicios proporcionados en el alcance del presente proyecto.
- En caso de una falla en alguno de los servicios, el prestador de servicios adjudicado deberá solucionar la falla en un plazo no mayor a 4 horas, sin embargo si la afectación sobrepasa el tiempo de más de 4 horas, el prestador de servicios adjudicado deberá escalar la problemática con el fabricante, así como enviar personal técnico especializado presencialmente en las oficinas de la SCJN para la revisión de la solución afectada (en caso de que la solución sea en modalidad on premise o que la falla este afectando a algún equipo de cómputo de la SCJN como equipos de usuario o servidores).

Mejora continua:

- El Centro de Operaciones de Ciberseguridad deberá realizar de manera continua un análisis cualitativo y cuantitativo de los eventos de seguridad informática presentados en los servicios de seguridad informática, determinando y proponiendo mejoras de configuración o de operación sobre las soluciones tecnológicas.
- El Centro de Operaciones de Ciberseguridad deberá realizar una revisión técnica al menos cada 4 meses con el personal de la SCJN y el fabricante de las soluciones tecnológicas de los servicios de seguridad informática, verificando: configuraciones aplicadas, niveles de operación, mejoras aplicadas en la solución, nivel de protección y acciones para mejora continua.

MONITOREO DE AMENAZAS INTERNAS:

- El Centro de Operaciones de Ciberseguridad deberá realizar el monitoreo, revisión, alertamiento, solucionar y documentar todos los eventos de seguridad presentados en los servicios de seguridad informática, considerando lo siguiente:
- A través de las soluciones de seguridad informática se deberá monitorear el estado de salud de los activos de información de la SCJN, tales como: equipos de usuarios, equipos servidores, comunicación interna (flujos de red en la LAN de la SCJN), portales web y correo electrónico.
- Por cada solución de seguridad se deberá monitorear, revisar, alertar, solucionar y documentar cada uno de los eventos de seguridad, para aquellas soluciones de seguridad que tengan su propia gestión de eventos de seguridad interna (como la solución de XDR) se deberá administrar el ciclo de vida de los eventos de seguridad dentro de la propia herramienta.
- Se deberá atender los eventos de seguridad por su nivel de criticidad siguiendo el marco de referencia MITTRE ATT&CK.
- Para los eventos de categoría: Critical/Crítico y High/Alto se deberá alertar de manera inmediata al personal de la SCJN y deberá dar solución en un periodo no mayor de 4 horas a partir de la hora en la que se presentó el evento.
- Por cada evento de seguridad se deberá generar un ticket correspondiente y documentar las acciones correctivas realizadas, ya sea por la herramienta o por el personal del centro de operaciones.
- Se realizará un corte de eventos por ciclo de facturación, en el cual se deberán haber cerrado y atendido todos los eventos de seguridad generados durante el periodo correspondiente.
- Mediante la herramienta de correlación y clasificación de eventos de seguridad (logs), se deberá determinar:
  - Identificar si existe algún comportamiento anómalo o afectación dentro de los activos de información de la SCJN.
  - Si existe una correlación entre los eventos de las soluciones de seguridad.
  - Determinar la severidad del incidente de seguridad informática.
  - Apoyar en el análisis de trazabilidad del incidente de seguridad.
  - Apoyar a determinar el origen del incidente de seguridad informática.
  - Determinar si se está materializando un incidente crítico, como puede un ataque dirigido, explotación de alguna vulnerabilidad, dispersión de un malware o cualquier incidente que pueda comprometer a más de un activo informático de la SCJN a la vez.
- Para la atención de incidentes críticos de seguridad informática (donde diversos activos de información de la SCJN están siendo afectados la vez) el Centro de Operaciones de Ciberseguridad deberá establecer elaborar y poner en operación un **"Plan de Atención y Respuesta a Incidentes Críticos",** el plan debe considerar al menos los siguientes puntos:
  - Determinación del alcance del incidente.
  - Proponer y ejecutar las medidas de contención y remediación necesarias.
  - Apoyo técnico en las actividades de contención y mitigación del incidente.
  - Identificar necesidades de reestructuración de reglas o políticas en las herramientas de seguridad de la SCJN.

- Diagnosticar y evaluar los niveles de riesgo e impacto operativo, para determinar la severidad del incidente.
- Determinar las causas y afectaciones del incidente
- Elaboración un informe detallado del incidente, así como de sus medidas de contención.
- Se deben considerar su alineación a los marcos nacionales (Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos) e internacionales como NIST 800-61, ISO/IEC 27035.
- El plan deberá ser entregado de manera física y digital

- Para aquellos incidentes críticos en los que se determine que el origen del incidente de seguridad fue un activo de información (Equipos de usuarios o Equipos Servidores) la investigación se deberá extender al equipo o equipos en particular, debiendo realizar para ello un análisis forense para determinar las causas que dieron origen a dicho evento.
- Para aquellos incidentes de seguridad informática donde la herramienta de XDR no pueda realizar una eliminación total de una amenaza malware, el prestador de servicios adjudicado mediante el uso de herramientas especializas propias, deberá realizar el análisis de malware del equipo y la eliminación de la amenaza correspondiente (por ejemplo, en modo LIVE).
- En caso de que se identifique o se reporte por parte del personal de la SCJN de archivos infectados con malware en algún equipo de usuario o servidor de la SCJN, el prestador de servicios adjudicado mediante el uso de herramientas especializas propias deberá realizar la limpieza o desinfección de dichos archivos.
- En caso de que se identifique o se reporte por parte del personal de la SCJN de una infección de adware en algún equipo de usuario o servidor de la SCJN, el prestador de servicios adjudicado mediante el uso de herramientas especializas propias, deberá realizar la limpieza del equipo correspondiente.

MONITOREO DE AMENAZAS EXTERNAS, CIBERINTELIGENCIA:

El prestador de servicios adjudicado a través de su Centro de Operaciones de Ciberseguridad deberá proporcionar un servicio ciberinteligencia mediante el monitoreo continuo de amenazas externas en Internet, deepweb y darkweb conforme lo siguiente:

- Deberá realizar el monitoreo continuo del ciberespacio (Internet, deepweb y darkweb) para detección de escenarios de riesgos para la SCJN, tales como:
  - Robo, fuga o hurto de información interna o de sus empleados de la SCJN.
  - Cuentas comprometidas de usuarios o de infraestructura de la SCJN.
  - Venta ilegal de información, accesos, cuentas o vulnerabilidades de infraestructura, que puedan poner en riesgo los activos informáticos de la SCJN.
  - Campañas de difamación o que afecte la reputación de la SCJN.
  - Campañas de odio que puedan poner en riesgo a personal de la SCJN.
  - Campañas de phishing, extorsión o fraude mediante correo electrónico, portales apócrifos o cualquier medio electrónico, que suplanten la identidad de la SCJN.
  - Campañas de ataque por grupos cibercriminales que atenten contra infraestructura de la SCJN, tales como sus portales web, correo electrónico, servicios en línea, redes sociales oficiales, entre otros.
- Ante la detección de alguna amenaza cibernética, deberá reportar inmediatamente al personal autorizado de la SCJN, documentar el evento y generar su reporte correspondiente; así mismo, en caso de requerirlo por la SCJN, deberá levantar una denuncia ante la policía cibernética del descubrimiento correspondiente.
- En el caso particular de identificación de un portal apócrifo, el cual suplante alguno de los portales oficiales de la SCJN y a solicitud de la SCJN, el proveedor de servicios deberá realizar la baja (takedown) del sitio apócrifo.
- Deberá realizar un análisis de tendencias, información e inteligencia relacionada con los siguientes elementos:
  - Información relacionada con 20 usuarios de alto nivel que la SCJN determine.

- Casos analizados en el pleno de la SCJN o casos que por su importancia estén en tendencias de los medios de difusión.
- Portales web oficiales de la SCJN
- Cuentas oficiales de la SCJN en las diferentes redes sociales.
- Tendencias en redes sociales relacionadas con la SCJN.

- De manera continua deberá generar y enviar al personal autorizado de la SCJN, boletines de seguridad, los cuales incluyan los siguientes rubros:
  - Vulnerabilidades tecnológicas de día zero.
  - Información de ataques informáticos, descripción de sus vectores de ataque e indicadores de compromiso.
  - Información de malware, afectaciones e indicadores de compromiso.
  - Información de vulnerabilidades críticas de las diferentes tecnologías, que pudiesen afectar a la infraestructura tecnológica de la SCJN.
  - Información de eventos de ataques informáticos e infecciones de malware en el mundo, incluyendo la descripción del evento, afectación, vector de ataque, así como los indicadores de compromiso.
- Deberá realizar el análisis de los activos de la SCJN expuestos a Internet, considerando sus segmentos públicos de IP homologadas en sus diversos edificios, tanto de usuarios como de servicios, que permita:
  - Descubrimiento e identificación continua (escaneo automático) de todos los activos de la SCJN conectados a Internet.
  - Inventario actualizado de los activos informáticos detectados.
  - Gestión de la superficie de ataque a partir de los activos detectados y sus vulnerabilidades.
  - Análisis de los activos, puertos y vulnerabilidades detectados y expuestos a internet.

ATENCIÓN Y SOPORTE:

El prestador de servicios adjudicado deberá proporcionar asistencia técnica, atención de incidentes/requerimientos/reportes en una modalidad 24x7x365 a través de los siguientes medios:

- Asistencia vía telefónica, se deberá contar con un número local para comunicación con el Centro de Operaciones en Ciberseguridad.
- Asistencia vía correo electrónico, se deberá proveer una cuenta única de correo electrónico para la SCJN.
- Asistencia remota (software de conexión remota/ VPN site to site/ software de videoconferencia).
- Asistencia vía mensajería instantánea (WhatsApp/Telegram).
- Asistencia presencial en las oficinas de la SCJN en la CDMX (a demanda).
- Proporcionará una matriz de escalación multinivel, en la que se incluirá el nombre de contacto, número celular, rol y nivel de atención.

Los componentes mínimos que deberá considerar para la prestación del servicio son:

- Software: suscripciones a servicios en la nube, suscripción para almacenamiento en la nube (90 días), licenciamiento de servicios de seguridad informática.
- Servicios especializados: instalación, puesta en operación, administración/gestión, atención de altas, bajas y cambios (ABC), mantenimiento (preventivo y correctivo), resolución de fallas, soporte en sitio y a distancia.

En el caso que su solución requiera equipo(s) servidor(es) en sitio para concentrador y envió de logs a la nube de la herramienta de correlación de eventos:

- Hardware: equipo(s) servidores físicos.

- Accesorios: Patchs Cord (categoría 6/6a o superior), rieles, soportes/montajes, tornillos, cables de alimentación eléctrica.

4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI

La SCJN requiere de un servicio integral de consultoría que permita dar continuidad, actualizar y fortalecer el MIGSI existente, el cual actualmente está orientado y tiene aplicabilidad sobre los activos informáticos de la DGTI. El servicio requerido estará enfocado en mejorar la visibilidad del riesgo y la resiliencia ante amenazas y vulnerabilidades que pudiesen ocasionar posibles interrupciones a los activos informáticos críticos de la SCJN, así como la alineación de los esfuerzos en materia de seguridad informática y ciberseguridad, a la estrategia, los objetivos y lineamientos establecidos por la SCJN.

Un componente esencial dentro del MIGSI es el SGSI, por ello el presente servicio deberá incluir las actividades para actualizar e implementar los mecanismos correspondientes según lo estipulado en el estándar internacional **ISO/IEC 27001 – Requisitos para la seguridad de la información y el marco ISO/IEC 27002 – Código de prácticas para los controles de seguridad de la información,** ambas en función a su **versión más reciente (mínimo 2022).**

El prestador de servicios adjudicado deberá contemplar como parte de este servicio, todos los recursos materiales y humanos necesarios para realizar las actividades que forman parte de éste, las cuales deberá desarrollar durante la vigencia del contrato y por las cuales incluirá en su propuesta un monto fijo mensual.

A continuación, se describen los componentes que como mínimo deberá contemplar el licitante como parte de su propuesta, sin embargo, derivado del análisis del presente anexo técnico y con base en los estándares considerados, así como otros marcos de referencia o mejores prácticas de seguridad de la información o ciberseguridad, el licitante podrá proponer las actividades o componentes adicionales necesarios para el cumplimiento del objeto del presente servicio.

COMPONENTES DEL SERVICIO

<u>Evaluación del estado actual y deseado</u>

- Identificación del contexto: La SCJN proporcionará al prestador de servicios adjudicado, de manera inicial, la documentación actual de su Sistema de Gestión de Seguridad de la Información (SGSI) y de su Modelo Institucional de Seguridad de la Información (MIGSI), a partir de la cual el prestador de servicios adjudicado identificará el contexto actual y los requerimientos adicionales de información que deberá realizar a la DSI para identificar el estado actual y deseado de la Seguridad Informática. Aunado a ello, el prestador de servicios adjudicado deberá realizar un seguimiento de la operación del actual MIGSI, lo anterior deberá considerarse dentro de la fase de implementación del servicio (3 meses previos a la operación).
- Identificación de la situación actual: Con la información obtenida de la actividad previa, el prestador de servicios adjudicado deberá determinar el nivel de madurez del MIGSI, así como el grado de cumplimiento en función de lo establecido por los estándares ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27014 en sus versiones más reciente. El marco de referencia utilizado actualmente corresponde al CMMI, sin embargo, el prestador de servicios adjudicado podrá proponer e integrar otro marco en función de las necesidades que identifique durante la ejecución del servicio.
- Determinación de la situación deseada: A partir de la situación actual, el prestador de servicios adjudicado deberá establecer una propuesta que refleje las necesidades de la SCJN para mejorar la gobernanza, de tal forma que se mantengan los objetivos de: orquestar todos los componentes del servicio, mejorar la toma decisiones estratégicas y de operación de la seguridad informática, mejorar los niveles de protección de los activos informáticos de la SCJN, así como la actualización del SGSI.

Mejora al modelo de gobierno

- Optimización del modelo de gobierno: El prestador de servicios adjudicado deberá proponer mejoras al MIGSI enfocadas al logro de la situación deseada mediante la optimización, por ejemplo, a lo relacionado con la gestión documental, ciclos de aprobación, gestión de los repositorios, sistemas de métricas, medios de comunicación, entre otros. Dichas propuestas serán evaluadas por la Dirección de Seguridad Informática (DSI) para determinar la viabilidad de éstas. Para la implementación de dichas optimizaciones, el prestador de servicios adjudicado deberá considerar la implementación de una herramienta tecnológica tipo GRC orientada a la automatización de la gestión del MIGSI y del SGSI, al menos la gestión de procesos, gestión documentas y riesgos, considerando que su uso y administración sea de manera compartida con al menos 3 usuarios de la DSI.

Operación del modelo de gobierno

- Actualización del Programa de Seguridad Informática: Tomando como base los resultados de las actividades previas, sí como la implementación y resultados del componente de Gestión de Riesgos, regulaciones internas y externas aplicables, requisitos y directrices institucionales, requisitos del cuerpo de gobierno y las propuestas de mejora al MIGSI; el prestador de servicios adjudicado deberá establecer un nuevo Programa de Seguridad Informática, con un enfoque holístico que garantice la gobernabilidad y operación de la seguridad informática, mediante el diseño, mejora y acompañamiento continuo en la operación de los procesos y controles del SGSI.
- Actualización del SGSI: El prestador de servicios adjudicado deberá actualizar o implementar los mecanismos correspondientes del SGSI conforme a lo estipulado en los estándares ISO/IEC 27001 e ISO/IEC 27002, ambas en su última versión, toda vez que la base para un modelo de gobierno de seguridad informática es el SGSI. Lo anterior, alineado con el Programa de Seguridad Informática y con los requisitos del cuerpo de gobierno. Este sistema deberá generar un historial de funcionamiento demostrable de al menos tres meses que permitan a la SCJN estar preparada para una posible certificación.

