ACTA DE JUNTA DE ACLARACIONES

En la Ciudad de México, el veintiocho de noviembre de dos mil veintitres, a las once horas, inició la tolerancia de diez minutos para incorporarse al evento de junta de aclaraciones que se lleva a cabo de manera electrónica mediante videoconferencia a través de la plataforma de Microsoft Teams; una vez transcurrida la tolerancia se encuentran presentes por parte de la Suprema Corte de Justicia de la Nación:

Representante	Area
C.P. Antonio Prieto Revilla Lic. Miguel Ángel Esquinca Vila Lic. Adriana Hernández López	Dirección General de Recursos Materiales
Lic. Pedro Eduardo García Vázquez	Dirección General de Asuntos Jurídicos
Mtro Omar Salinas García	Dirección General de Tecnologías de la Información
C.P. Verónica Marcela López López Mtra. Amelia Karina Armenta Romero	Dirección General de la Tesorería

Asimismo, se encuentran presentes los representantes de las empresas:

Representante	Empresa
Michelle López Villa•	B DRIVE IT, S.A. de C.V.
Dulce Perla Ortega Flores	Totalsec, S.A. de C.V.
Gerardo Garibay Aymes	Silent4Business, S.A. de C.V.
Jose Renato Melendez Galván	Soluciones Integrales e Innovación Tecnológica Sustentable, S.A. de C.V.
José David Tellez Medrano Diana Abigail Hernández De La Cruz	Scitum, S.A. de C.V.
Juan Carlos Ramírez Fabián Sánchez Vargas	IQSEC, S.A. de C.V.
Daniel Estrada Gallegos	Arteria Comunicaciones, S.A. de C.V.

A efecto de llevar a cabo la junta de aclaraciones de carácter no obligatorio del presente procedimiento, de conformidad con lo señalado en el numeral 5.3 de las bases y en el artículo 65 del Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración.

SE HACE CONSTAR

3. Calendario de eventos	
Fecha de entrega de los pliegos de preguntas y carta manifiesto para participar en la junta de aclaraciones	**Junta de aclaraciones**
23 de noviembre de 2023 Horario de 08:30 a 12:30 horas	28 de noviembre de 2023 Horario 11:00 horas

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

5.3 Junta de aclaraciones, numeral 5.3.4
Los pliegos de preguntas deberán remitirse en el formato de Microsoft Word proporcionado por la convocante **(Anexo 6)**, y serán recibidos exclusivamente vía electrónica en el correo electrónico procpublicosdgrm@mail.scjn.gob.mx, en la fecha y horario establecidos en el calendario de eventos. Es requisito que las preguntas de los participantes estén relacionadas con el procedimiento de contratación. El acuse de la recepción de preguntas se realizará por vía electrónica. El horario de recepción será el que registren los servidores de la Suprema Corte de Justicia de la Nación y no se aceptarán preguntas recibidas antes, ni después, del día y horario establecidos. Se recomienda realizar el envío de su documentación al inicio del plazo establecido, toda vez que cualquier retraso en su recepción por cuestiones propias de internet no será responsabilidad de la Convocante. La Dirección General de Tecnologías de la Información proporcionará el seguimiento del registro de recepción de los correos electrónicos, a través del reporte de la herramienta perimetral de correo electrónico institucional, el cual formará parte del acta correspondiente y servirá como base para determinar las preguntas y documentación que se recibió dentro del plazo establecido.

Dentro del plazo establecido, se recibieron los correos electrónico enviado por parte de las empresas:

1. B DRIVE IT, S.A. de C.V.
2. Totalsec, S.A. de C.V.
3. Consultoría y Capacitación en Soluciones Avanzadas de Seguridad Informática, S.A. de C.V.
4. Silent4Business, S.A. de C.V.
5. Soluciones Integrales e Innovación Tecnológica Sustentable, S.A. de C.V.
6. Scitum, S.A. de C.V.
7. TIC DEFENSE, S.A. de C.V.
8. IQSEC, S.A. de C.V.
9. Arteria Comunicaciones, S.A. de C.V.

Mediante los cuales remitieron carta manifiesto para participar y se formularon diversas preguntas conforme al numeral 5.3.1 de las bases.

A continuación, se listan las preguntas recibidas en tiempo y forma, así como las respuestas correspondientes:

1 PREGUNTAS DE LA EMPRESA: B DRIVE IT, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	Anexo Técnico, pág. 10	4.1.1.Servicio de protección para portales web. Certificados SSL	Se solicita amablemente a la convocante indique si los certificados SSL requeridos, deberán incluir subdominios Favor de pronunciarse al respecto.	Si
2	Anexo Técnico, pág. 10	4.1.1.Servicio de protección para portales web. Certificados SSL	De ser afirmativa la respuesta a la pregunta anterior, favor de indicar la cantidad de subdominios requeridos. Favor de pronunciarse al respecto.	Se debe considerar hasta un máximo inicial de 10 subdominios por certificado, teniendo que considerar el crecimiento correspondiente de acuerdo al anexo.
3	Anexo Técnico, pág. 13	4.1.2 Servicio de protección para correo electrónico.	Die: 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".	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: Con la finalidad de no limitar la participación, se solicita amablemente que se permita que la solución ofertada se encuentre posicionada al menos en la sección de contenders de la metodología de investigación denominada "Forrester Wave" para soluciones "Enterprise Email Security". Favor de pronunciarse al respecto.	
4	Anexo Técnico, pág. 13	4.1.2 Servicio de protección para correo electrónico. a) Comunicación con Correo electrónico:	Dice: 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) **Pregunta:** Es correcto entender que esta funcionalidad podrá ser cubierta con la funcionalidad de forwarding. Favor de pronunciarse al respecto.	Si, siempre que cumpla con la funcionalidad requerida; en caso de necesitar, deberá integrar a su solución elementos complementarios de hardware y/o software.
5	Anexo Técnico, pág. 13	4.1.2 Servicio de protección para correo electrónico. b) Protección Correo electrónico:	**Dice:** Contar con un repositorio para cuarentena de correo electrónico, que permita almacenar correos SPAM por un mínimo de 90 días **Pregunta:** Es correcto entender que con la finalidad de no limitar la participación, se acepta que el repositorio para cuarentena de correo electrónico permita almacenar correos SPAM por un mínimo de 30 días. Favor de pronunciarse al respecto.	Se establece que el mínimo requerido para almacenar correo SPAM será por un periodo de 60 días
6	Anexo Técnico, pág. 13	4.1.2 Servicio de protección para correo electrónico. c) Protección Antispam:	**Dice:** 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. **Pregunta:** ¿Es correcto entender que las categorías mencionadas son enunciativas más no limitativas y la solución propuesta podrá contar con una clasificación distintas a las mencionadas sin que esto sea causa de desechamiento. Favor de pronunciarse al respecto.	Es correcta su apreciación, siempre y cuando su solución propuesta cuente con un sistema de clasificación interno de correo electrónico.
7	Anexo Técnico, pág. 13	4.1.2 Servicio de protección para correo electrónico. c) Protección Antispam:	Dice: Bloqueo automático de IPs debido a alta cantidad de envío de spam. **Pregunta:** Con la finalidad de evitar falsos positivos y que de manera	Es una funcionalidad con la que debe contar su solución propuesta, en la que de acuerdo con un rango de recepción de correos la solución pueda limitar automáticamente la recepción de correos al exceder el rango establecido.

ARYABHOi44FgzTb1zSSeNkfc0b7T901O2dDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			automática se realicen bloqueos que puedan provocar daño en la operación, ¿Es correcto entender que esta función podrá ser manual? Favor de pronunciarse al respecto.	
8	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Generales	Dice: 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). **Pregunta:** Es correcto entender que con la finalidad de no limitar la participación de soluciones SaaS, se solicita atentamente a la convocante que la alta disponibilidad en la solución no dependa de equipamiento propuesto, si no de la conexión a los servicios SaaS del proveedor. Favor de pronunciarse al respecto.	No se acepta su propuesta.
9	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Generales	Dice: 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". **Pregunta:** Con la finalidad de no limitar la participación, se solicita amablemente que se permita que la solución ofertada se encuentre posicionada al menos en la sección de Niche Players de la metodología de investigación denominada "Gartner Magic Quadrant" para soluciones "NGFW". Favor de pronunciarse al respecto	No se acepta su propuesta.
10	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. a) Protección en línea en tiempo real:	Dice: Protección en línea de la infraestructura de servidores y de comunicación interna (LAN) de la SCJN. **Pregunta:** ¿Es correcto entender que esta funcionalidad podrá ser cubierta con un puerto espejo? Favor de pronunciarse al respecto	Es incorrecta su apreciación, los equipos propuestos deberán analizar los flujos de datos de la infraestructura tecnológica de la SCJN a la cual se interconecten con la red LAN institucional.
11	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y	Dice: Análisis, detección, contención y bloqueo en tiempo real de amenazas	No es correcta su apreciación.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		protección de amenazas avanzadas con base en comportamiento. a) Protección en línea en tiempo real:	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. **Pregunta:** ¿Es correcto entender que esta funcionalidad podrá ser cubierta por el XDR sin que esto sea causa de desechamiento? Favor de pronunciarse al respecto	
12	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. a) Protección en línea en tiempo real:	Dice: Actuación reactiva ante la ocurrencia de un incidente de seguridad mediante indicadores de ataque, con múltiples puntos de visibilidad, detección y mitigación. **Pregunta:** ¿Es correcto entender que esta funcionalidad podrá ser cubierta por el XDR sin que esto sea causa de desechamiento? Favor de pronunciarse al respecto	No es correcta su apreciación.
13	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en Comportamiento. b) Servicios de protección:	Dice:) Servicios de protección: o Protección de DNS. o Control de usuarios y de aplicaciones. o Inspección de tráfico cifrado SSL. **Pregunta:** Se solicita amablemente a la convocante indique si lo requerido para este punto es un NGFW Favor de pronunciarse al respecto	Es correcta su apreciación.
14	Anexo Técnico, pág. 18	4.1.4 Servicio de protección para puntos finales (XDR) a) Compatibilidad:	Dice: MS Windows Server en sus versiones 2008, 2012, 2016, 2022 y nuevas versiones liberadas durante la vigencia del servicio. **Pregunta:** Con la finalidad de realizar un correcto dimensionamiento de la solución a ofertar, se solicita amablemente a la convocante indicar la cantidad de versiones 2008 y 2012 con las que cuenta actualmente y requieren protección Favor de pronunciarse al respecto	Un aproximado de 20 equipos servidores con esas versiones.
15	Anexo Técnico, pág. 18	4.1.4 Servicio de protección para puntos finales (XDR) a) Compatibilidad:	Dice: Sistemas Operativos Linux x86/x64, tales como Red Hat, Ubuntu, CentOS, CentOS Stream, Debian, entre otros, en sus versiones vigentes y nuevas	Se cuenta con un aproximado de 10 versiones diferentes de sistemas operativos Linux.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			versiones liberadas durante la vigencia del servicio. **Pregunta:** Con la finalidad de realizar un correcto dimensionamiento de la solución a ofertar, se solicita amablemente a la convocante indicar la cantidad de versiones de sistemas operativos con los que cuenta actualmente y requieren protección Favor de pronunciarse al respecto	
16	Anexo Técnico, pág. 15	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Generales:	Dice: 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. **Pregunta:** Con la finalidad de que la convocante cuente con la información que pueda ser requerida en auditorías o bien análisis, se propone que el histórico en la nube pueda ser como mínimo de 1 año. Favor de pronunciarse al respecto	No se acepta su propuesta.
17	Anexo Técnico, pág. 20	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) GENERALES	Dice: 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 **Pregunta:** Con la finalidad de que el cliente asegure una buena gestión del servicio y de su seguridad se sugiere que como mínimo el Centro de Operaciones de Ciberseguridad deberá contar con al menos 10 procesos certificados en ISO/IEC 27001 en su versión 2013, dentro de los cuales deberán estar CERT, CSIRT Favor de pronunciarse al respecto	No se acepta su propuesta.
18	Anexo Técnico, pág. 20		Dice: 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). **Pregunta:** Con la finalidad de asegurar una buena gestión del servicio y de su seguridad a la SCJN se sugiere que como mínimo el Centro de Operaciones de Ciberseguridad deba contar con al	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			menos 10 procesos certificados en ISO/IEC 20000 en su versión 2013 e ISO/IEC 9000, dentro de los cuales deberán estar CSIRT y NOC Favor de pronunciarse al respecto	
19	Anexo Técnico, pág. 36	7.1 Requisitos técnicos de las soluciones propuestas	Dice: Para su acreditación de cada solución, se deberá proveer de una copia de la metodología de investigación correspondiente. **Pregunta:** ¿Es correcto entender que la metodología que se deberá presentar es la metodología del servicio del licitante? Favor de pronunciarse al respecto	No es correcta su apreciación, las metodologías de investigación son las del Gartner Magic Quadrant y Forrester Wave de acuerdo con cada solución.
20	Anexo Técnico, pág. 37	7.3 Experiencia comprobable	Dice: 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 IQNET 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 **Pregunta:** ¿Es correcto entender que este punto se cubrirá presentando certificación de algún ISO/IEC que contenga la certificación del centro en el SOC-CERT, CSIRT, y NOC? Favor de pronunciarse al respecto	No es correcta su apreciación.
21	Anexo Técnico, pág. 38, 39	7.4.4 Personal requerido:	Dice: "Consultor Senior 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: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad. 5 años de experiencia o más como Líder implementador en ISO/IEC	No es correcta su apreciación. Sólo se acepta la presentación de la certificación como Líder Implementador de ISO/IEC 27001

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			27001" Cédula o título profesional Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información ciberseguridad de: o Especialidad o Maestría o Diplomado Certificado vigente comoLíder Implementador de ISO/IEC 27001. Curriculum vitae **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requisito del Certificado vigente como Líder Implementador ISO/IEC 27001, se aceptará la presentación de la certificación Líder Implementador de ISO/IEC 27001 o el certificado ISO/IEC 27001 INFORMATION SECURITY LEAD AUDITOR. Esto se plantea considerando que ambas certificaciones avalan el conocimiento necesario para el Perfil Consultor Senior de Seguridad de la Información Favor de pronunciarse al respecto	
22	Anexo Técnico, pág. 38, 39	7.4.4 Personal requerido:	Dice: "Consultor Senior de Seguridad de la Información, presentar : Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o en ciberseguridad de: o Especialidad o Maestría o Diplomado **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requerimiento se deberá presentar Título o Diploma o Curso o Certificado que avalen el conocimiento en Seguridad de la Información o en ciberseguridad del Consultor Senior de Seguridad de la Información	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Favor de pronunciarse al respecto	
23	Anexo Técnico, pág. 39	7.4.4 Personal requerido:	Dice: 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: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o 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: o Especialidad o Maestría o Diplomado Certificado vigente como Líder Implementador de ISO/IEC 27001. Curriculum vitae **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requisito del Certificado vigente como Líder Implementador ISO/IEC 27001, se aceptará la presentación de la certificación Líder Implementador de ISO/IEC 27001 o el certificado ISO/IEC 27001 INFORMATION SECURITY LEAD AUDITOR. Esto se plantea considerando que ambas certificaciones abarcan las habilidades necesarias para el Perfil Consultor Junior de Gestión de Seguridad de la información Favor de pronunciarse al respecto	No es correcta su apreciación. Sólo se acepta la presentación de la certificación como Líder Implementador de ISO/IEC 27001
24	Anexo Técnico, pág. 39	7.4.4 Personal requerido:	Dice: Consultor Junior de Gestión de Seguridad de la Información. Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de: o Especialidad o Maestría o Diplomado **Pregunta:**	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo

ARYABHOi44FgzfTb1zSSeNtc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requerimiento se deberá presentar Título o Diploma o Curso o Certificado que avalen su conocimiento en Seguridad de la Información o en ciberseguridad del Perfil Consultor Junior de Gestión de Seguridad de la información. Favor de pronunciarse al respecto	reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
25	Anexo Técnico, pág. 39	7.4.4 Personal requerido:	Dice: Especialista técnico en controles de ciberseguridad Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad. Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de: o Especialidad o Maestría o Diplomado **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requerimiento se deberá presentar Título o Diploma o Curso o Certificado que avalen su conocimiento en Seguridad de la Información o en Ciberseguridad del Perfil Especialista técnico en controles de ciberseguridad Favor de pronunciarse al respecto	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CISSP o CISM o CRISC o Líder Implementador de ISO/IEC 27001, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso
26	Anexo Técnico, pág. 40	7.4.4 Personal requerido:	Dice: Coordinador de Equipo de Respuesta a Incidentes. Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de: o Especialidad o Maestría o Diplomado **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con el requerimiento se deberá presentar Título o Diploma o Curso o Certificado que avalen su conocimiento en Seguridad de la Información o en Ciberseguridad del Perfil Coordinador de Equipo de Respuesta a Incidentes Favor de pronunciarse al respecto	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CIH – EC Council Certified Incident Handler o MILE2 Certified incident Handling Engineer o ISO/IEC 27035 Lead Incident Manager, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.

ARYABHO4F9zTb1zS5eNkfc0b7T9t02ddSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
27	Anexo Técnico, pág. 40	7.4.4 Personal requerido:	Dice: Especialista de Ciberinteligencia. Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o 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. Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad de: o Especialidad o Maestría o Diplomado **Pregunta:** Se solicita amablemente a la convocante que aclare si es correcto entender que, para cumplir con lo solicitado se deberá presentar Título o Diploma o Curso o Certificado que avalen su conocimiento en Seguridad de la Información o en Ciberseguridad del Perfil Especialista de Ciberinteligencia. Favor de pronunciarse al respecto	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como GIAC Cyber Threat Intelligence o Offensive Security – OSCP, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso
28	Anexo Técnico, pág. 20	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) GENERALES:	Dice: 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). **Pregunta:** Es correcto entender que esta funcionalidad se refiere a que solución de XDR solicitada pueda enviar información al SIEM propiedad de la SCJN. Favor de pronunciarse al respecto	No es correcta su apreciación, el licitante deberán ofertar la Solución de seguridad informática en la nube (SIEM o solución de análisis superior
29	Anexo Técnico	4. Descripción de los servicios	Es correcto entender que la convocante brindará las facilidades para la instalación de la infraestructura requerida para el cumplimiento de los servicios solicitados, tales como: espacio en rack, conexiones eléctricas, protección de variaciones de corriente eléctrica y las necesarias para el buen funcionamiento de la solución propuesta.	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 regulada. • Condiciones climáticas

ARYABHOi44FgzfTb1zSSeNkfc0b77901O2ddDSLkOCg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Favor de pronunciarse al respecto	
30	Anexo Técnico, pág. 16	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Equipos switches:	Dice: 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. **Pregunta:** Se solicita amablemente a la convocante indique si los switches requeridos son en capa 2 o capa 3. Favor de pronunciarse al respecto	El tipo de switches será determinado por el licitante de acuerdo con su arquitectura propuesta para la solución, cumpliendo con lo requerido en la licitación.
31	Anexo Técnico, pág. 16	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Equipos switches:	Dice: 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. **Pregunta:** Se solicita amablemente a la convocante indique la cantidad de puertos requeridos por cada switch solicitado y la velocidad a la que se requieren. Favor de pronunciarse al respecto	Deberá dimensionarla conforme a su solución propuesta, considerando todos los equipos físicos a integrar.
32	Anexo Técnico, pág. 16	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Equipos switches:	Dice: 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	De lado de la red LAN de la SCJN se pueden integrar en cobre o fibra a 1 Gbps.

AQRYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0CgF

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			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. **Pregunta:** Se solicita amablemente a la convocante indique si los switches requeridos serán integrados por cobre o por fibra. Favor de pronunciarse al respecto	
33	Anexo Técnico, pág. 16	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Equipos switches:	Dice: 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. **Pregunta:** En caso de que la respuesta a la pregunta anterior sea en fibra, se solicita amablemente a la convocante indique la velocidad requerida. Favor de pronunciarse al respecto	Deberá dimensionar los puertos conforme a su solución propuesta.
34	Anexo Técnico, pág. 35	7 Requisitos técnicos	Dice: 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	Es correcta su apreciación, excepto cuando el personal sea requerido en sitio por la SCJN para casos en específico

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			con los niveles de servicio requeridos por la SCJN. **Pregunta:** ¿Es correcto entender que el personal designado para la prestación de los servicios podrá realizar la administración, gestión y soporte técnico del servicio de manera remota. Favor de pronunciarse al respecto	
35	Anexo Técnico, pág. 9	4. Descripción de los servicios	Dice: 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. **Pregunta:** Es correcto entender que la convocante proporcionara las facilidades de un acceso seguro para la administración y monitor desde las Instalaciones del COC proveedor. Favor de pronunciarse al respecto	El licitante deberá considerar su infraestructura tecnológica para su conexión remota a la infraestructura tecnológica de la SCJN, para realizar las actividades descritas, tal como puede ser VPN site to site o el mecanismo que proponga el licitante.
36	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.8 Carta del prestador de servicios 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. **Pregunta:** ¿Es correcto entender que esta carta solicitada es la misma solicitada en el numeral 9.7? Favor de pronunciarse al respecto.	Se aclara que la carta solicitada en el numeral 9.8 debe de contener la redacción que se indica en el anexo 2a numeral 7.1 inciso 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.”
37	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.8 Carta del prestador de servicios 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. **Pregunta:** En caso de que la respuesta anterior sea positiva, los licitantes darán	Se aclara que la carta solicitada en el numeral 9.8 debe de contener la redacción que se indica en el anexo 2a numeral 7.1 inciso 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.”

