SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS

1. **Antecedentes**

La Corte Suprema de Justicia, en cumplimiento de las normativas y leyes vigentes en la República, incluyendo la Resolución MITIC Nro. 277/2020 (CIS Controls), el Manual de Gobierno y Control de las Tecnologías de la Información (MGCTI) del Banco Central del Paraguay, y las recomendaciones de los marcos de trabajo y estándares internacionales ISO/IEC 27001, NIST SP 800-137, ISACA, SANS Institute, COBIT (teniendo presente el conjunto de objetivos de control relacionado) e ITIL (en sus aparados de procesos de gestión de incidentes y de gestión de problemas), busca contratar los servicios de una empresa especializada en ciberseguridad para un servicio de monitoreo 24x7x365 de los nodos de su infraestructura crítica, a través de un servicio SOCaaS (Security Operation Center as a Service) que permita generar alertas tempranas en cuanto a tráfico malicioso, posibilidades de accesos no autorizados o gestación de ataques cibernéticos.

2. **Alcance del Proyecto**

Los servicios proporcionados por el SOCaaS deben incluir, pero no estar limitados a:

1. Monitoreo constante de los sistemas de información y la infraestructura de red de la Corte Suprema de Justicia.
2. Análisis de registros de seguridad (logs) y alertas de seguridad generadas por sistemas y aplicaciones.
3. Detección y análisis de comportamientos y actividades sospechosas.
4. Respuesta a incidentes, incluyendo la coordinación con el personal interno para la mitigación de amenazas.
5. Generación de informes periódicos de seguridad que incluyan análisis de amenazas, incidentes y recomendaciones de mejora.
6. Asesoramiento y apoyo en la implementación de mejores prácticas de seguridad cibernética.
7. Cumplimiento con normativas y regulaciones de seguridad aplicables a la Corte Suprema de Justicia.

3. **Objetivos**

El objetivo general de este llamado es proporcionar a la Corte Suprema de Justicia un servicio SOCaaS integral que incluya, pero no se limite a:

1. Supervisión y análisis de la seguridad de la red y sistemas en tiempo real.
2. Detección proactiva de amenazas y vulnerabilidades.
3. Respuesta a incidentes y coordinación de acciones de mitigación.
4. Informes y análisis periódicos de seguridad.
5. Asesoramiento y recomendaciones para mejorar la postura de seguridad cibernética.

4. **Confidencialidad y Seguridad de Datos Sensibles.**

El SOCaaS deberá cumplir con estrictas normas de confidencialidad y seguridad de datos, garantizando la protección de la información de la Corte Suprema de Justicia.

Para tal propósito, el oferente que resulte ganador deberá firmar un acuerdo de confidencialidad al inicio de la provisión de sus servicios.

5. **Requisitos Técnicos Solicitados.**

Se solicita la provisión de un servicio SOCaaS (Security Operation Center as a Service), para labores de monitoreo de ciberseguridad y gestión de alarmas, eventos e incidentes de ciberseguridad.

Inventario de equipos y servicios existentes en la CSJ

Equipos	Descripción	Cantidad	Físico	Virtual
Hipervisores		10	10	0
Servidores		106	29	77
Storage+Expansión		10		

San Switch		5		
Servicios	DB	22		
	Correo	2		
	AntiSpam	1		
	Antivirus	1		
	Controladores de dominio	12		
	Servidor de Aplicaciones	14		
Router/firewall		20		
Switch		6		
Proxy		3		
	Total	**212**		

El oferente debe tener en cuenta la provisión de todos los recursos necesarios para suministrar el servicio, en base a la **PLANILLA DE DATOS GARANTIZADOS** presentada más abajo en este apartado.

PLANILLA DE DATOS GARANTIZADOS: Además de completar (Cumple/No Cumple), los oferentes deberán especificar la característica ofertada presentando la evidencia técnica de cumplimiento en oferta, en la columna de DETALLE.