Incremento de la cultura organizacional de seguridad (concientización)

- Identificación del nivel actual de concientización: Realizar evaluaciones periódicas a los funcionarios de la SCJN, sobre el nivel de conciencia de las amenazas de seguridad informática y de los impactos que pueden generarse por no participar activamente en los programas y proyectos de protección de datos en los sistemas informáticos. Para ello el prestador de servicios adjudicado deberá considerar una plataforma para la ejecución de ataques de correo phishing simulados para 3500 usuarios, y si así lo considera, además podrá proponer cualquier otro tipo de evaluación para identificar el nivel actual de concientización. Dichos ejercicios o evaluación se deberán realizar al menos de manera semestral durante la vigencia del contrato.
- Mejora del nivel de concientización: el objetivo principal es que los funcionarios adquieran los conocimientos y adopten las actitudes que fomenten una cultura de identificación y mitigación de los riesgos. Contemplando la actualización y mejora del actual Programa de Concientización de Seguridad Informática, que se desarrolle en ciclos a lo largo de la vigencia del servicio, el cual deberá estar basado en las cuatro fases del proceso de aprendizaje de Maslow, además de contemplar los resultados de la identificación del nivel actual de concientización para establecer las acciones necesarias para identificar grupos de interés focalizados, proponer temas a impartir, definir evaluaciones para medir la concientización de manera periódica, así como la implementación de una plataforma tipo LMS (propiedad del prestador de servicios adjudicado) que permita la operación de lo establecido en dicho programa.
- El prestador de servicios adjudicado será responsable de la gestión y administración de la plataforma, la cual deberá estar disponible de manera continua y bajo la modalidad en línea, así como del desarrollo y generación del contenido didáctico durante la vigencia del servicio. Considerando dicha plataforma para 3500 usuarios que deberán acceder

mediante la cuenta de correo institucional de cada uno correspondiente (dominio de la SCJN). El contenido a desarrollar para la anterior plataforma deberá estar en idioma español.

Comprobación técnica

- Ejecutar análisis de vulnerabilidades y pruebas de intrusión (pentest): El prestador de servicios adjudicado deberá realizar la detección y clasificación de vulnerabilidades en los activos de información requeridos por el personal técnico de la SCJN, así como pruebas de intrusión (pentest), tanto de "caja negra" como de "caja gris", con base en mejores prácticas y estándares internacionales, tales como como PTES, OSSTMM, ISSAF, NIST 800-115, entre otros. El prestador mencionará en su propuesta técnica qué marcos, metodología o buenas prácticas internacionales utilizará. Lo anterior a fin de identificar posibles fallos de seguridad en servicios o configuraciones que pudieran constituirse en una violación a la seguridad de la información. El prestador de servicios adjudicado podrá proponer y hacer uso de las herramientas tecnológicas de su propiedad que considere oportunas y necesarias, así como considerar todos los recursos necesarios para la ejecución y logro de los objetivos del actual componente.

El prestador de servicios adjudicado deberá considerar dentro de su propuesta, al menos las siguientes actividades:

  - Generar una Declaración de Trabajo (SoW, por sus siglas en inglés) considerando: objetivos, alcance, descripción del servicio, lista de activos, requerimientos, roles y responsabilidades, entregables, (definición del plan de trabajo, incluyendo ejecución, y presentación de resultados), metodología de trabajo (pruebas de seguridad a activos de información, métricas para la evaluación de vulnerabilidades), condiciones en las que se ejecutará el servicio, herramientas de trabajo, y consideraciones generales.
  - Formalizar la autorización por parte de la DGTI de la SCJN para poder ejecutar las pruebas de intrusión (pentest) a los activos informáticos definidos en el alcance.
  - Llevar a cabo el análisis de vulnerabilidades y pruebas de intrusión de manera externa de "caja negra" e interna de "caja gris", pudiendo ser realizados de forma manual o automática según lo establezca el propio prestador de servicios adjudicado.
  - En caso de que aplique, las herramientas propuestas deberán estar posicionadas en el cuadrante mágico de Gartner o en la metodología "The Forrester Wave".
  - Los resultados obtenidos deberán analizarse con base en el marco MITRE ATT&CK, con el objetivo de identificar aquellas vulnerabilidades y amenazas asociadas a las tácticas y técnicas de dicho marco y que representen las amenazas cuya progresión (identificar el flujo) impliquen los riesgos más críticos, de tal forma que permita identificar aquellas vulnerabilidades que deban remediarse de manera prioritaria, con base en el análisis anterior y no sólo a partir de la severidad de las vulnerabilidades de manera individual.
  - Se deberá considerar realizar un ejercicio de análisis de vulnerabilidades proactivo y pruebas de intrusión (pentest) cada 12 meses (una vez por año) durante la vigencia del contrato, incluyendo los escaneos/análisis necesarios para validar las acciones correctivas (remediación, contención o mitigación) correspondientes.
  - Desarrollar un reporte técnico y un reporte ejecutivo con los resultados obtenidos.
  - Se deberá considerar realizar análisis de vulnerabilidades a los servidores o infraestructura que así lo requieran otras áreas de la DTGI en cualquier momento durante la vigencia del contrato previa solicitud por parte de la DSI.
- **Ejecutar el análisis de código estático (SAST):** El prestador de servicios adjudicado deberá realizar la detección de vulnerabilidades para el código fuente de los sistemas informáticos críticos identificados en la gestión de riesgos, mediante la aplicación de un análisis en código estático, a fin de detectar fallos causados por deficiencias de codificación que pudieran constituirse en una violación a la seguridad de la información. Lo anterior, se realizará con las herramientas provistas por el prestador de servicios adjudicado que considere más convenientes, las cuales

deberán estar posicionadas como “líderes” en el cuadrante mágico de Gartner o en la metodología “The Forrester Wave”. Aunado a lo anterior debe considerase lo siguiente:

- La identificación de los riesgos mencionados en OWASP Top 10 en su última versión y CWE/SANS Top 25 Most Dangerous Programming Errors como mínimo.
- Entregar un reporte técnico y un reporte ejecutivo con los resultados obtenidos, correlacionando los resultados del análisis de vulnerabilidades y pruebas de intrusión, para poder identificar y priorizar las vulnerabilidades en código que representen los riesgos más altos.
- Realizar un ejercicio de análisis de código estático (SAST) cada 12 meses (una vez por año) durante la vigencia del contrato, incluyendo los escaneos/análisis necesarios para validar las acciones correctivas (remediación, contención o mitigación) correspondientes.
- Como referencia, sin ser limitativos, los lenguajes que se han analizado hasta ahora son principalmente: C#, Java, Javascript, VbScript, Common y Python, se debe considerar que dichos lenguajes podrían variar en función de actualizaciones por parte de las áreas de sistemas.

- **Desarrollar acciones de contención/remediación:** El prestador de servicios adjudicado deberá desarrollar las actividades de contención y remediación que apliquen en las herramientas tecnológicas que el mismo prestador administre y estén dentro de su alcance como parte del presente servicio, así como brindar el acompañamiento al personal de la DGTI, para que en conjunto planeen y desarrollen las actividades de contención o remediación de las vulnerabilidades detectadas y notificadas que correspondan a la infraestructura y aplicaciones como parte de este componente.

Para todos los análisis que forman parte del actual componente (Comprobación técnica), se deberá considerar como parte de los reportes correspondientes, que la lista de recomendaciones de las remediaciones o mitigaciones se presente lo más clara y precisa posible y en idioma español para cada recomendación, e incluir las referencias para su solución, así como la forma de prevenirlas.

Diagnóstico y análisis de amenazas de la red interna

Mediante el uso y resultados generados por las herramientas de seguridad informática de la SCJN para análisis de la red interna, el prestador de servicios adjudicado deberá llevar a cabo de forma continua y reportando de manera mensual, las siguientes actividades:

- Detectar y priorizar las amenazas: Proporcionar el servicio de detección y caza de amenazas avanzadas para cada uno de los incidentes “críticos” o “altos” identificados, estableciendo cada una de las tácticas y técnicas del ataque conforme al marco MITRE ATT&CK, que permita clasificar y priorizar su atención de acuerdo con el nivel de severidad.
- Notificar amenazas: Realizar las notificaciones de los eventos que pueden constituirse en una amenaza o incidente de seguridad, con el fin de que el equipo brinde respuesta a incidentes de seguridad de la información de la SCJN cuente con información oportuna para la atención de éstos y reducir el impacto.
- Desarrollar acciones de contención/remediación: El prestador de servicios adjudicado deberá desarrollar las actividades de contención y remediación que apliquen en las herramientas tecnológicas que el mismo prestador administre y estén dentro de su alcance como parte del presente servicio, así como brindar el acompañamiento al personal de la DGTI, para que en conjunto planeen y desarrollen las actividades de contención o remediación de las vulnerabilidades detectadas y notificadas que correspondan a la infraestructura y aplicaciones como parte de este componente.

Gestión de riesgos

- **Ejecutar análisis inicial del riesgo actual:** el prestador de servicios adjudicado, haciendo uso de la información recopilada en la **Identificación del contexto**, deberá realizar un análisis de riesgo que, considere los resultados históricos derivados de los ejercicios de análisis de vulnerabilidades, reportes de incidentes, la detección y priorización de amenazas, así como lo derivado de la relación de los procesos, tecnología y personas con la administración, operación y ciclo de vida de los activos informáticos de la DGTI, que le permita conocer las áreas críticas y los impactos, así como los niveles de tolerancia del riesgo de la SCJN.
- **Proponer mejoras al método para el análisis de riesgos:** como parte de la Optimización del modelo de gobierno, el prestador de servicios adjudicado deberá considerar la mejora del proceso de gestión de riesgos actual en función de las técnicas de evaluación de riesgo propuestas en el marco ISO 31010 Gestión de riesgos, Técnicas de evaluación de riesgos; en su versión vigente, u otros marcos que considere aplicables; además de tomar como fuente de información los resultados derivados de los ejercicios de análisis de vulnerabilidades, pruebas de intrusión, la detección y priorización de amenazas, así como lo derivado de la relación de los procesos, tecnología y personas con la administración, operación y ciclo de vida de los activos informáticos de la DGTI, así como información externa adicional que considere necesaria.
- Analizar los riesgos de seguridad: A partir de la actualización del método antes descrito, el análisis de los riesgos deberá realizarse de manera periódica cada doce meses, en donde en cada ciclo permita conocer la evolución y eficacia del modelo de gobierno, así como el estado de los niveles de riesgo. Se deberán analizar e identificar aquellos riesgos, que por su nivel de criticidad deben ser tratados, así como el tipo o nivel de tratamiento a realizar.

Acompañamiento en el tratamiento de riesgos

- **Diseñar acciones para el tratamiento de riesgos:** Con base en los resultados de los análisis de riesgos, incluyendo los resultados de la **Comprobación técnica** y considerando lo estipulado en el **Programa de Seguridad Informática**, el prestador de servicios adjudicado deberá brindar el acompañamiento al personal de la DGTI para el tratamiento de aquellos riesgos que representan un mayor impacto posible para la SCJN. Dicho acompañamiento consiste, entre otras actividades, en la remediación de vulnerabilidades, así como el diseño de acciones encaminadas a la reducción de riesgos, las cuales pueden ser mejora de los procesos de seguridad de la información, diseño o mejora de políticas o **recomendaciones** de mejora a los controles tecnológicos. El prestador de servicios adjudicado no podrá brindar dentro de este componente ninguna acción de remediación que implique instalar, operar o configurar alguna solución tecnológica que no sea parte del alcance de este servicio. El prestador de servicios adjudicado deberá considerar como parte del tratamiento de riesgos, desarrollar las actividades de contención y remediación que apliquen en las herramientas tecnológicas que el mismo prestador administre y estén dentro de su alcance como parte del actual servicio, y brindará las recomendaciones y acompañamiento sobre las actividades de contención o remediación a ejecutar sobre infraestructura de la SCJN
- **Planear las acciones para el tratamiento de riesgos:** Con base en las acciones identificadas para el tratamiento de riesgos, el prestador de servicios adjudicado deberá generar un **plan para el tratamiento de riesgos**, que permita desarrollar las actividades e identificar los recursos necesarios, considerando proporcionar la asesoría técnica requerida para brindar el acompañamiento al personal de la DGTI, así como a los responsables de la operación del COC, para la adecuada ejecución de las tareas de mitigación.
- **Dar seguimiento a las acciones para el tratamiento de riesgos:** El prestador de servicios adjudicado deberá dar el seguimiento al plan para el tratamiento de riesgos, así como también deberá evaluar que las acciones de remediación, los controles o procesos relacionados se hayan implementado conforme a lo planeado y medir la eficacia de estos.

Propuesta de mejora continua

- **Evaluar y mejorar el modelo:** el prestador de servicios adjudicado deberá asegurar que todos los componentes del servicio se encuentran debidamente orquestados de tal manera que cuentan con criterios de medición que permitan identificar las desviaciones o mejoras en las acciones.
- El prestador de servicios adjudicado deberá considerar como criterio mantener un concepto de simplificación en los procesos de mejora continua e involucrar un equipo de trabajo que tenga conocimiento de técnicas creativas de resolución de problemas.
- El prestador de servicios adjudicado deberá establecer en conjunto con el personal de la SCJN un plan de mejora continua que considere un calendario de evaluación y replanificación periódica como parte de este componente, así como del procedimiento para el análisis de resultados y generación de los informes ejecutivos de los mismos.

- **Gestión del proyecto**
- Dar seguimiento al plan de trabajo: a lo largo del proyecto, el prestador de servicios adjudicado deberá asegurar un puntual seguimiento a las actividades establecidas y que las mismas se realicen de manera oportuna.
- Comunicar eficientemente los avances, hitos y riesgos del proyecto: el prestador de servicios adjudicado deberá establecer un plan de comunicación que asegure que la información relevante del proyecto sea comunicada a través de los medios establecidos, y a las personas involucradas para lo cual deberá convocar a reuniones de avance semanales.
- Asegurar la calidad y oportunidad de los entregables del servicio: el prestador de servicios adjudicado deberá asegurar que los entregables cumplen con los criterios y tiempos de entrega establecidos en el presente anexo.

5 Entregables

Memoria técnica.

El prestador de servicios adjudicado deberá de proporcionar posterior a los trabajos de instalación y puesta en operación de los servicios de seguridad informática:

- Servicio de protección para portales web.
- Servicio de protección de correo electrónico.
- Servicio de detección y protección de amenazas avanzadas con base en comportamiento.
- Servicio de protección para puntos finales (XDR).
- Servicio de Centro de Operaciones en Ciberseguridad (COC).

Una **Memoria Técnica**, donde se indique por cada servicio, los componentes que lo integran y sus características, las configuraciones realizadas, diagramas de conexión (física y lógica), así como dependencias entre componentes.

La **Memoria Técnica** deberá ser entregada por el prestador de servicios adjudicado en un máximo de 30 días naturales al inicio de operación de los servicios de seguridad informática.

Entregables mensuales de las soluciones de seguridad informática.