ARYABHOi44FgzfTb1zSSeNkfc0u7Y9Ti2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			cumplimiento a una sola carta? Favor de pronunciarse al respecto.	
38	Anexo Técnico, pág. 37	7.3 Experiencia comprobable	Dice: 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 Pregunta: ¿Es correcto entender que, en la medida que hace más de tres años se dejaron de expedir certificados de CERT-FIRST, los licitantes para dar cumplimiento al requerimiento pueden presentar certificaciones de CERT de otras entidades internacionales? Favor de pronunciarse al respecto	No se acepta su propuesta. No se solicita certificado de CERT-FIRST, se solicita este afilado a dicha organismo de acuerdo con lo requerido en la licitación.
39	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.18 La Suprema Corte de Justicia de la Nación manifiesta que no se permite la subcontratación. Para los efectos de esta contratación, se entiende por subcontratación el acto mediante el cual la persona adjudicada encomienda a otra persona física o jurídica, la ejecución parcial o total del objeto. **Pregunta:** ¿Es correcto entender que para asegurar la prestación de los servicios, los licitantes deberán presentar el alta del IMSS de cada uno de los recursos propuestos? Favor de pronunciarse al respecto.	No es correcta su apreciación. Se deberá considerar lo establecido en el numeral 20.5 de las bases, en particular el segundo párrafo que establece: La Suprema Corte de Justicia de la Nación estará facultada para requerir a la persona adjudicada los comprobantes de afiliación de su personal al IMSS, así como los comprobantes de pago de las cuotas al SAT, INFONAVIT e IMSS.
40	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.12 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 la persona participante o representante legal 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	No es correcta su apreciación, no se limita a los mismos procesos.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			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. **Pregunta:** ¿Es correcto entender que al menos los 5 procesos de seguridad de la información deberán ser los mismos para los certificados ISO/IEC 9001 e ISO/IEC 20000? Favor de pronunciarse al respecto.	
41	Anexo Técnico	MONITOREO DE AMENAZAS INTERNAS:	Dice: 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: **Pregunta:** ¿Es correcto entender que el Plan de Atención y Respuesta a Incidentes Críticos será entregado por el licitante adjudicado? Favor de pronunciarse al respecto.	Es correcta su apreciación.
42	Anexo Técnico	ATENCIÓN Y SOPORTE:	Dice: el Centro de Operaciones en Ciberseguridad. o Asistencia vía correo electrónico, se deberá proveer una cuenta única de correo electrónico para la SCJN. **Pregunta:** ¿Es correcto entender que el software de conexión remota/ VPN site to site/ y el software de videoconferencia será proporcionado por la SCJN? Favor de pronunciarse al respecto.	Deberá ser proporcionado por el licitante ganador.
43	Anexo Técnico	COMPONENTES DEL SERVICIO	Dice: 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. **Pregunta:** Con el objetivo de realizar un correcto dimensionamiento, se solicita a la SCJN aclare la cantidad de servidores o equipos a los cuales se requiere	Se deberá considerar al menos 500 equipos.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			realizar el análisis de vulnerabilidades. Favor de pronunciarse al respecto.	
44	Anexo Técnico	ANEXO 3	Dice: Cantidad Mínima de usuarios 4000 **Pregunta:** ¿Es correcto entender que los 4000 usuarios se refieren a la cantidad máxima de servicios de protección para puntos finales (XDR)? Favor de pronunciarse al respecto	La cantidad mínima son 3,500 y la máxima 4,000 usuarios para el servicio de protección para puntos finales (XDR).
45	Anexo Técnico	ANEXO 3	Dice: Cantidad Mínima de usuarios 4000 **Pregunta:** En caso de que la respuesta anterior sea positiva, ¿Es correcto entender que la convocante realizará una precisión para realizar este ajuste? Favor de pronunciarse al respecto	La cantidad mínima son 3,500 y la máxima 4,000 usuarios para el servicio de protección para puntos finales (XDR).
46	Anexo Técnico, pág. 25	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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). **Pregunta:** Se solicita amablemente a la convocante indicar si es correcto entender que únicamente se requiere la consultoría y no se buscará obtener la certificación ISO/IEC 27001 para la convocante. Favor de pronunciarse al respecto.	Se debe considerar la consultoría necesaria conforme los requerimientos del numeral 4.1.6. Específicamente con lo señalado en el componente "Operación del modelo de gobierno" apartado **Actualización del SGSI**.
47	Anexo Técnico, pág. 25	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	En caso de que la respuesta anterior sea negativa, se solicita amablemente a la convocante indicar si es correcto entender que la convocante será la responsable de realizar el procedimiento para obtener esta certificación. Favor de pronunciarse al respecto.	El licitante deberá considerar como parte de su propuesta de servicio brindar el acompañamiento durante el proceso de certificación una vez que el SGSI haya generado un historial de funcionamiento demostrable de al menos tres meses que permitan a la SCJN estar preparada para una posible certificación. Será responsabilidad de la convocante realizar la contratación de la casa certificadora para llevar a cabo dicho proceso.
48	Anexo Técnico, pág. 26	4.1.6 Servicio de actualización y mejora del Modelo Institucional de	Dice: Identificación del nivel actual de concientización: Realizar evaluaciones periódicas a los funcionarios de la SCJN, sobre el nivel de conciencia de las	Se deben considerar 2 ejercicios anuales, dando un resultado de 6 en total por la vigencia del contrato (36 meses).

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Gobierno de Seguridad de la Información - MIGSI Incremento de la cultura organizacional de seguridad (concientización)	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. **Pregunta:** Se solicita amablemente a la convocante indicar la cantidad de campañas de phishing que se realizarán durante la vigencia del contrato. Favor de pronunciarse al respecto.	
49	Anexo Técnico, pág. 26	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI Incremento de la cultura organizacional de seguridad (concientización)	Dice: 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. **Pregunta:** Se solicita amablemente a la convocante indicar si es correcto entender que la plataforma deberá estar en línea durante la vigencia del servicio. Favor de pronunciarse al respecto.	Es correcta su apreciación
50	Anexo Técnico, pág. 27	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Pregunta: 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	Se deberá considerar al menos dos ejercicios de pentest (prueba y validación) a los activos que determine la SCJN por año.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Comprobación técnica	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. **Pregunta:** Se solicita amablemente a la convocante indicar la cantidad de Pruebas de Penetración que se realizarán durante la vigencia del servicio. Favor de pronunciarse al respecto.	
51	Anexo Técnico, pág. 27	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI Ejecutar el análisis de código estático (SAST):	Dice: 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. **Pregunta:** Se solicita amablemente a la convocante indicar la cantidad de análisis de código estático que se llevarán a cabo durante la vigencia del contrato. Favor de pronunciarse al respecto.	El prestador de servicios deberá realizar la detección de vulnerabilidades para el código fuente de los sistemas informáticos críticos identificados en la **gestión de riesgos**. Como referencia, sin ser limitativos, actualmente se tienen identificados 10 sistemas críticos candidatos a dicho análisis.
52	9. Propuesta Técnica 9.16 Presentar al menos 3 contratos formalizados en copia simple, en donde demuestre que tiene experiencia y capacidad técnica.	9.16	Se solicita a la Convocante confirmar si es correcto entender que se podrán presentar contratos vigentes para dar cumplimiento al presente numeral. Favor de manifestarse al respecto.	Se podrán presentar contratos no vigentes y vigentes, siempre y cuando se hayan formalizado dentro del periodo solicitado y a nombre del licitante.
53	9. Propuesta Técnica 9.16 Presentar al menos 3 contratos	9.16	Se solicita a la Convocante confirmar si es correcto entender que el participante deberá acreditar un total de 3 años de experiencia para el cumplimiento del	Para cumplimiento del numeral deberá proporcionar al menos 3 contratos formalizados en copia simple conforme a lo solicitado en el punto 9.16.

ARYABHCI44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	formalizados en copia simple, en donde demuestre que tiene experiencia y capacidad técnica.		presente numeral. Favor de manifestarse al respecto.	
54	10. Propuesta Económica	10.4	Dado que el presente proceso es de carácter presencial y debido a que la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social gozará de vigencia durante el día de la fecha en que haya sido generada, se solicita a la Convocante acepte que el documento cuente con una vigencia de 24 horas previo a la fecha de presentación. Favor de manifestarse al respecto.	Las constancias solicitadas en el numeral 10.4 de las bases deberán tener una vigencia máxima de 15 días naturales previos al día de la sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas. En su momento, el licitante que resulte adjudicado deberá presentar dichas constancias actualizadas con una vigencia máxima de 15 días naturales previos a la firma del contrato respectivo.
55	11. Sesión de presentación de documentación legal y financiera, apertura de propuestas técnicas y económicas.	11.3	Se solicita a la Convocante que para la recepción y apertura de propuestas (técnica, económica así como documentación legal y financiera) acepte que un tercero podrá presentar CARTA PODER SIMPLE en donde se otorguen las facultades correspondientes sin necesidad de ser el Representante Legal o Apoderado Legal el que participe en todo el acto. Favor de pronunciarse al respecto.	En relación a la posibilidad de que pueda asistir una persona distinta al representante legal con carta poder a la “Sesión pública de presentación de documentación legal y financiera, y apertura de propuestas técnicas y económicas”, se aclara que no se acepta su propuesta, ya que de acuerdo con el numeral 11.6 de las Bases, la persona participante o su representante legal al momento de entregar los sobres deberá firmar de recibido el documento de acuse correspondiente y la Dirección General de Recursos Materiales conservará una copia de éste. Asimismo, el artículo 69, quinto párrafo, del Acuerdo General de Administración XIV/2019, dispone que “el licitante deberá entregar copia de su identificación o la del representante legal que asista y exhibir original para su cotejo”, por lo que los servidores públicos requerirán de dicha identificación al representante legal. Por lo tanto, la persona que asista a la referida sesión pública deberá ser el licitante o su representante o apoderado legal. En dichos términos al ser una persona moral no se permitirá la presentación de una carta poder simple para acudir en nombre del representante legal, apoderado legal o el licitante, ya que en términos del artículo 10 de la Ley General de Sociedades Mercantiles la representación de las sociedades mercantiles corresponderá a su administrador o

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
				administradores, o en su caso a la persona a la que se le haya otorgado un poder protocolizado ante un notario público.
56	29. Anexos	29.	Es correcto entender que los documentos: Anexo 4 Modelo de contrato ordinario y Anexo 5 Formato de garantía de cumplimiento, son de carácter informativo y la no presentación de ellos no causará desechamiento de la propuesta del Licitante. Favor de manifestarse al respecto.	Es correcto, dichos modelos son únicamente de carácter informativo.
57	12.3 EVALUACIÓN DE DOCUMENTACIÓN FINANCIERA	12.3.1.	Es correcto entender que el dictamen resolutivo financiero en el cual se verificará que el índice de liquidez sea mayor o igual a 1 (para ser satisfactorio), se determinará calculándose con los Estados Financieros presentados del año 2022 y parciales del 2023.	Su apreciación **no** es correcta, el índice de liquidez se determinará con la información financiera más reciente presentada por el participante, en este caso se aplicará a los estados financieros parciales de 2023. En el supuesto de que el índice anterior no alcance la puntuación señalada (mayor o igual 1.0), se procederá a aplicar este índice a la información financiera de cada uno de los ejercicios (2021, 2022 y parciales 2023) que presentó el participante y se aplicará un promedio, el cual, para ser satisfactorio, deberá ser mayor o igual a 1.0
58	6.2. Documentación Financiera	6.2.2.	Es correcto entender que para dar cumplimiento al presente numeral, se podrán presentar los Estados Financieros parciales al 31 de octubre de 2023. Favor de pronunciarse al respecto.	Es correcta su apreciación
59	7. PARTICIPACIÓN CONJUNTA	7	¿Es correcto entender que los licitantes que forman parte del consorcio que presente propuesta conjunta deberán contener la facultad expresa de "delegación de poderes" en el instrumento público que acredita su personalidad? Esto en el entendido de que le delegarán poderes al representante común. Favor de manifestarse al respecto.	Es correcta su apreciación, en caso de participación conjunta, para poder delegar poderes al representante común que para el efecto se designe, cada una de las personas que integren el conjunto deberán realizar tal acto a través de su representante o apoderado(a) legal que, en tal sentido, cuente con las facultades bastantes y suficientes para efectuar la delegación de los poderes correspondientes.
60	21. GARANTÍA DE CUMPLIMIENTO	21.1	Se solicita a la convocante confirmar el porcentaje a garantizar ya que no es muy claro si es el 10% ó el 20%.	De conformidad con el numeral 21.1 de las Bases, la fianza de cumplimiento se constituirá por el 10% (diez por ciento) del importe neto del instrumento contractual (sin incluir los impuestos aplicables) que para el efecto se suscriba y deberá indicase en la misma que cubrirá hasta el 20% (veinte por ciento) más en el supuesto de que por algún motivo deba incrementarse el precio de los servicios contratados o el plazo pactado.
61	21. GARANTÍA DE CUMPLIMIENTO	21.1	Se solicita a la convocante confirmar que, al ser un contrato plurianual, se podrá presentar la garantía de	No es correcta su apreciación, en términos del apartado 21 de las Bases de la Licitación, se deberá constituir fianza de cumplimiento

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			cumplimiento por el 10% por cada ejercicio fiscal que corresponda y deberá ser presentada dentro de los diez días hábiles siguientes a la fecha en que se hubiere firmado el instrumento contractual respectivo, en las oficinas de la Dirección General de Recursos Materiales de la Suprema Corte de Justicia de la Nación. Favor de manifestarse al respecto.	por el 10% (diez por ciento) del importe total neto del instrumento contractual que para el efecto se suscriba, sin incluir los impuestos aplicables, y señalar que cubrirá hasta 20% (veinte por ciento) más en el supuesto de que por algún motivo deba incrementarse el precio de los servicios contratados o el plazo pactado. Dicha fianza deberá ser presentada dentro de los diez días hábiles siguientes a la fecha en que se hubiere firmado el instrumento contractual respectivo y contratarse de modo que esté vigente hasta que los servicios del contrato hayan sido prestados en su totalidad a entera satisfacción del Alto Tribunal y, en su caso, la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por autoridad competente. Por ello, se deberá constituir con base en el importe neto o monto total del contrato que para tal efecto se suscriba y no así, por cada uno de los ejercicios fiscales que contempla la contratación.
62	22. PENAS CONVENCIONALES	22.1. AL 22.7	Se solicita a la convocante informar a los licitantes el procedimiento para la rectificación de las penas convencionales, una vez notificadas.	De conformidad con lo establecido en el numeral 26 de las Bases de la Licitación, así como lo establecido en los artículos 205 a 210 del Acuerdo General de Administración XIV/2019; en tales casos, una vez notificadas las respectivas cuantificaciones para la aplicación de penas convencionales a las que pudiera ser acreedora la persona adjudicada, ésta podrá manifestar lo que a su derecho convenga y, en su caso, presentar su solicitud para iniciar el procedimiento de conciliación conducente en términos de los artículos anteriormente citados.

2 PREGUNTAS DE LA EMPRESA: TOTALSEC, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	BASES	9.8	LOS NUMERALES 9.7 Y 9.8 DE LAS BASES PRESENTAN LA MISMA REDACCIÓN, SOLICITO A LA CONVOCANTE ACLARE SI LA CARTA SOLICITADA EN EL NUMERAL 9.8 DEBE DE CONTENER LA REDACCIÓN QUE SE INDICA EN EL ANEXO 2A NUMERAL 7.1 INCISO E.	Es correcta su apreciación.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			"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."	
2	BASES	10.4	SE SOLICITA A LA CONVOCANTE CONFIRME QUE, EN RELACIÓN A LO PRECISADO EN EL ACUERDO ACDO.AS2.HCT.250423106.P.DIR DICTADO EN SESIÓN ORDINARIA, CELEBRADA EL DÍA 25 DE ABRIL DEL PRESENTE AÑO, POR EL QUE SE APROBARON LAS DISPOSICIONES TRANSITORIAS APLICABLES A LAS REGLAS DE CARÁCTER GENERAL PARA LA OBTENCIÓN DE LA OPINIÓN DEL CUMPLIMIENTO DE OBLIGACIONES FISCALES EN MATERIA DE SEGURIDAD SOCIAL, PUBLICADAS EL 22 DE SEPTIEMBRE DE 2022 EN EL DOF DEL 04 DE MAYO DE 2023 Y QUE EN SU DISPOSICIÓN TRANSITORIA PRIMERA SEÑALA:… "PRIMERA. LA OPINIÓN DEL CUMPLIMIENTO DE OBLIGACIONES FISCALES EN MATERIA DE SEGURIDAD SOCIAL SERÁ VALIDA DURANTE EL PLAZO DE QUINCE DÍAS NATURALES QUE EL CONTRIBUYENTE TIENE PARA LA FORMALIZACIÓN DE LAS CONTRATACIONES REFERIDAS EN EL ARTÍCULO 32-D DEL CÓDIGO FISCAL DE LA FEDERACIÓN, EN TÉRMINOS DE LAS DISPOSICIONES JURÍDICAS APLICABLES…" ¿ES CORRECTO ENTENDER QUE SE PODRÁ PRESENTAR LA OPINIÓN DE CUMPLIMIENTO CON FECHA DE EMISIÓN ANTERIOR A LA FECHA DE PRESENTACIÓN Y APERTURA DE PROPUESTAS, CUIDANDO QUE LOS 15 DÍAS DE VIGENCIA CUBRAN EL DÍA DE PRESENTACIÓN Y APERTURA DE PROPUESTAS?	Las constancias solicitadas en el numeral 10.4 de las bases deberán tener una vigencia máxima de 15 días naturales previos al día de la sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas. En su momento, el licitante que resulte adjudicado deberá presentar dichas constancias actualizadas con una vigencia máxima de 15 días naturales previos a la firma del contrato respectivo.

ARYABHOi44EgdTb1ZSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
3	ANEXO 2a	7.3	REFERENCIA: 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. ¿ES CORRECTO ENTENDER QUE PARA DAR CUMPLIMIENTO A ESTE INCISO ÚNICAMENTE SE DEBE PRESENTAR COPIA SIMPLE DEL CERTIFICADO ISO/IEC 27001?	Es correcta su apreciación, siempre y cuando el certificado este a nombre del licitante y contenga su domicilio actual
4	ANEXO 2a	7.4.4	¿ES CORRECTO ENTENDER QUE PARA DAR CUMPLIMIENTO AL PERSONAL REQUERIDO, SE DEBE PRESENTAR COPIA SIMPLE DE LA DOCUMENTACIÓN SEÑALADA EN CADA PERFIL?	Es correcta su apreciación.
5	ANEXO 4	ANEXO 4	¿ES CORRECTO ENTENDER QUE EL ANEXO 4 MODELO DE CONTRATO ORDINARIO ES DE CARÁCTER INFORMATIVO? POR LO TANTO, NO SE DEBE PRESENTAR DENTRO DE NUESTRA PROPUESTA.	Es correcto, dicho modelo es únicamente de carácter informativo.
6	ANEXO 5	ANEXO 5	¿ES CORRECTO ENTENDER QUE EL ANEXO 5 FORMATO DE GARANTÍA DE CUMPLIMIENTO ES DE CARÁCTER INFORMATIVO Y POR TANTO, NO SE DEBE PRESENTAR DENTRO DE NUESTRA PROPUESTA?	Es correcto, dicho modelo es únicamente de carácter informativo.
7	DICE: SE DEBERÁ CONSIDERAR LO NECESARIO PARA GESTIONAR AL MENOS UN MÍNIMO DE 3,600 CUENTAS DE CORREO ELECTRÓNICO.	4.1.2, APARTADO GENERALES	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE PARA EL CUMPLIMIENTO DE ESTE REQUERIMIENTO SE PODRÁ INTEGRAR Y HACER REFERENCIA A UN LISTADO DE COMPONENTES HARDWARE / SOFTWARE DETALLADO DENTRO DE LA PROPUESTA TÉCNICA	Es correcta su apreciación
8	APARTADO GENERALES. DICE: LA SOLUCIÓN TECNOLÓGICA DEBERÁ ESTAR POSICIONADA COMO UNA DE LAS SOLUCIONES LÍDERES EN EL	4.1.2, APARTADO GENERALES	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE, DEBIDO A QUE EL MERCADO DE SOLUCIONES "EMAIL SECURITY" PUEDE ABARCAR SOLUCIONES DE DISTINTOS FABRICANTES Y DIVERSOS PUNTOS DE EVALUACIÓN, SE PODRÁN	No se acepta su propuesta.

ARYABHDi44FgzfTb1zSdeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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".		PROPONER SITIOS DE ANÁLISIS Y GUÍAS DE MERCADO TECNOLÓGICO SIEMPRE Y CUANDO, LOS FABRICANTES MENCIONADOS EN ESTOS SITIOS SE MANTENGAN COMO LÍDERES DE LA SOLUCIÓN DE EMAIL SECURITY	
9	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: CON FIGURACIONES APLICADAS, NIVELES DE OPERACIÓN, MEJORAS APLICADAS EN LA SOLUCIÓN, NIVEL DE PROTECCIÓN Y ACCIONES PARA MEJORA CONTINUA	4.1.5 SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COC)	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE LA REVISIÓN TÉCNICA POR PARTE DEL FABRICANTE EN COMPLEMENTO CON NUESTRA REPRESENTADA Y LA SCJN, SE REFIERE A LA INTEGRACIÓN DE TRABAJO EN EQUIPO POR PARTE DEL EJECUTIVO DE CUENTA POR PARTE DEL FABRICANTE Y SU INGENIERO DE PREVENTA, ¿ES CORRECTA NUESTRA APRECIACIÓN ACORDE AL REQUERIMIENTO?	No es correcta su apreciación, el acompañamiento se deberá realizar con personal técnico del fabricante que pueda validar las configuraciones realizadas sobre las soluciones tecnológicas por parte del licitante ganador.
10	ANEXO 2a	ANEXO TÉCNICO	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE SE DEBERÁ INTEGRAR EN LA PROPUESTA TÉCNICA LISTADO DE HARDWARE Y SOFTWARE (NO LIBRE O DE COMUNIDAD) A PROPONER, SIEMPRE Y CUANDO INTEGRE PÓLIZAS DE SOPORTE Y	Si es correcta su apreciación.