REQUISITO TÉCNICO	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
Tiempo de Servicio: 24/7/365		
Tiempo de notificación ante incidentes: ≤ 60 (sesenta) minutos.		
Tiempo de notificación al oferente de servicios: ≤ 60 (sesenta) minutos.		
Asistencia in situ ante incidentes críticos: ≤ 2 (dos) horas.		
ASPECTOS GENERALES EN LA PROVISIÓN DEL SERVICIO	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
El oferente debe contar con todas las herramientas y servicios descriptos en esta planilla de datos garantizados para realizar el servicio solicitado por la contratante, quedando a su entera responsabilidad los recursos tecnológicos y de conectividad necesarios para la prestación del servicio SOC. La modalidad del servicio es “llave en mano”.		
El servicio debe contar con suscripciones a servicios de inteligencia de amenazas para disponer de información de inteligencia sobre ataques, detección de IoC y/o APTs.		
El servicio debe contar con un sistema de gestión de incidentes, que genere tickets sobre los mismos y las acciones de mitigación auditables, con interacción con el usuario para realizar confirmación de actividad sospechosa. Este sistema de gestión de incidentes debe tener la capacidad de identificar el equipo afectado, mantener un historial de eventos por cada equipo monitoreado y ofrecer estadísticas auditables. El esquema de notificaciones debe tener niveles de escalación de comunicaciones.		
El oferente debe realizar la transferencia tecnológica al personal técnico de la CSJ en cuanto a las buenas prácticas de ciberseguridad.		
El oferente debe realizar análisis del comportamiento de la infraestructura administrada y monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación.		
Debe realizar análisis de tendencias sobre los eventos y plataformas monitoreadas.		
Debe contar con informes de análisis de la capacidad de la infraestructura administrada para identificar		

tendencias para prevenir proactivamente incidentes y/o degradación del servicio.		
Debe contar con un informe mensual detallado sobre alertas mundiales que puedan afectar la seguridad de la infraestructura monitoreada, así como las recomendaciones para elevar el nivel de la seguridad en la misma.		
FUNCIONALIDADES BÁSICAS DEL SERVICIO SOC	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
Debe contar con herramientas digitales para la gestión de eventos vía sistema de ticket, email, mensaje y/o teléfono.		
Debe contar con herramientas y métodos para prevenir la fuga de información en todos los dispositivos utilizados para la provisión del servicio, incluyendo dispositivos portátiles que salgan de las instalaciones del SOC.		
Debe almacenar y precautelar las bitácoras (logs) de los equipos y dispositivos utilizados para la provisión del servicio, para análisis cuando se requiera.		
Debe contar con procesos de eliminación segura de la información que ya no se requiera para la provisión del servicio.		
PLANTEL TÉCNICO	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
Debe contar con presupuesto anual destinado para entrenamiento de personal del SOC en temas de ciberseguridad y servicios relacionados a SOC.		
Debe contar con un equipo de investigación y desarrollo dedicado para los aspectos de amenazas que complementen el servicio SOC ofrecido.		
Debe contar con una capacidad operativa dedicada al SOC para un soporte 24x7x365.		
Debe contar con capacidad de análisis de investigación y detección de la causa raíz de los incidentes detectados.		
Debe contar con personal en los niveles SOC L1 (Monitorización y análisis), L2 (Estudio y respuesta) y L3 (Investigación profunda y prevención).		
PROCESOS INTERNOS DEL SOC	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
El servicio SOC debe disponer de un proceso de Gestión de Conocimiento y de una Base de Datos de conocimiento actualizada.		
Para el servicio SOC se deben tener discriminados claramente los procesos, personas y roles que intervienen en las tareas de operación de seguridad, con las funciones de inteligencia de amenazas, monitoreo, correlación y análisis de tendencias en seguridad en niveles SOC L1, L2 y L3.		
El servicio SOC debe contar con procesos de priorización de atención de incidentes, los cuales se deben basar en una metodología clara de riesgos e impacto.		
El oferente debe contar con su propio equipo de CSIRT (Computer Security Incident Response Team)		
El esquema de operación del SOC debe contar con un DRP (Disaster Recovery Plan) que garantiza la continuidad del servicio.		