Los entregables de operación de las soluciones de Seguridad Informática se deberán entregar de forma mensual, como máximo en los primeros 10 días naturales del mes, los cuales se describen a continuación:

Servicio	Entregables
Servicio de protección para portales web.	Reporte mensual que integre los siguientes componentes de la solución de seguridad informática: • Estado de salud de la solución. • Estadísticas del servicio. • Portales web protegidos en la solución. • Altas, Bajas y Cambios de portales y dominios web. • Incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC). • Actividades realizadas por el centro de operaciones durante el periodo (incluyendo acción, tiempo de atención y solución).
Servicio de protección de correo electrónico.	Reporte mensual que integre los siguientes componentes de la solución de seguridad informática: • Estado de salud de la solución. • Estadísticas del servicio. • Incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC). • Actividades realizadas por el centro de operaciones durante el periodo (incluyendo acción, tiempo de atención y solución).
Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Reporte mensual que integre los siguientes componentes de la solución de seguridad informática: • Estado de salud de la solución. • Estadísticas del servicio. • Incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC). • Actividades realizadas por el centro de operaciones durante el periodo (incluyendo acción, tiempo de atención y solución).
Servicio de protección para puntos finales (XDR).	Reporte mensual que integre los siguientes componentes de la solución de seguridad informática: • Estado de salud de la solución. • Estadísticas del servicio. • Equipos protegidos por la solución (equipos de usuario / servidores) • Altas, Bajas y Cambios de equipos protegidos (equipos de usuario/servidores). • Incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC). • Actividades realizadas por el centro de operaciones durante el periodo (incluyendo acción, tiempo de atención y solución).
Servicio de Centro de Operaciones de Ciberseguridad (COC)	Reporte mensual integral que deberá integrar los siguientes componentes: • Nivel de disponibilidad de los servicios de seguridad informática. • Resumen ejecutivo de los eventos de seguridad presentados en cada servicio de seguridad informática.

Servicio	Entregables
	• Resumen ejecutivo de las actividades realizadas por el centro de operaciones durante el periodo por servicio de seguridad informática. • Incidentes críticos en la prestación del servicio y las acciones realizadas para su solución. • Incidentes y comportamientos anómalos en el ciberespacio (externo). • Estado de salud y vulnerabilidades detectadas de los servicios de la SCJN expuestos a internet. • Análisis cualitativo y cuantitativo de los eventos de seguridad informática presentados (internos y externos), así como determinar si existe una correlación. • Recomendaciones técnicas de mejora en los servicios de seguridad informática.

De manera complementaria, el personal de la SCJN podrá solicitar la modificación de los reportes o solicitar reportes adicionales determinando su contenido para un análisis de mayor profundidad.

En caso de que los plazos fenezcan en día inhábil, la entrega se recorrerá al día hábil inmediato siguiente.

Entregables del Modelo Institucional de Gobierno de Seguridad de la Información.

Plan de actividades.

Aunado al inicio de los trabajos de instalación y puesta en operación de las soluciones de seguridad informática, el proveedor de servicios deberá iniciar con el proceso de planeación y distribución de las actividades (conforme a la "Tabla de entregables MIGSI") a realizar durante la prestación del "Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación (SCJN)", con lo cual, en un plazo no mayor a 5 días hábiles a partir del inicio de operación de los servicio, deberá entregar el plan de actividades que incluya el "**Cronograma de entregables de los componentes**" con el cual se dará seguimiento y complimiento durante la vigencia del contrato.

Tabla de entregables MIGSI.

A continuación, se desglosan los componentes y requerimientos mínimos a cumplir respecto al MIGSI y sus correspondientes entregables, los cuales deberán ser entregados durante la vigencia del contrato y en los primeros 10 días naturales de cada mes, conforme al "**Cronograma de entregables de los componentes**":

Componente	Requerimiento	Entregables
Evaluación del estado actual y deseado	Identificación del contexto	Solicitud formal de información
		Inventario de contextualización de los componentes del MIGSI y del SGSI: objetivos, marco regulatorio, funciones sustantivas, funciones de soporte, datos, sistemas, tecnologías y controles actualmente implementados.
		Plan de implementación del servicio
		Informe del nivel de madurez o situación actual.

Componente	Requerimiento	Entregables
	Identificación de la situación actual	Informe de comparación y equivalencias sobre el grado cumplimiento (ISO/IEC 27001:2013 e ISO/IEC 27001:2022)
	Determinar la situación deseada	Informe de situación deseada.
		Declaración de la aplicabilidad (ISO/IEC 27001:2022)
		Identificación de los requisitos del cuerpo de gobierno
Mejora al modelo de gobierno	Optimización del modelo de gobierno	Objetivos de mejora
		Sugerencias de mejora
		Soporte documental de las sugerencias de mejora
		Plan de implementación sobre las sugerencias de mejora aprobadas
		Evidencia de operación (3 meses)
		Identificación y solución de desviaciones
Operación del modelo de gobierno	Establecimiento del programa de seguridad informática	Programa de Seguridad Informática (PSI)
	Actualización del SGSI	Documentación del SGSI actualizada (ISO/IEC 27001:2022)
		Evidencia de operación (3 meses)
Incremento de la cultura organizacional (concientización)	Identificación del nivel actual de concientización	Identificación de grupos de interés
		Propuestas de mejora al temario actual
		Estrategia de evaluación del nivel de concientización
		Informe de nivel actual de concientización
	Mejorar el nivel de concientización	Estrategia de formación de conciencia (Programa de Concientización de Seguridad Informática)
		Material cargado a la plataforma
		Evidencia de evaluaciones conforme al programa
Comprobación técnica	Ejecutar análisis de vulnerabilidades y pruebas de intrusión (pentest)	-Reporte técnico de hallazgos y recomendaciones de remediación. -Reporte Ejecutivo de hallazgos y recomendaciones de remediación.
	Ejecutar el análisis de código estático (SAST)	-Reporte técnico de hallazgos y recomendaciones de remediación. -Reporte Ejecutivo de hallazgos y recomendaciones de remediación.
Diagnóstico y análisis de amenazas de la red interna	Detectar y priorizar las amenazas	-Reporte técnico de incidentes relacionados con el marco MITRE ATT&CK, identificando las acciones de notificación y de contención asociadas. -Reporte ejecutivo de incidentes relacionados con el marco MITRE ATT&CK, identificando las acciones de notificación y de contención asociadas.
	Notificar amenazas	

Componente	Requerimiento	Entregables
Gestión de riesgos	Ejecutar análisis inicial del riesgo actual	Informe inicial de riesgos
	Proponer mejoras al para el análisis de riesgos	Metodología de gestión de riesgos mejorada
		Formato de Plan de tratamiento
	Analizar los riesgos de seguridad	Informe actualizado de riesgos
	Tratamiento de riesgos	Plan de tratamiento por riesgos
	Acompañamiento a las acciones de remediación	Evidencia de seguimiento a la implementación de los planes de tratamiento y acciones de remediación.
	Identificar la eficiencia de las acciones de remediación implementadas	Identificación de desviaciones al plan de tratamiento de riesgos
Propuesta de mejora continua	Evaluar y mejorar el modelo	Lecciones aprendidas
		Identificar/proponer de acciones de mejora
		Reporte con evidencia de la implementación de las acciones de mejora
Gestión del proyecto	Generar y dar seguimiento al plan de trabajo	Plan de trabajo
	Comunicar eficientemente los avances, hitos y riesgos del proyecto	Convocatorias de reunión mensuales
		Minutas de seguimiento mensuales
	Asegurar la calidad y oportunidad de los entregables del servicio	Acta de inicio del proyecto
		Actas de entrega recepción mensuales
		Acta de cierre del proyecto

En caso de que los plazos fenezcan en día inhábil, la entrega se recorrerá al día hábil inmediato siguiente.

El coordinador del proyecto por parte el prestador de servicios adjudicado presentará en todos los casos la documentación de los entregables en idioma español y será entregada en medio impreso y en medio electrónico editable.

Cabe señalar que los componentes, requerimientos y entregables de la presente tabla conforman una base, sin embargo, el proveedor de servicios mediante su personal especializado de consultoría podrá ampliar dichos componentes y entregables correspondientes de acuerdo con los estándares y marcos de referencia en Seguridad de la Información utilizados como parte del servicio.

6 Generales

La SCJN a través de su área técnica, proporcionará las siguientes facilidades de acceso y comunicación al prestador de servicios adjudicado:

- Acceso a los inmuebles de la SCJN.
- Acceso a los centros de datos de la SCJN.
- Área de trabajo en las instalaciones de la SCJN, cuando sea requerido atención en sitio.
- Conexión Segura VPN de usuario / VPN site to site.

Para aquellos equipos/componentes de las soluciones propuestas por el prestador de servicios adjudicado que deban ser instalados en los centros de datos de la SCJN, se proporcionarán las siguientes facilidades:

- Espacio en gabinete o rack.
- Energía eléctrica.
- Condiciones climáticas.

A continuación, se describen las consideraciones de los centros de datos de la SCJN:

- Los centros de datos de la SCJN donde se implementará la infraestructura de los servicios de seguridad informática requeridos en el presente anexo se encuentran en la CDMX.
- Los equipos de red de la SCJN a interconectar con la infraestructura de los servicios de seguridad informática se encuentran dentro del mismo centro de datos por edificio, existiendo una distancia no mayor de 40 metros el más lejano, entre los gabinetes de los equipos de red de la SCJN y de los gabinetes asignados para la infraestructura de servicios de seguridad informática.
- El prestador de servicios adjudicado deberá considerar los patchs cord, fibras ópticas y Gbics (tanto del equipo de su servicio y del equipo de la SCJN) para la interconexión entre la infraestructura de los servicios de seguridad y la infraestructura de red de la SCJN, considerando que todos se encontrarán dentro de la misma área y que se realizarán conexiones punto a punto.

7 Requisitos técnicos

El licitante deberá tener la capacidad técnica suficiente para la integración, diseño e implementación de las soluciones de seguridad informática que permitan cubrir los servicios técnicos requeridos en el presente anexo, debiendo considerar el personal técnico especializado suficiente, con los conocimientos y habilidades necesarias para implementar, administrar, monitorear y mantener todos los componentes de las soluciones de seguridad informática que formarán parte del servicio; responder de manera correcta y oportuna ante eventos de seguridad, incidentes de operación y atención de requerimientos, cumpliendo con los niveles de servicio requeridos por la SCJN.

Asimismo, deberá asignar el personal suficiente, con al menos los perfiles solicitados en la tabla de **Personal requerido** para cumplir con los requerimientos planteados y el cronograma de actividades dentro del servicio de mejora y actualización del MIGSI para la Suprema Corte de Justicia de la Nación (SCJN).

7.1 Requisitos técnicos de las soluciones propuestas.

La solución tecnológica propuesta para el **servicio de protección de portales web** deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución propuesta deberá estar posicionado en el cuadrante de líderes de la metodología de investigación denominada “Gartner Magic Quadrant” para soluciones “WAF”.

La solución tecnológica propuesta para el **servicio de protección de correo electrónico** deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución propuesta deberá estar posicionado en la sección de líderes de la metodología de investigación denominada “Forrester Wave” para soluciones “Enterprise Email Security”.

La solución tecnológica propuesta para el **servicio de detección y protección de amenazas avanzadas con base a comportamiento** deberá estar posicionada como una de las soluciones líderes en el mercado, para lo cual el fabricante de la solución propuesta deberá estar posicionado en el cuadrante de líderes de la metodología de investigación denominada “Gartner Magic Quadrant” para soluciones “NGFW”.

La solución propuesta para el **servicio de protección para puntos finales (XDR)** deberá integrarse con la solución del servicio de detección y protección de amenazas avanzadas con base a comportamiento, debiendo ser de la misma familia de productos del mismo fabricante.

A continuación, se describen los requerimientos de acreditación:

a. Para su acreditación de cada solución, se deberá proveer de una copia de la metodología de investigación correspondiente.
b. Carta emitida por el licitante dirigida a la SCJN, en la que realice una descripción completa de la solución propuesta por cada uno de los servicios de seguridad informática.
c. El licitante deberá acreditar que las soluciones de seguridad informática propuestas para cada servicio, cumplen con las funcionalidades técnicas requeridas por la SCJN en el presente anexo técnico, para lo cual deberá integrar en su propuesta técnica las hojas de especificaciones (datasheets) del producto (únicamente se permiten en idioma español o ingles), indicando (subrayado) en ellas su correspondiente cumplimiento, en caso de un idioma diferente al español, se deberá realizar traducción simple del cumplimiento.
d. Carta del licitante firmada por éste o representante legal, donde garantice que todo el equipamiento propuesto que instale será nuevo de última generación, original en todas y cada una de sus partes y que no cuente con aviso de fin de vida.
e. Carta del licitante firmada por éste o representante legal comprometiéndose a que, en caso de resultar adjudicado, las piezas, partes y/o refacciones que se cambien en los mantenimientos correctivos serán nuevas, de características iguales o superiores a las originales y de la misma marca.

7.2 Distribuidor autorizado/certificado.

Para cada una de las soluciones de seguridad informática propuestas para brindar los servicios de protección para portales web, protección de correo electrónico, detección y protección de amenazas avanzadas con base en comportamiento y protección para puntos finales (XDR) el licitante deberá presentar carta membretada expedida por el fabricante de las soluciones, firmada por su representante legal, reconociéndolo como distribuidor autorizado. No se admitirán cartas de apoyo a través de un tercero (Distribuidor o Mayorista).

El licitante deberá contar con personal certificado en cada una de las soluciones propuestas para cubrir los servicios de seguridad informática del presente anexo, por lo que deberá presentar documentación del personal propuesto, en el entendido de que al menos 2 personas cuenten con la misma certificación, sin perjuicio de que dicho personal en su conjunto abarque todas las certificaciones vigentes para cada una de las soluciones de seguridad informática de los servicios:

a. protección para portales web.
b. protección de correo electrónico
c. detección y protección de amenazas avanzadas con base en comportamiento
d. protección para puntos finales (XDR)

Cabe precisar que de las personas propuestas deberán contar con título a nivel licenciatura en las áreas de comunicaciones, electrónica, informática o carrera a fin, para lo cual deberá presentar currículum vitae, así como, copia simple del documento que lo acredite.

7.3 Experiencia comprobable

A continuación, se describen los requerimientos de acreditación:

a. El licitante deberá acreditar que cuenta con un COC de su propiedad y que se encuentra dentro del territorio mexicano. Este requisito se acreditará con la certificación ISO/IEC 27001 donde conste su nombre y domicilio en territorio mexicano.
b. Copia del certificado ISO/IEC 27001 en al menos 5 procesos de Seguridad de la Información en su versión 2013 o superior, debidamente acompañado de una carta firmada por el representante legal del licitante en la que bajo protesta de decir la verdad manifieste que se compromete a mantener la vigencia de este durante la prestación del servicio. La acreditación de los procesos podrá realizarse, adicional al certificado, mediante carta emitida por la entidad certificadora, en la que señale los procesos que se encuentran certificados por la ISO/IEC 27001.
c. Copia de los certificados ISO 9001 versión 2015 o superior, ISO/IEC 20000-1 versión 2018 o superior, acompañado de una carta firmada por el representante legal del licitante en la que bajo protesta de decir la verdad manifiesta que se compromete a mantener la vigencia de este durante la prestación del servicio y en la cual se incluya la URL del organismo emisor en la que se puedan verificar.

d. El licitante deberá acreditar estar afiliado al Foro de Grupos de Seguridad y de Respuesta a Incidentes (FIRST – Forum of Incident Response and Security Teams), mediante una impresión de pantalla de la página oficial del FIRST con su liga web o en su caso documento emitido por el FIRST que reconoce al COC del licitante como miembro, acompañado de una carta emitida por su representante legal en el que ratifica que el COC del licitante está afiliado al FIRST y que se compromete a mantener su afiliación durante la vigencia del contrato.
e. El licitante deberá presentar al menos 3 contratos formalizados en copia simple, en donde demuestre que tiene experiencia de por lo menos tres años (dentro del periodo de 2017 al 2023) en la prestación del presente servicio o equivalente, en los cuales se pueda verificar (se solicita a los licitantes subrayen o resalten los datos siguientes):

    - Nombre del cliente
    - Nombre del proveedor/prestador de servicios adjudicado
    - Objeto del contrato/servicio
    - Vigencia del contrato/servicio
    - Firmas

f. Carta en papel membretado del licitante y firmada por su representante legal, en la que manifieste que cuenta y se compromete durante la vigencia del servicio, a mantener la capacidad técnica, financiera y de recursos humanos, así como con el equipamiento, instrumentos, refacciones, componentes y herramientas tanto de hardware como de software necesarios para proporcionar los servicios objeto del presente anexo técnico.