ARYABbIO44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			MANTENIMIENTO DURANTE LA VIGENCIA DEL CONTRATO, ¿ES CORRECTA NUESTRA APRECIACIÓN?	
11	ANEXO 2a	ANEXO TÉCNICO	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE NO DEBERÁN PROPONERSE SOLUCIONES DE SOFTWARE LIBRE PARA CADA UNO DE LOS REQUERIMIENTOS DEL ANEXO TÉCNICO, ¿ES CORRECTO EL ENTENDIMIENTO?	Si es correcta su apreciación.
12	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	4.1.5 SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COC)	TODA VEZ QUE EL PERSONAL ASIGNADO POR PARTE DEL LICITANTE ADJUDICADO NO CONTARÍA CON LAS FACULTADES LEGALES PARA LA REALIZACIÓN DE UNA DENUNCIA ANTE LA POLICÍA CIBERNÉTICA, LAS ACTIVIDADES DEL LEVANTAMIENTO DE DENUNCIA SE DEBERÁN CONSIDERAR DE ACOMPAÑAMIENTO Y ASESORÍA PARA LA GENERACIÓN DE ESTA, POR LO QUE SE PROPONE QUE POR MEDIO DE MESAS DE TRABAJO SE LIMITEN LAS ACTIVIDADES Y/O RESPONSABILIDADES ENTRE EL PROVEEDOR ADJUDICADO Y LA SCJN, ¿SE ACEPTA NUESTRA PROPUESTA?	Se acepta su propuesta.
13	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	4.1.5 SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COC)	SE SOLICITA AMABLEMENTE A LA CONVOCANTE ACLARAR SI ES CORRECTO ENTENDER QUE PARA EL ANÁLISIS FORENSE SE UTILIZARÁN ÚNICAMENTE LAS SOLUCIONES REQUERIDAS EN EL PRESENTE ANEXO TÉCNICO	No es correcta su apreciación, mediante herramientas propias del licitante ganador, deberá realizar el análisis forense de acuerdo al tipo de caso que se pueda presentar en la SCJN.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	USUARIO Y SERVIDORES. DESINFECCIÓN DE MALWARE EN ARCHIVOS DE USUARIOS. ELIMINACIÓN DE ADWARE EN EQUIPOS DE USUARIO.			
14	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.	4.1.5 SERVICIO DE CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COC)	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE, LA DESINFECCIÓN DEL MALWARE TAL COMO ES REQUERIDA SE DEBE ENFOCAR A EQUIPOS DE USUARIO Y SERVIDORES, ¿ES CORRECTO EL ENTENDIMIENTO?	Es correcta su apreciación
15	C) ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS: O CUATRO EQUIPOS NUEVOS Y DE ÚLTIMA GENERACIÓN DE PROPÓSITO ESPECÍFICO PARA SEGURIDAD DE LA RED (GATEWAY) TIPO DATA CENTER. O FUENTES DE PODER REDUNDANTES HOT-SWAP EN CADA	**4.1.3**	¿PODRÍA LA CONVOCANTE ESPECIFICAR Y ACLARAR SI LA VELOCIDAD MENCIONADA EN LA PÁGINA 15, INCISO C), DE 5GB THREAT PREVENTION ES PRECISA, O SI DEBERÍA SER UN VALOR SUPERIOR, CONSIDERANDO LA SOLICITUD DE INTERFACES DE 40GB, LO QUE PODRÍA REQUERIR UNA CAPACIDAD DE THROUGHPUT MAYOR?	La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	UNO. **O UN THREAT PREVENTION THROUGHPUT DE 5 GBPS COMO MÍNIMO, CON TODAS LAS FUNCIONALIDADES HABILITADAS SIMULTÁNEAMENTE.** O 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).			
16	DEL INCISO "**C) ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS:"** DICE: O CONTARÁN CON GARANTÍA CON EL FABRICANTE ANTE CUALQUIER FALLA DURANTE LA VIGENCIA DEL CONTRATO	**4.1.3**	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE PARA ESTE REQUERIMIENTO SE DEBE INTEGRAR CARTA DE FABRICANTE AUTÓGRAFA POR REPRESENTANTE LEGAL O REFERENCIA PÚBLICA QUE INDIQUE EL NÚMERO DE ATENCIÓN TELEFÓNICA PARA CUALQUIER FALLA COMO PARTE DE LA GARANTÍA PARA BRINDAR SOPORTE EN CASO DE REQUERIRSE DADO DICHO REQUERIMIENTO PARA LOS EQUIPOS DE INCISO C COMO ES REQUERIDO ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	Este requerimiento se puede acreditar con una carta emitida por la licitante firmada por su representante legal, indicando que, en caso de resultar adjudicado, se compromete a presentar las garantías de las soluciones tecnológicas que se pondrán en operación en la SCJN
17	PARA CADA UNA DE LAS SOLUCIONES DE SEGURIDAD INFORMÁTICA PROPUESTAS PARA BRINDAR LOS	**7.2 DISTRIBUIDOR AUTORIZADO/ CERTIFICADO**	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE, PARA EFECTO DE CUMPLIMIENTO A LA ENTREGA DE LAS CARTAS SOLICITADAS DE DISTRIBUIDOR	Es correcta su apreciación

ARYABHDi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	SERVICIOS DE PROTECCIÓN PARA PORTALES WEB, PROTECCIÓN DE CORREO ELECTRÓNICO, DET ECCIÓN 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).		AUTORIZADO DE FABRICANTE SE ESPERA QUE LAS MISMAS ESTÉN FIRMADAS POR EL REPRESENTANTE LEGAL DE LA MARCA, DE FORMA AUTÓGRAFA ORIGINAL Y NO UNA CERTIFICADA EN ELECTRÓNICA, FACSÍMIL O EN PROPIEDAD DE UN TERCERO	
18	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	**7.1 REQUISITOS TÉCNICOS DE LAS SOLUCIONES PROPUESTAS.**	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE, TODOS LOS REQUERIMIENTOS DE ANEXO TÉCNICO Y AL NO ENCONTRARSE TODA LA DOCUMENTACIÓN EN HOJAS DE ESPECIFICACIONES DEL PRODUCTO, SE DEBERÁN INTEGRAR DE SER NECESARIO, AQUELLOS EXTRACTOS DE DISTINTAS FUENTES ELECTRÓNICAS, GUÍAS DE USUARIO, O CUALQUIER OTRO TIPO DE DOCUMENTO QUE REFIERAN A LAS CARACTERÍSTICAS EN COMENTO, SIEMPRE Y CUANDO SOPORTEN EL CUMPLIMIENTO DE LOS REQUERIMIENTOS DE LA SCJN,	Se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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.		¿SE ACEPTA NUESTRA PROPUESTA?	
19	MEJORA AL MODELO DE GOBIERNO	**4.1.6 SERVICIO DE ACTUALIZACIÓN Y MEJORA DEL MODELO INSTITUCIONAL DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN - MIGSI**	SE SOLICITA AMABLEMENTE A LA CONVOCANTE INDICAR SI ES CORRECTO ENTENDER QUE, PARA LA MEJORA AL MODELO DE GOBIERNO SE DEBERÁ CONSIDERAR LA EVALUACIÓN DE LA SITUACIÓN ACTUAL, DOCUMENTACIÓN, IMPLEMENTACIÓN Y LA GESTIÓN DEL GRC CONTINUO DURANTE LA VIGENCIA DEL CONTRATO, ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	Es correcta su apreciación, no se omite señalar que se debe considerar y alinear todo lo requerido para el servicio del modelo de gobierno.

ARYABHOi44FgzFTbdz6SeNkfc0b7T901O2JdDSLk0Cg=

3 PREGUNTAS DE LA EMPRESA: CONSULTORÍA Y CAPACITACIÓN EN SOLUCIONES AVANZADAS DE SEGURIDAD INFORMÁTICA, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	2. Objetivos específicos Dice: 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.	2. Objetivos específicos	Es correcto entender que el personal de la SCJN realiza actividades de Ciberinteligencia con base a la información que recaben las soluciones/herramientas solicitadas en el presente anexo	No es correcta su apreciación.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
2	4. Descripción de los servicios Dice: 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	4. Descripción de los Servicios	Se le solicita amablemente a la SCJN contestar los siguientes incisos: a) Lugar donde serán implementadas las soluciones de Ciberseguridad solicitadas en el anexo técnico. b) En caso de que se implementen en varios sitios, indicar si estos sitios están interconectados entre si, a través de una red MPLS, VPN, LAN to LAN u otro. Indicar si cuenta con un **sitio central** y cual es su ubicación.	Respuesta a): Para los equipos on premise serán instalados en los centros de datos de la SCJN ubicados en 2 edificios en la CDMX. Respuesta b): Si están interconectados por una red institucional. Respuesta: No se cuenta con un sitio central.
3	4.1.1. Servicio de protección para portales web. Dice: Deberá permitir la protección de todos los portales web de la SCJN publicados en internet, así como de sus registros DNS públicos.	4.1.1. Servicio de protección para portales web.	Se le solicita amablemente a la SCJN mencionar el número total de portales web, así como sus registros DNS que se están considerado proteger durante la vigencia del contrato.	Un máximo de 90 sitios web y los registros DNS serán revisados con el licitante adjudicado.
4	Certificados SSL Dice: Como referencia actualmente se cuentan en operación dos certificados EV, dos certificados OV y dos Certificados WildCard.	Certificados.	Se le solicita amablemente a la SCJN mencionar el número total de certificados SSL y tipo de cada uno de ellos que se están considerado durante la vigencia del contrato.	Los tipos de certificados son EV (Extended Validation), OV (Organization Validation) y WildCard y como referencia se cuenta con 2 de cada uno.
5	Sistema de monitoreo portales web. Dice: 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.	Sistema de monitoreo portales web	Es correcto entender que la “Herramienta de monitoreo de portales Web” deberá ser un complemento al “Servicio de protección para portales web.” Es decir una herramienta independiente y no un módulo embebido en la solución de seguridad propuesta. Favor de pronunciarse al respecto.	Es correcta su apreciación.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
6	4.1.2 Servicio de protección para correo electrónico. Dice: 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.	4.1.2 Servicio de protección para correo electrónico.	Es correcto entender que la SCJN proporcionara el espacio en Rack y energía para que el licitante ganador pueda instalar los componentes de las soluciones de seguridad propuestas.	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 regulada. • Condiciones climáticas.
7	4.1.2 Servicio de protección para correo electrónico. Dice: Compatible con el servicio de correo de Microsoft Exchange On Premise y con Office 365 (en la nube de Microsoft).	4.1.2 Servicio de protección para correo electrónico.	Se le solicita amablemente a la SCJN indicar el tipo de correo con que cuenta actualmente (Microsoft Exchange On Premise y con Office 365 u otro)	Microsoft Exchange On Premise y Office 365
8	4.1.2 Servicio de protección para correo electrónico. Dice: Permitir la integración con Directorio Activo de Microsoft AD para identificación de cuentas de correo electrónico válidas.	4.1.2 Servicio de protección para correo electrónico.	Es correcto entender que el Licitante Ganador podrá hacer uso del "Directorio Activo" propiedad de la SCJN, en caso de que una solución de seguridad la necesite. Favor de pronunciarse al respecto.	En caso de que una solución del licitante adjudicado requiera la conexión con el AD institucional, la actividad se realizará en conjunto con la convocante y bajo su supervisión.
9	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Dice: El prestador de servicios adjudicado deberá proporcionar un	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Se le solicita amablemente a la SCJN indicar si existe un canal comunicación (VPN, LAN to LAN, MPLS, otro) entre los dos sitios ubicados en CDMX	Si están interconectados por una red institucional.

ARYABHOi44Fgzfb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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			
10	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Dice: 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.	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Se le solicita amablemente a la SCJN indicar si los dos sitios ubicados en CDMX cuentan con salida a internet	Si cuentan con salida a internet.
11	4.1.4 Servicio de protección para puntos finales (XDR) Dice: 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	4.1.4 Servicio de protección para puntos finales (XDR)	Se le solicita amablemente a la SCJN indicar si los equipos de cómputo y servidores cuentan con salida a internet.	Si cuentan con salida a internet.
12	4.1.4 Servicio de protección para puntos finales (XDR) Dice: a) Compatibilidad: □ MS Windows en sus versiones 10, 11 y nuevas versiones	4.1.4 Servicio de protección para puntos finales (XDR)	Es correcto entender que la SCJN cuenta con los sistemas operativos y versiones en equipos de cómputo y servidores descritos en el Inciso "a) Compatibilidad:" de la sección "4.1.4 Servicio de protección para puntos finales (XDR)"	Si es correcta su apreciación.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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.			
13	4.1.4 Servicio de protección para puntos finales (XDR) Dice: 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.	4.1.4 Servicio de protección para puntos finales (XDR)	Se le solicita amablemente a la SCJN indicar la cantidad de Servidores, equipos de cómputo y contenedores con los que cuenta actualmente y que están considerados durante la vigencia del contrato.	La cantidad de equipos servidores, equipos de usuarios y contenedores considerados para la solución de XDR son Mínimo 3500 y máximo 4000.
14	4.1.4 Servicio de protección para puntos finales (XDR) Dice:	4.1.4 Servicio de protección para puntos finales (XDR)	Se le solicita amablemente a la SCJN mencionar si los contenedores están alojados de forma On-Premise ó en una nube publica y que tipo de nube es.	On premise

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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.			
15	4.1.4 Servicio de protección para puntos finales (XDR) Dice: Actividades de migración: o 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.	4.1.4 Servicio de protección para puntos finales (XDR)	Se le solicita amablemente a la SCJN mencionar el nombre y fabricante de la solución de XDR con la que cuneta actualmente, con el fin de considerar las medidas necesarias para llevar acabó la migración de manera eficiente.	Los datos de las soluciones de seguridad informática actualmente activas en la SCJN únicamente serán compartidas con el licitante adjudicado.
16	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 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).	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Con el fin de no limitar la libre participación, se le solicita amablemente a la SCJN que este punto sea opcional: • "afiliado al Foro de Grupos de Seguridad y de Respuesta a Incidentes (FIRST – Forum of Incident Response and Security Teams)" y que este sea reemplazado con un proceso certificado en "Respuesta a incidentes" en la norma ISO/IEC 27001:2013 por parte del licitante. Se acepta nuestra propuesta.	No se acepta su propuesta.
17	Ejecutar el análisis de código estático (SAST): El prestador de servicios adjudicado		Con el fin de realizar el correcto dimensionamiento y no sobre costear el proyecto, Se le solicita	Como referencia, sin ser limitativos, ya que este valor puede variar en función de los cambios que tenga cada sistema, actualmente se han analizado en promedio

ARYABHOi44FgzfTb12G3ekfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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.		amablemente a la SCJN responder los siguientes incisos: a) Numero de aplicaciones a analizar b) Cantidad de líneas de código por aplicación c) Tipo de lenguaje de programación en la que están desarrolladas Número total de desarrolladores.	650 mil líneas de código por sistema. El mayor con 1,332,337 líneas de código y el menor con 147,773. Hasta un máximo de 10 aplicaciones y de 3 a 5 desarrolladores por aplicación.
18	Certificado SSL TLS:	4.1.2 Servicio de protección para correo electrónico	¿La convocante considera que una solución que se integra mediante API a través de un canal seguro mediante TLS cumple con los requisitos de seguridad, sin necesidad de implementar un certificado TLS adicional?	No se acepta su propuesta.
19	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).	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Es correcto entender, que no se requieren puertos ethernet 10/100/1000 GE.	Los puertos de 40 y 10 Gbps establecidos en el anexo son el mínimo requerido, pudiendo su solución contar con interfaces de 1 Gbps.
20	4.1.4 Servicio de protección para puntos finales (XDR)	4.1.4 Servicio de protección para puntos finales (XDR)	¿La función de XDR se aplica únicamente al servicio Endpoint?	Equipos de usuario, equipos servidores y contenedores de aplicaciones.
21	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿La convocante requiere que los equipos tengan un rendimiento mínimo de 10 Gbps con todas las funciones de prevención de amenazas encendidas, incluso cuando se espera un tráfico de al menos 40 Gbps a través de la cantidad de interfaces requeridas? Si la respuesta es afirmativa, ¿la convocante acepta que la solución pueda aumentar su rendimiento	La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps.

ARY AGHDi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			agregando un componente, como memoria?	
22	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento	¿La convocante considera que la solución debe tener al menos 15 años de liderazgo en el mercado para ser considerada?	Es obligatorio que 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”.
23	4.1.4 Servicio de protección para puntos finales (XDR)	4.1.4 Servicio de protección para puntos finales (XDR)	¿La convocante considera que una solución que no haya presentado vulnerabilidades altas en el último año es segura para los puntos finales?	El licitante podrá determinar las soluciones más adecuadas para cumplir con los servicios requeridos en la presente licitación. Señalando que 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 y que cada servicio debe cumplir con el nivel requerido de la metodología de investigación por solución correspondiente.
24	9.17 Deberá contar con personal certificado en cada un de las soluciones propuestas para cubrir los servicios de seguridad informática del Anexo 2ª 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. Protección para portales web. Protección de correo electrónico.	Pág. 10. Bases de licitación. Punto 9.17	Si el Certificado no indica las soluciones que cubre, es posible que este punto sea aclarado mediante carta de fabricante?	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T9t1O2ldDSLkoOg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	Detección y protección de amenazas avanzadas con base en comportamiento. Protección para puntos finales. (XDR)			

4 PREGUNTAS DE LA EMPRESA: SILENT4BUSINESS, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	Certificados SSL	4.1.1. Servicio de protección para portales web.	Se solicita amablemente a la convocante especificar la cantidad de certificados requeridos del tipo EV, OV y Wildcard	Como referencia se tiene en operación 5 certificados de cada tipo.
2	Sistema de monitoreo portales web. 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.	4.1.1. Servicio de protección para portales web.	Es correcto entender que la solución propuesta deberá de alertar los diferentes códigos de error que pudiera mostrar a nivel de HTTP 400, 401,403,404, 429, 500, 502, 503, 504, entre otros)	Es correcta su apreciación.
3	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)	4.1.2 Servicio de protección para correo electrónico.	Se solicita a la convocante especificar la cantidad de buzones a proteger, debido a que solicita un total de 4000 buzones y mas adelante en el descriptivo de la solución especifican "Se deberá considerar lo necesario para gestionar al menos un mínimo de 3,600 cuentas de correo electrónico.", favor de aclarar la volumetría esperada.	Se debe considerar el máximo de 4000 buzones.
4	Permitir el relay o envío de correo electrónico directamente desde equipos servidores en las instalaciones de la SCJN (debiendo	4.1.2 Servicio de protección para correo electrónico.	Para un correcto dimensionamiento de la solución, se solicita amablemente a la convocante especifique la cantidad actual de correo transaccional en 1 mes, tamaño promedio del correo	No se cuenta con esa información.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLkmCg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	considerar lo necesario para establecer esta comunicación, por ejemplo: equipo servidor o algún servicio adicional).		transaccional y pico máximo de correo en 1 hora.	
5	Contar con un repositorio para cuarentena de correo electrónico, que permita almacenar correos SPAM por un mínimo de 90 días.	4.1.2 Servicio de protección para correo electrónico.	Se solicita a amablemente a la convocante permitir como mínimo 30 días para el almacenamiento de los correos en cuarentena, ¿se acepta la propuesta?	Se establece que el mínimo requerido para almacenar correo SPAM será por un periodo de 60 días.
6	Identificación de archivos o códigos maliciosos en el contenido del correo y adjuntos, eliminando todo archivo malicioso.	4.1.2 Servicio de protección para correo electrónico.	Al momento de recibir uno o varios correos con archivos infectados o maliciosos, por seguridad y mejores prácticas se recomienda mandar el correo a cuarentena para el análisis correspondiente (Cuenta origen, Cuenta destino, Dominio, Reputación entre otros). En este entendido, se solicita amablemente a la convocante permitir el envío de los correos a cuarentena para su análisis permitiendo el bloqueo instantáneo de las amenazas, ¿Se acepta la propuesta?	La operación será revisada con el licitante ganador, el servicio propuesto deberá cumplir con lo indicado en bases.
7	Certificado SSL TLS	4.1.2 Servicio de protección para correo electrónico.	¿Es correcto entender que el certificado solicitado es adicional a los solicitados en el punto Certificados SSL?.	Es correcta su apreciación.
8	Servicio de detección y protección de amenazas avanzadas con base en comportamiento	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿Es correcto entender que por cada equipo solicitado se deberán de considerar los Gbics para 4 interfaces de 40 Gbps y 6 interfaces de 10 Gbps por equipo?	Se deben considerar los Gbics de todos los puertos que su solución propuesta tenga, así como los del lado de la SCJN para garantizar una correcta comunicación.
9	Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente.	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿Sería posible que la convocante aclare si la velocidad indicada en la página 15, inciso c), de 5GB Threat Prevention es exacta, o si debería ser un valor superior, dada la solicitud de interfaces de 40GB, lo que podría implicar una necesidad de mayor capacidad de Throughput?	La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps.
10	Se deberá proporcionar equipos switches en alta disponibilidad (dos) para al menos 2 sitios de la SCJN dentro de la CDMX,	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿Es correcto entender que la cantidad de Switches solicitados es un total de 4, es decir dos equipos en alta disponibilidad por sitio?	Es correcta su apreciación.

AARYABHOi44FgzfTb1zSSeNkfc0bzTa01O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
11	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.	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Se solicita amablemente a la convocante especificar la cantidad de interfaces, el tipo de interfaz y Throughput esperado para un correcto dimensionamiento de los equipos.	De manera obligatoria los equipos propuestos deben contender 4 interfaces de 40 Gbps y 6 de 10 Gbps. La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps.
12	Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD).	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Se solicita amablemente a la convocante especificar el alcance esperado de la solución solicitada.	Auditoria, reporte y alertamiento de acciones ejecutadas en directorios activos.
13	Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD).	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	¿Es correcto entender que la solución puede ser ofertada en un esquema tipo nube?	No hay requisitos específicos, sin embargo, el licitante deberá considerar las especificaciones solicitadas en el anexo para la selección de la solución más adecuada que cumpla con lo que requerido.
14	Se deberá dimensionar para un aproximado de 20 servidores	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Se solicita amablemente a la convocante especificar en cuantas localidades se encuentran distribuidos los 20 servidores.	En al menos 6 localidades en la CDMX.
15	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	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Para un correcto dimensionamiento de la solución, se solicita amablemente a la convocante especificar la cantidad de Eventos por Segundo con los que cuenta actualmente.	El licitante deberá dimensionar su solución de SIEM propuesta conforme a sus soluciones propuestas.
16	Para el dimensionamiento de la capacidad de la solución, deberá considerar el flujo de logs de las soluciones de seguridad informática, así como	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Para un correcto dimensionamiento de la solución, se solicita a amablemente a la convocante especificar los tipos de servidores mencionados (Directorio activo, Servidores Web, Servidores de Base de Datos, Correo, Aplicaciones etc) para el establecimiento de los Eventos por Segundo.	Directorio activo, Servidores Web, Servidores de Base de Datos, Correo, y Aplicaciones etc

ARYABHOi44FgzfTb1zSSeNkf0o7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	un aproximado de 100 servidores, con un periodo de retención de logs de al menos 90 días en la nube.			
17	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.	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Para un correcto dimensionamiento de la solución, se solicita a amablemente a la convocante especificar, si de los servidores mencionados (Directorio activo, Servidores Web, Servidores de Base de Datos, Correo, Aplicaciones etc), ¿se requiere la correlación de los eventos a nivel sistema operativo o a nivel de aplicación?, favor de aclarar	A nivel Sistema Operativo.
18	Monitoreo de servicios	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Para el monitoreo de los servicios, ¿es correcto entender que el alcance solo es sobre la infraestructura habilitada por mi representada y no se deberá de considerar servidores o infraestructura propiedad de la convocante?, favor de aclarar el punto.	Es correcta su apreciación.
19	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.	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Se solicita amablemente a la convocante especificar la cantidad de análisis de vulnerabilidades realizadas a la infraestructura durante el ultimo año, para un correcto dimensionamiento del servicio.	Al menos 2 por servidor
20	Viñeta 9	4. Descripción de los servicios Servicio de actualización y mejora del MIGSI Modelo Institucional de Gobierno de Seguridad de la Información	Se entiende que el Programa de Concientización en Seguridad Informática (PCSI) se encuentra definido, y lo que se espera del proveedor es actualización del mismo respecto a la estrategia de seguridad de la información definida durante el servicio, ¿Es correcto? ¿es correcto que se deberá respetar algún componente del Programa en Seguridad informática (PCSI) implementado por la DGTI?	Respuesta1: Es correcta su apreciación. Respuesta 2: Se realizará el análisis correspondiente con el licitante adjudicado, previo a la definición de este rubro.
21	Un componente esencial dentro del MIGSI es el SGSI, por ello el presente servicio	4.1.6 Servicio de actualización y mejora del Modelo	¿Cuántos activos, procesos, personas, áreas, aplicativos se encuentran dentro del alcance del SGSI?	Como referencia sin ser limitativos, actualmente se están implementando 15 procesos y se tienen 175 activos declarados, 13 personas gestionando el MIGSI-SGSI, 171

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	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).	Institucional de Gobierno de Seguridad de la Información - MIGSI		personas pertenecientes a la Dirección General de Tecnologías de la Información, distribuidas en 5 Subdirecciones Generales, sin embargo, esta cantidad podrá variar al cierre de este.
22	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.	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información – MIGSI	Se solicita a la convocante especificar cada cuando se estarían llevando a cabo las evaluaciones sobre el nivel de conciencia de las amenas de seguridad, favor de aclarar.	Los ejercicios o evaluación se deberá realizar al menos de manera semestral durante la vigencia del contrato.
23	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	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	se solicita a la convocante especificar cuántas personas estarán incluidas en las evaluaciones periódicas, favor de aclarar.	Se deberá considerar como referencia un máximo de 3500 personas a evaluar. Este número podrá variar y se precisará conforme a lo identificado durante la ejecución del servicio.