El SOC debe contar con procesos definidos para la detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad, así como una matriz de escalamiento identificando al personal clave de la contratante que debe ser involucrado.		
SERVICIO DE GESTIÓN, CORRELACIÓN Y MONITOREO DE LOGS, EVENTOS, ALARMAS E INCIDENTES	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
El SOC debe ser capaz de procesar, monitorear y correlacionar todas las fuentes de datos descriptas en la sección "INVENTARIO DE EQUIPOS Y SERVICIOS EXISTENTES EN LA CSJ", siendo posible incluso un aumento de al menos un 20%, sin pérdidas de logs o eventos.		
EL SOC debe tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos: - Syslog (TCP o UDP). - Transferencia remota de archivos con logs crudos por SCP (Secure Copy), SFTP (Secure FTP). - Archivos de logs en sistemas de archivos remotos mediante NFS y CIFS. - APIs.		
La remisión de los eventos hacia el SOC debe ser realizada a través del protocolo de transporte TCP y con técnicas de cifrado SSL (Secure Sockets Layer). Toda la comunicación, además, debe estar encriptada a nivel de VPN SSL redundante con la CSJ.		
Debe ser factible enviar eventos y logs en tiempo real hacia el servicio de gestión y correlación. También debe ser factible el envío bajo demanda en modalidad asíncrona, según requerimientos de la CSJ.		
El servicio debe proveer los componentes de recolección automática a nivel de software que permitan, desde el origen, la normalización completa de los eventos, es decir únicamente enviarán hacia el servicio de monitoreo los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporte de los eventos.		
Los componentes que realizan la recolección de eventos deben utilizar el protocolo TCP como medio de transporte hacia el servicio de correlación, verificando constantemente el estado de la conexión por medio de un pulso o “Heartbeat”. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.		
La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación debe utilizar mecanismos de compresión de datos.		
Debe ser posible configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.		
Debe ser posible configurar el retraso voluntario en el envío de eventos al motor de correlación basado en horarios, de tal forma que el componente recolector guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad.		

Debe ser posible el filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación en conformidad a la publicación NIST SP 800-92.		
El servicio debe permitir correlacionar la información de Accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades.		
El servicio debe ser capaz de detectar fluctuaciones en la recepción de logs por fuente de información y proveer el estado de la conectividad de los mismos al motor de correlación (UP/DOWN).		
El servicio debe ofrecer mecanismos de búsquedas rápidas, eficientes y que permitan ser exportadas a formatos tales como CSV.		
El servicio debe incluir la provisión de herramientas y conectores orientados a gestionar el ciclo completo de un incidente desde su detección, análisis, escalamiento, cierre y documentación (con archivos de evidencias adjuntas), con la finalidad de generar una base de conocimiento para los analistas. La herramienta debe ser capaz de correlacionar los eventos con los Activos de la Entidad.		
El servicio de detección y evaluación de vulnerabilidades debe estar integrado con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.		
El servicio debe soportar, procesar y almacenar 6 meses de información en línea como mínimo.		
El servicio debe ser alimentado por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso (IoC).		
El motor analítico de la solución SIEM utilizada por el SOC debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.		
El servicio debe incluir la generación de indicadores de compromiso para cada activo monitoreado, basándose en los ataques recibidos y el uso de amenazas identificadas.		
Debe ser capaz de identificar al menos los siguientes ataques e información de los ataques (lista enunciativa, no exhaustiva): - Accesos no autorizados. - Denegación de servicio. - Explotación de vulnerabilidades. - Fuerza bruta/login. - Escaneo de puertos. - Principales orígenes de ataque. - Principales destinos de ataque. - Ubicación geográfica del ataque. - Orígenes/destinos reportados por fuentes de inteligencia de seguridad. - Acceso por parte de los usuarios a dominios diferentes a los autorizados.		
Debe ser capaz de detectar el uso de aplicaciones o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso.		
Debe ser capaz de recolectar eventos de aplicaciones, sistemas o plataformas no predefinidas, usando para ellos alguna característica de parsing.		