7.4 Equipo de trabajo

A continuación, se describe el personal mínimo requerido para dar seguimiento y cumplimiento al proyecto por parte del prestador de servicios adjudicado:

7.4.1 Ejecutivo de cuenta

El prestador de servicios adjudicado deberá garantizar durante la vigencia del contrato la adecuada atención administrativa y técnica asignando a un ejecutivo de cuenta para la SCJN, quien será el punto de contacto con el administrador del contrato por parte de la SCJN, el cual deberá realizar funciones administrativas y de gestión en materia contractual, asegurándose de que se lleve el cumplimiento en tiempo y forma de los servicios requeridos en el presente anexo.

Dentro de sus principales funciones, como mínimo, serán: la entrega en tiempo y forma de los entregables mensuales y asegurar una respuesta oportuna a las solicitudes de los administradores del servicio por de la SCJN, fungiendo como el primer nivel de escalación para todas las actividades que formen parte del servicio integral.

7.4.2 Administrador del proyecto

El prestador de servicios adjudicado deberá asignar un administrador de proyectos desde el inicio de la prestación del servicio, así como durante la ejecución de cada una de sus etapas que incluyen: la fase de implementación y puesta en operación de los servicios tecnológicos, así como para las actividades dentro de los componentes del servicio de actualización y mejora del Modelo Institucional de Gobierno de la Seguridad de la Información para la SCJN, el cual deberá contar con certificación vigente que lo acredite como Scrum Master o PMP durante toda la vigencia del contrato.

Durante la vigencia del contrato se realizarán reuniones de seguimiento y mesas de trabajo en las que participen: el ejecutivo de cuenta, el administrador del proyecto, los administradores del servicio por parte de la SCJN y el personal técnico involucrado que por parte del prestador de servicios adjudicado considere pertinente para dar seguimiento a las actividades objeto del presente documento y resolver cualquier situación emergente relacionada con el servicio integral.

El administrador del proyecto deberá realizar las minutas de seguimiento para cada uno de estos eventos las cuales deberá compartir con las áreas y personal involucrado y asegurar el cumplimiento de estas, así como conseguir las firmas correspondientes.

7.4.3 Actividades administrativas y de seguimiento:

El prestador de servicios adjudicado, a través del ejecutivo de cuenta y el administrador del proyecto, serán responsables de llevar a cabo la administración, seguimiento y revisión del servicio, para lo cual deberá contemplar como mínimo las siguientes actividades:

- Dirección estratégica enfocada en asegurar el logro de objetivos.
- Asignación de roles y responsabilidades a los recursos involucrados en el servicio.
- Controlar la ejecución del servicio.
- Gestión de riesgos del servicio.
- Supervisar el cumplimiento de los niveles de servicio.
- Gestionar la formalización de entregables, conciliación de niveles de servicio que incidirá en el pago de penalizaciones, deductivas y liberación de pagos por parte de la SCJN.
- Procedimientos de verificación de los servicios entregados durante las diferentes “etapas del servicio”.
- Procedimientos de atención y escalamiento.
- Planes de comunicación.
- Propuesta de formatos para la documentación generada durante el proyecto, tales como:
    - Minutas de trabajo
    - Entregables mensuales o por evento
    - Reportes de incidentes
    - Solicitud de servicios “En Demanda”
    - Acuerdos de nivel operacional (OLAs)

7.4.4 Personal requerido:

A continuación, se detallan los roles, requerimientos y requisitos de comprobación para el personal base con el que debe contar el prestados de servicios durante la vigencia del presente proyecto por lo que los licitantes deberán acreditar con las documentales señaladas:

Personal requerido		
Rol	**Requerimiento**	**Comprobación**
Ejecutivo de cuenta	• Titulado a nivel licenciatura o superior • 3 años de experiencia o más en proyectos o áreas de Seguridad de la Información	• Cédula o título profesional • Curriculum vitae
Administrador del proyecto	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas computacionales, carrera afín ó Licenciatura en Administración de Proyectos. • Profesional en Administración de Proyectos. • 3 años de experiencia o más en proyectos o áreas de Seguridad de la Información.	• Cédula o título profesional • Certificado Scrum Máster o PMP vigente. • Curriculum vitae
Consultor Senior de Seguridad de la	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas	• Cédula o título profesional • Título, diploma o certificado

Personal requerido		
Rol	**Requerimiento**	**Comprobación**

Información	computacionales, tecnologías de la Información o carreras afines.
	• Contar con **alguna** de las siguientes:
	  ○ Especialidad en Seguridad de la Información o ciberseguridad,
	  ○ Maestría en Seguridad de la Información o ciberseguridad
	  ○ Diplomado en Seguridad de la Información o ciberseguridad.
	• 5 años de experiencia o más como Líder implementador en ISO/IEC 27001.
		que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de:
		  ○ Especialidad
		  ○ Maestría
		  ○ Diplomado
		• Certificado vigente como Líder Implementador de ISO/IEC 27001.
		• Curriculum vitae

Consultor Junior de Gestión de Seguridad de la información	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines.
	• Contar con alguna de las siguientes:
	  ○ Especialidad en Seguridad de la Información o ciberseguridad,
	  ○ Maestría en Seguridad de la Información o ciberseguridad
	  ○ Diplomado en Seguridad de la Información o ciberseguridad.
	• 3 años de experiencia o más en proyectos o áreas de implementación y operación de Sistemas de Gestión de Seguridad de la Información basado en ISO/IEC 27001.
		• Cédula o título profesional
		• Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de:
		  ○ Especialidad
		  ○ Maestría
		  ○ Diplomado
		• Certificado vigente como Líder Implementador de ISO/IEC 27001.
		• Curriculum vitae

Especialista técnico en controles de ciberseguridad	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines.
	• Contar con alguna de las siguientes:
	  ○ Especialidad en Seguridad de la Información o ciberseguridad,
	  ○ Maestría en Seguridad de la Información o ciberseguridad
	  ○ Diplomado en Seguridad de la Información o ciberseguridad.
	• Alguna de las siguientes certificaciones:
	  ○ CISSP
	  ○ CISM
	  ○ CRISC
	  ○ Líder Implementador de ISO/IEC 27001.
		• Cédula o título profesional
		• Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de:
		  ○ Especialidad
		  ○ Maestría
		  ○ Diplomado
		• Al menos un certificado vigente como: CISSP, CISM, CRISC o Líder Implementador de ISO/IEC 27001.
		• Curriculum vitae.

Personal requerido		
Rol	**Requerimiento**	**Comprobación**
	• 3 años de experiencia o más en proyectos o áreas que administren y operen los controles de ciberseguridad	

Coordinador de Equipo de Respuesta a Incidentes.	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines.
	• Contar con alguna de las siguientes:
	  ○ Especialidad en Seguridad de la Información o ciberseguridad,
	  ○ Maestría en Seguridad de la Información o ciberseguridad
	  ○ Diplomado en Seguridad de la Información o ciberseguridad.
	• 3 años de experiencia o más en respuesta a incidentes de seguridad.
		• Cédula o título profesional
		• Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de:
		  ○ Especialidad
		  ○ Maestría
		  ○ Diplomado
		• Al menos un certificado vigente como: ECIH – EC Council Certified Incident Handler, MILE2 Certified incident Handling Engineer, ISO/IEC 27035 Lead Incident Manager o equivalente.
		• Curriculum vitae

Especialista de Ciberinteligencia.	• Titulado a nivel licenciatura o superior en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines.
	• Contar con alguna de las siguientes:
	  ○ Especialidad en Seguridad de la Información o ciberseguridad,
	  ○ Maestría en Seguridad de la Información o ciberseguridad
	• Diplomado en Seguridad de la Información o ciberseguridad.3 años de experiencia o más en Investigación en actividades de Ciberinteligencia
		• Cédula o título profesional
		• Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de:
		  ○ Especialidad
		  ○ Maestría
		  ○ Diplomado
		• Al menos un certificado vigente como: GIAC Cyber Threat Intelligence, Offensive Security – OSCP o equivalente.
		• Curriculum vitae

A continuación, se describen los requerimientos de acreditación:

a. Carta del licitante en donde se presente al equipo de trabajo propuesto para atender a la SCJN, considerando el personal certificado (**numeral 7.2** del presente anexo) por cada solución propuesta, así como los establecidos en la tabla de "**Personal requerido**" anterior, incluyendo por cada perfil, la información del personal propuesto y la documentación comprobatoria o certificación correspondiente.
b. Carta del licitante expedida por el representante legal, manifestando que su representada cuenta con el personal suficiente y técnicamente capacitado para atender cualquier solicitud relacionada con el presente anexo técnico.

Cabe precisar que la SCJN se reserva el derecho de solicitar el cambio de cualquier personal de los equipos de trabajo antes descritos, que no alcance los resultados esperados para el desarrollo del servicio durante la vigencia del contrato.

Así mismo, es importante mencionar que el personal que tenga a bien designar el prestador de servicios adjudicado para cubrir determinados roles podrá ser susceptible de incorporarse a dos o más roles que éste proponga, siempre y cuando no impacte en las actividades a realizar, así como en los resultados esperados por cada grupo de trabajo y que cumpla con las certificaciones solicitadas para cada uno de los roles.

7.5 Confidencialidad y Seguridad de la información

a) El prestador de servicios adjudicado se obliga y compromete por escrito a utilizar la información a que tenga acceso en el proyecto para los fines técnicos estrictamente necesarios para la ejecución de actividades del proyecto. El manejo de la información será el estrictamente necesario para garantizar la implementación y en ningún caso se podrá utilizar para otro fin. La SCJN se reserva el derecho de establecer las políticas, controles, formatos o verificaciones que considere necesarias para asegurar la confidencialidad y seguridad de la información.

b) Ambas partes se obligan a guardar absoluta reserva sobre la información y documentación que le sean proporcionados durante la prestación del servicio, por lo que se obligan a no divulgarlos por ningún medio escrito, oral, electrónico o de cualquier otra forma, ni usarlos para cualquier fin, sin la autorización previa y por escrito de este Alto Tribunal.

c) Queda establecido que toda la documentación incluido el formato establecido será propiedad exclusiva de la SCJN.

8 Plan de trabajo

El licitante deberá presentar dentro de su propuesta técnica, un Plan de trabajo, incluyendo una gráfica de Gantt que describa todas actividades de las etapas del proyecto, considerando como mínimo lo siguiente:

Fase de implementación:

- Reunión de presentación del proyecto.
- Planeación y levantamiento de configuraciones
- Aprovisionamiento de equipos y accesorios.
- Instalación, configuración y puesta en operación.

Fase de operación:

- Inicio de operación de los servicios de seguridad informática y del servicio de actualización y mejora del MIGSI.

Los servicios considerados deberán estar completamente instalados y configurados para iniciar la operación a partir de las 00:00 horas del 1° de abril de 2024, por lo que la persona que resulte adjudicada deberá considerar todo lo necesario para cumplir con la citada fecha.

El prestador de servicios adjudicado revisará el plan de trabajo propuesto con el personal de la Dirección de Seguridad informática para su aprobación, lo anterior sin perjuicio de que dicho plan sea susceptible de ajuste, cumpliendo en todo momento con el plazo de implementación.

9 Lugar donde se prestará el servicio.

Los trabajos de implementación, operación, mantenimiento preventivo y correctivo, y soporte técnico de los servicios de seguridad informática del presente proyecto, se llevarán a cabo en los inmuebles de la SCJN ubicados en la Ciudad de México.

Como excepción, para el servicio de protección para puntos finales (XDR) se deberá dar soporte de manera remota a los inmuebles de las Casas de la Cultura Jurídicas (CCJ), edificios distribuidos en la República Mexicana.

Para el servicio de actualización y mejora del MIGSI se prestarán en los inmuebles de la SCJN ubicados en la Ciudad de México.

10 Niveles de servicio.

A continuación, se describen los niveles de servicio que deberá acatar el proveedor de servicios:

Concepto	SLA
Servicio de Centro de Operaciones de Ciberseguridad (COC)	**1)** Para eventos de seguridad de nivel crítico o alto, se deberá dar solución en un plazo no mayor a 4 horas a partir del evento. **2)** Para eventos de seguridad de nivel informativo, bajo o medio, se deberá dar solución en un plazo no mayor a 24 horas a partir del evento. **3)** Para la atención de requerimientos (Altas, Bajas, Cambios) se deberá dar solución en un plazo no mayor a 4 horas a partir del envío del requerimiento.
Servicio de protección para portales web. Servicio de protección de correo electrónico Servicio de detección y protección de amenazas avanzadas con base en comportamiento Servicio de protección para puntos finales (XDR)	**4)** El servicio deberá iniciar conforme al Plan de Trabajo, con una vigencia a partir de su puesta en operación y hasta la finalización del contrato. **5)** Disponibilidad comprometida >= 99.99% mensual. **6)** En caso de falla del servicio, éste deberá ser restablecido en un plazo no mayor a 4 horas a partir del levantamiento del reporte. **7)** En caso de requerirse el cambio de algún componente del servicio por falla técnica, este deberá ser reemplazado por un componente de las mismas características o superiores en un plazo no mayor a 7 días naturales, a partir de la restauración del servicio sin costo adicional para la SCJN. Todo mantenimiento preventivo necesario de la solución tecnológica deberá ser aprobado por el personal técnico de la SCJN, los tiempos de inactividad por mantenimiento autorizado no será considerado como indisponibilidad del servicio.

11 Forma y términos en que se realizará la verificación de las especificaciones técnicas y la aceptación del servicio.

El administrador del contrato por parte de la SCJN verificará el cumplimiento en tiempo y forma de los servicios brindados a través de los entregables mensuales y de los reportes de servicio, en el entendido que cualquier desviación deberá registrarse.

El administrador del contrato validará de forma mensual que los reportes entregados cumplan con lo requerido y que estos sean consistentes con el servicio brindado en el mes vencido y que cumpla con el objeto de las presentes especificaciones técnicas.

En caso de que exista algún incumplimiento en los niveles de servicio, el administrador del contrato por parte de la SCJN realizará el cálculo de las penas convencionales que apliquen, y se establecerá por escrito la aplicación de éstas, para el procedimiento administrativo correspondiente.