ARYABHOA4gzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	de protección de datos en los sistemas informáticos.			
24	incluyendo los escaneos/análisis necesarios para validar las acciones correctivas (remediación, contención o mitigación) correspondientes.	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Siendo que la seguridad al código es crítica, y parte importante del proceso de desarrollo, al hablar de remediación, la herramienta debe proporcionar las recomendaciones de remediación a las vulnerabilidades encontradas, de acuerdo a los criterios mencionados en el anexo técnico, así como también proporcionar laboratorios de capacitación a los desarrolladores en código seguro del mismo fabricante de la herramienta, para optimizar gradualmente el proceso de desarrollo seguro de la convocante. ¿Es correcta nuestra apreciación?	Cada licitante, propondrá lo que considere más adecuado y eficaz como parte de las actividades para 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.
25	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.	7.1 Requisitos técnicos de las soluciones propuestas.	Con el objeto de facilitar la entrega de la propuesta se solicita a la convocante permita la entrega de la sección del manual en donde se especifica el cumplimiento técnico de la solución propuesta, ¿se acepta la propuesta?	Se podrá presentar caratula de la hoja de especificaciones (datasheet/folletos documentación técnica); así como las páginas que corresponden a la especificación técnica a la que se está haciendo referencia de su solución propuesta.
26	Consultor Senior de Seguridad de la Información	7.4.4 Personal requerido	Es correcto entender que al referirse a Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad se podrá comprobar con la emisión de certificados vigentes y avalados por organismos de	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o

ARIAABHDi44FgzfTb1zSSeNkfc0b7T901O2JdDSLkC0g=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			certificación en materia de seguridad de la información o ciberseguridad. ¿Es correcta la apreciación?	ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
27	Consultor Junior de Gestión de Seguridad de la información	7.4.4 Personal requerido	Es correcto entender que al referirse a Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad se podrá comprobar con la emisión de certificados vigentes y avalados por organismos de certificación en materia de seguridad de la información o ciberseguridad. ¿Es correcta la apreciación?	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
28	Especialista técnico en controles de ciberseguridad	7.4.4 Personal requerido	Es correcto entender que al referirse a Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad se podrá comprobar con la emisión de certificados vigentes y avalados por organismos de certificación en materia de seguridad de la información o ciberseguridad. ¿Es correcta la apreciación?	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CISSP o CISM o CRISC o Líder Implementador de ISO/IEC 27001, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
29	Coordinador de Equipo de Respuesta a Incidentes.	7.4.4 Personal requerido	Es correcto entender que al referirse a Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad se podrá comprobar con la emisión de certificados vigentes y avalados por organismos de certificación en materia de seguridad	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			de la información o ciberseguridad. ¿Es correcta la apreciación?	reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CIH – EC Council Certified Incident Handler o MILE2 Certified incident Handling Engineer o ISO/IEC 27035 Lead Incident Manager, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
30	Especialista de Ciberinteligencia.	7.4.4 Personal requerido	Es correcto entender que al referirse a Título, diploma o certificado que avale los estudios correspondientes en Seguridad de la Información o ciberseguridad se podrá comprobar con la emisión de certificados vigentes y avalados por organismos de certificación en materia de seguridad de la información o ciberseguridad. ¿Es correcta la apreciación?	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como GIAC Cyber Threat Intelligence o Offensive Security – OSCP, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
31	Numeral 6.1 - Documentación Legal y Financiera	Numeral 6.1 - Documentación Legal y Financiera	¿Es correcto entender que en el sobre1 únicamente se deberá presentar la documentación legal como copia simple de los documentos solicitados en los numerales 6.1.1, 6.1.2, 6.1.3, 6.1.4 y 6.1.5, 6.1.6, 6.1.7 y, en su caso el 6.1.8. para su revisión, cotejo y posterior devolución, sin agregar o anexar ningún "formato para efectos de suscripción de la proposición", puesto que en los Anexos no viene algo similar?	Es correcta su apreciación, para dar cumplimiento con lo establecido en el numeral 6.1 de las bases únicamente se deberá presentar en el sobre número "1", en original o copia certificada ante fedatario público y copia simple para cotejo, según corresponda, la documentación descrita en los numerales 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.1.7 y, en su caso el 6.1.8. Por tanto, no se requiere de formato en particular para efectos de suscripción o presentación de la documentación legal.
32	Como establece La Ley, en el Código de Comercio, Libro Primero, Título Segundo, Capítulo II, Artículo 21, Fracción VII, ESTABLECE: VII. Para efectos del comercio y consulta electrónicos, opcionalmente, los poderes y nombramientos de funcionarios, así como sus renuncias o revocaciones.	Numeral 6.1 - Documentación Legal y Financiera	¿Es correcto entender que no seremos descalificados si el poder del Representante Legal no cuenta con Registro Público de la Propiedad (RPP), puesto que las facultades otorgadas a mi persona no exigen mayor requisito y/o formalidad que su protocolización, lo anterior, con fundamento en el artículo 21 fracción 7 del Código de Comercio?	Es correcta su apreciación, con la salvedad de que el acto de otorgamiento de las facultades respectivas conste en el acta constitutiva de la persona moral participante, en cuyo caso, deberá contar con la inscripción ante el Registro Público de la Propiedad, correspondiente.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
33	Como establece La Ley, en el Código de Comercio, Libro Primero, Título Segundo, Capítulo II, Artículo 21, Fracción XII, ESTABLECE: XII: El cambio de denominación o razón social, domicilio, objeto social, duración y el aumento o disminución del capital mínimo fijo	Numeral 6.1 - Documentación Legal y Financiera	¿Es correcto entender que no seremos descalificados si en las reformas presentadas no cuenta con el Registro Público de la Propiedad (RPP), si no es por “el cambio de denominación o razón social, domicilio, objeto social, duración y el aumento o disminución del capital mínimo fijo” (es decir, al variable no es registrable), no se registra el acta, y tampoco movimientos en la administración o accionistas, porque son artículos derogados, lo anterior conforme al artículo 21 fracción XII del código de comercio?	La inscripción ante las instituciones registrales correspondientes será objeto de verificación en aquellos actos cuya normatividad disponga que deben encontrarse debidamente inscritos ante los registros que estas determinen, como son el acta constitutiva, reformas en la denominación, objeto social, duración; escisiones, fusiones, entre otras. En tales términos si las disposiciones normativas no establecen una obligatoriedad expresa para inscribir determinado acto, no será objeto de valoración en el Dictamen Resolutivo Legal.
34	Comprobante de domicilio legal expedido a nombre de la persona participante durante el último semestre por algún órgano del Estado Mexicano (boleta predial, comprobante de derechos por consumo de agua, comprobante de consumo de energía eléctrica expedido por la Comisión Federal de Electricidad). Cuando este documento corresponda a la versión electrónica, se entregará de manera impresa sin tachaduras ni enmendaduras, debiendo presentar una carta bajo protesta de decir verdad en la que manifieste que el documento es fidedigno (Anexo 1b).	Numeral 6.1.3 – Documentación Legal y Financiera	4. Para dar cumplimiento al numeral 6.1.3 solicita el comprobante de domicilio legal a nombre de la persona participante durante el último semestre (boleta predial, comprobante derechos por consumo de agua, comprobante consumo energía eléctrica), cuando el comprobante de domicilio de referencia no esté a nombre de la persona participante, será necesario acreditar un acto jurídico (ejemplo contrato de arrendamiento, comodato o de servicios de oficinas compartidas). Es correcto entender que de encontrarse en el segundo supuesto (comprobante no esté a nombre de la persona participante), ¿Únicamente se deberá presentar el acto jurídico?	No es correcta su apreciación. En términos del numeral 6.1.3, tercer párrafo, cuando el comprobante de domicilio de referencia no esté a nombre de la persona participante, adicionalmente será necesario que acredite un acto jurídico o relación contractual vigente con la persona diversa (ejemplo contrato de arrendamiento, comodato o de servicios de oficinas compartidas) en virtud del cual tiene la propiedad o posesión derivada del inmueble correspondiente; por tanto deberá coincidir el nombre de las personas que aparecen en el comprobante de domicilio presentado y de la persona participante, así como la dirección del domicilio que se pretende acreditar
35	Documento donde conste el registro patronal expedido por el Instituto Mexicano del Seguro Social (Cuando este documento corresponda a la versión electrónica, se entregará el	Numeral 6.1.5 – Documentación Legal y Financiera	Es correcto entender que para la presentación del Documento donde conste el registro patronal expedido por el Instituto Mexicano del Seguro Social y en su momento el trámite fue efectuado de forma presencial donde otorgaron los documentos originales, ¿ya no sería necesario presentar el Anexo 1c?	Es correcta su apreciación. Solo cuando este documento corresponda a la versión electrónica, se entregará el documento impreso sin tachaduras ni enmendaduras, debiendo presentar la carta bajo protesta de decir verdad en la que manifieste que el documento es fidedigno, Anexo 1c, de las bases de licitación.

ARYABbG14FgzfTbIzSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	documento impreso sin tachaduras ni enmendaduras, debiendo presentar una carta bajo protesta de decir verdad en la que manifieste que el documento es fidedigno (Anexo 1c).			
36	Sesión de presentación de documentación legal y financiera, apertura de propuestas técnicas y económicas	Sesión de presentación de documentación legal y financiera, apertura de propuestas técnicas y económicas	Es correcto entender que, para la presentación de documentación legal y financiera, apertura de propuestas técnicas y económicas, en caso de presentarse alguna persona diferente al representante legal ¿no se requiere algún poder simple para la recepción y entrega de propuesta?	En relación a la posibilidad de que pueda asistir una persona distinta al representante legal con carta poder a la “Sesión pública de presentación de documentación legal y financiera, y apertura de propuestas técnicas y económicas”, se aclara que no se acepta su propuesta, ya que de acuerdo con el numeral 11.6 de las Bases, el participante o su representante legal al momento de entregar los sobres deberá firmar de recibido el documento de acuse correspondiente y la Dirección General de Recursos Materiales conservará una copia de éste. Asimismo, el artículo 69, quinto párrafo, del Acuerdo General de Administración XIV/2019, dispone que “el licitante deberá entregar copia de su identificación o la del representante legal que asista y exhibir original para su cotejo”, por lo que los servidores públicos requerirán de dicha identificación al representante legal. Por lo tanto, la persona que asista a la referida sesión pública deberá ser el licitante o su representante o apoderado legal. En dichos términos al ser una persona moral no se permitirá la presentación de una carta poder simple para acudir en nombre del representante legal, apoderado legal o el licitante, ya que en términos del artículo 10 de la Ley General de Sociedades Mercantiles la representación de las sociedades mercantiles corresponderá a su administrador o administradores, o en su caso a la persona a la que se le haya otorgado un poder protocolizado ante un notario público.
37	Anexo 4	Numeral 29 – Anexos	7. Es correcto entender que el Anexo 4 – Modelo de contrato ordinario y el Anexo 5- Formato de Garantía de Cumplimiento, ¿son únicamente de carácter informativo?	Es correcto, dichos modelos son únicamente de carácter informativo.

5 PREGUNTAS DE LA EMPRESA: SOLUCIONES INTEGRALES E INNOVACIÓN TECNOLÓGICA SUSTENTABLE, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	ANEXO 2ª PROPUESTA TÉCNICA	4.1.2 Servicio de protección para correo electrónico	**Dice:** Certificado SSL TLS: **Pregunta**: ¿La convocante considera que una solución que se integra mediante API a través de un canal seguro mediante TLS cumple con los requisitos de seguridad, sin necesidad de implementar un certificado TLS adicional?	No se acepta la propuesta.
2	ANEXO 2ª PROPUESTA TÉCNICA	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	**Dice:** 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). **Pregunta:** Es correcto entender, que no se requieren puertos ethernet 10/100/1000 GE.	Los puertos de 40 y 10 Gbps establecidos en el anexo son el mínimo requerido, pudiendo su solución contar con interfaces de 1 Gbps.
3	ANEXO 2ª PROPUESTA TÉCNICA	4.1.4 Servicio de protección para puntos finales (XDR)	¿La función de XDR se aplica únicamente al servicio endpoint?	Equipos de usuario, equipos servidores y contenedores de aplicaciones.
4	ANEXO 2ª PROPUESTA TÉCNICA	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿La convocante requiere que los equipos tengan un rendimiento mínimo de 10 Gbps con todas las funciones de prevención de amenazas encendidas, incluso cuando se espera un tráfico de al menos 40 Gbps a través de la cantidad de interfaces requeridas? Si la respuesta es afirmativa, ¿la convocante acepta que la solución pueda aumentar su rendimiento agregando un componente, como memoria?	La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps. El licitante podrá determinar la configuración mas adecuada para los equipos propuestos para cubrir lo requerido en el Servicio de detección y protección de amenazas avanzadas con base en comportamiento, siempre y cuando cumpla con lo requerido en la presente licitación.
5	ANEXO 2ª PROPUESTA TÉCNICA	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	¿La convocante considera que la solución debe tener al menos 15 años de liderazgo en el mercado para ser considerada?	Es obligatorio que 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”.
6	ANEXO 2ª	4.1.4 Servicio de protección para	¿La convocante considera que una solución que no haya presentado	El licitante podrá determinar las soluciones más adecuadas para cumplir con los servicios

ARYABHO044FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	PROPUESTA TÉCNICA	puntos finales (XDR)	vulnerabilidades altas en el último año es segura para los puntos finales?	requeridos en la presente licitación. Señalando que 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 y que cada servicio debe cumplir con el nivel requerido de la metodología de investigación por solución correspondiente.
7	ANEXO 2ª PROPUESTA TÉCNICA	Pág. 9. Bases de licitación Punto 9.10. Y Anexo técnico	Se debe de presentar una carta por solución aún y cuando sea el mismo fabricante?	En caso de que sea el mismo fabricante el propuesto para más de una de las soluciones requeridas, se podrá presentar una carta indicando las soluciones que se presentarán de la misma marca, debiendo contar la carta con todos los requisitos solicitados en las bases de la licitación.
8	ANEXO 2ª PROPUESTA TÉCNICA	Pág. 10. Bases de licitación. Punto 9.17 y Anexo Técnico	Adicional al certificado es posible agregar una carta de licitante o de fabricante confirmando las tecnologias que cubre cada certificado?	No se acepta su propuesta.
9	ANEXO 2ª PROPUESTA TÉCNICA	Pág. 21. Anexos. Puesta en operación.	Con la finalidad de no encarecer la propuesta se solicita a la convocante confirmar si con: en compañía del fabricante, se refiere a que el Fabricante unicamente validará la arquitectura propuesta. ¿ ES CORRECTO?	El fabricante deberá validar la arquitectura y las configuraciones realizadas por el licitante adjudicado en las soluciones propuestas.
10	ANEXO 2ª PROPUESTA TÉCNICA	Pág. 22. Anexos. Mejora continua	Con la finalidad de optimizar costos, se solicita a la convocante considerar las revisiones con el fabricante al menos cada 6 meses. ¿ ACEPTA LA CONVOCANTE ?	Se acepta su propuesta.
11	ANEXO 2ª PROPUESTA TÉCNICA	4.1.2.Servicio de protección para correo electrónico. Y Formato económico.	Se solicita a la convocante confirmar que el servicio de Protección de correo electronico. Cantidad: 1. Indicado en el formato económico debe de contemplar 4000 buzones. ¿ ES CORRECTO?	Hasta 4000 buzones.
12	ANEXO 2ª PROPUESTA TÉCNICA	7.4.4 Personal requerido: Consultor Junior de Gestión de Seguridad de la información Comprobación: • Certificado vigente como Líder Implementador de ISO/IEC 27001.	A fin de no limitar la participación de los LICITANTES se pide a la CONVOCANTE de la manera más atenta permitir cumplir con la comprobación del certificado de la certificación: Líder Implementador de ISO/IEC 27001 con la certificación: Líder Auditor ISO/IEC 27001, derivado a que el perfil requiere un nivel de conocimientos de toda la norma. ¿ACEPTA LA CONVOCANTE?	No es correcta su apreciación. Sólo se acepta la presentación de la certificación como Líder Implementador de ISO/IEC 27001

6 PREGUNTAS DE LA EMPRESA: SCITUM, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	8. REQUISITOS GENERALES PARA LA PRESENTACIÓN DE PROPUESTAS TÉCNICAS Y ECONÓMICAS	8.5 Cada una de las hojas de los formatos anexos a las bases deberá ser requisitada en su totalidad con los siguientes datos: c. Nombre y firma de la persona licitante o su representante legal.	¿Es correcto entender que se dará cumplimiento a este requisito con la rúbrica del apoderado legal en todas las hojas que integren la propuesta y la firma autógrafa en los anexos en donde aparezca el nombre del apoderado legal?	No es correcta su apreciación, la propuesta la deberá firmar de manera autógrafa por la persona licitante o quien funja como representante legal.
2	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.2 La persona licitante deberá entregar su propuesta técnica en idioma español, en papeleríamembretada de la persona participante, foliadas, firmadas en todas sus hojas por la persona licitante o quien funja como representante legal…	¿Es correcto entender que se dará cumplimiento a este requisito con la rúbrica del apoderado legal en todas las hojas que integren la propuesta y la firma autógrafa en los anexos en donde aparezca el nombre del apoderado legal?	No es correcta su apreciación, en todas las hojas de su propuesta técnica deben ser firmadas de manera autógrafa por la persona licitante o quien funja como representante legal.
3	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.10 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	Se solicita amablemente a la convocante aceptar que las cartas sean firmadas por el representante en México de los fabricantes, ya que, en algunos casos, el apoderado legal del fabricante se encuentra en el extranjero o no existe la figura de representante legal. ¿Se acepta la propuesta?	No se acepta su propuesta.

ARYABHOi44FgzfTb1SeBkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		deberá presentar carta membretada expedida por el fabricante de las soluciones, firmada por su representante legal, reconociéndolo como distribuidor autorizado…		
4	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.10 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…	Se solicita amablemente a la convocante aceptar el formato de carta de distribuidor autorizado que maneje cada fabricante, ya que estos cuentan con su propio template para la emisión de esta carta. ¿Se acepta la propuesta?	El formato es libre, siempre y cuando sea emitida por el fabricante y cumpla con lo descrito en el numeral 9.10.
5	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.12 Copia del certificado ISO/IEC 27001 en al menos 5 procesos de seguridad de la información en su versión 2013 o superior…	Se solicita amablemente a la convocante tenga a bien aceptar un documento emitido por la entidad certificadora en donde acredite que la emisión del certificado está en trámite; en caso de que no se cuente con el certificado emitido en la fecha de presentación y apertura de propuestas. ¿Se acepta la propuesta?	No se acepta su propuesta.