El servicio debe realizar correlación de incidentes de seguridad, con capacidad de integrar inteligencia derivada de incidentes similares en el sector o región relacionada a la CSJ.		
El servicio debe tener la posibilidad de integrar las vulnerabilidades detectadas por la CSJ con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.		
CUADRO DE MANDOS Y REPORTERIA EN LÍNEA	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
El servicio debe incluir un portal web donde se permita ver el estado de seguridad, indicadores, reportes y datos en tiempo real.		
El portal debe permitir a los usuarios la visualización de alertas escaladas a través del mismo.		
El portal debe permitir a los usuarios iniciar y realizar la trazabilidad de alertas relacionadas con las actividades de mitigación.		
El portal debe permitir la generación de reportes para las actividades de mitigación pendientes basados en análisis de antigüedad.		
El portal debe suministrar información sobre los activos, tales como: propiedades de los activos, eventos e incidentes, vulnerabilidades y trazabilidad de la mitigación del problema con asignación individual a los activos/usuarios.		
El portal debe incluir una base de conocimiento y buenas prácticas para vulnerabilidades de seguridad.		
El portal debe permitir el diseño de reportes gerenciales que cubran el desempeño de seguridad de las diferentes unidades de negocio, cumplimiento y estado de los activos.		
El portal debe contar con uno o varios mapas de riesgos, que permita identificar el nivel de riesgo de la organización desde la óptica brindada por el servicio de gestión de incidentes.		
El portal debe contar con diferentes cuadros de mandos enfocados a suministrar información a: la DGTIC, equipo de operaciones (infraestructura, redes y soporte) y a la Dirección de Ciberseguridad y Protección de la Información.		
El portal debe permitir exportar los datos soportando múltiples formatos, incluyendo CSV, XML, PDF y/o DOC.		
CAPACIDADES DE PREDICCIÓN Y TENDENCIAS	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
El servicio SOC debe contar con varias técnicas de procesamiento avanzado de datos, con el fin de establecer modelos de predicción general, individual e incluso por micro-ecosistemas.		
El servicio debe permitir crear una línea base de comportamientos asociados a los dispositivos, aplicaciones usuarios y demás fuentes de información que hagan parte del servicio, de tal manera que se pueda determinar una desviación del comportamiento que normalmente tiene la organización y de esta forma realizar un escalamiento de incidente frente a esto.		
El servicio debe tener la capacidad de correlacionar eventos e incidentes de seguridad, así como analítica predictiva con tópicos sobre los activos monitoreados, vulnerabilidades, indicadores de compromiso,		

superficies de ataques, mapa de riesgos, e históricos de incidentes.		
RESPUESTA A INCIDENTES, ANALÍTICA Y CAPACIDADES DE CONTENCIÓN	**Cumple / No Cumple**	**DETALLE (especificar en qué documento incluido en la oferta se acredita)**
Debe contar con un Centro de Incidentes que permita la intercomunicación entre los diferentes componentes del servicio.		
El Centro de Incidentes debe contar con la capacidad de categorizar los eventos de seguridad detectados y correlacionados por el servicio.		
El servicio debe contar con observables (base de información de incidentes propias del SOC) los cuales permitan comparar IP (fuente o destino), usuarios, procesos, nombre de host, URL, dominios, archivos, hash y cualquier potencial componente de un evento de seguridad para construir nuevos IoC (indicadores de compromiso) sin la necesidad de fuentes externas de inteligencia de amenazas.		
El servicio debe permitir usar los datos del score de riesgos, la prioridad del evento, la urgencia, impacto del negocio, importancia del usuario o activo afectado para priorizar cual debe ser el primer evento de la cola a ser tratado por todo el ciclo de procesos que hacen parte del ejercicio de respuesta a incidentes de ciberseguridad.		
El Centro de Incidentes debe permitir ejecutar ciclos o procesos de respuesta a incidentes de forma paralela, los cuales pueden ser ejecutados de forma automática o manual por el grupo de respuesta a incidentes.		

Observación: El oferente deberá presentar todas las documentaciones respaldatorias de lo solicitado en la Planilla de Datos Garantizados que sean pertinentes.

Reemplazo de Profesionales: Se aclara que la Corte Suprema de Justicia se reserva el derecho de solicitar el reemplazo de profesionales durante la ejecución del contrato, si los mismos no cumplen con el desempeño esperado. El nuevo profesional propuesto deberá contar con la aprobación de la Corte Suprema de Justicia, estando obligado a cumplir con el mismo perfil original solicitado o superior.

Una vez recibida la solicitud de reemplazo de personal por parte de la Corte Suprema de Justicia, el oferente adjudicado deberá considerar hasta un máximo de 45 (cuarenta y cinco) días calendario, para la incorporación de este profesional sin afectar la continuidad del servicio, salvo orden expresa de la institución en la solicitud de reemplazo.