12 Estándares aplicables

La ejecución de las actividades en el presente proyecto deberá de realizarse en apego al menos, a la normatividad y estándares aplicables siguientes, en sus versiones más recientes:

- **ISO/IEC 27001 – Requisitos para la seguridad de la información.**
- **ISO/IEC 27002 – Código de prácticas para los controles de seguridad.**
- **ISO/IEC 27014 – Gobernanza de seguridad de la información.**
- **ISO/IEC 27005 – Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información.**
- **ISO 31010 Gestión de riesgos, Técnicas de evaluación de riesgos.**
- **ISO/IEC 20000 - Gestión de servicios de TI.**
- **ISO/IEC 9000 - Control y gestión de la calidad.**

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 2b

CUMPLIMIENTO DE NORMAS
(Personas morales) (En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
PRESENTE

(Nombre del representante legal de la empresa participante) actuando a nombre y representación de (Nombre de la empresa participante), por medio de la presente manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que mi representada cumple con las Normas Nacionales e Internacionales respecto del _____, conforme lo establece la Ley de Infraestructura de la Calidad y demás disposiciones aplicables, según se indica a continuación:

I. Normas Nacionales
II. Normas Internacionales

ATENTAMENTE

Nombre de la empresa participante
Nombre y firma de la persona representante legal de la persona moral

---

CUMPLIMIENTO DE NORMAS
(Personas físicas) (En papel membretado del participante)

FECHA: _____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
PRESENTE

(Nombre de la persona física), por mi propio derecho, por medio de la presente manifiesto bajo protesta de decir verdad y apercibido en las penas en que incurren los que declaran falsamente ante autoridad distinta a la judicial que cumplo con las Normas Nacionales e Internacionales respecto del _____, conforme lo establece la Ley de Infraestructura de la Calidad y demás disposiciones aplicables, según se indica a continuación:

I. Normas Nacionales
II. Normas Internacionales

ATENTAMENTE

Nombre y firma de la persona participante
(Persona física)

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 2c

CARTA MANIFIESTO PARA PARTICIPAR EN LA JUNTA DE ACLARACIONES
(En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
PRESENTE

De conformidad con el artículo 65, segundo párrafo, del Acuerdo General de Administración XIV/2019, así como el numeral 5.3 de las bases del procedimiento de contratación en cita, manifiesto bajo protesta de decir verdad el interés de (Nombre o Razón Social), con Registro Federal de Contribuyentes _____ para participar en la junta de aclaraciones derivada de la Licitación Pública Nacional No. LPN/SCJN/DGRM/005/2023, la cual se efectuará vía electrónica a través de la plataforma de Microsoft Teams.

Asimismo, en mi carácter de representante legal, declaro que por parte de mi representada quien asistirá a la junta de aclaraciones electrónica, registrando para tal efecto el correo electrónico y teléfono del contacto que se señala, únicamente para efecto de conexión a la misma, será:

- Nombre de quien participará en la junta de aclaraciones:
- Correo electrónico
- Teléfono

Protesto lo necesario

[Nombre y firma de la persona física
o la persona representante legal de la persona moral]

Nota: Los participantes deberán adjuntar a la presente carta manifiesto, copia de la Identificación Oficial Vigente del que suscribe y de quien asistirá a la junta de aclaraciones.

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 3

FORMATO DE PROPUESTA ECONÓMICA
(En papel membretado del participante)

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
PRESENTE

Servicio	Unidad de medida	Cantidad	Costo mensual	Meses	Subtotal
Servicio de protección para portales web.	Servicio	1	$	36	$
Servicio de protección de correo electrónico	Servicio	1	$	36	$
Servicio de Detección y Protección de amenazas avanzadas con base en comportamiento	Servicio	1	$	36	$
Servicio de Centro de Operaciones de Ciberseguridad (COC)	Servicio	1	$	36	$
Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación	Servicio	1	$	36	$
			SUBTOTAL 1		$

Servicio	Unidad de medida	Cantidad Mínima de usuarios	Cantidad Mínima de usuarios	Costo Mensual por unidad de medida	Meses	Subtotal Mínimo Mensual	Subtotal Máximo Mensual
Servicio de Protección para puntos finales (XDR)	Usuario	3500	4000	$	36	$	$
				SUBTOTAL 2		$	$

SUBTOTAL 1	$
SUBTOTAL 2 **MÍNIMO**	$
SUMA SUBTOTAL 1 / SUBTOTAL 2 MÍNIMO	$
I.V.A.	$
TOTAL MÍNIMO	**$**

SUBTOTAL 1	$
SUBTOTAL 2 **MÁXIMO**	$
SUMA SUBTOTAL 1 / SUBTOTAL 2 MÁXIMO	$
I.V.A.	$
TOTAL **MÁXIMO**	$

Las operaciones aritméticas se deberán efectuar con redondeo a dos decimales.
Importe total global en letra TOTAL MÁXIMO: _____.

Incluir detalladamente en su propuesta, los conceptos del a) al g):

a) Vigencia del servicio:

Implementación:
La implementación de los servicios considerados deberá iniciar a partir del día hábil siguiente a la notificación de fallo y será sin costo para Suprema Corte de Justicia de la Nación.

Inicio de operaciones
Los servicios considerados deberán estar completamente instalados y configurados para iniciar la operación a partir de las 00:00 horas del 1° de abril de 2024, por lo que la persona que resulte adjudicada deberá considerar todo lo necesario para cumplir con la citada fecha.

Operación:
La operación del servicio será de 36 meses devengados contados a partir del 1ro de abril de 2024 y hasta el 31 de marzo de 2027.

b) Lugar de prestación de los servicios: Los trabajos de implementación, operación, mantenimiento preventivo y correctivo, soporte técnico de los servicios de seguridad informática y actualización y mejora del MIGSI, se llevarán a cabo en los inmuebles de la Suprema Corte de Justicia de la Nación ubicados en la Ciudad de México.

Como excepción, para el servicio de protección para puntos finales (XDR) se deberá dar soporte de manera remota a los inmuebles de las Casas de la Cultura Jurídicas (CCJ), edificios distribuidos en la República Mexicana. Previa comunicación con quien administre el contrato.

c) Forma de pago:

Mediante transferencia bancaria, a mes vencido de conformidad con los datos que sean proporcionados, a los 15 días hábiles a partir del día hábil siguiente de la presentación del Comprobante Fiscal Digital por Internet (CFDI) generado por Internet y autorizado, acompañado del documento que acredite la prestación de los servicios a entera satisfacción de este Alto Tribunal.

Los importes correspondientes a los ejercicios fiscales 2024 a 2027 estarán sujetos a que este Alto Tribunal cuente con los recursos presupuestales desinados para tales efectos, de conformidad con lo establecido en los artículos 39, fracciones II y III del Acuerdo General de Administración XIV/2019 y, 35 y 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendara, sin que la falta de estaos origine responsabilidad para la Suprema Corte de Justicia de la Nación sin que la falta de éstos origine responsabilidad para la Suprema Corte de Justicia de la Nación..

En términos de los Artículos 159 y 177 del Acuerdo General de Administración XIV/2019, en ningún caso procederán pagos por concepto de servicios no recibidos a entera satisfacción.

d) Vigencia de la propuesta: Las propuestas permanecerán vigentes por un plazo no menor de 60 días hábiles siguientes de la fecha de entrega de éstas.

e) Nombre y firma de la persona licitante o quien funja como su representante legal.

f) Los precios se mantendrán firmes hasta el cumplimiento total del contrato.

g) Los impuestos y derechos que se causen con motivo de la contratación serán pagados por la persona adjudicada, salvo los que por disposición legal deba cubrir la Suprema Corte de Justicia de la Nación.

Se deberá adjuntar como parte de su propuesta económica, las constancias solicitadas en el numeral 10.4 de las bases. Cuando se acuda al procedimiento en participación conjunta, todas las personas deberán presentar los documentos en los que consten la opinión positiva. La documentación presentada deberá considerar, en su caso, las modificaciones efectuadas en la junta de aclaraciones.

Razón Social_____
R.F.C._____
Domicilio _____
Nombre y firma del participante o su representante o apoderado legal_____

Domicilio para firma del contrato respectivo: Señalar en su propuesta que, en caso de resultar adjudicado, el representante legal deberá presentarse a firmar el instrumento contractual respectivo, en la Dirección General de Recursos Materiales, con dirección en calle Bolívar 30, cuarto piso, colonia Centro de la Ciudad de México, código postal 06000, Alcaldía Cuauhtémoc, Ciudad de México, previa cita.

ANEXO 4

MODELO DE CONTRATO ORDINARIO

CONTRATO DE PRESTACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, QUE CELEBRAN, POR UNA PARTE, LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, EN LO SUCESIVO LA "SUPREMA CORTE", REPRESENTADA POR [ ], EN SU CARÁCTER DE [ ] Y, POR LA OTRA, [ ],** ***[EN PARTICIPACIÓN CONJUNTA CON [ ]**, REPRESENTADA*****[S]*** **EN ESTE ACTO POR [ ],** ***Y POR [ ], SEÑALANDO AL [ ] COMO REPRESENTANTE COMÚN*****,** ***EMPRESAS QUE EN SU CONJUNTO SE LES DENOMINARÁ]*** **EN LO SUCESIVO EL "PROVEEDOR", A QUIENES DE MANERA CONJUNTA SE LES IDENTIFICARÁ COMO "LAS PARTES", DE CONFORMIDAD CON LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:**

D E C L A R A C I O N E S

I. LA "SUPREMA CORTE" DECLARA POR CONDUCTO DE SU REPRESENTANTE QUE:

I.1. Es uno de los órganos depositarios del Poder Judicial de la Federación, en términos de lo dispuesto en los artículos 94 de la Constitución Política de los Estados Unidos Mexicanos y 1°, fracción I, de la Ley Orgánica del Poder Judicial de la Federación.

I.2. Requiere contratar el servicio administrado centro de operaciones de Ciberseguridad.

I.3. El Comité de Adquisiciones y Servicios, Obras y Desincorporaciones, en su *primera/segunda/tercera/cuarta/otra* sesión [ ], celebrada el **[ ]**, autorizó el fallo de la licitación pública nacional ***LPN/SCJN/DGRM/[ ]/2023***, adjudicando al *"Prestador de Servicios" la presente contratación/la/s partida/s*…, con fundamento en *el/los artículo/s* [ ], *fracción/fracciones* [ ], del Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil diecinueve, por el que se regulan los procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos por la Suprema Corte de Justicia de la Nación, en lo sucesivo "Acuerdo General de Administración XIV/2019".

I.4. La suficiencia presupuestal se encuentra contemplada en el Programa Anual de Necesidades 2023 para cubrir las erogaciones provenientes del presente contrato y se encuentra disponible en la partida presupuestaria [ ], denominada [" "], de la Unidad Responsable [" "], del presupuesto autorizado para el ejercicio 2023.

Los importes correspondientes a los ejercicios fiscales 2024 a 2027 estarán sujetos a que este Alto Tribunal cuente con los recursos presupuestales desinados para tales efectos, de conformidad con lo establecido en los artículos 39, fracción fracciones II y III del Acuerdo General de Administración XIV/2019 y; 35 y 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, sin que la falta de estaos origine responsabilidad para la Suprema Corte de Justicia de la Nación sin que la falta de éstos origine responsabilidad para la Suprema Corte de Justicia de la Nación

I.5. *El/La* **[ ]**, en su carácter de **[ ]** de la "Suprema Corte", está *facultado/a* para suscribir el presente contrato, según lo dispuesto en el artículo **[,]** *fracción* **[ ]** del *Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación*, y el artículo [ ], del "Acuerdo General de Administración XIV/2019".

I.6. Cuenta con la clave de inscripción en el Registro Federal de Contribuyentes **SCJ9502046P5** expedida a nombre de la Suprema Corte de Justicia de la Nación, por el Servicio de Administración Tributaria.

I.7. Para todo lo relacionado con el presente contrato señala como su domicilio el ubicado en avenida José María Pino Suárez, número 2, colonia Centro, alcaldía Cuauhtémoc, código postal 06060, Ciudad de México.

II. EL *"PRESTADOR DE SERVICIOS"/ LOS "PRESTADORES DE SERVICIOS",* POR CONDUCTO DE SU *APODERADO/A [ ]*, DECLARA BAJO PROTESTA DE DECIR VERDAD, QUE:

[DENOMINACIÓN DE LA EMPRESA] (Empresa "A")

II.1. Es una sociedad mercantil, legalmente constituida y registrada conforme las leyes mexicanas, en términos del testimonio notarial **[ ]** del **[ ]**, pasado ante la fe del/de la licenciado/a **[ ]**, Notario***/***a Público***/***a **[ ]** de/del/de la estado/ciudad; y está debidamente inscrita en el Registro **[ ]** ,en el folio mercantil **[ ]** del **[ ]**.

II.2. El/La señor/a **[ ]**, en su carácter de apoderado general/especial/administrador único de la empresa **[ ]**, cuenta con las facultades suficientes para suscribir el presente contrato, en términos del **[ ]**, otorgado mediante testimonio notarial **[ ]** del **[ ]**, pasado ante la fe del/de la licenciado/a, Notario***/***a Público***/***a **[ ]** de/del/de la estado/ciudad; las cuales, a la fecha, no le han sido revocadas ni limitadas en forma alguna. Es una persona física que cuenta con la capacidad de ejercicio para actuar en el presente contrato.

II.3. Cuenta con la clave de inscripción en el Registro Federal de Contribuyentes **[ ]**, expedida por el Servicio de Administración Tributaria, según cédula de identificación fiscal que exhibe.

II.4. Tiene como domicilio el ubicado en calle/avenida **[ ]**, número **[ ]**, colonia **[ ]**, alcaldía **[ ]**, código postal **[ ]**, **[ ]**.

[*DENOMINACIÓN DE LA EMPRESA] (Empresa "B")*

II.5. *Es una sociedad mercantil, legalmente constituida y registrada conforme las leyes mexicanas, en términos del testimonio notarial **[ ]** del **[ ]**, pasado ante la fe del/de la licenciado/a **[ ]**, Notario**/**a Público**/**a **[ ]** de/del/de la estado/ciudad; y está debidamente inscrita en el Registro **[ ]** ,en el folio mercantil **[ ]** del **[ ]**.*

II.6. *El/La señor/a **[ ]**, en su carácter de apoderado general/especial/administrador único de la empresa **[ ]**, cuenta con las facultades suficientes para suscribir el presente contrato, en términos del poder otorgado mediante testimonio notarial **[ ]** del **[ ]**, pasado ante la fe del/de la licenciado/a, Notario**/**a Público**/**a **[ ]** de/del/de la estado/ciudad; las cuales, a la fecha, no le han sido revocadas ni limitadas en forma alguna.*

II.7. *Cuenta con la clave de inscripción en el Registro Federal de Contribuyentes **[ ]**, expedida por el Servicio de Administración Tributaria, según cédula de identificación fiscal que exhibe.*

II.8. *Tiene como domicilio para todo lo relacionado con el presente contrato el ubicado en calle/avenida **[ ]**, número **[ ]**, colonia **[ ]**, alcaldía **[ ]**, código postal **[ ]**, **[ ]**.*

III. "EL PRESTADOR DE SERVICIOS" A TRAVÉS DE SU REPRESENTANTE COMÚN, MANIFIESTA QUE:

III.1. *El [ ] de [ ] del año [ ] las empresas [y] celebraron un convenio de participación conjunta, cuyas obligaciones deberán cumplirse solidariamente en términos del mismo, por lo que la "Suprema Corte" reconoce el convenio para efectos del presente instrumento jurídico, documento que forma parte integrante del presente contrato como **"Anexo Uno".***

III.2. *Acepta que la presente relación contractual se regirá por las disposiciones del "Acuerdo General de Administración XIV/2019".*

III.3. *A la fecha de la adjudicación de la presente contratación, no se encuentra en ninguno de los supuestos previstos en los artículos 62, fracciones XV y XVI y 193 del "Acuerdo General de Administración XIV/2019".*

III.4. *Conoce perfectamente las especificaciones técnicas y de operación de los servicios, objeto del presente contrato, y cuenta con los recursos o elementos, humanos, técnicos, administrativos, económicos y financieros, así como con la experiencia y todos los requisitos de ley, necesarios para entregarlos a entera a entera satisfacción de la "Suprema Corte".*

III.5. *Designa como domicilio común para todo lo relacionado con el presente contrato el ubicado en calle/avenida* ***[ ]****, número* ***[ ]****, colonia* ***[ ]****, alcaldía* ***[ ]****, código postal* ***[ ]****, [ ].*

Asimismo, manifiesta que comunicará a este Alto Tribunal, por medio de escrito original firmado por el representante en común cualquier cambio de domicilio que realice.