ARYABHOi44Fgof61zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
6	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.13 Copia de los certificados ISO 9001 versión 2015 o superior, ISO/IEC 20000-1 versión 2018 o superior…	Se solicita amablemente a la convocante tenga a bien aceptar un documento emitido por la entidad certificadora en donde acredite que la emisión del certificado está en trámite; en caso de que no se cuente con el certificado emitido en la fecha de presentación y apertura de propuestas. ¿Se acepta la propuesta?	No se acepta su propuesta.
7	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.16 Presentar al menos 3 contratos formalizados en copia simple.	¿Es correcto entender que la totalidad de los servicios solicitados (6 servicios) se deberán demostrar entre al menos 3 contratos? 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). Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación.	No es correcta su apreciación, se deben presentar al menos 3 contratos con cualquiera de los servicios contenidos en la presente licitación.
8	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.16 Presentar al menos 3 contratos formalizados en copia simple	¿Podrá la convocante indicar el número máximo de contratos con los que se deberá demostrar experiencia en los servicios solicitados?	No existe un máximo de contratos, siempre y cuando se demuestre que tenga experiencia de al menos 3 años dentro del periodo de 2017 a 2023.
9	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.16 “de por lo menos tres años (dentro del periodo de 2017 al 2023)”	Se solicita a la convocante, aceptar contratos dentro del periodo de 10 anteriores al 2023, esto con el objetivo de demostrar mayor experiencia y no limitar la libre participación. ¿Se acepta nuestra propuesta?	No se acepta su propuesta.
10	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	9.16 “de por lo menos tres años (dentro del periodo de 2017 al 2023)”	¿Es correcto entender que, se consideraran aquellos contratos cuya suma de varios contratos de diferentes dependencias y celebrados en distintos periodos demuestren experiencia de por lo menos tres años? Favor de pronunciarse.	Es correcta su apreciación.
11	9. PROPUESTA TÉCNICA (SOBRE	9.16 “de por lo menos tres años (dentro del	¿Es correcto entender que para el Servicio de actualización y mejora del Modelo Institucional de Gobierno	No es correcta su apreciación, se deben presentar al menos 3 contratos con

ARYABHOi44FgzfTb1zSSeNkfc0b7T90IO2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	CERRADO NÚMERO 3)	periodo de 2017 al 2023) en la prestación del presente servicio o equivalente”	de Seguridad Informática (MIGSI) para la Suprema Corte de Justicia de la Nación, se podrá demostrar experiencia y capacidad técnica suficiente con contratos que contengan servicios de Sistemas de gestión de la calidad? Favor de pronunciarse.	cualquiera de los servicios contenidos en la presente licitación.
12	ANEXO 2a PROPUESTA TÉCNICA	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 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).	¿Es correcto entender que la convocante se refiere a las certificaciones de las Normas ISO/IEC 20000-1 (Sistema de Gestión de Servicios), versión 2018 o superior e ISO/IEC 9001 (Sistema de Gestión de Calidad), versión 2015 o superior solicitadas en el numeral 9.13 de las bases?	Es correcta su apreciación.
13	ANEXO 2a PROPUESTA TÉCNICA	7.4.4 Personal requerido: Consultor Senior de Seguridad de la Información	Es correcto entender que para acreditar que el personal cuenta con Especialidad / Diplomado en Seguridad de la Información o ciberseguridad, se podrán presentar certificaciones tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc.	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
14	ANEXO 2a PROPUESTA TÉCNICA	7.4.4 Personal requerido: Consultor Junior de Gestión de Seguridad de la información	Es correcto entender que para acreditar que el personal cuenta con Especialidad / Diplomado en Seguridad de la Información o ciberseguridad, se podrán presentar certificaciones tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc.	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional,

ABYABHOr4tFgzlTblZSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
				Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
15	ANEXO 2a PROPUESTA TÉCNICA	7.4.4 Personal requerido: Especialista técnico en controles de ciberseguridad	Es correcto entender que para acreditar que el personal cuenta con Especialidad / Diplomado en Seguridad de la Información o ciberseguridad, se podrán presentar certificaciones tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc.	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CISSP o CISM o CRISC o Líder Implementador de ISO/IEC 27001, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
16	ANEXO 2a PROPUESTA TÉCNICA	7.4.4 Personal requerido: Coordinador de Equipo de Respuesta a Incidentes	Es correcto entender que para acreditar que el personal cuenta con Especialidad / Diplomado en Seguridad de la Información o ciberseguridad, se podrán presentar certificaciones tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc.	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CIH – EC Council Certified Incident Handler o MILE2 Certified incident Handling Engineer o ISO/IEC 27035 Lead Incident Manager, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
17	ANEXO 2a PROPUESTA TÉCNICA	7.4.4 Personal requerido: Especialista de Ciberinteligencia.	Es correcto entender que para acreditar que el personal cuenta con Especialidad / Diplomado en Seguridad de la Información o ciberseguridad, se podrán presentar certificaciones tales como: Certified in Information Systems Security Professional, Offensive Security	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc.	reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como GIAC Cyber Threat Intelligence o Offensive Security – OSCP, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
18	10. PROPUESTA ECONÓMICA (SOBRE CERRADO NÚMERO 4)	10.4 Será obligatorio el presentar las constancias con la que acredite que cuenta con la opinión del cumplimiento de las obligaciones fiscales en sentido positivo, expedidas por el SAT, el IMSS y el INFONAVIT.	Derivado de que la opinión del cumplimiento de las obligaciones fiscales, expedida por el IMSS, únicamente es vigente el día en que se emite, se solicita amablemente a la convocante aceptar la opinión del cumplimiento de las obligaciones fiscales, expedida por el IMSS, emitida dentro del mes en que se llevará a cabo el acto de presentación y apertura de propuestas del presente procedimiento. ¿Se acepta la propuesta?	Las constancias solicitadas en el numeral 10.4 de las bases deberán tener una vigencia máxima de 15 días naturales previos al día de la sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas. En su momento, el licitante que resulte adjudicado deberá presentar dichas constancias actualizadas con una vigencia máxima de 15 días naturales previos a la firma del contrato respectivo.
19	10. PROPUESTA ECONÓMICA (SOBRE CERRADO NÚMERO 4)	10.4 Será obligatorio el presentar las constancias con la que acredite que cuenta con la opinión del cumplimiento de las obligaciones fiscales en sentido positivo, expedidas por el SAT, el IMSS y el INFONAVIT.	En caso de que la respuesta a la pregunta anterior sea en sentido negativo, se hace del conocimiento de la convocante que de conformidad con el acuerdo ACDO. AS2.HCT.250423/106.P.DIR de fecha 25 de abril de 2023, publicado en el Diario Oficial de la Federación el 4 de mayo de 2023, la opinión de cumplimiento de obligaciones en materia de seguridad social emitida por el IMSS tiene una vigencia de 15 días naturales, con base en lo expuesto, se solicita amablemente a la convocante aceptar la opinión del cumplimiento de las obligaciones fiscales, expedida por el IMSS, emitida dentro del mes en que se llevará a cabo el acto de presentación y apertura de propuestas del presente procedimiento. ¿Se acepta la propuesta?	Las constancias solicitadas en el numeral 10.4 de las bases deberán tener una vigencia máxima de 15 días naturales previos al día de la sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas. En su momento, el licitante que resulte adjudicado deberá presentar dichas constancias actualizadas con una vigencia máxima de 15 días naturales previos a la firma del contrato respectivo.
20	Anexo 2a Propuesta técnica	4. Descripción de los servicios	Dice: • 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,	Se proporcionará al licitante adjudicado.

ARYABHOI4IFgzfTb1zSSeNkfc0b7T9O12ddDSLkOOg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			soportes/montajes, tornillos, cables de alimentación eléctrica y PDU. Pregunta: ¿Podría la convocante compartir el voltaje y corriente que manejan sus racks, así como el tipo de conector que se requiere para montar los PDU´s?	
21	Anexo 2a Propuesta técnica	4. Descripción de los servicios	Dice: • 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. ¿Podría especificar la convocante de su lado que considerara para la implementación de las tecnologías (por ejemplo, racks, nodo de alimentación, nodo de red, etc.)?	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 regulada. • Condiciones climáticas.
22	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) GENERALES:	Dice: El Centro de Operaciones de Ciberseguridad deberá pertenecer al prestador de servicios adjudicado y ubicarse dentro del territorio nacional. Pregunta: ¿Es correcto precisar que el servicio de operación y gestión de los servicios de seguridad informática podrán ser brindados de manera remota desde un centro de operaciones de ciberseguridad (COC)?	Es correcta su apreciación, excepto cuando el personal del COC sea requerido en sitio por la SCJN para casos en específico.
23	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 7.1 Requisitos técnicos de las soluciones propuestas.	Dice: a. Para su acreditación de cada solución, se deberá proveer de una copia de la metodología de investigación correspondiente. Pregunta: ¿Es correcto precisar que, a metodología de investigación, se refiere la convocante a aquel documento que evidencie que las soluciones tecnológicas se encuentran dentro del "cuadrante de Gartner" o "Forrester Wave", dependiendo del tipo de tecnología solicitada?	Es correcta su apreciación, siempre que la solución ofertada se encuentre posicionada en la sección o cuadrante correspondiente solicitada en el anexo 2A
24	Anexo 2a Propuesta técnica	.1.5 Servicio de Centro de Operaciones de	Dice: c. El licitante deberá acreditar que las soluciones de seguridad informática propuestas para cada servicio cumplen con las	Se podrá presentar caratula de la hoja de especificaciones (datasheet/folletos o documentación técnica); así como las páginas que corresponden a la especificación

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Ciberseguridad (COC) 7.1 Requisitos técnicos de las soluciones propuestas.	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. Pregunta: En el entendido que hay soluciones las cuales cuentan con documentación con mas de 1,000 hojas, se le solicita amablemente a la convocante poder presentar solo el extracto o página que haga referencia al cumplimiento solicitado en lugar del documento completo. ¿Acepta la convocante la propuesta?	técnica a la que se está haciendo referencia de su solución propuesta.
25	Anexo 2a Propuesta técnica	9. Lugar donde se prestará el servicio.	Dice: 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. Pregunta: Se le solicita amablemente a la convocante considerar los servicios de operación con respecto a los servicios de seguridad informática de manera remota en el entendido que se debe manejar dichos servicios desde un COC en territorio nacional	Es correcta su apreciación, excepto cuando el personal del COC sea requerido en sitio por la SCJN para casos en específico.
26	ANEXO 3 FORMATO DE PROPUESTA ECONÓMICA (En papel membretado del participante)	a) Vigencia del servicio:	Dice: 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	El aprovisionamiento está considerado dentro de la etapa de implementación, considerando la fecha de inicio del servicio el día 1º de abril de 2024.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			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. Pregunta: ¿Es correcto precisar que dentro de este tiempo indicado para la implementación (desde el fallo hasta abril), se puede considerar el aprovisionamiento de las tecnologías requeridas como parte del proceso de implementación? Favor de la convocante pronunciarse al respecto	
27	Anexo 2a Propuesta técnica	4.1.1. Servicio de protección para portales web.	Dice: Manejo de dominios DNS: se deberá considerar la capacidad de soportar al menos 20 zonas de DNS o dominios públicos. Pregunta: ¿Es correcto precisar que la convocante cuenta con hasta 20 dominios Web?	Es correcta su apreciación.
28	Anexo 2a Propuesta técnica	4.1.1. Servicio de protección para portales web.	Dice: El módulo de WAF deberá considerar los necesario para gestionar hasta 90 portales o dominios web Pregunta: ¿Es correcto precisar que la convocante cuenta con hasta 90 subdominios Web?	Es correcta su apreciación.
29	Anexo 2a Propuesta técnica	4.1.1. Servicio de protección para portales web.	Dice: El módulo de WAF deberá considerar los necesario para gestionar hasta 90 portales o dominios web Pregunta: ¿Podría especificar la convocante el tráfico o ancho de banda utilizado del total de portales web mencionados?	512 Mbps (ancho de banda del enlace a internet de los portales web de la SCJN).
30	Anexo 2a Propuesta técnica	4.1.1 Servicio de protección para portales web Certificados SSL	Dice: • 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 tipos de certificados son EV (Extended Validation), OV (Organization Validation) y WildCard, como referencia se tiene en operación 2 de cada tipo.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: ¿Podría especificar la convocante los tipos certificados SSL y cuantos requerirá en total para cubrir la totalidad de dominios?	
31	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico. Certificado SSL TLS	Dice: 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 Pregunta: Podría especificar la convocante el tipo de certificado SSL requerido (por ejemplo, OV, EV, Wildcard, etc.)	OV (Organization Validation)
32	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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". Pregunta: Con el objetivo de fomentar la libre participación se le solicita amablemente a al convocante que la solución solamente se encuentre posicionada en la "Forrester Wave" sin importar que se encuentre como líder,	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			siempre y cuando pueda cubrir con los requerimientos solicitados	
33	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: Compatible con el servicio de correo de Microsoft Exchange On Premise y con Office 365 (en la nube de Microsoft)." ¿Podría especificar la convocante cuantos buzones o cuentas de correo se deben considerar por separado para Exchange on premise y office 365?	Aproximadamente 3700 buzones en office 365 y 300 buzones en exchange on premise, considerando como máximo 4000 buzones para el servicio requerido.
34	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: Compatible con el servicio de correo de Microsoft Exchange On Premise y con Office 365 (en la nube de Microsoft)." ¿Podría especificar la convocante si se puede manejar la integración con ambientes híbridos de Office 365?	El licitante podrá proponer su esquema de operación que requiera su solución propuesta, siempre y cuando cumpla con lo solicitado en bases.
35	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico. Certificado SSL TLS	Dice: 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 Pregunta: ¿Podría especificar La convocante acepta que una solución que se integra mediante API a través de un canal seguro mediante TLS protocolos no requiera la implementación de un certificado	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T9016220dSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			TLS adicional, dado que ya lo integra de forma nativa?	
36	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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). Pregunta: ¿Podría la convocante compartir el estimado de correos de entrada y de salida que se manejan por hora, en horas pico?	No se cuenta con esa información.
37	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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). ¿Podría especificar la convocante la cantidad de correos transaccionales y aparte la cantidad de correos corporativos que manejan?	No se cuenta con esa información.
38	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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). ¿Podría especificar la convocante el tamaño promedio del correo transaccional que manejan?	No se cuenta con esa información.
39	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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). ¿Podría especificar la convocante el estimado del pico máximo de correos transaccionales que manejan en un tiempo estimado de 1 hora?	No se cuenta con esa información.
40	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: Capacidad de recibir tráfico con conexiones SMTP/TLS y poder hacer conexiones con otros servidores de SMTP/TLS. ¿Es correcto entender que la convocante maneja utilizan SMTP	No es correcta su apreciación, se requiere él envió de correo electrónico de manera segura por TLS.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			autenticado para el envío de los correos?	
41	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: Contar con un repositorio para cuarentena de correo electrónico, que permita almacenar correos SPAM por un mínimo de 90 días Pregunta: Se le solicita amablemente a la convocante considerar un tiempo menor de aproximadamente 30 días para el repositorio solicitado	Se establece que el mínimo requerido para almacenar correo SPAM será por un periodo de 60 días.
42	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: Identificación de archivos o códigos maliciosos en el contenido del correo y adjuntos, eliminando todo archivo malicioso. Pregunta: Se le solicita amablemente a la convocante manejar como una opción la detección y bloqueo del correo completo en lugar de solo el archivo malicioso.	La operación será revisada con el licitante ganador, el servicio propuesto deberá cumplir con lo indicado en bases.
43	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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. Pregunta: Se le solicita amablemente a la convocante manejar como opcionales las cuentas de lectura y se puedan manejar como opción en lugar de cuentas de lectura, cuentas de administrador siempre y cuando se lleven los procesos necesarios para el correcto manejo de dichas cuentas.	La operación será revisada con el licitante ganador, el servicio propuesto deberá cumplir con lo indicado en bases.
44	Anexo 2a Propuesta técnica	4.1.2 Servicio de protección para correo electrónico.	Dice: 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).	Si se cuenta y es proporcionada mediante un equipo antispam on premise.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2ddDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: ¿Podría especificar la convocante si actualmente dentro de la infraestructura actual de correo que manejan, cuentan con alguna funcionalidad de relay?	
45	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: 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". Pregunta: Con el objetivo de fomentar la libre participación se le solicita amablemente a al convocante que la solución solamente se encuentre posicionada dentro del Cuadrante de Gartner" sin importar que se encuentre como líder, siempre y cuando pueda cubrir con los requerimientos solicitados	No se acepta su propuesta.
46	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: 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: Pregunta: ¿Es correcto entender que se requiere considerar 2 equipos en arreglo de alta disponibilidad en dos sitios independientes dentro de la CDMX, en total 2 equipos por sitio para tener alta disponibilidad?	Es correcta su apreciación.
47	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	o Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente. o 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	La especificación de estos elementos se revisarán con el licitante ganador y deberán ser compatibles entre los equipos propuestos por el licitante y los equipos de la SCJN a los cuales sean conectados.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			equipo del servicio y del equipo a conectar para garantizar su correcta conectividad). Pregunta: ¿Es correcto entender que los transcievers o Gbics solicitados se podrán manejar como short range?	
48	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: o Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente. o 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). Pregunta: ¿Es correcto entender que los transcievers o Gbics solicitados se podrán manejar como short range?	La especificación de estos elementos se revisarán con el licitante ganador y deberán ser compatibles entre los equipos propuestos por el licitante y los equipos de la SCJN a los cuales sean conectados.
49	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: o Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente. o 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). Pregunta: ¿Podría la convocante aclarar si se pueden manejar como opcionales las interfaces de 40 Gbps?, ya que esas interfaces son consideradas para un throughput mucho mayor al de mínimo 5 Gbps de Threat Prevention solicitado.	No, las interfaces de 40 Gbps son obligatorias. La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput superiores conforme a las interfaces solicitadas de 40 Gbps.
50	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y	Dice: o Un Threat Prevention Throughput de 5 Gbps como	Se proporcionará al licitante ganador, sin embargo, se debe considerar el uso de todos

ARYABHOi44FgzfTb1zSSeNkfc0bsT80E24dDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		protección de amenazas avanzadas con base en comportamiento.	mínimo, con todas las funcionalidades habilitadas simultáneamente. o 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). Pregunta: ¿Podría la convocante indicar a cuantos equipos de red se requiere conectar cada equipo firewall?	los puertos con los que cuente el equipo propuesto.
51	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: o Un Threat Prevention Throughput de 5 Gbps como mínimo, con todas las funcionalidades habilitadas simultáneamente. o 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). Pregunta: Podría la convocante indicar, cuántas interfaces, de que tipo (F.O., Cobre RJ45, etc.) y a qué velocidad (1 gb, 10 gb, etc.) se tienen que considerar por cada equipo firewall en total. Favor de pronunciarse al respecto.	Se debe considerar al menos 6 interfaces de 10 Gbps en Fibra Optica
52	Anexo 2a Propuesta técnica	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	Dice: 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	Deberá dimensionarla conforme a su solución propuesta, considerando todos los equipos físicos a integrar.

ARYABHOi44ggzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			equipo o servidor que requiera para brindar los servicios de seguridad en alcance el presente proyecto. Pregunta: Podría la convocante indicar cuantas interfaces, de que tipo (F.O., Cobre RJ45, etc.) y a qué velocidad (1 gb, 10 gb, etc.) se tienen que considerar por cada equipo switch para equipos de la LAN propiedad de la SCJN que se interconectaran con los equipos de seguridad propuestos por el licitante ganador	
53	Anexo 2a Propuesta técnica	4.1.4 Servicio de protección para puntos finales (XDR)	Dice: 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. Pregunta: Con el objetivo de fomentar la libre participación se le solicita amablemente a al convocante manejar como opcional que la solución sea de la misma familia de solución del servicio de detección y protección de amenazas avanzadas, siempre y cuando pueda cubrir cabalmente con o solicitado en el apartado del servicio de protección para puntos finales (XDR)	No se acepta su propuesta.
54	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD). o Se deberá dimensionar para un aproximado de 20 servidores. Pregunta: Se le solicita amablemente a la convocante permitir el análisis de directorio activo mediante la recolección y análisis de información de los servidores de directorio activo ya	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			sea mediante el SIEM solicitado o las herramientas de XDR. Favor de pronunciarse al respecto	
55	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD). o Se deberá dimensionar para un aproximado de 20 servidores. Pregunta: ¿Podría especificar la convocante la cantidad de cuentas de directorio activo que se deben considerar?	Un auditor de AD se basa en el número de equipos servidores a incluir, no en cuentas, por lo que este dato no es relevante.
56	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: Solución de seguridad informática para análisis, alertamiento y reportes de eventos en directorios activos de la SCJN (MS Windows AD). o Se deberá dimensionar para un aproximado de 20 servidores. Pregunta: ¿Es correcto precisar que los 20 servidores indicados tienen funcionalidad de directorio activo?	Es correcta su apreciación.
57	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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). o 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. o 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.	Cada licitante, propondrá lo que considere más adecuado y eficaz para proporcionar el servicio conforme lo requerido en la licitación, pudiendo encontrase el servicio en nube pública o nube privada.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			o 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. Pregunta: Se le solicita amablemente a la convocante considerar como una opción para brindar este servicio, manejar dicho servicio mediante un SIEM en la nube privada del proveedor	
58	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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. Pregunta: ¿Es correcto precisar que monitoreo se requiere para las herramientas de seguridad que operará el licitante ganador?	Dicha herramienta se requiere para monitorear todos los componentes tecnológicos que sean puestos en operación por el licitante ganador.
59	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: Deberá realizar el monitoreo continuo del ciberespacio (Internet, Deep web y dark web) para detección de escenarios de riesgos para la SCJN, tales como: O Robo, fuga o hurto de información interna o de sus empleados de la SCJN. O Cuentas comprometidas de usuarios o de infraestructura de la SCJN. O Venta ilegal de información, accesos, cuentas o vulnerabilidades de infraestructura, que puedan poner en riesgo los activos informáticos de la SCJN. O Campañas de difamación o que afecte la reputación de la SCJN. O Campañas de odio que puedan poner en riesgo a personal de la SCJN. O Campañas de phishing, extorsión o fraude mediante correo electrónico, portales apócrifos o	Información relacionada con 20 usuarios de alto nivel que la SCJN determine, los demás parámetros de operación serán revisados con el licitante ganador.

ARYABHOi44FgzfTb1zSSeRk0077T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			cualquier medio electrónico, que suplanten la identidad de la SCJN. O 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. Pregunta: ¿Podría especificar la convocante la cantidad de usuarios, cuentas de correo, palabras clave que se deben monitorear en el internet, deep web y dark web?	
60	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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. Pregunta: ¿Podría especificar la convocante la cantidad de takedowns estimados anuales que se deben considerar?	Como referencia se puede considerar al menos 2 servicios anuales, sin embargo, esta cantidad al ser totalmente ajena de la SCJN no se puede determinar con exactitud.
61	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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: O Descubrimiento e identificación continua (escaneo automático) de todos los activos de la SCJN conectados a Internet. O Inventario actualizado de los activos informáticos detectados. O Gestión de la superficie de ataque a partir de los activos detectados y sus vulnerabilidades. O Análisis de los activos, puertos y vulnerabilidades detectados y expuestos a internet. Pregunta: ¿Podría especificar la convocante para este punto la cantidad de activos expuestos a internet que se deben analizar?	Se deben considerar al menos 2 segmentos de IP homologadas de mascara de 24.

ARYABHOi44FgzfTb1zSSeNKcb7AT901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
62	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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: O Descubrimiento e identificación continua (escaneo automático) de todos los activos de la SCJN conectados a Internet. O Inventario actualizado de los activos informáticos detectados. O Gestión de la superficie de ataque a partir de los activos detectados y sus vulnerabilidades. O Análisis de los activos, puertos y vulnerabilidades detectados y expuestos a internet. Pregunta: ¿Podría especificar la convocante para este punto la cantidad de dominios públicos que se deben analizar?	Al menos 20 dominios y sus subdominios.
63	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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: O Descubrimiento e identificación continua (escaneo automático) de todos los activos de la SCJN conectados a Internet. O Inventario actualizado de los activos informáticos detectados. O Gestión de la superficie de ataque a partir de los activos detectados y sus vulnerabilidades. O Análisis de los activos, puertos y vulnerabilidades detectados y expuestos a internet. Pregunta: ¿Podría especificar la convocante para este punto la cantidad de palabras clave que se deben analizar?	Los parámetros de operación se revisarán con el licitante ganador.
64	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo	Dice: Comprobación técnica • Ejecutar análisis de vulnerabilidades y pruebas de	Para términos de referencia, sin ser limitativos se consideran 90 sitios web.

ARYABHOi44FgzfTb1rSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Institucional de Gobierno de Seguridad de la Información - MIGSI	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. ¿Podría especificar la convocante la cantidad de objetivos (infraestructura critica de la convocante por ejemplo servidores) que se deben considerar en las pruebas de pentest tanto en caja negra como en caja gris?	
65	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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	Los parámetros de operación se revisarán con el licitante ganador.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			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. ¿Podría especificar la convocante la cantidad de pruebas de pentest por separado en caja negra y en caja gris que se deben realizar al año?	
66	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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. Pregunta: ¿Es correcto entender que el análisis de vulnerabilidades solicitado es el indicado en el apartado 4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC), el cual indica que se debe realizar análisis de vulnerabilidades para 500 servidores?	La solución de análisis de vulnerabilidades se debe dimensionar para 500 servidores, la cantidad de análisis que se ejecutará y los equipos a los cuales se aplicará dentro del servicio del Modelo de Gobierno se determinarán con el licitante ganador.
67	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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. ¿Podría especificar la convocante de este punto cuantos análisis al año se pueden llegar a requerir?	Los parámetros de operación se revisarán con el licitante ganador, siendo necesario que la solución de análisis de vulnerabilidades cuente con la capacidad para 500 servidores, y los análisis se puedan realizar conforme se reciban requerimientos de la DGTI.

ARYABHGJ44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
68	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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. ¿Podría especificar la convocante de este punto cuantos servidores o infraestructura se debe considerar por análisis?	Hasta 500 servidores
69	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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 Pregunta: ¿Podría especificar la convocante la cantidad de aplicaciones que se deben considerar en el análisis?	El prestador de servicios deberá realizar la detección de vulnerabilidades para el código fuente de los sistemas informáticos críticos identificados en la gestión de riesgos. Como referencia, sin ser limitativos, actualmente se tienen identificados 10 sistemas críticos candidatos a dicho análisis.
70	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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 Pregunta: ¿Podría especificar la convocante la cantidad de líneas de código estimada que se deben considerar por aplicación?	Como referencia, sin ser limitativos, ya que este valor puede variar en función de los cambios que tenga cada sistema, actualmente se han analizado en promedio 650 mil líneas de código por sistema. El mayor con 1,332,337 líneas de código y el menor con 147,773.
71	Anexo 2a Propuesta técnica	9. Lugar donde se prestará el servicio.	Dice: 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. Pregunta: ¿Podría especificar la convocante la cantidad de mantenimientos preventivos que se deben considerar al año?	Los que requieran las soluciones tecnológicas propuestas para garantizar el nivel de disponibilidad requerido.

ARYABHOi44FgzfTb1zSSeNkfobT0O2dSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
72	Anexo 2a Propuesta técnica	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC)	Dice: 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. Pregunta: Se le solicita amablemente a la convocante acepte como opcional en lugar de un acompañamiento directo del fabricante, que se pueda manejar la validación con personal especializado por parte del licitante ganador en cada tecnología	No se acepta su propuesta.
73	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.10 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). Pregunta: Se solicita a la convocante confirmar si es correcto entender que en caso de que sea el mismo fabricante el propuesto para más de una de las soluciones requeridas, se podrá presentar una carta indicando las soluciones que se presentarán de la misma marca.	Se acepta su propuesta, debiendo contar la carta con todos los requisitos solicitados en las bases de la licitación.
74	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE	Dice: 9.17 Deberá contar con personal certificado en cada una de las soluciones propuestas para cubrir los servicios de seguridad	Se debe presentar el certificado de su personal de acuerdo con las soluciones tecnológicas propuestas por el licitante, no

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		CERRADO NÚMERO 3)	informática del Anexo 2a, 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: • Protección para portales web. • Protección de correo electrónico • Detección y protección de amenazas avanzadas con base en comportamiento • Protección para puntos finales (XDR) Pregunta: En caso de que las certificaciones del fabricante a proponer no indiquen de forma expresa el concepto requerido por la convocante en su certificado, ¿acepta la convocante carta del fabricante que indique que la certificación emitida por el fabricante incluye los rubros requeridos por la convocante?	específicamente con el nombre particular de cada servicio en la presente licitación. Por ejemplo, para Detección y protección de amenazas avanzadas con base en comportamiento, se deberán presentar certificados de su personal en el uso de NGFW de su solución propuesta.
75	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.4 La persona licitante deberá entregar la descripción técnica del servicio que se oferte, en concordancia con lo requerido en el anexo técnico Anexo 2a. Pregunta: ¿Es correcto precisar que se requiere para este punto documentación donde se afirme que se esta cumpliendo con el Anexo 2a?	Se refiere a hacer una descripción conforme al anexo 2A emitida por el licitante, en la cual se señalen los elementos tecnológicos que ofertará.
76	BASES DE LA LICITACIÓN PÚBLICA NACIONAL	9. PROPUESTA TÉCNICA (SOBRE CERRADO NÚMERO 3)	Dice: 9.1 La persona licitante deberá integrar en su propuesta técnica información de los servicios solicitados, independientemente del formato de presentación de la propuesta técnica, deberá incluir un índice que indique claramente en donde inicia y termina cada uno de los requisitos establecidos en el Anexo 2a, para que la Suprema Corte de Justicia de la Nación los revise ordenadamente. Pregunta: Se le solicita amablemente a la convocante	No se acepta su propuesta.

AAY4BHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			aceptar un solo entregable para el punto 9.1 y 9.5 ya que lo que se solicita en ambos es muy similar	
77	ANEXO 3 FORMATO DE PROPUESTA ECONÓMICA (En papel membretado del participante)	a) Vigencia del servicio:	Dice: 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. Pregunta: ¿Es correcto precisar que los soportes y licenciamientos de las tecnologías consideradas por el licitante adjudicado se deberán considerar desde el proceso de implementación?	Queda a decisión del licitante adjudicado, conforme a su plan de trabajo para la implementación y puesta en operación de las soluciones tecnológicas.
78	ANEXO 3 FORMATO DE PROPUESTA ECONÓMICA (En papel membretado del participante)	a) Vigencia del servicio:	Dice: 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. Pregunta: En caso de que la pregunta anterior sea afirmativa, ¿Es correcto precisar que se requiere considerar el soporte y licenciamiento de las tecnologías propuestas por el licitante por 39 meses?	Queda a decisión del licitante adjudicado, conforme a su plan de trabajo para la implementación y puesta en operación de las soluciones tecnológicas.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2ddSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
79	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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). Pregunta: ¿Podría especificar la convocante si se cuenta con SGSI documentado en la versión 2013 u otra?	Se cuenta con documentación del SGSI conforme a la versión ISO/IEC 27001 versión 2013.
80	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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). Pregunta: ¿Podría especificar la convocante si se ha certificado en alguna ocación?	No se han realizados procedimientos de certificación en ISO 27001
81	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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).	No se han realizados procedimientos de certificación en ISO 27001

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: ¿Podría especificar la convocante si se ha certificado en alguna ocasión?	
82	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: 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 verEsión más reciente (mínimo 2022). Pregunta: ¿Podría la convocante enunciar el alcance contemplado dentro del SGSI en términos de ubicaciones físicas, sitios, centros de datos, áreas, procesos o servicios a incluir?	De manera enunciativa, más no limitativa, se tiene: edificios de la SCJN en la CDMX y sus correspondientes centros de datos, las áreas administrativas bajo la dirección de la Oficialía Mayor, los procesos y servicios se revisarán con el licitante ganador.
83	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio. Evaluación del estado actual y deseado Pregunta: Se solicita a la convocante indicar que actividades concretas se esperan durante el seguimiento del MIGSI a lo largo de los tres meses.	El detalle de las actividades se revisará con el licitante adjudicado.
84	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio. Evaluación del estado actual y deseado Pregunta: ¿Podría especificar la convocante si se requiere algún tipo de informe periódico o actualización durante este periodo de seguimiento al MIGSI?	El detalle de las actividades se revisará con el licitante adjudicado.
85	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio. Evaluación del estado actual y deseado Pregunta: ¿Podría especificar la convocante si existe alguna área particular dentro de estos estándares que consideren de mayor importancia o enfoque inicial para la evaluación?	El detalle de las actividades se revisará con el licitante adjudicado.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLkJC9=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
86	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio. Evaluación del estado actual y deseado. Pregunta: ¿Podría especificar la convocante que áreas específicas de la gobernanza de la seguridad informática consideran actualmente prioritarias para mejorar?	El detalle de las actividades se revisará con el licitante adjudicado.
87	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si hay requisitos específicos (Casos de uso) en cuanto a la funcionalidad que debería tener esta herramienta GRC para cumplir con las necesidades del MIGSI y SGSI?	No hay requisitos específicos, sin embargo, el licitante deberá considerar las necesidades establecidas en el servicio del MIGSI para el dimensionamiento y selección de la solución GRC más adecuada que cumpla con lo que requerido.
88	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: Podría especificar la convocante si existen preferencias o limitaciones tecnológicas para la selección e implementación de esta herramienta (Nube. On premise).	No hay requisitos específicos, sin embargo, el licitante deberá considerar las necesidades establecidas en el servicio del MIGSI para el dimensionamiento y selección de la solución GRC más adecuada que cumpla con lo que requerido. No se omite señalar que el licitante debe considerar e incluir en su propuesta técnica, todos los elementos tecnológicos para la adecuada operación de la herramienta GRC.

ARYABHOi44FgzfTb1zSSeNkc0971901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Favor de pronunciarse al respecto.	
89	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si hay requisitos específicos (Casos de uso) en cuanto a la funcionalidad que debería tener esta herramienta GRC para cumplir con las necesidades del MIGSI y SGSI?	No hay requisitos específicos, sin embargo, el licitante deberá considerar las necesidades establecidas en el servicio del MIGSI para el dimensionamiento y selección de la solución GRC más adecuada que cumpla con lo que requerido.
90	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante qué nivel se espera respecto a que la gestión de la herramienta sea compartida entre el prestador de servicios adjudicado y al menos 3 usuarios de la Dirección de Seguridad Informática?	Al ser un tema de operación, se revisará con el licitante ganador.
91	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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	Todo lo relacionado a la gestión del modelo de gobierno y del SGSI conforme al estándar de seguridad de la información ISO/IEC 27001-2022, cuyos detalles se validarán con el licitante adjudicado.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLkaCg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			que su uso y administración sea de manera compartida con al menos 3 usuarios de la DSI. Pregunta: ¿Podría especificar la convocante qué áreas de gestión de riesgos, cumplimiento normativo o controles internos desean cubrir con esta herramienta?	
92	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si la herramienta GRC deberá integrarse con sistemas o plataformas ya utilizadas en la organización?	No es requerido.
93	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si existe algún requerimiento particular de interoperabilidad con otras herramientas o sistemas dentro de la empresa?	No hay algún requerimiento particular de interoperabilidad.
94	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de	Dice: Componentes del servicio Mejora al modelo de gobierno El prestador de servicios adjudicado deberá	Al ser un tema de operación, se revisará con el licitante ganador.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Seguridad de la Información - MIGSI	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. Pregunta: ¿Podría especificar la convocante qué roles o niveles de acceso se necesitarán dentro de la herramienta para distintos tipos de usuarios?	
95	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si esperan poder personalizar o configurar la herramienta según las necesidades específicas de la organización?	Es correcta su apreciación.
96	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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.	Al ser un tema de operación, se revisará con el licitante ganador.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: ¿Podría especificar la convocante qué grado de flexibilidad desean tener en términos de adaptar la herramienta a sus procesos internos?	
97	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante qué tipo de informes y análisis desean obtener de esta herramienta GRC?	Al ser un tema de operación, se revisará con el licitante ganador.
98	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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. Pregunta: ¿Podría especificar la convocante si se requerirá capacitación para los usuarios de la herramienta?	Es correcta su apreciación.
99	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Mejora al modelo de gobierno 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	El mantenimiento y soporte necesario para que la herramienta cumpla con los niveles de disponibilidad (a nivel solución). Mantenimiento y soporte del contenido constante, mediante el personal de consultoría para actualizar la información que se vaya elaborando conforme el avance del SGSI para dar cumplimiento con los objetivos del servicio.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSL50Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			documentas y riesgos, considerando que su uso y administración sea de manera compartida con al menos 3 usuarios de la DSI. Pregunta: ¿Podría especificar la convocante qué tipo de soporte esperan recibir una vez implementada?	
100	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Actualización del Programa de Seguridad Informática: Pregunta: ¿Podría especificar la convocante qué áreas de la organización están actualmente involucradas con este programa?	Las Direcciones Generales a cargo de la Oficialía Mayor de la SCJN.
101	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Actualización del Programa de Seguridad Informática: Pregunta: ¿Podría especificar la convocante quiénes serán los principales actores involucrados en la gestión y ejecución de este programa?	Las Direcciones Generales a cargo de la Oficialía Mayor de la SCJN.
102	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Actualización del Programa de Seguridad Informática: Pregunta: ¿Podría especificar la convocante si tienen sistemas o herramientas que se deseen integrar o reforzar con este programa?	Al ser un tema de operación, se revisará con el licitante ganador.
103	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Actualización del Programa de Seguridad Informática: Pregunta: ¿Podría especificar la convocante cómo medirán el éxito o la efectividad de este programa de seguridad informática?	Al ser un tema de operación, se revisará con el licitante ganador.
104	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la	Dice: Componentes del servicio Operación del modelo de gobierno Actualización del Programa de Seguridad Informática:	Al ser un tema de operación, se revisará con el licitante ganador.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Información - MIGSI	Pregunta: ¿Podría especificar la convocante si existen regulaciones o estándares específicos que deben cumplirse con este programa de seguridad informática?	
105	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Ejecutar análisis inicial del riesgo actual: Pregunta: ¿Podría especificar la convocante cuántos ejercicios de análisis de riesgos anuales se llevarán a cabo?	Al menos una vez al año.
106	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Ejecutar análisis inicial del riesgo actual: Pregunta: ¿Podría especificar la convocante cuántas ubicaciones físicas deben de considerarse para la ejecución de los análisis de riesgos?	Hasta 5 edificios de la SCJN en la CDMX.
107	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Ejecutar análisis inicial del riesgo actual: Pregunta: ¿Podría especificar la convocante si los procesos se encuentran documentados, en ellos se pueden identificar los activos y a los dueños del proceso y activos?	Al ser un tema de operación, se revisará con el licitante ganador.
108	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Ejecutar análisis inicial del riesgo actual: Pregunta: ¿Podría especificar la convocante si los análisis de riegos se deberán registrar en GRC de esta propuesta?	Es correcta su apreciación.
109	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si el universo de 3500 usuarios es la cantidad que se debe considerar para una evaluación, o se puede considerar una muestra?	Se deberá considerar como referencia un máximo de 3500 personas a evaluar. Este número podrá variar y se precisará conforme a lo identificado durante la ejecución del servicio
110	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de	Dice: Componentes del servicio Operación del modelo de gobierno	Al ser un tema de operación, se revisará con el licitante ganador.

ARYABHOi44FgzfTb12SSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Gobierno de Seguridad de la Información - MIGSI	Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante qué temas específicos de seguridad informática desean abordar a través de esta plataforma?	
111	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si tiene un plan detallado de los contenidos que desean impartir o esperan desarrollar este plan en colaboración con el proveedor del servicio?	Al ser un tema de operación, se revisará con el licitante ganador.
112	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si la plataforma estará dirigida a todos los colaboradores o a grupos específicos?	A todos los usuarios de la SCJN
113	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante que funcionalidades específicas buscan en esta plataforma para la capacitación en seguridad informática?,	Todas las funcionalidades que provea una plataforma tipo LMS.
114	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual	Al ser un tema de operación, se revisará con el licitante ganador.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdD9LLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
			Pregunta: ¿Podría especificar la convocante cómo requiere medir la efectividad o el impacto de esta plataforma en la concientización en seguridad informática?	
115	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si se tienen métricas específicas para evaluar el éxito de esta implementación?	Al ser un tema de operación, se revisará con el licitante ganador.
116	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante cuál será la directriz que defina la convocante para la creación de contenido, gestión y mantenimiento continuo de la plataforma?	Al ser un tema de operación, se revisará con el licitante ganador.
117	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si necesita que la plataforma se integre con algún otro sistema o plataforma utilizada actualmente por la organización?	No se requiere integración.
118	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si se tiene alguna preferencia en cuanto al tipo de infraestructura (en la nube, local, híbrida) para alojar esta plataforma?	No hay requisitos específicos. No se omite señalar que el licitante debe considerar e incluir en su propuesta técnica, todos los elementos tecnológicos para la adecuada operación de la plataforma de concientización.

ARYABHOi44FgzfTb1zSSeNdc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
119	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante cuál es la cantidad estimada de usuarios concurrentes que la plataforma debe soportar?,	Se puede considerar una cantidad estimada de 30 usuarios concurrentes.
120	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si se espera un crecimiento significativo en el número de usuarios a lo largo del tiempo?	No se espera un crecimiento significativo de usuarios.
121	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si es necesario personalizar la interfaz de usuario y los contenidos dentro de la plataforma?,	Es correcta su apreciación.
122	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante qué formatos de contenido son necesarios considerar con la herramienta (videos, documentos, presentaciones, etc.)?	Documentos, presentaciones, cuestionarios, material interactivo y emisión de constancias.
123	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual	Es correcta su apreciación.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2dDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Información - MIGSI	Pregunta: ¿Podría especificar la convocante si la herramienta debe incluir capacidades de análisis y generación de informes sobre el progreso y desempeño de los usuarios?,	
124	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante qué tipo de métricas o análisis se deben considerar desde la plataforma?	Progreso y desempeño de los usuarios.
125	Anexo 2a Propuesta técnica	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	Dice: Componentes del servicio Operación del modelo de gobierno Incremento de la cultura organizacional de seguridad (concientización) Identificación del nivel actual Pregunta: ¿Podría especificar la convocante si se debe proporcionar capacitación para algún rol administrador administradores y usuarios finales sobre el uso efectivo de la herramienta?	No se requiere capacitación para algún rol de administrador o de usuarios finales, sin embargo, deberá considerar documentos guía para el uso de la herramienta.

7 PREGUNTAS DE LA EMPRESA: TIC DEFENSE, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	ANEXO 2ª PROPUESTA TÉCNICA	7.4.4 Personal requerido: Consultor Senior de Seguridad de la Información Comprobación: • Certificado vigente como Líder Implementador de ISO/IEC 27001	Con la finalidad de no limitar la participación de los LICITANTES se pide a la CONVOCANTE de la manera más atenta permitir cumplir con la comprobación del certificado de la certificación: Líder Implementador de ISO/IEC 27001 con la certificación: Líder Auditor Senior ISO/IEC 27001, derivado a que el perfil requiere un nivel más experto de conocimientos y el perfil de auditor senior cuenta con los conocimientos y competencias de toda la norma desde su implementación como de los controles auditados. ¿ACEPTA LA CONVOCANTE?	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSdNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
2	ANEXO 2ª PROPUESTA TÉCNICA	7.4.4 Personal requerido: Consultor Junior de Gestión de Seguridad de la información Comprobación: • Certificado vigente como Líder Implementador de ISO/IEC 27001	Con la finalidad de no limitar la participación de los LICITANTES se pide a la CONVOCANTE de la manera más atenta permitir cumplir con la comprobación del certificado de la certificación: Líder Implementador de ISO/IEC 27001 con la certificación: Líder Auditor ISO/IEC 27001, derivado a que el perfil requiere un nivel de conocimientos de toda la norma. ¿ACEPTA LA CONVOCANTE?	No se acepta su propuesta

8 PREGUNTAS DE LA EMPRESA: IQSEC, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	Anexos, Pagina 39	7.4.4 Personal requerido: Consultor Junior de Gestión de Seguridad de la información Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	Se solicita amablemente a la convocante aclare si es correcto entender que se cumple con el requisito de Especialidad en Seguridad de la Información o ciberseguridad presentando la certificación CISSP (Certified Information Systems Security Professional) la cual es una certificación internacional de alta especialidad en temas de Seguridad de la Información y Ciberseguridad ¿Se acepta nuestra propuesta?	Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
2	Anexos, Pagina 39	7.4.4 Personal requerido: Consultor Junior de Gestión de Seguridad de la información Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	Se solicita amablemente a la convocante si por Maestría en Seguridad de la Información o ciberseguridad se acepta la Maestría como Maestro en Ingeniería Eléctrica, Siempre y cuando se entregue el título y/o cedula profesional ¿Se acepta nuestra propuesta?	No se acepta su propuesta.
3	Anexos, Pagina 40	7.4.4 Personal requerido:	Se solicita amablemente a la convocante aclare si es	Puesto que la certificación referida corresponde a uno los requerimientos del

ARYABbO44Fg2fTb1zSSeNkf0b07T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Coordinador de Equipo de Respuesta a Incidentes. Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	correcto entender que se cumple con el requisito de Especialidad en Seguridad de la Información o ciberseguridad presentando la certificación Certified Incident Handling Engineer la cual es una certificación internacional de alta especialidad en temas de Seguridad de la Información y Ciberseguridad ¿Se acepta nuestra propuesta?	perfil, además de este, para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún **otro** certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc., es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
4	Anexos, Pagina 40	7.4.4 Personal requerido: Coordinador de Equipo de Respuesta a Incidentes. Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	Se solicita amablemente a la convocante acepte se presente solo Cédula o título profesional ¿Se acepta nuestra propuesta?	La cédula o título profesional se acepta para comprobar los estudios a nivel licenciatura en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines. Sin embargo, Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como CIH – EC Council Certified Incident Handler o MILE2 Certified incident Handling Engineer o ISO/IEC 27035 Lead Incident Manager, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso
5	Anexos, Pagina 40	7.4.4 Personal requerido: Especialista de Ciberinteligencia Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	Se solicita amablemente a la convocante aclare si es correcto entender que se cumple con el requisito de Especialidad en Seguridad de la Información o ciberseguridad presentando la certificación OSCP (Offsec Certified Professional) la cual es una certificación internacional de alta especialidad en temas de Seguridad de la Información y Ciberseguridad ¿Se acepta nuestra propuesta?	Puesto que la certificación referida corresponde a uno los requerimientos del perfil, además de este, para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún **otro** certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Certified in Information Systems Security Professional, Offensive Security Certified Professional, Offensive Security Web Expert, GREM GIAC

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
				Reverse Engineering Malware, etc. , es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso.
6	Anexos, Pagina 40	7.4.4 Personal requerido: Especialista de Ciberinteligencia. Contar con alguna de las siguientes: o Especialidad en Seguridad de la Información o ciberseguridad, o Maestría en Seguridad de la Información o ciberseguridad o Diplomado en Seguridad de la Información o ciberseguridad	Se solicita amablemente a la convocante acepte se presente solo Cédula o título profesional ¿Se acepta nuestra propuesta?	La cédula o título profesional se acepta para comprobar los estudios a nivel licenciatura en electrónica, informática, sistemas computacionales, tecnologías de la Información o carreras afines. Sin embargo, Para acreditar que el personal cuenta con estudios correspondientes en Seguridad de la Información o ciberseguridad, en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia, se podrá presentar algún certificado en materia de Seguridad de la Información o ciberseguridad emitido por organismo reconocido, tales como: Offensive Security Web Expert, GREM GIAC Reverse Engineering Malware, etc. Esto adicional e independiente al certificado vigente como GIAC Cyber Threat Intelligence o Offensive Security – OSCP, es decir, deberá presentar dos certificados para dicho perfil, si fuere el caso
7	Anexos, Pagina 36	7.2 Distribuidor autorizado/certificado. 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	Se solicita a la convocante acepte el título a nivel licenciatura en las áreas de comunicaciones, electrónica, informática o carrera a fin al menos para una de las 2 personas propuestas que cuenten con el mismo certificado ¿Se acepta la propuesta?	No se acepta su propuesta.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.		
8	Anexos, Pagina 36	7.2 Distribuidor autorizado/certificado. 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	Se solicita a la convocante acepte que las certificaciones puedan ser de nombres distintos entre 2 personas siempre y cuando sean de la solución propuesta considerando que el nombre de la certificación se actualizó por parte del fabricante ¿Se acepta la propuesta?	Mientras que sea demostrable que el certificado corresponde a la misma solución propuesta por el licitante y sea una certificación oficial por parte del fabricante, se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		del documento que lo acredite.		
9	Anexos, Pagina 36	7.2 Distribuidor autorizado/certificado. 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.	Se solicita a la convocante acepte que las certificaciones presentadas para protección para puntos finales (XDR) apliquen para comprobar la solución de detección y protección de amenazas avanzadas con base en comportamiento ¿Se acepta la propuesta?	Son soluciones diferentes, por lo que no se acepta su propuesta.
10	Anexos, Pagina 36	7.2 Distribuidor autorizado/certificado. 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	Se solicita a la convocante acepte al menos una persona con el certificado de la solución de detección y protección de amenazas avanzadas con base en comportamiento ¿Se acepta la propuesta?	No se acepta su propuesta.