III.6. *Para recibir los pagos en moneda nacional, derivados del presente contrato, señala la cuenta* ***[ ]****, de la institución de banca múltiple* ***[ ]****, plaza* ***[ ]****, sucursal* ***[ ]****, con CLABE interbancaria* ***[ ].***

La cuenta bancaria señalada en la presente declaración podrá sustituirse mediante escrito original firmado por el representante común del "Prestador de Servicios".

IV. "LAS PARTES" DECLARAN RESPECTIVAMENTE POR CONDUCTO DE SUS REPRESENTANTES QUE:

IV.1. Se reconocen mutuamente la personalidad y capacidad jurídica con la que comparecen para la celebración del presente instrumento contractual, sin mediar vicio del consentimiento y manifiestan que todas las comunicaciones que se realicen entre ellas se dirigirán a los domicilios indicados en las declaraciones I.7 y [II.4/III.5] de este instrumento contractual.

IV.2. Conocen el alcance y contenido de este contrato, por lo que están de acuerdo en someterse a las siguientes:

C L Á U S U L A S

PRIMERA. OBJETO DEL CONTRATO.

El objeto del presente contrato consiste en la prestación del servicio administrado centro de operaciones de Ciberseguridad, que la "Suprema Corte" contrata, y el *"Prestador de Servicios" presta*, conforme lo siguiente:

Descripción general **

Servicio	Unidad de medida	Cantidad	Costo mensual	Meses	Subtotal
Servicio de protección para portales web.	Servicio	1	$	36	$
Servicio de protección de correo electrónico	Servicio	1	$	36	$
Servicio de Detección y Protección de amenazas avanzadas con base en comportamiento	Servicio	1	$	36	$
Servicio de Centro de Operaciones de Ciberseguridad (COC)	Servicio	1	$	36	$
Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación	Servicio	1	$	36	$
			SUBTOTAL 1		$

Servicio	Unidad de medida	Cantidad Mínima de usuarios	Cantidad Mínima de usuarios	Costo Mensual por unidad de medida	Meses	Subtotal Mínimo	Subtotal Máximo
Servicio de Protección para puntos finales (XDR)	Usuario	3500	4000	$	36	$	$
				SUBTOTAL 2		$	$

SUBTOTAL 1	$
SUBTOTAL 2 **MÍNIMO**	$
SUMA SUBTOTAL 1 / SUBTOTAL 2 MÍNIMO	$
I.V.A.	$
TOTAL MÍNIMO	**$**

SUBTOTAL 1	$
SUBTOTAL 2 **MÁXIMO**	$
SUMA SUBTOTAL 1 / SUBTOTAL 2 MÁXIMO	$
I.V.A.	$
TOTAL **MÁXIMO**	$

**Fuente de Información: Propuesta técnica económica presentada por el *"Prestador de Servicios"* el [ ].

Para la prestación *de los servicios*, objeto del presente contrato, el *"Prestador de Servicios"* debe cumplir con las normas nacionales e internacionales y demás disposiciones y ordenamientos que resulten aplicables.

Cualquier característica, término o condición no especificados en esta cláusula, serán aplicables los contenidos en la propuesta técnica-económica, presentada por el *"Prestador de Servicios" el **[ ]**, (y) en el "Requerimiento Técnico" anexo a las bases de la licitación pública nacional **LPN/SCJN/DGRM/[ ]/2023**, (en su caso, agregar:) [y en el acta de la Junta de Aclaraciones de **[ ]**,]* ; documentos que forman parte integrante del presente contrato como **"Anexo Dos"**.

Para efectos del presente contrato, el *"Prestador de Servicios"* se compromete a *prestar el/los servicio/s*, objeto del presente contrato, y la "Suprema Corte" a efectuar su pago.

SEGUNDA. MONTO DEL CONTRATO.

El monto del presente contrato es por la cantidad de **$[ ],[ ].[ ] (*pesos[ ]/100 M.N.*)**, más el 16 por ciento del Impuesto al Valor Agregado, equivalente a **$[ ],[ ].[ ] (*pesos[ ]/100 M.N.*)**, resultando un monto total de **$[ ],[ ].[ ] (*pesos [ ]/100 M.N.*)**.

El monto pactado en la presente cláusula cubre el total *del/de los servicio/s*, objeto del presente instrumento contractual, por lo cual, la "Suprema Corte" no tiene obligación de cubrir monto adicional.

El *"Prestador de Servicios"* se obliga a respetar y mantener sin modificación los precios y condiciones de pago pactados en este contrato hasta su conclusión.

. FORMA DE PAGO.

La "Suprema Corte" pagará, al *"Prestador de Servicios",* el monto indicado en la cláusula Segunda del presente instrumento contractual de la manera siguiente:

Los pagos se realizarán a mes vencido, y se realizarán a la empresa [ ] (designada por el "Prestador de Servicios"] *a los 15 días hábiles a partir del día hábil siguiente de la presentación del Comprobante Fiscal Digital generado por Internet (CFDI) correspondiente,* acompañado de la documentación que en líneas posteriores se indica, en la [ ] de la "Suprema Corte", ubicada en [ ], en el siguiente horario: [ ] de [ ] a [ ] horas. No se realizará el pago *del/de los Comprobante/s Fiscal/es Digital/es generado/s* por Internet que *ampare/n los servicio/s* que no se hayan recibido en su totalidad y a entera satisfacción de la "Suprema Corte".

[El "Prestador de Servicios" designa a la empresa [ ] como la emisora del Comprobante Fiscal Digital (CFDI) correspondiente, la cual debe entregar la siguiente documentación: /El "Prestador de Servicios" debe entregar la siguiente documentación:]

A la Dirección General de Recursos Materiales de la "Suprema Corte":

I. Carta membretada en la que se indiquen sus datos bancarios (original):

a. Cuenta
b. Clave bancaria estandarizada a 18 posiciones (CLABE)
c. Banco
d. Sucursal
e. Beneficiario

Al "Administrador del Contrato":

II. Comprobante fiscal digital generado por Internet (CFDI) original a nombre de la Suprema Corte de Justicia de la Nación, con número de Registro Federal de Contribuyentes SCJ 950204 6P5, expedido por el Servicio de Administración Tributaria, que cumpla con los requisitos establecidos por la legislación fiscal vigente, con el Impuesto al Valor Agregado desglosado y con los datos señalados en las declaraciones I.5 y I.6 de este instrumento contractual.

III. Anexar las validaciones del Servicio de Administración Tributaria.

IV. Enviar los archivos "XML" a la dirección de correo electrónico [ ] del administrador del contrato, o a la que comunique por escrito la "Suprema Corte".

V. Anexar constancia de situación fiscal actualizada.

Para la procedencia de los pagos, *los servicios contratados deberán* haber sido recibidos a entera satisfacción de la "Suprema Corte", con base en la validación técnica *del/de la "Administrador/a"* de este contrato, mediante el oficio emitido en ese sentido por éste. Asimismo, previo a emitir el primer pago se deberá haber recibido copia de la póliza de fianza de cumplimiento, validada por la Dirección General de Asuntos Jurídicos de la "Suprema Corte".

Los pagos que realice la "Suprema Corte" en favor del *"Prestador de Servicios"* solo podrán realizarse mediante transferencia electrónica en la cuenta bancaria señalada en la declaración III.6 de este instrumento contractual, la que podrá sustituirse

mediante escrito original firmado por *el/la apoderado/a general, especial, el/la administrador/a único/a*, del *"Prestador de Servicios"*.

"Las Partes" convienen que la "Suprema Corte" podrá, en cualquier momento, retener los pagos que tenga pendientes de cubrir al *"Prestador de Servicios"*, en caso de que este último incumpla cualesquiera de las obligaciones pactadas en el presente instrumento contractual.

CUARTA. PLURIANUALIDAD

Toda vez que la prestación de los servicios, objeto de este contrato, abarcará diversos ejercicios presupuestales, los pagos descritos en la cláusula Segunda de este instrumento contractual estarán condicionados a que la "Suprema Corte" cuente con los recursos presupuestales destinados para tales efectos en los años 2024, 2025, 2026 y 2027.

En tal virtud, de conformidad con lo establecido en el artículo 50, fracción IV, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, y en el artículo 39, fracción II, inciso d), del "Acuerdo General de Administración XIV/2019", a continuación , se desglosan los recursos presupuestales correspondientes a cada ejercicio fiscal:

Año	Partida presupuestal	Gasto Corriente		Costo total del Proyecto Gasto Corriente
		Importe Sin IVA	IVA	Importe Total con IVA
2024	33301	$34,055,083.71	$5,448,813.40	$39,503,897.10
2025	33301	$45,406,778.28	$7,265,084.52	$52,671,862.80
2026	33301	$45,406,778.28	$7,265,084.52	$52,671,862.80
2027	33301	$11,351,694.57	$1,816,271.12	$13,167,965.70
Total		**$136,220,334.84**	**$21,795,253.56**	**$158,015,588.40**

QUINTA. VIGENCIA DEL CONTRATO (*LUGAR Y DURACIÓN DE LOS SERVICIOS*).

El presente instrumento contractual tendrá una vigencia conforme lo siguiente:

Lugar de prestación de los servicios:

Los trabajos de implementación, operación, mantenimiento preventivo y correctivo, y soporte técnico de los servicios de seguridad informática del presente proyecto, se llevarán a cabo en los inmuebles de la "Suprema Corte" ubicados en la Ciudad de México.

Como excepción, para el servicio de protección para puntos finales (XDR) se deberá dar soporte de manera remota a los inmuebles de las Casas de la Cultura Jurídicas (CCJ), edificios distribuidos en la República Mexicana.

Para el servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática se prestarán en los inmuebles de la "Suprema Corte" ubicados en la Ciudad de México

Duración de los servicios:

La vigencia del servicio tendrá una duración conforme a lo siguiente:

La operación del servicio será de 36 meses devengados contados a partir del 1ro de abril de 2024 y hasta el 31 de marzo de 2027.

La vigencia de prestación de servicios y fechas para los entregables, pactados en el presente contrato, únicamente podrán ser prorrogado por causas plenamente justificadas y por caso fortuito o fuerza mayor, previa presentación de la solicitud respectiva, antes del vencimiento del plazo de entrega, por parte del *"Prestador de Servicios"* y su aceptación por parte de la "Suprema Corte".

En caso de que ***la prestación de los servicios***, materia de este instrumento contractual, no sea posible por causas imputables a la "Suprema Corte", ésta se realizará en la fecha que por escrito le señale *el/la "Administrador/a"* del contrato al *"Prestador de Servicios".*

SEXTA. IMPUESTOS.

"Las Partes" convienen que cada una es exclusivamente responsable de dar cumplimiento, conforme la legislación aplicable, a sus respectivas obligaciones fiscales originadas con motivo de la celebración del presente contrato.

SÉPTIMA. PAGOS EN EXCESO.

Tratándose de pagos en exceso que haya recibido el *"Prestador de Servicios"*, éste deberá reintegrar las cantidades excedentes, más los intereses que se hayan generado, mismos que se calcularán conforme a una tasa que será igual a la establecida por el Código Fiscal de la Federación y la Ley de Ingresos de la Federación para el ejercicio fiscal correspondiente a la fecha de pago, para el supuesto de prórroga en el pago de créditos fiscales.

Los cargos se calcularán sobre las cantidades recibidas en exceso en cada caso y se computarán por días naturales, desde la fecha en la que se recibió el excedente hasta que se pongan efectivamente las cantidades a disposición de la "Suprema Corte".

OCTAVA. PROCESO DE RECEPCIÓN DE LOS SERVICIOS.
El proceso de recepción de *los servicios,* objeto del presente contrato, debe realizarse bajo la estricta responsabilidad del/de la *"Administrador/a"* de este contrato, de acuerdo con el procedimiento que este determine, en términos de lo pactado en el presente instrumento contractual y de conformidad con lo dispuesto por el "Acuerdo General de Administración XIV/2019" y en las bases de la licitación pública nacional ***LPN/SCJN/DGRM/[ ]/2023***.

NOVENA. ACCESO AL INTERIOR DE LOS INMUEBLES.

La "Suprema Corte" permitirá al *"Prestador de Servicios"* el acceso necesario a los lugares en donde deban prestarse los servicios, objeto de este contrato, así como en las ocasiones que la "Suprema Corte" lo solicite, reconociendo el *"Prestador de Servicios"* la existencia de los métodos de control y seguridad que tiene la "Suprema Corte", incluyendo aquellos relativos

a prevenir la transmisión de la enfermedad causada por el virus SARS CoV2 (COVID 19) o cualquier otra enfermedad contagiosa, y se compromete a acatarlos y respetarlos.

DÉCIMA. RESPONSABILIDAD CIVIL.

El *"Prestador de Servicios"* responderá por los daños que se causen a los bienes en posesión o en propiedad de la "Suprema Corte" con motivo de la entrega-recepción de los servicios objeto del presente contrato, o por defecto de estos, aun cuando no exista negligencia. La reparación del daño consistirá, a elección de la "Suprema Corte", en el restablecimiento de la situación anterior, cuando ello sea posible, o en el pago de daños y perjuicios, con independencia de ejercer las acciones legales a que haya lugar.

DÉCIMA PRIMERA. GARANTÍA DE CUMPLIMIENTO*.*

Para garantizar el fiel y exacto cumplimiento de todas y cada una de las obligaciones que el *"Prestador de Servicios"* asume con la celebración del presente contrato, así como para el pago de las penas estipuladas y posibles pagos en exceso con los intereses correspondientes, se obliga a otorgar fianza de compañía legalmente autorizada por el equivalente al 10 (diez) por ciento del importe neto del instrumento contractual, sin incluir los impuestos aplicables, esto es, por la cantidad de **$[ ],[ ].[ ] (*pesos 00/100 M.N.*)**, y hasta 20 (veinte) por ciento más en el supuesto de que por algún motivo deban incrementarse *la cantidad de los servicios contratados, el monto o el plazo pactados.*

La presente garantía deberá contratarse de modo que esté vigente hasta que **[ ]** materia del contrato de referencia hayan sido recibidos en su totalidad y a entera satisfacción de la "Suprema Corte". Dicha fianza sólo podrá ser cancelada con el consentimiento expreso y por escrito de la "Suprema Corte".

I. En la póliza de fianza que se expida por la institución autorizada, deberá constar la siguiente leyenda:

"- Nombre de la afianzadora- en ejercicio de la autorización que le fue otorgada por la Comisión Nacional de Seguros y Fianzas de conformidad con lo dispuesto en la Ley de Instituciones de Seguros y de Fianzas, se constituye ante la Suprema Corte de Justicia de la Nación, en fiadora hasta por la cantidad de **$[ ],[ ].[ ] (*pesos 00/100 M.N.*)**, y hasta un 20 por ciento más en el supuesto de que por algún motivo deban incrementarse *la cantidad de los servicios contratados, el monto o el plazo pactado,* para garantizar, por parte de **[ ]**, con domicilio en **[ ]**, el fiel y exacto cumplimiento de todas y cada una de las obligaciones a su cargo, derivadas del contrato número **SCJN/DGRM/[ ]-[ ]/[ ]/[ ]**, celebrado entre la Suprema Corte de Justicia de la Nación y **[ ]**, con un monto total contratado que asciende a la cantidad de **$[ ],[ ].[ ] (*pesos [ ]/100 M.N.)***, más el Impuesto al Valor Agregado.