ARYABHOi44FgzfTb1zSSeNfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.		
11	Anexos, Pagina 26	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	Se solicita amablemente a la convocante aclarar si ¿Se deberán considerar crecimientos en casos de uso, además de gestión de procesos y documental y riesgos?	Es viable considerar posibles crecimientos en casos de uso, además de gestión de procesos y documental y riesgos, conforme al avance y resultados del propio servicio.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.		
12	Anexos, Pagina 26	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.	Se solicita amablemente a la convocante aclarar si ¿Se deberán considerar crecimientos en el número de usuarios de la plataforma?	Se deberá considerar un posible crecimiento a un máximo de 5 usuarios de la DSI.
13	Anexos, Pagina 26	Mejora al modelo de gobierno Optimización del modelo de gobierno: El prestador de servicios adjudicado deberá proponer mejoras al MIGSI	Se solicita amablemente a la convocante aclarar si ¿Se deberán considerar servicios de implementación y configuración de la	El licitante deberá considerar e incluir en su propuesta técnica, todos los elementos necesarios para la adecuada operación y uso de la herramienta GRC.

ARYABHDi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.	herramienta como parte del servicio?	
14	Anexos, Pagina 26	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	Se solicita amablemente a la convocante si es correcto entender que designará personal para administrar la herramienta de GRC ¿Es correcto nuestra apreciación?	El licitante deberá considerar e incluir en su propuesta técnica, todos los elementos necesarios para la adecuada operación y uso de la herramienta GRC, incluyendo la administración, la cual será de manera compartida con al menos 3 usuarios de la DSI.

ARYABHDi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.		
15	Anexos, Pagina 10	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:	Se solicita a la convocante confirmar si ¿Todos los portales web son públicos o se consideran portales internos?	Para este servicio todos los portales son públicos y expuestos en internet.
16	Anexos, Pagina 11	4.1.1. Servicio de protección para portales web. Generales: El módulo de WAF deberá considerar los necesario para gestionar hasta 90 portales o dominios web	Se solicita a la convocante indicar ¿Cuál es el tráfico de los portales o dominios web?	512 Mbps (ancho de banda del enlace internet de los portales web de la SCJN).
17	Anexos, Pagina 11	4.1.1. Servicio de protección para portales web. Generales: El módulo de WAF deberá considerar los necesario para gestionar hasta 90 portales o dominios web	Se solicita a la convocante aclarar si se consideran 90 dominios o subdominios o ¿Cuántos son dominios y Cuantos subdominios?	Para esta solución se consideran portales web publicados, por lo que se proporciona el número de portales a proteger que son 90.
18	Anexos, Pagina 11	4.1.1. Servicio de protección para portales 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.	Se solicita a la convocante aclarar si es correcto entender que se requieren 2 certificados del tipo EV para 90 dominios y/o subdominios con una vigencia de 12 meses y este puede ser renovado por hasta 86 o 94 dominios y/o subdominios para el siguiente año ¿Es correcta la apreciación?	Como referencia, se tiene en operación 2 certificados EV (Extended Validation) con 10 SAN, pudiendo incrementarse las SAN de acuerdo con el anexo técnico.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JSDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		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.		
19	Anexos, Pagina 11	4.1.1. Servicio de protección para portales 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 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.	Se solicita a la convocante aclarar si es correcto entender que se requieren 2 certificados del tipo OV para 90 dominios y/o subdominios con una vigencia de 12 meses y este puede ser renovado por hasta 86 o 94 dominios y/o subdominios para el siguiente año ¿Es correcta la apreciación?	Como referencia, se tiene en operación 2 certificados OV (Organization Validation) con 10 SAN, pudiendo incrementarse las SAN de acuerdo con el anexo técnico.
20	Anexos, Pagina 11	4.1.1. Servicio de protección para portales 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 solicita a la convocante aclarar si es correcto entender que se requieren 2 certificados del tipo Wildcard para 90 dominios y/o subdominios con una vigencia de 12 meses y este puede ser renovado por hasta 86 o 94 dominios y/o subdominios para el siguiente año ¿Es correcta la apreciación?	Como referencia, se tiene en operación 2 certificados WildCard con 10 SAN, pudiendo incrementarse las SAN de acuerdo con el anexo técnico.

ARYABHOi44FgfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		Se deberá considerar certificados SSL de tipo EV (Extended Validation), OV (Organization Validation) y WildCard. 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.		
21	Anexos, Pagina 12 y 13	4.1.2 Servicio de protección para correo electrónico. Generales: 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). Se deberá considerar lo necesario para gestionar al menos un mínimo de 3,600 cuentas de correo electrónico.	Se solicita a la convocante aclarar con el fin de estar en igualdad de condiciones si para efectos de evaluación se deben considerar 4000 buzones o 3600. ¿Cuál es la cantidad correcta a considerar?	Se debe considerar el máximo de 4000 buzones.
22	Anexos, Pagina 14	4.1.2 Servicio de protección para correo electrónico. 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:	Se solicita a la convocante indicar ¿Qué tipo de certificado TLS se requiere OV o EV?	OV
23	Anexos, Pagina 16	4.1.3 Servicio de detección y protección de amenazas avanzadas con base en comportamiento. Equipos switches: Se deberá proporcionar equipos switches en alta disponibilidad (dos) para al	Se solicita a la convocante indicar ¿Cuántos puertos y de que tipo serán considerados para la interconexión con la infraestructura LAN de la SCJN?	1 puerto en cada switch, pudiendo ser cobre o fibra a 1 Gbps.

ARYABHOi44FgzfTb12SeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		menos 2 sitios de la SCJN dentro de la CDMX, los cuales se interconectará con la infraestructura LAN de la SCJN		
24	Anexos, Pagina 19	4.1.4 Servicio de protección para puntos finales (XDR) Actividades de migración: o 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.	Se solicita a la convocante indicar ¿Cuál es la solución de XDR actualmente operando en los equipos de cómputo y de servidores de la SCJN?	Información no relevante para el proceso.
25	Anexos, Pagina 21	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 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).	Es correcto entender que deberá atender la falla en un plazo no mayor a 4 horas, en caso de sobrepasar más de 4 horas deberá enviar personal especializado a sitio y escalar con el fabricante ¿Es correcta la apreciación?	La solución de la falla deberá ser en un plazo no mayor a 4 horas, realizando todas las acciones necesarias para lograr la resolución de la misma. En caso de no dar solución en este periodo se aplicarán los SLA correspondientes, y de manera obligatoria se requiere el escalamiento de la incidencia con el fabricante y personal especializado en sitio del licitante adjudicado en las oficinas de la SCJN donde se presente la incidencia.
26	Anexos, Pagina 22	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 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	Se solicita a la convocante considerar un tiempo de atención no mayor a 4 horas considerando que la solución para un evento puede variar dependiendo de este ¿Se acepta la propuesta?	No se acepta su propuesta

ARYABHOid4EgzfTb1Z8SeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		a partir de la hora en la que se presentó el evento.		
27	Anexos, Pagina 24	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) MONITOREO DE AMENAZAS EXTERNAS, CIBERINTELIGENCIA: 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:	Se solicita a la convocante indicar ¿Cuál es el número de activos de la SCJN expuesto a internet que requiere sean monitoreados?	Se deben considerar al menos 2 segmentos de IP homologadas de mascara de 24.
28	Anexos, Pagina 20 y 27	4.1.5 Servicio de Centro de Operaciones de Ciberseguridad (COC) 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. 4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI Comprobación técnica 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,	Es correcto entender que se debe considerar un análisis de vulnerabilidades anual para 500 servidores para la comprobación técnica del servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información – MIGSI. ¿Es correcta la apreciación?	La solución de análisis de vulnerabilidades se debe dimensionar para 500 servidores, la cantidad de análisis que se ejecutará y los equipos a los cuales se aplicará dentro del servicio del Modelo de Gobierno se determinarán con el licitante ganador

AFIABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		contención o mitigación) correspondientes.		
29	Anexos, Pagina 28	4.1.6 Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI Comprobación técnica 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.	Se solicita a la convocante indicar para ¿cuántas aplicaciones y de cuantas líneas de código por aplicación se considera el análisis de código estático?	Como referencia, sin ser limitativos, ya que este valor puede variar en función de los cambios que tenga cada sistema, actualmente se han analizado en promedio 650 mil líneas de código por sistema. El mayor con 1,332,337 líneas de código y el menor con 147,773. Hasta un máximo de 10 aplicaciones.
30	Anexos, Pagina 30	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:	Se solicita a la convocante aceptar los entregables como máximo en los primeros 10 días hábiles ¿Se acepta la propuesta?	No se acepta su propuesta.
31	Anexos, Pagina 32	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":	Se solicita a la convocante aceptar los entregables como máximo en los primeros 10 días hábiles ¿Se acepta la propuesta?	No se acepta su propuesta.
32	Anexos, Pagina 36	7.1 Requisitos técnicos de las soluciones propuestas. Para su acreditación de cada solución, se deberá proveer de una copia de la metodología de investigación correspondiente	Se solicita a la convocante especificar ¿a qué metodología de investigación se refiere?	las metodologías de investigación son las del Gartner Magic Quadrant y Forrester Wave de acuerdo con cada solución propuesta.
33	Anexos, Pagina 12	4.1.2 Servicio de protección para correo electrónico	Se sugiere a la convocante solicitar que la solución	No se acepta.

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLkC0g=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		El servicio deberá garantizar una disponibilidad del 99.99% mensual.	ofertada garantice la disponibilidad del 99.999% dado que se trata de un servicio por donde se reciben el 90% de los ataques hoy día. ¿Se acepta nuestra sugerencia?	
34	Anexos, Pagina 14	e) Protección por identificación de contenido. Creación de reglas que establezcan que palabras o frases no están permitidas en ningún mensaje o adjunto.	Se sugiere a la convocante permitir esta funcionalidad o la detención de ataques de compromiso tipo BEC para evitar la usurpación de la identidad o robo de información a través de mensajes con técnicas de ataque social. ¿Se acepta nuestra sugerencia?	El licitante podrá proponer su esquema de operación que requiera su solución propuesta, siempre y cuando cumpla con lo solicitado en bases.
35	Anexos, Pagina 14	e) Protección por identificación de contenido.	Se sugiere a la convocante solicitar que la solución ofertada incluya un PRA (Phishing Risk Assessment) para medir la susceptibilidad que los usuarios sean comprometidos con ataques de phishing y proactivamente concientizar y educar a los usuarios a no ser víctimas de correos con contenido malicioso. ¿Se acepta nuestra sugerencia siempre y cuando no se incurra en un costo adicional hacia la convocante?	No se acepta su propuesta, sin embargo, el licitante puede integrar lo que crea conveniente para garantizar la correcta prestación del servicio, siempre y cuando cumpla con lo solicitado en bases.
36	BASES DE LA LICITACIÓN PÚBLICA NACIONAL Página 8	9.2 La persona licitante deberá entregar su propuesta técnica en idioma español, en papelería membretada de la persona participante, foliadas, firmadas en todas sus hojas por la persona licitante o quien funja como representante legal, no deberán contener tachaduras o enmendaduras, con la descripción detallada de los servicios, conforme al Anexo 2a.	Solicitamos amablemente a la Convocante permita que la propuesta pueda presentarse firmada por la persona licitante o quien funja como representante legal únicamente en la última hoja y con rubrica en el resto de las hojas que forma parte de la propuesta. ¿Se acepta nuestra propuesta?	No se acepta su propuesta, deberá presentarse la propuesta firmada en todas sus hojas.
37	BASES DE LA LICITACIÓN PÚBLICA NACIONAL Página 6	6.2.2 Estados Financieros parciales correspondientes al ejercicio en que se está llevando a cabo el procedimiento de contratación, que deberán incluir, cuando menos, el balance general y el estado	Solicitamos amablemente a la convocante confirme que es correcto entender que por *“Estados Financieros parciales correspondientes al ejercicio en que se está llevando a cabo el procedimiento de contratación”,* se refieren a los	Es correcto su entendimiento

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
		de resultados con una antigüedad no mayor de dos meses anteriores a la fecha en que se publicó la convocatoria, debiendo estar firmados por contador público, quien acreditará su calidad con copia fotostática de su cédula profesional o impresión de ésta, en caso de haberse obtenido por medios electrónicos.	Estados Financieros del mes de octubre de 2023 y que bastará con incluirlos en nuestra propuesta para dar cumplimiento a dicho requisito. ¿Es correcto nuestro entendimiento?	

9 PREGUNTAS DE LA EMPRESA: ARTERIA COMUNICACIÓN, S.A. DE C.V.

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
1	Servicio de centro de operaciones de ciberseguridad	4.1.5	¿Es necesario y obligatorio contar con la certificación GIAC Cyber Threat Intelligence, Offensive Security – OSCP o equivalente Y la ECIH – EC Council Certified Incident Handler, MILE2 Certified incident Handling Engineer, ISO/IEC 27035 Lead Incident Manager o equivalente?	El licitante deberá demostrar que cuenta con el personal solicitado por la SCJN en el Anexo 2A, conforme a cada perfil, considerando las precisiones que resulten de la junta de aclaraciones.
2	Servicio de centro de operaciones de ciberseguridad	4.1.5	¿Es necesario y obligatorio contar con la certificación ISO20000 para prestar el servicio?	Es obligatorio contar con la certificación ISO/IEC 20000-1 (Sistema de Gestión de Servicios), versión 2018 o superior
3	Servicio de centro de operaciones de ciberseguridad	4.1.5	¿Es necesario y obligatorio contar con la certificación ISO/IEC 9000 (control y gestión de la calidad), para prestar el servicio?	Es obligatorio contar con la certificación ISO/IEC 9001 (Sistema de Gestión de Calidad), versión 2015 o superior
4	Servicio de protección para puntos finales (XDR)	4.1.4	¿Qué solución de XDR se tiene actualmente?	Información no relevante para el proceso
5	Servicio de detección y protección de amenazas avanzadas con base en comportamiento	4.1.3	¿Qué cantidad de usuarios y ancho de banda, se cuenta en cada sitio donde se instalara el equipo NGFW ?	Información no relevante para el proceso, se deberá dimensionar su solución conforme a los puertos y troughtput mínimo solicitado
6	Servicio de detección y protección de amenazas avanzadas con base en comportamiento	4.1.3	¿Qué cantidad de usuarios se considera para acceso VPN	Para el Servicio de detección y protección de amenazas avanzadas con base en comportamiento no se solicita la funcionalidad de VPN
7	Servicio de detección y protección de amenazas avanzadas	4.1.3	¿Se considera activar MFA?	Se revisará la viabilidad de implementar esta característica con el licitante adjudicado.

4RYABHOi4FgzfTb1zSSelkc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	con base en comportamiento			
8	Monitoreo de portales	4.1.1	¿Cuál es la cantidad de portales web a monitorear?	Hasta 90 portales.
9	Servicio de actualización y mejora del Modelo Institucional de Gobierno de Seguridad de la Información - MIGSI	4.1.6	¿Qué cantidad de aplicaciones se consideran en el análisis de código estático?	Cómo referencia, sin ser limitativos, se pueden considerar un máximo de 10 aplicaciones para análisis de código estático.
10	Servicio de protección para correo electrónico	4.1.2	**Dice**: Certificado SSL TLS: **Pregunta**: ¿La convocante acepta que una solución que se integra mediante API a través de un canal seguro mediante TLS no requiera un certificado TLS adicional?.	No se acepta la propuesta
11	Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	4.1.3	**Dice**: 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). **Pregunta**: ¿La convocante considera que la solución propuesta debe tener módulos intercambiables para agregar, cambiar o intercambiar módulos de tarjetas para alcanzar la cantidad de puertos requeridos? SI, es correcto, no se requieren puertos 10/100/100 GE	No se acepta la propuesta.
12	Servicio de protección para puntos finales (XDR)	4.1.4	**Pregunta**: ¿La convocante requiere que la función de XDR se aplique a todos los servicios del fabricante, incluyendo el servicio de protección para puntos finales, servicio de detección y protección de amenazas avanzadas, servicio de protección de correo electrónico?, si es correcto, ¿acepta la convocante que estos 3 servicios sean del mismo fabricante?	El licitante podrá determinar las soluciones más adecuadas para cumplir con los servicios requeridos en la presente licitación. Señalando que 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 y que cada servicio debe cumplir con el nivel requerido de la metodología de investigación por solución correspondiente.
13	Servicio de detección y protección de amenazas avanzadas	4.1.3	¿La convocante requiere que los equipos tengan la capacidad de manejar un	La velocidad de troughtput de 5 Gbps es solo una referencia mínima, el equipo propuesto podrá considerar velocidades de troughtput

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

No	Concepto de Bases o Anexo	Numeral	Pregunta	Respuesta
	con base en comportamiento.		tráfico de al menos 10 Gbps con todas las funciones de prevención de amenazas encendidas? Si la respuesta es afirmativa, ¿la convocante acepta que la solución pueda aumentar su rendimiento agregando un componente, como memoria?	superiores conforme a las interfaces solicitadas de 40 Gbps. El licitante podrá determinar la configuración más adecuada para los equipos propuestos para cubrir lo requerido en el Servicio de detección y protección de amenazas avanzadas con base en comportamiento, siempre y cuando cumpla con lo requerido en la presente licitación.
14	Servicio de detección y protección de amenazas avanzadas con base en comportamiento.	4.1.3	**Dice**: 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". **Pregunta**: ¿La convocante considera que los 15 años de experiencia en el mercado son un requisito indispensable para la solución?	Es obligatorio que 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".
15	Servicio de protección para puntos finales (XDR)	4.1.4	**Pregunta**: ¿La convocante requiere que una solución que proteja al punto final y que no haya presentado vulnerabilidades altas en el último año sea considerada para esta convocatoria?	El licitante podrá determinar las soluciones más adecuadas para cumplir con los servicios requeridos en la presente licitación. Señalando que 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 y que cada servicio debe cumplir con el nivel requerido de la metodología de investigación por solución correspondiente.

Siendo las quince horas con treinta minutos se abre un receso de treinta minutos a efecto de revisar las repreguntas remitidas por las empresas participantes.

Siendo las dieciséis horas se continua la presente, por lo que se señala:

De conformidad con el numeral 5.3 de las bases del procedimiento Junta de Aclaraciones:

5.3.5 En la junta de aclaraciones se atenderán las preguntas recibidas en el plazo establecido y se permitirá formular, de manera verbal, preguntas relacionadas con las respuestas producidas, de las cuales se dará respuesta a aquellas que se califiquen como procedentes por quien represente a la Dirección General de Recursos Materiales con base en su naturaleza y la opinión del área correspondiente.

5.3.6 Excepcionalmente podrán responderse nuevas preguntas, cuando lo determine conveniente la persona representante de la Suprema Corte de Justicia de la Nación que corresponda, conforme a la naturaleza de las preguntas.

Se responden las siguientes preguntas:

Totalsec S.A. de C.V (Invitado)

Pregunta 31, del licitante Bdrive, respecto a los switches requeridos, toda vez que los equipos switches tendrán el propósito específico de conexión física de los equipos NGFW, se solicita amablemente a la convocante que se acepte que la capa 3 se gestione en los equipos NGFW o se permita que el licitante adjudicado plantee la arquitectura definida de conexión, siempre y cuando se describan detalladamente los componentes solicitados y estos cumplan con lo requerido en el anexo técnico.

Respuesta: El tipo de switches será determinado por el licitante de acuerdo con su arquitectura propuesta para la solución, cumpliendo con lo requerido en la licitación.

LICITANTE IQSEC SA DE CV

Respecto a la pregunta 13 del licitante Scitum: se solicita amablemente a la convocante aceptar la certificación OSWP OffSec Wireless Professional ¿Se acepta nuestra Propuesta?

Respuesta: Si se acepta para comprobar estudios en seguridad de la información o ciberseguridad en caso de no contar con documento que avale estudios de Especialidad o Maestría o Diplomado en la materia. Esto adicional e independiente al certificado vigente como Líder Implementador de ISO/IEC 27001 solicitado, reiterando, que deberá presentar dos certificados para el perfil de consultor senior de seguridad de la información, si fuere el caso.

Se solicita a la Convocante compartir el acta de junta de aclaraciones en formato editable para facilitar su consideración en la propuesta técnica ¿Se acepta nuestra propuesta?
Respuesta: No se acepta la propuesta.

Respecto a la respuesta 3 de IQSEC.
Se solicita amablemente a la convocante aclare si es posible cubrir el perfil considerando 2 recursos siempre y cuando se cumple con lo requerido ¿Se acepta la propuesta?.

Respuesta: No se acepta su propuesta.

Respecto a la respuesta 5 de IQSEC.
Se solicita amablemente a la convocante aclare si es posible cubrir el perfil considerando 2 recursos siempre y cuando se cumple con lo requerido ¿Se acepta la propuesta?

Respuesta: No se acepta su propuesta.

Respecto a la respuesta 10 de IQSEC.
Se solicita a la convocante que en caso de no contar con certificado se pueda avalar con carta del fabricante ¿Se acepta la propuesta?

Respuesta: No se acepta su propuesta.

Respecto a la respuesta 24 de IQSEC.
Se solicita a la convocante indicar si se apoyará en la desinstalación de la solución de XDR actual, en caso contrario se requiere conocer ¿Cuál es la solución de XDR a desinstalar?