"La afianzadora" expresamente declara que:

- La presente fianza se expide de conformidad con lo establecido en el "Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil diecinueve, por el que se regulan los procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos por la Suprema Corte de Justicia de la Nación" y en el contrato número **SCJN/DGRM/[ ]-[ ]/[ ]/[ ]**, celebrado entre la Suprema Corte de Justicia de la Nación y **[ ]**, con el objeto de garantizar el fiel y exacto cumplimiento de todas y cada una de las obligaciones a cargo de **[ ]**, relativo a **[ ]**, con un monto contratado por la cantidad de **$[ ],[ ].[ ] (pesos 00/100 M.N.)**, más el Impuesto al Valor Agregado.

- La fianza se otorga atendiendo a las cláusulas contenidas en el Contrato número **SCJN/DGRM/[ ]-[ ]/[ ]/[ ]**.

- La presente fianza tendrá vigencia durante toda la duración del Contrato número **SCJN/DGRM/[ ]-[ ]/[ ]/[ ]**y la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por

autoridad competente, y sólo podrá ser cancelada con el consentimiento previo, expreso y por escrito de la Suprema Corte de Justicia de la Nación.

- La afianzadora acepta someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y de Fianzas para la efectividad de la fianza, aun para el caso de que procediera el cobro de intereses con motivo del pago extemporáneo del importe de la fianza requerida.

- La fianza garantiza el cumplimiento total de lo contratado, aun cuando exista subcontratación con la autorización expresa de la Suprema Corte de Justicia de la Nación.

- En caso de incumplimiento contractual de **[ ]**, la Suprema Corte de Justicia de la Nación o la Tesorería de la Federación podrán reclamar el pago de la cantidad establecida en la presente póliza de fianza, conforme a los procedimientos señalados en los artículos 279 y 282 de la Ley de Instituciones de Seguros y de Fianzas.

- La presente fianza podrá ser liberada a **[ ]**, siempre y cuando la Suprema Corte de Justicia de la Nación emita su consentimiento por escrito en el que conste el cumplimiento del contrato.

- La presente fianza garantizará la obligación principal del contrato debiendo cubrir el importe correspondiente a la obligación principal, así como el pago de penas convencionales a que se haga acreedor **[ ]**, pagos en exceso y los intereses que correspondan por los mismos. Tratándose de prórrogas en el plazo de ejecución pactadas en algún instrumento de la misma naturaleza del contrato original, la presente fianza quedará vigente por un plazo igual al acordado en el convenio modificatorio que, en su caso, llegare a suscribirse, o el que corresponda al plazo de atraso. De existir incremento en el monto o plazo de ejecución, la fianza cubrirá hasta un 20 (veinte) por ciento adicional al originalmente pactado.

- Para la interpretación y cumplimiento de las cláusulas contenidas en el presente contrato de fianza, así como en caso de controversia, siempre que una de las partes en contienda sea la Suprema Corte de Justicia de la Nación, la institución de fianzas se somete expresamente a las decisiones del Tribunal Pleno de la Suprema Corte de Justicia de la Nación, órgano competente para interpretar y hacer cumplir lo pactado en este contrato, en términos de lo dispuesto en el artículo 11, fracción XXII, de la Ley Orgánica del Poder Judicial de la Federación, renunciando en forma expresa a cualquier otro fuero que en razón del domicilio tenga o llegare a tener."

II. "Las Partes" convienen en que la fianza deberá ser presentada dentro de los 10 (diez) días hábiles siguientes a la fecha en que se firme el contrato. En caso de que transcurrido el plazo señalado no se hubiere presentado la fianza en la forma y términos pactados, la "Suprema Corte" podrá rescindir el presente contrato.

El "Prestador de Servicios", por medio de este instrumento, renuncia expresamente al derecho de compensación que pudiera hacer valer en contra de la "Suprema Corte", dando con esta renuncia cumplimiento a lo que se establece en el último párrafo del artículo 289 de la Ley de Instituciones de Seguros y de Fianzas.

"Las Partes" convienen que la presente garantía será exigible cuando el "Prestador de Servicios" incumpla cualquiera de las cláusulas previstas en el presente instrumento jurídico.

DÉCIMA SEGUNDA. PENA CONVENCIONAL.

Las penas convencionales serán determinadas por la "Suprema Corte", en función del incumplimiento decretado, conforme a lo siguiente:

Se aplicarán las penas convencionales por atraso en el cumplimiento de las fechas pactadas de entrega o con motivo del incumplimiento parcial o deficiente en que pudiera incurrir la persona adjudicada, respecto de los servicios prestados, mismas que de forma enunciativa se relacionan a continuación:

En caso de incumplimiento de las responsabilidades, obligaciones pactadas en el instrumento contractual entregables, actividades, plazos de prestación de los servicios, materia del presente contrato, o bien, no se hayan recibido a entera satisfacción, la "Suprema Corte" podrá aplicar al "Prestador de Servicios" una pena convencional hasta por el 30 (treinta) por ciento del monto que corresponda al valor de los servicios sin incluir el Impuesto al Valor Agregado, que no se hayan prestado, o bien, no se hayan recibido a entera satisfacción de la "Suprema Corte".

En caso de que no se otorgue prórroga al "Prestador de Servicios" respecto al cumplimiento de los plazos establecidos en el contrato, se aplicará una pena convencional por atrasos que le sean imputables en la entrega de los bienes o prestación del servicio equivalente al monto que resulte de aplicar el 1% (uno por ciento) por cada día natural a la cantidad que importen los servicios no prestados, y no podrán exceder del 30% (treinta por ciento) del monto total del contrato, sin incluir el Impuesto al Valor Agregado.

Sin perjuicio de las penas antes indicadas, se podrán aplicar penas convencionales, conforme a lo siguiente:

CONCEPTO	SLA	PENALIZACIONES
Servicio de Centro de Operaciones de Ciberseguridad (COC)	**1)** El servicio deberá iniciar conforme al plan de trabajo establecido (numeral 8 del anexo técnico), con una vigencia a partir de su puesta en operación y hasta la finalización del contrato. **2)** Criticidad: • Para eventos de seguridad de nivel crítico o alto, se deberá dar solución en un plazo no mayor a 4 hrs. a partir del evento. • Para eventos de seguridad de nivel informativo, bajo o medio, se deberá dar solución en un plazo no mayor a 24 hrs. a partir del evento. • Para la atención de requerimientos (Altas, Bajas, Cambios) se deberá dar solución en un plazo no mayor a 4 hrs. a partir del envío del requerimiento.	**1)** En caso de que el prestador de servicios no pueda iniciar el servicio en el periodo establecido en el plan de trabajo (numeral 8 del anexo técnico) para esta actividad, se aplicará una penalización del **1% por cada día natural** de retraso, a la cantidad que importen los servicios pendientes de prestar. **2)** En el supuesto de que el prestador de servicios no pueda solucionar los eventos de seguridad o la atención de requerimientos en los tiempos establecidos de acuerdo con la prioridad correspondiente, se aplicará una penalización del **1% por cada hora** de atraso, sobre el **monto mensual del servicio**, por cada incidente no resuelto.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

CONCEPTO	SLA	PENALIZACIONES
Servicio de protección para portales web. Servicio de protección de correo electrónico Servicio de detección y protección de amenazas avanzadas con base en comportamiento Servicio de protección para puntos finales (XDR)	**1)** El servicio deberá iniciar conforme al plan de trabajo establecido (numeral 8 del anexo técnico), con una vigencia a partir de su puesta en operación y hasta la finalización del contrato. **2)** En caso de falla del servicio, éste deberá ser restablecido en un plazo no mayor a 4 horas, a partir del levantamiento del reporte. **3)** En caso de requerirse el cambio de algún componente del servicio por falla técnica, este deberá ser reemplazado por un componente de las mismas características o superiores en un plazo no mayor a 7 días naturales, a partir de la restauración del servicio.	**1)** En caso de que el prestador de servicios no pueda iniciar el servicio en el periodo establecido en el plan de trabajo (numeral 8 del anexo técnico) para esta actividad, se aplicará una penalización del **1% por cada día natural** de retraso, a la cantidad que importen los servicios pendientes de prestar. **2)** En caso de que el prestador de servicios no pueda reestablecer los servicios por falla de la solución en un plazo menor a 4 horas a partir del levantamiento del reporte, se aplicará una penalización de **1% por cada hora** de indisponibilidad posterior al tiempo máximo para recuperación del servicio, sobre el **monto mensual del servicio por evento.** **3)** En caso de que el prestador de servicios no pueda reemplazar algún componente del servicio por falla técnica, en un plazo máximo de 7 días naturales a partir de la restauración del servicio, se aplicará una penalización de **1% por cada día natural** de retraso, sobre el **monto mensual del servicio por evento.**
Entregables	**1)** Tiempo establecido en el apartado de entregables (numeral 5 del anexo técnico).	**1)** En caso de que el prestador de servicios no cumpla con los tiempos establecidos para los entregables (numeral 5 del anexo técnico), se aplicará una penalización del **1% por cada día natural** de retraso, sobre el **monto mensual del servicio**.

De existir incumplimiento parcial, la pena se ajustará proporcionalmente al porcentaje incumplido.

Si las penas convencionales rebasan el porcentaje señalado anteriormente, se podrá iniciar el procedimiento de rescisión del contrato.

El *"Prestador de Servicios"*, responsable del incumplimiento, se hará acreedor a las penas convencionales previstas en los párrafos que anteceden, con independencia de que se hagan efectivas las garantías otorgadas.

Las penas podrán descontarse de los montos pendientes de cubrir por parte de la "Suprema Corte" al *"Prestador de Servicios"* o, de ser necesario, ingresando su monto a la Tesorería de este Alto Tribunal.

DÉCIMA TERCERA. PROPIEDAD INTELECTUAL.

El "Prestador de Servicios" asume totalmente la responsabilidad para el caso de que al prestar *el/los servicio/s*, objeto de este contrato descritos en la cláusula primera del presente contrato, infrinja derechos de propiedad intelectual, así como respecto a su origen lícito y por lo tanto libera a la "Suprema Corte" de cualquier responsabilidad de carácter civil, penal, fiscal o de cualquier otra índole.

Los servicios ejecutados total o parcialmente, especificaciones y en general toda documentación que se hubiese entregado al "Prestador de Servicios" o de la que hubiere tenido conocimiento con motivo de la prestación *de/l el/los servicio/s* o de su estancia al interior de la "Suprema Corte", son propiedad de la misma, por lo que el "Prestador de Servicios" se obliga a devolver a la "Suprema Corte", el material que le hubiesen proporcionado para la prestación de los servicios materia de este instrumento contractual, así como el material que llegue a realizar, obligándose a abstenerse de reproducirlos en medio electrónico o físico.

Asimismo, todo material que llegue a realizar el "Prestador de Servicios" como producto de esta contratación, es propiedad de la "Suprema Corte", por lo que bajo ninguna circunstancia podrá ser divulgada.

El material y/o información que sea entregado al "Prestador de Servicios", con motivo del presente contrato, no podrá ser duplicado ni reproducido de forma total o parcial, salvo para la reproducción exclusiva del servicio solicitado. Ante cualquier uso indebido de material y/o información, o de los resultantes del proceso, la "Suprema Corte" podrá ejercer las acciones legales conducentes, por lo que el "Prestador de Servicios" es responsable en su totalidad de la violación que, en su caso, se haga de los derechos de propiedad intelectual.

DÉCIMA CUARTA. SUBCONTRATACIÓN.

La "Suprema Corte" manifiesta que no aceptará la subcontratación para el cumplimiento del objeto de la presente contratación.

Para los efectos de esta contratación, se entiende por subcontratación el acto mediante el cual el *"Prestador de Servicios"* encomienda a otra persona física o jurídica, la ejecución parcial o total del objeto del contrato.

DÉCIMA QUINTA. INTRANSMISIBILIDAD DE LOS DERECHOS Y OBLIGACIONES DERIVADOS DEL PRESENTE CONTRATO.

El "Prestador de Servicios" no podrá ceder, gravar, transferir o afectar bajo cualquier título, parcial o totalmente a favor de otra persona, física o moral, los derechos y obligaciones que deriven del presente contrato, con excepción de los derechos de cobro, con autorización previa y expresa de la "Suprema Corte".

DÉCIMA SEXTA. RESCISIÓN DEL CONTRATO.

"Las Partes" aceptan que la "Suprema Corte" podrá rescindir, de manera unilateral, el presente contrato sin que medie declaración judicial, en caso de que el *"Prestador de Servicios"* deje de cumplir cualesquiera de las obligaciones que asume en el presente contrato por causas que le sean imputables, o bien, en caso de ser objeto de embargo, huelga estallada, concurso mercantil o liquidación.

Antes de declarar la rescisión, la "Suprema Corte" notificará por escrito las causas de rescisión al *"Prestador de Servicios"* en el domicilio señalado en la declaración [*II.4/ III.5]* de este instrumento contractual, con quien en el acto se encuentre, otorgándole un plazo de 5 (cinco) días hábiles para que manifieste lo que a su derecho convenga y anexe los documentos que estime convenientes y, vencido este plazo, con su respuesta o sin ella, el órgano competente de la "Suprema Corte" resolverá sobre la procedencia de la rescisión, lo que se comunicará al "Prestador de Servicios" en su domicilio señalado en la declaración *[II.4/III.5]* del presente instrumento contractual con quien en el acto se encuentre.

Serán causas de rescisión del presente instrumento contractual las siguientes:

1. Si el *"Prestador de Servicios"* no exhibe la garantía en los términos y condiciones pactados en este contrato.

2. Si el *"Prestador de Servicios"* suspende *la prestación de los servicios* objeto del presente contrato.

3. Si el *"Prestador de Servicios"* incurre en falsedad total o parcial respecto de la información proporcionada para la celebración del presente contrato.

4. En general, por el incumplimiento por parte del *"Prestador de Servicios"* a cualesquiera de las obligaciones derivadas del presente contrato.

En los supuestos a que se refiere esta cláusula, "Las Partes" convienen que la "Suprema Corte" podrá descontarle al "Prestador de Servicios" del monto pendiente por pagar, la pena convencional decretada por la "Suprema Corte" a que se refiere la cláusula Décima Segunda del presente instrumento, considerando las causas que hayan motivado la rescisión, o bien, en caso de que ya no existan montos pendientes de pago, el *"Prestador de Servicios"* se compromete a ingresar el monto de la pena convencional a la Tesorería de la "Suprema Corte"; ello, independientemente de que haga efectiva la garantía de cumplimiento establecida en este contrato.

DÉCIMA SÉPTIMA. SUPUESTOS DE TERMINACIÓN DEL CONTRATO, DIVERSOS A LA RESCISIÓN.

El presente contrato podrá darse por terminado, además de los supuestos de rescisión a que se refiere la cláusula Décima Sexta de este instrumento contractual, al cumplimentarse su objeto; o bien, de manera anticipada, cuando existan causas justificadas, en términos de lo previsto en los artículos 153, 154, 155 y 156 del "Acuerdo General de Administración XIV/2019".

DÉCIMA OCTAVA. SUSPENSIÓN TEMPORAL DEL CONTRATO.

"Las Partes" acuerdan que la "Suprema Corte" podrá, en cualquier momento, suspender temporalmente, en todo o en parte el objeto materia de este contrato, por causas justificadas, sin que ello implique su terminación definitiva y, por tanto, el presente contrato podrá continuar produciendo todos sus efectos legales una vez desaparecidas las causas que motivaron dicha suspensión. El procedimiento de suspensión se regirá por lo dispuesto en el artículo 150 del "Acuerdo General de Administración XIV/2019".

DÉCIMA NOVENA. MODIFICACIÓN AL CONTRATO.