Respuesta: la licitante apoyara en el proceso de desinstalación de la solución XDR actual.
Respuesta a la pregunta número 32 del Licitante silent4bussines;

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

Se solicita amablemente a la Convocante confirme que el Poder del representante legal en caso de no estar dentro del Acta Constitutiva de la persona moral, podrá estar o no inscrito en el RPPyC, toda vez que de conformidad con lo establecido en los Artículos 3071 del Código Civil para el Distrito Federal y 110 del Reglamento de la Ley Registral para la Ciudad de México y Articulo 42 Párrafo Tercero Fracción I de la Ley Registral para la Ciudad de México; Artículo 110 del Reglamento de la Ley Registral, no es materia de inscripción en la sección de personas morales, toda vez que no se encuentra dentro de los actos inscribibles.

Respuesta: Si el poder del representante legal no se encuentra en el acta constitutiva o algún otro documento que deba ser inscribible por disposición de ley, no será objeto de verificación.

SCITUM REPREGUNTAS
Repregunta No.10. DE SOLUCIONES INTEGRALES Y INOVACIÓN SUSTENTABLE

Se le solicita a la convocante aclarar si es correcto entender que el acompañamiento y validación del fabricante es solo durante la fase de puesta de la operación, ya que asi viene indicado en el anexo, y por lo tanto no es un servicio continuo. Favor de pronunciarse al respecto

Respuesta: El licitante adjudicado deberá considerar que a través de su Centro de Operaciones de Ciberseguridad realizará una revisión técnica al menos cada 6 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.

Repregunta No.20 de Scitum
Se le solicita a la convocante indicar si este ancho de banda de 512 Mbps es exclusivo para la publicación de sitios web o es un enlace de internet compartido para la navegación web de usuarios internos. Favor de pronunciarse al respecto.

Respuesta: Es exclusivo de los portales web de la SCJN.

REPREGUNTA 32 IQSEC.
¿Es correcto entender que estas metodologías de investigación como Gartner y Forrester deberán ser las mas recientemente publicadas por el organismo que avala dichas metodologías?

Respuesta: Es correcta su apreciación.

REPREGUNTA 30 DE SCITUM

¿PODRIA ESPECIFICAR SI LOS CERTIFICADOS ACTUALES OV Y EV SON MULTIDOMINIO?
Respuesta: Si son multidominio.

REPREGUNTA 31 DE SCITUM

¿PODRIA ESPECIFICAR LA CONVOCANTE SI ESL CERTIFICADO REQUERIDO OV PARA EL CORREO, SE REQUERIRA QUE SEA MULTIDOMINIO Y CUANTAS SANS SE REQUIEREN CONSIDERAR?

Respuesta: Es certificado multidominio y se pueden considerar hasta 10 SAN

Repregunta 54 SCITUM

Se le solicita amablemente a la convocante indicar si para cubrir este punto "Solución de seguridad informática para análisis, alertamiento, y reportes de eventos en directorios activos de la SCJN" será necesario emplear una herramienta dedicada para la seguridad y exposición del directorio activo, tales como, Tenable AD, Semperis, SentinelOne, entre otros. Favor de pronunciarse al respecto

Respuesta: para este cubrir este rubro se deberá utilizar una herramienta dedicada para la seguridad y exposición del directorio activo

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

Repregunta 54 SCITUM

¿Podria especificar la convocante si actualmente cuenta con una herramienta dedicada para el analisis de directorio activo?

Respuesta: No se cuenta con una herramienta.

Pregunta 34 de Silent 4 Business. Solicitamos a la convocante sea tan amable de considerar el siguiente supuesto; derivado de que mi arrendataria, por fusión ha adquirido la titularidad del inmueble que legalmente ocupamos, la gestión del traslativo de dominio no ha quedado registrada a la fecha, por lo que las constancias de contribuciones continúan apareciendo a nombre del titular registral anterior, solicitamos a la convocante que, para acreditar lo solicitado en el numeral 6.1.3 Comprobante de domicilio legal, tenga a bien aceptar el contrato de arrendamiento y el comprobante de domicilio a nombre del anterior titular registral.

Respuesta: Para acreditar el numeral 6.1.3 el comprobante de domicilio deberá tener una vigencia no mayor a 6 meses y, en el caso específico, deberá existir plan coincidencia del domicilio y del nombre que aparece en el comprobante presentado, con los nombres que aparecen en el contrato de arrendamiento (mismo que deberá encontrarse vigente).

La convocante realiza las siguientes modificaciones a las bases y sus anexos, con fundamento en el artículo 63, primer párrafo, del Acuerdo General de Administración XIV/2019

Bases, 3 Calendario de eventos:

Dice:

Eventos	Fecha	Horario
Sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas	5 de diciembre de 2023	11:00 hrs
Sesión pública de fallo	21 de diciembre de 2023	11:00 hrs.

Debe decir:

Eventos	Fecha	Horario
Sesión pública de entrega de documentación legal y financiera, presentación y apertura de propuestas técnicas y económicas	5 de diciembre de 2023	10:00 hrs
Sesión pública de fallo	21 de diciembre de 2023	12:00 hrs.

CIERRE DE ACTA

Siendo las dieciseis horas con treinta minutos del día de la fecha y no habiendo más que agregar, se da por concluida la presente junta de aclaraciones y previa lectura de la presente, firman los servidores públicos que participaron, para los efectos procedentes. -CONSTE

Servidor Público	RFC
L.C. Antonio Prieto Revilla	PIRA690926
Lic. Miguel Àngel Esquinca Vila	EUVM740615
Lic. Adriana Hernandez López	HELA770925
Mtra. Amelia Karina Armenta Romero	AERA621015

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2ddDSLk0Cg=

C.P. Verónica Marcela López López	LOLV810902
Mtro Omar Salinas García	SAGO741211
Lic. Pedro Eduardo Garcìa Vàzquez	GAVP930531987

Forman parte del acta, las listas de asistencia de participantes emitidas por la plataforma Microsoft Teams como Anexo 1 y el reporte AntiSpam emitido por la Dirección General de Tecnologías de la Información de los correos recibidos el 23 de noviembre de 2023 en el horario establecido, como Anexo 2.

Se enviará copia del acta

EMPRESAS	Correo electrónico
B DRIVE IT, S.A. de C.V.	mlopez@b-drive.com.mx
Totalsec, S.A. de C.V.	dulce.ortega@totalcybersec.com
Silent4Business, S.A. de C.V.	gerardo.garibay@silent4business.com
Soluciones Integrales e Innovación Tecnológica Sustentable, S.A. de C.V.	jrenato.melendez@siitecs.mx
Scitum, S.A. de C.V.	jose.tellez@scitum.com.mx abigail.hernandez@scitum.com.mx
IQSEC, S.A. de C.V.	juan.ramirez@iqsec.com.mx; fabian.sanchez@iqsec.com.mx
Arteria Comunicaciones, S.A. de C.V.	daniel.estrada@arteria.com.mx

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

Anexo 1

Lista de asistencia de participantes emitida por la plataforma Microsoft Teams

Nombre completo	Acción del usuario	Marca de tiempo
ADRIANA HERNANDEZ LOPEZ	Unido	28/11/2023, 10:44:51
ADRIANA HERNANDEZ LOPEZ	Abandonó	28/11/2023, 10:45:33
ADRIANA HERNANDEZ LOPEZ	Unido	28/11/2023, 10:53:08
Juan Ramírez	Se unió antes	28/11/2023, 10:44:51
Juan Ramírez	Abandonó	28/11/2023, 15:28:53
Diana Abigail Hernández De La Cruz	Se unió antes	28/11/2023, 10:53:08
Diana Abigail Hernández De La Cruz	Abandonó	28/11/2023, 15:28:04
María Fernanda Hernández Pintado	Se unió antes	28/11/2023, 10:53:08
María Fernanda Hernández Pintado	Abandonó	28/11/2023, 11:07:45
PEDRO EDUARDO GARCIA VAZQUEZ	Se unió antes	28/11/2023, 10:53:08
PEDRO EDUARDO GARCIA VAZQUEZ	Abandonó	28/11/2023, 14:41:54
PEDRO EDUARDO GARCIA VAZQUEZ	Unido	28/11/2023, 14:42:27
PEDRO EDUARDO GARCIA VAZQUEZ	Abandonó	28/11/2023, 14:43:39
PEDRO EDUARDO GARCIA VAZQUEZ	Unido	28/11/2023, 14:48:03
AMELIA KARINA ARMENTA ROMERO	Se unió antes	28/11/2023, 10:53:08
Gerardo Garibay Aymes	Se unió antes	28/11/2023, 10:53:08
Gerardo Garibay Aymes	Abandonó	28/11/2023, 10:56:51
Gerardo Garibay Aymes	Unido	28/11/2023, 10:57:04
Gerardo Garibay Aymes	Abandonó	28/11/2023, 15:28:16
RAMON CABALLERO LEDESMA	Se unió antes	28/11/2023, 10:53:08
VERONICA MARCELA LOPEZ LOPEZ	Se unió antes	28/11/2023, 10:53:08
VERONICA MARCELA LOPEZ LOPEZ	Abandonó	28/11/2023, 14:59:04
VERONICA MARCELA LOPEZ LOPEZ	Unido	28/11/2023, 14:59:07
Omar Salinas García	Se unió antes	28/11/2023, 10:53:08
Daniel Estrada	Se unió antes	28/11/2023, 10:53:08
Daniel Estrada	Abandonó	28/11/2023, 10:59:59
Daniel Estrada	Unido	28/11/2023, 11:00:08
Daniel Estrada	Abandonó	28/11/2023, 15:28:33
JOSE EDUARDO GIRON CAMACHO	Se unió antes	28/11/2023, 10:53:08
MIGUEL ANGEL ESQUINCA VILA	Se unió antes	28/11/2023, 10:53:08
Totalsec S.A. de C.V (Invitado)	Se unió antes	28/11/2023, 10:53:08
Totalsec S.A. de C.V (Invitado)	Abandonó	28/11/2023, 15:29:05
Totalsec S.A. de C.V (Invitado)	Unido	28/11/2023, 15:38:48
Totalsec S.A. de C.V (Invitado)	Abandonó	28/11/2023, 15:38:54
JOSE RENATO MELENDEZ (SIITECS) (Ir	Se unió antes	28/11/2023, 10:53:08
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 10:57:39
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 10:58:00
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 11:01:44
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 11:04:26
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 13:31:25
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 13:34:25
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 14:38:33
Alfredo Ramírez Olivera	Unido	28/11/2023, 10:53:13
Alfredo Ramírez Olivera	Abandonó	28/11/2023, 11:08:32
EDUARDO CUEVAS CARDOSO	Unido	28/11/2023, 10:53:44
EDUARDO CUEVAS CARDOSO	Unido	28/11/2023, 10:54:05
Uriel Martinez Cano	Unido	28/11/2023, 10:54:05
Uriel Martinez Cano	Abandonó	28/11/2023, 10:54:41
José David Tellez Medrano	Unido	28/11/2023, 10:54:54
José David Tellez Medrano	Abandonó	28/11/2023, 10:59:51
José David Tellez Medrano	Unido	28/11/2023, 11:03:00
José David Tellez Medrano	Abandonó	28/11/2023, 15:28:38
Scitum, S.A. de C.V. (Invitado)	Unido	28/11/2023, 10:58:13
Scitum, S.A. de C.V. (Invitado)	Abandonó	28/11/2023, 11:04:31
Michelle López Villa/B DRIVE IT (Invit	Unido	28/11/2023, 11:00:17
Michelle López Villa/B DRIVE IT (Invit	Abandonó	28/11/2023, 12:31:07
Michelle López Villa/ B DRIVE IT (Invit	Unido	28/11/2023, 11:02:29
Michelle López Villa/ B DRIVE IT (Invit	Abandonó	28/11/2023, 11:02:38
Alfonso Zuñiga Urbano	Unido	28/11/2023, 11:09:42
Alfonso Zuñiga Urbano	Abandonó	28/11/2023, 11:10:22
ANTONIO PRIETO REVILLA	Unido	28/11/2023, 11:09:46
ANTONIO PRIETO REVILLA	Abandonó	28/11/2023, 11:33:34
ANTONIO PRIETO REVILLA	Unido	28/11/2023, 11:34:49
ANTONIO PRIETO REVILLA	Abandonó	28/11/2023, 15:13:28
ANTONIO PRIETO REVILLA	Unido	28/11/2023, 15:16:25
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 12:29:16
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 12:29:16
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 13:31:17
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 13:34:30
JOSE RENATO MELENDEZ (SIITECS) (Ir	Unido	28/11/2023, 14:37:03
JOSE RENATO MELENDEZ (SIITECS) (Ir	Abandonó	28/11/2023, 15:28:41
PAVEL GARCIA RAZO	Unido	28/11/2023, 15:25:21

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

Nombre completo	Acción del usuario	Marca de tiempo
ADRIANA HERNANDEZ LOPEZ	Unido	28/11/2023, 16:01:29
Gerardo Garibay Aymes	Se unió antes	28/11/2023, 16:01:29
Gerardo Garibay Aymes	Abandonó	28/11/2023, 16:28:27
EDUARDO CUEVAS CARDOSO	Se unió antes	28/11/2023, 16:01:29
VERONICA MARCELA LOPEZ LOPEZ	Se unió antes	28/11/2023, 16:01:29
Juan Ramírez	Se unió antes	28/11/2023, 16:01:29
Juan Ramírez	Abandonó	28/11/2023, 16:28:33
Diana Abigail Hernández De La Cruz	Unido	28/11/2023, 16:01:31
Diana Abigail Hernández De La Cruz	Abandonó	28/11/2023, 16:28:36
José David Tellez Medrano	Unido	28/11/2023, 16:05:22
José David Tellez Medrano	Abandonó	28/11/2023, 16:28:34
ANTONIO PRIETO REVILLA	Unido	28/11/2023, 16:09:01
PEDRO EDUARDO GARCIA VAZQUEZ	Unido	28/11/2023, 16:09:05
AMELIA KARINA ARMENTA ROMERO	Unido	28/11/2023, 16:09:24
MIGUEL ANGEL ESQUINCA VILA	Unido	28/11/2023, 16:09:39
Omar Salinas García	Unido	28/11/2023, 16:10:35
RAMON CABALLERO LEDESMA	Unido	28/11/2023, 16:10:39
JOSE EDUARDO GIRON CAMACHO	Unido	28/11/2023, 16:10:56
JOSE RENATO MELENDEZ (SIITECS) (Invitado)	Unido	28/11/2023, 16:12:12
JOSE RENATO MELENDEZ (SIITECS) (Invitado)	Abandonó	28/11/2023, 16:28:41
Dulce Perla Ortega Flores	Unido	28/11/2023, 16:33:57
Dulce Perla Ortega Flores	Abandonó	28/11/2023, 16:34:04
Dulce Perla Ortega Flores	Unido	28/11/2023, 16:34:59
Dulce Perla Ortega Flores	Abandonó	28/11/2023, 16:35:06
Dulce Perla Ortega Flores	Unido	28/11/2023, 16:35:22
Dulce Perla Ortega Flores	Abandonó	28/11/2023, 16:35:26
Dulce Perla Ortega Flores	Unido	28/11/2023, 16:36:02
Dulce Perla Ortega Flores	Abandonó	28/11/2023, 16:36:50

ARYABHOi44FgzfTb1zSSeNkfc0b7T901O2JdDSLk0Cg=

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

Anexo 2
Reporte de la herramienta de seguridad perimetral de correo electrónico (AntiSpam)

Hora de aceptación	Remitente	Destinatario	Asunto	Archivos adjuntos	Acciones del analizador
jueves, 23 nov, 2023 12:39:45 PM CST	abigail.hernandez@scitum.com.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: lpn/scjn/dgrm/005/2023_preguntas_junta_de_aclaraciones		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:32:13 PM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: lpn/scjn/dgrm/005/2023_preguntas_junta_de_aclaraciones		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:32:17 PM CST	fabian.sanchez@iqsec.com.mx	procpublicosdgrm@mail.scjn.gob.mx	rv: pliego de preguntas iqsec, s.a. de c.v.	iqsec_anexo2c_scjn.pdf, iqsec_anexo6_scjn.pdf, iqsec_anexo6_scjn_word.docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:31:11 PM CST	aespinosaz@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: preguntas - licitación del servicio de desinfección cpsm/dgrm/094/2023 - fumicam		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:31:10 PM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: control de plagas internacional centinela, s.a de c.v. pliego de preguntas.		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:30:48 PM CST	fabian.sanchez@iqsec.com.mx	procpublicosdgrm@mail.scjn.gob.mx	re: pliego de preguntas iqsec, s.a. de c.v.		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:30:11 PM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:29:11 PM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto de interés y preguntas junta de aclaraciones		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:28:26 PM CST	fabian.sanchez@iqsec.com.mx	procpublicosdgrm@mail.scjn.gob.mx	pliego de preguntas iqsec, s.a. de c.v.	iqsec_anexo2c_scjn.pdf, iqsec_anexo6_scjn.pdf, iqsec_anexo6_scjn_word.docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:26:20 PM CST	gerardo.garibay@silent4business.com	procpublicosdgrm@mail.scjn.gob.mx	read: lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:26:12 PM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto de interes en participar y preguntas para j.a- consultoría y capacitación en soluciones avanzadas de seguridad informática s.a. de c.v. (cycsas)		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:24:26 PM CST	carolina.miranda@cycsas.com.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto de interes en participar y preguntas para j.a- consultoría y capacitación en soluciones avanzadas de seguridad informática s.a. de c.v. (cycsas)		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 12:14:45 PM CST	abigail.hernandez@scitum.com.mx	procpublicosdgrm@mail.scjn.gob.mx	lpn/scjn/dgrm/005/2023_preguntas_junta_de_aclaraciones	image002.png, anexo_2c_carta_junta_de_aclaraciones_final.pdf, anexo_6_pliego_de_preguntas_final.pdf, anexo_6_pliego_de_preguntas_final.docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 11:59:53 AM CST	servcliente@cpicsa.com	procpublicosdgrm@mail.scjn.gob.mx	control de plagas internacional centinela, s.a de c.v. pliego de preguntas.	image001.png, identificación oficial vigente.pdf, formato de pliego de preguntas_ control de plagas internacional centinela.pdf, formato de pliego de preguntas_ control de plagas	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 11:50:58 AM CST	jrenato.melendez@siitecs.mx	procpublicosdgrm@mail.scjn.gob.mx	manifiesto de interés y preguntas junta de aclaraciones	carta intención .pdf, preguntas siitecs.pdf	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 11:28:53 AM CST	spslicitaciones@gmail.com	procpublicosdgrm@mail.scjn.gob.mx	sistemas prácticos en seguridad privada s.a. de c.v. cpsi/dgrm/078/2023 san luis potosi	sistemas prácticos en seguridad privada_economica.zip	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 11:13:58 AM CST	gerardo.garibay@silent4business.com	procpublicosdgrm@mail.scjn.gob.mx	lpn/scjn/dgrm/005/2023	image001.png, image002.png, image003.png, image004.png, identificación oficial gga.pdf, anexo 2c.pdf, junta de aclaraciones.docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 11:09:50 AM CST	carolina.miranda@cycsas.com.mx	procpublicosdgrm@mail.scjn.gob.mx	manifiesto de interes en participar y preguntas para j.a- consultoría y capacitación en soluciones avanzadas de seguridad informática s.a. de c.v. (cycsas)	image001.png, interes en participar cycsas.pdf, preguntas cycsas_scjn (002).pdf	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 10:55:24 AM CST	grupobarrutia.contabilidad@hotmail.com	procpublicosdgrm@mail.scjn.gob.mx	re: grupo barrze seguridad privada de occidente - cpsi/dgrm/0792023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 10:38:46 AM CST	pbm@lasaulec.nl	procpublicosdgrm@mail.scjn.gob.mx	re: solicitud para compra		Eliminar mensaje
jueves, 23 nov, 2023 10:31:24 AM CST	servicios@fumicam.com.mx	procpublicosdgrm@mail.scjn.gob.mx	preguntas - licitación del servicio de desinfección cpsm/dgrm/094/2023 - fumicam	image001.png, aclaraciones.docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 10:12:26 AM CST	nahum.dillanes@totalcybersec.com	procpublicosdgrm@mail.scjn.gob.mx	leído: preguntas totalsec, s.a. de c.v. - licitación pública nacional lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 10:10:45 AM CST	valeria.giordano@ticdefense.global	procpublicosdgrm@mail.scjn.gob.mx	manifiesto de interés en participar en la junta de aclaraciones	image001.gif, image002.png, image003.png, image004.png, image005.png, image006.png, carta manifiesto de interes.pdf, pliego de preguntas scj.pdf	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 10:06:18 AM CST	nahum.dillanes@totalcybersec.com	procpublicosdgrm@mail.scjn.gob.mx	preguntas totalsec, s.a. de c.v. - licitación pública nacional lpn/scjn/dgrm/005/2023	image001.gif, image002.jpg, ine certificada víctor rodríguez fuentes ts 22-32.pdf, anexo 2c. manifiesto junta aclaraciones.pdf, anexo 6. formato pliego de preguntas..pdf, anexo 6. formato pliego de preguntas..docx	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:57:20 AM CST	daniel.estrada@arteria.com.mx	procpublicosdgrm@mail.scjn.gob.mx	entrega del pliego de preguntas y carta manifiesto de interés en participar en la junta de aclaraciones para la licitación pública lpn/scjn/dgrm/005/2023	image001.png, anexo 6 - formato de pliego de preguntas.docx, anexo 2c - carta manifiesto para participar en la junta deaclaraciones.pdf	Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:23:35 AM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto y solicitud para participar en la junta de aclaraciones no. lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:21:04 AM CST	meperezt@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: concurso público sumario cpsi/dgrm/093/2023 - motivos de no presentar propuesta (reemplaza anterior)		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:21:04 AM CST	meperezt@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: motivo no presentar propuesta - concurso público sumario cpsi/dgrm/093/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:05:56 AM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto y solicitud para participar en la junta de aclaraciones no. lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:04:59 AM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: entrega del pliego de preguntas y carta manifiesto de interés en participar en la junta de aclaraciones para la licitación pública lpn/scjn/dgrm/005/2023		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 09:04:58 AM CST	ecuevasc@mail.scjn.gob.mx	procpublicosdgrm@mail.scjn.gob.mx	leído: manifiesto de interes en participar		Distribuir el mensaje normalmente
jueves, 23 nov, 2023 08:58:35 AM CST	hantunes@b-drive.com.mx	procpublicosdgrm@mail.scjn.gob.mx	manifiesto y solicitud para participar en la junta de aclaraciones no. lpn/scjn/dgrm/005/2023	carta manifiesto para participar en la junta de aclaraciones.pdf, solicitud de aclaraciones suprema corte finales.docx, solicitud de aclaraciones suprema corte finales.pdf	Distribuir el mensaje normalmente

ARYABHOj44FgzfTb1zSSeNkfc0b7T9O1O2JdDSLk0Cg=