"Las Partes" convienen que cualquier modificación al presente instrumento contractual procederá por mutuo acuerdo, previa aprobación del órgano competente de la "Suprema Corte" de conformidad con lo dispuesto en el artículo 148 del "Acuerdo General de Administración XIV/2019".

VIGÉSIMA. ADMINISTRADOR DEL CONTRATO.

La "Suprema Corte" designa *a/al* **[ ]** adscrito a la *Dirección General de [ ]* de la "Suprema" Corte", como "*Administrador/a*" del presente contrato, quien tendrá las facultades de administración del presente contrato y para supervisar su estricto cumplimiento; en consecuencia, deberá revisar e inspeccionar las actividades que desempeñe el *"Proveedor"*, así como girar por escrito o correo electrónico las instrucciones que considere oportunas, mismas que el *" Proveedor"* queda obligado a atender a la brevedad y a satisfacción de "La Suprema Corte"; asimismo, deberán verificar que los bienes, objeto de este contrato, cumplan con las especificaciones señaladas en el presente instrumento.

La [ ] de la "Suprema Corte" podrá sustituir al/a la "Administrador/a", lo que informará por escrito al "*Proveedor"*.

VIGÉSIMA PRIMERA. INEXISTENCIA DE LA RELACIÓN LABORAL.
Todas las personas que intervengan para la realización del objeto de este contrato, serán trabajadores del *"Prestador de Servicios"*, por lo que de ninguna manera existirá relación laboral entre ellos y la "Suprema Corte". Será responsabilidad del "Prestador de Servicios" cumplir con todas las obligaciones que a cargo de los patrones establecen las disposiciones que regulan SAR, INFONAVIT, IMSS y las contempladas en la Ley Federal del Trabajo; por tanto, responderá a todas las reclamaciones administrativas y juicios de cualquier orden que los trabajadores del *"Prestador de Servicios"* presenten en su contra o de la "Suprema Corte", en relación con el objeto del presente contrato. El gasto que implique el cumplimiento de estas obligaciones correrá a cargo del "Prestador de Servicios", el que será el único responsable de las obligaciones adquiridas con sus trabajadores.

La "Suprema Corte" estará facultada para requerir al *"Prestador de Servicios"* los comprobantes de afiliación de sus trabajadores al IMSS, así como los comprobantes de pago de las cuotas al SAR, INFONAVIT e IMSS.

En caso de que alguno o algunos de los trabajadores del *"Prestador de Servicios"* ejecuten o pretendan ejecutar alguna reclamación administrativa o juicio en contra de la "Suprema Corte", el "Prestador de Servicios" deberá rembolsar la totalidad de los gastos que erogue la "Suprema Corte" con motivo de las demandas instauradas por concepto de traslado, viáticos, hospedaje, transportación, alimentos y demás inherentes, con el fin de acreditar ante la autoridad competente que no existe relación laboral alguna con los mismos, y deslindar a la "Suprema Corte" de cualquier tipo de responsabilidad en ese sentido.

"Las Partes" acuerdan que el importe de los referidos gastos que se llegaran a ocasionar podrá ser deducido por la "Suprema Corte" de los Comprobantes Fiscales Digitales generados por Internet (CFDI) que se encuentren pendientes de pago, independientemente de las acciones legales que se pudieran ejercer.

VIGÉSIMA SEGUNDA. CONFIDENCIALIDAD, FOMENTO A LA TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

"Las Partes" reconocen que la información contenida en el presente contrato y los entregables que se generen podrán ser susceptibles de clasificarse como reservada y/o confidencial, en términos de los artículos 106, 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, así como 98, 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública.

El *"Prestador de Servicios"* se obliga a no realizar acciones que comprometan la seguridad de las instalaciones de la "Suprema Corte" o pongan en riesgo la integridad de su personal, así como abstenerse, conforme a las disposiciones aplicables, de dar a conocer por cualquier medio a quien no tenga derecho, documentos, registros, imágenes, constancias, estadísticas, reportes o cualquier otra información clasificada como reservada o confidencial de la que se tenga conocimiento en el ejercicio y con motivo de la entrega de los servicios.

De conformidad con lo establecido en el artículo 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el *"Prestador de Servicios"* asume el carácter de encargado del tratamiento de datos

personales que tenga acceso con motivo de la documentación que maneje o conozca al desarrollar las actividades objeto del presente contrato, así como los resultados obtenidos, por lo que no tendrá poder alguno de decisión sobre los datos personales.

En ese sentido, el *"Prestador de Servicios"* se obliga a lo siguiente:

a. Abstenerse de tratar los datos personales para finalidades distintas a las autorizadas por la "Suprema Corte";

b. Guardar confidencialidad y abstenerse de transferir los datos personales tratados, así como informar a la "Suprema Corte" cuando ocurra una vulneración a los mismos;

c. Eliminar y devolver los datos personales objeto de tratamiento una vez cumplido el presente contrato; y

d. No subcontratar servicios que conlleven el tratamiento de datos personales, en términos del artículo 61 de la LGPDPPSO.

VIGÉSIMA TERCERA. LEGISLACIÓN APLICABLE.

El acuerdo de voluntades previsto en este instrumento contractual se rige por lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, el Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, el "Acuerdo General de Administración XIV/2019", y en lo no previsto en estos, por el Código Civil Federal, el Código Federal de Procedimientos Civiles, la Ley Federal de Presupuesto y Responsabilidad Hacendaria, la Ley General de Responsabilidades Administrativas, la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Procedimiento Administrativo y la Ley Federal del Derecho de Autor en lo conducente.

VIGÉSIMA CUARTA. FORMALIZACIÓN DEL CONTRATO.

"Las Partes" manifiestan su conformidad en que el presente acuerdo de voluntades se pacta con fundamento en los artículos 1794 y 1796 del Código Civil Federal vigente, por lo que, *el/los plazo/s pactado/s debe/n* cumplirse en términos de lo establecido en la cláusula Quinta, con independencia de que, debido a los trámites y gestiones internas, el contrato se formalice (por escrito) en fecha posterior.

VIGÉSIMA QUINTA. PREVALENCIA DE BASES DE LA LICITACIÓN.

"Las Partes" aceptan que, en caso de que se actualice alguna discrepancia u omisión entre las bases de la Licitación Pública Nacional ***LPN/SCJN/DGRM/[ ]/2023*** y el presente contrato, prevalecerá lo estipulado en aquellas sobre el presente instrumento contractual.

VIGÉSIMA SEXTA. TRIBUNAL COMPETENTE.

Para la interpretación y cumplimiento de las cláusulas contenidas en el presente contrato, así como en caso de controversia, "Las Partes" se someten expresamente a las decisiones del Tribunal Pleno de la Suprema Corte de Justicia de la Nación, órgano competente para interpretar y hacer cumplir lo pactado en el mismo, en términos de los dispuesto en el artículo 11, fracción XXII, de la Ley Orgánica del Poder Judicial de la Federación, renunciando en forma expresa a cualquier otro fuero que, en razón de su domicilio o vecindad, tengan o llegaren a tener.

VIGÉSIMA SÉPTIMA. ANEXOS.

Forma parte integrante del presente contrato los siguientes anexos:

"Anexo Uno" Convenio de participación conjunta suscrito por el "Prestador de Servicios".

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

"Anexo Dos". La propuesta técnica-económica presentada por el *"Prestador de Servicios"* el **[ ]**, el "Requerimiento Técnico" anexo a las bases de la licitación pública nacional ***LPN/SCJN/DGRM/[ ]/2023*****,** *(en su caso, agregar:) [y el acta de la Junta de Aclaraciones de **[ ]**,]*

Leído y entendido el alcance del presente contrato, "las Partes" lo firman de conformidad por duplicado en la Ciudad de México, el **[ ]** de **[ ]** de **[ ].**

POR LA "SUPREMA CORTE"	**POR EL "PRESTADOR DE SERVICIOS"**
[ ]	**[ ]**
	REPRESENTANTE LEGAL DE LA EMPRESA [ ]
[ ]	**[ ]**
AVALA EL CONTENIDO ADMINISTRATIVO DEL CONTRATO	REPRESENTANTE LEGAL DE LA EMPRESA [ ]

GABP/LFCV/APR/MAEV/AHL/ECC

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

[ ]

AVALA QUE LOS ALCANCES SON PRECISAMENTE LOS QUE DARÁN SATISFACCIÓN A SU

REQUERIMIENTO

_____

[ ]

ADMINISTRADOR/A DEL CONTRATO

SCJN/DGRM/[ ]-[ ]/[ ]/[ ]

ESTA FOJA FORMA PARTE DEL CONTRATO DE [ ] DE [ ], SCJN/DGRM/[ ]-[ ]/[ ]/[ ], CELEBRADO POR LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN Y [ ], EN PARTICIPACIÓN CONJUNTA DE [ ].

“Anexo Uno”

Convenio de participación conjunta suscrito por el “Prestador de Servicios”

“Anexo Dos”

La propuesta técnica-económica presentada por

el *“Prestador de Servicios”* el [ ],

“Requerimiento Técnico” anexo a las bases

de la licitación pública nacional *LPN/SCJN/DGRM/[ ]/2023*,

(en su caso, agregar:) [y Acta de la

Junta de Aclaraciones de [ ],]

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ESTA FOJA FORMA PARTE DEL CONTRATO DE [ ] DE [ ], SCJN/DGRM/[ ]-[ ]/[ ]/[ ], CELEBRADO POR LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN Y [ ], EN PARTICIPACIÓN CONJUNTA DE [ ].

El presente modelo de contrato está sujeto a las adecuaciones que se estimen necesarias derivadas del propio procedimiento y/o de la revisión por parte de la instancia competente de la SCJN.

La participación conjunta es solo una opción.

La información del cuadro plasmado en la cláusula primera está sujeta a los cambios que deriven del propio procedimiento y/o de la revisión por parte de la instancia competente de la SCJN.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 5

FORMATO DE GARANTÍA DE CUMPLIMIENTO

Para garantizar el fiel y exacto cumplimiento de todas y cada una de las obligaciones que el "Prestador de Servicios" asume con la celebración del presente contrato, así como para el pago de las penas estipuladas y posibles pagos en exceso con los intereses correspondientes, se obliga a otorgar fianza de compañía legalmente autorizada por el equivalente al 10 (diez) por ciento del monto total del mismo, sin incluir los impuestos aplicables, esto es, por la cantidad de $_____ (_____ pesos __/100 moneda nacional), y hasta 20 (veinte) por ciento más, en el supuesto de que por algún motivo deba incrementarse la cantidad de los servicios contratados, el monto o el plazo del contrato.

La presente garantía deberá contratarse de modo que esté vigente hasta que los servicios, materia del contrato de referencia, hayan sido recibidos en su totalidad y a entera satisfacción de la "Suprema Corte". Dicha fianza solo podrá ser cancelada con el consentimiento expreso y por escrito de la "Suprema Corte".

I. En la póliza de fianza que se expida por institución autorizada, deberá constar la siguiente leyenda:
"Nombre de la afianzadora en ejercicio de la autorización que le fue otorgada por la Comisión Nacional de Seguros y Fianzas de conformidad con lo dispuesto en la Ley de Instituciones de Seguros y de Fianzas, se constituye ante la Suprema Corte de Justicia de la Nación, en fiadora hasta por la cantidad de $_____ (_____ pesos __/100 moneda nacional), y hasta un 20 (veinte) por ciento más en el supuesto de que por algún motivo deba incrementarse la cantidad de los servicios contratados, el monto, o el plazo del contrato, para garantizar, por parte de _____, _____, con domicilio en calle _____, número ___, colonia _____, Alcaldía _____, código postal ___, México, _____, el fiel y exacto cumplimiento de todas y cada una de las obligaciones a su cargo, derivadas del contrato número xxxxxxx, celebrado entre la Suprema Corte de Justicia de la Nación y _____, _____ con un monto contratado que asciende a la cantidad de $_____ (_____ pesos __/100 moneda nacional), más el Impuesto al Valor Agregado.

La afianzadora expresamente declara que:
- La presente fianza se expide de conformidad con lo establecido en el "Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil diecinueve, por el que se regulan los procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos por la Suprema Corte de Justicia de la Nación" y en el contrato número xxxxxxxxx, celebrado entre la Suprema Corte de Justicia de la Nación y _____, _____, con el objeto de garantizar el fiel y exacto cumplimiento de todas y cada una de las obligaciones a cargo de _____, _____, relativo a _____, con un monto contratado por la cantidad de $_____ (_____ pesos 00/100 moneda nacional), más el Impuesto al Valor Agregado.
- La fianza se otorga atendiendo a las cláusulas contenidas en el contrato número xxxxxxxxxx.

- La presente fianza tendrá vigencia en toda la duración del Contrato número XXXXXXXXXXXXXx y, la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por autoridad competente; y solo podrá ser cancelada con el consentimiento previo, expreso y por escrito de la Suprema Corte de Justicia de la Nación.
- La afianzadora acepta someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y de Fianzas para la efectividad de la fianza, aun para el caso de que procediera el cobro de intereses con motivo del pago extemporáneo del importe de la fianza requerida.
- La fianza garantiza el cumplimiento total de lo contratado, aun cuando exista subcontratación con autorización expresa de la Suprema Corte de Justicia de la Nación. En caso de incumplimiento contractual de _____, la Suprema Corte de Justicia de la Nación o la Tesorería de la Federación podrán reclamar el pago de la cantidad establecida en la presente póliza de fianza, conforme a los procedimientos señalados en los artículos 279 y 282 de la Ley de Instituciones de Seguros y de Fianzas.
- La presente fianza podrá ser liberada a _____, siempre y cuando la Suprema Corte de Justicia de la Nación emita su consentimiento por escrito en el que conste el cumplimiento del contrato.
- La presente fianza garantizará la obligación principal del contrato debiendo cubrir el importe correspondiente a la obligación principal, así como el pago de penas convencionales a que se haga acreedor _____, _____, pagos en exceso y los intereses que correspondan por los mismos. Tratándose de prórrogas en el plazo de ejecución pactadas en algún instrumento de la misma naturaleza del contrato original, la presente fianza quedará vigente por un plazo igual al acordado en el convenio modificatorio que, en su caso, llegare a suscribirse, o el que corresponda al plazo de atraso. De existir incremento en el monto o plazo de ejecución, la fianza cubrirá hasta un 20 (veinte) por ciento adicional al originalmente pactado.

- Para la interpretación y cumplimiento de las cláusulas contenidas en el presente contrato de fianza, así como en caso de controversia, siempre que una de las partes en contienda sea la Suprema Corte de Justicia de la Nación, la institución de fianzas se somete expresamente a las decisiones del Tribunal Pleno de la Suprema Corte de Justicia de la Nación, órgano competente para interpretar y

hacer cumplir lo pactado en este contrato, en términos de lo dispuesto en el artículo 11, fracción XXII, de la Ley Orgánica del Poder Judicial de la Federación, renunciando en forma expresa a cualquier otro fuero que, en razón del domicilio que tenga o llegare a tener."

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
LICITACIÓN PÚBLICA NACIONAL No. LPN/SCJN/DGRM/005/2023
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD, MEDIANTE CONTRATO ABIERTO

ANEXO 6

FORMATO DE PLIEGO DE PREGUNTAS

FECHA:_____

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
PRESENTE

Número de Procedimiento: LPN/SCJN/DGRM/005/2023
Descripción: Contratación del servicio administrado centro de operaciones de ciberseguridad para la SCJN mediante contrato abierto

No.	Concepto de Bases/Anexo	Numeral	Pregunta

Razón Social _____

R.F.C. _____

Nombre y firma del participante o su representante o apoderado legal_____