

TÉRMINOS DE REFERENCIA

SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA

1. DEPENDENCIA QUE REQUIERE EL SERVICIO

Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información del Congreso de la Republica.

2. OBJETO DEL SERVICIO

El objeto del servicio es la contratación de una solución de ciberseguridad delegada tipo SOAR para proveer, implementar, administrar y mantener de manera continua capacidades de monitoreo 24x7, prevención, detección, investigación y respuesta a amenazas cibernéticas a través de una plataforma de CYBER SOC delegada, que permita la coadministración de la gestión por parte del equipo del Congreso de la Republica a fin de asegurar la contención oportuna ante cualquier ataque dirigido y no dirigido sobre servidores y/o activos de misión crítica.

3. FINALIDAD PÚBLICA

La presente contratación de una solución de suscripción de plataforma de CYBER SOC delegada tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la Republica permitirá fortalecer las capacidades de vigilancia, detección y respuesta frente a amenazas de seguridad informática, asegurando la integridad y confidencialidad de la información institucional.

4. VINCULACIÓN CON EL PLAN OPERATIVO INSTITUCIONAL

CÓDIGO	ACTIVIDAD OPERATIVA
202504025160307	Implementación del plan de adquisición de equipamiento para la renovación de la infraestructura tecnológica, en el marco del Plan de Gobierno Digital.

5. NORMATIVA

La implementación de la solución de suscripción de plataforma de CYBER SOC delegada tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la Republica deberá realizarse en estricto cumplimiento de las disposiciones legales y normas técnicas vigentes aplicables. Estas normativas incluyen, pero no se limitan a, las siguientes: ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.

6. ANTECEDENTES

- El Departamento de Tecnologías de la Información tiene a su cargo la gestión de los Centros de Datos del Congreso de la República ubicado en el Edificio Luis Alberto Sánchez y en Palacio Legislativo.
- Así mismo, existen diversas observaciones al estado actual de los Centros de Datos mencionados, lo cual fue evidenciado en la Carta de Control Interno de la Auditoría a los Estados Financieros y Presupuestales al 31 de diciembre de 2022.

- Esta situación ha evidenciado falencias en la planificación y gestión de la vigilancia, detección y respuestas ante incidentes o amenazas de seguridad informática, asegurando la integridad y confidencialidad de la información institucional. Tales deficiencias ponen en riesgo la continuidad operativa, la seguridad de los datos críticos y limitan la capacidad de respuesta y expansión tecnológica del Congreso de la República.
- Frente a estos desafíos, es crucial alcanzar la certificación de los Centros de Datos bajo las normas ISO 27001:2022, NTP/ISO N° 22237 y ANSI/TIA 942. Este proceso incluirá un rediseño acorde a las especificaciones técnicas de estos estándares internacionales y una validación final para garantizar operaciones alineadas con las mejores prácticas internacionales.
- Debido al exponencial incremento del ciberdelincuencia y amplia variedad de nuevas amenazas cibernéticas, tales como ataques masivos de ransomware, estafas de phishing, robo de información, robo de credenciales, ataques dirigidos y más, el Congreso de la República viene integrándose en un proceso de mejoramiento continuo de sus actividades, encaminándose a la transformación digital. Es por ello por lo que parte de uno de los lineamientos de la gestión, es la ciberseguridad.
- El Congreso de la República necesita garantizar que sus activos de información no se vean afectados por alguna amenaza cibernética externa o interna, es por esto, que se requiere contratar la suscripción de una plataforma de CYBER SOC delegada, que permita realizar un monitoreo y correlacionamiento continuo de eventos de seguridad, a fin de PREVENIR, DETECTAR y RESPONDER ante cualquier incidente cibernético, a través de una plataforma de CYBER SOC que permita delegar las actividades propias de una gestión proactiva en ciberseguridad a un equipo de profesionales con un seguimiento activo 24x7.

7. CARACTERÍSTICAS DEL SERVICIO A REALIZAR

La plataforma deberá cubrir la seguridad, correlacionamiento de eventos de seguridad, detección, respuesta ante incidentes y [remediación](#)¹ tipo SOAR para la totalidad de los servidores de misión crítica y determinados activos estratégicos, brindando a través de una plataforma de CYBER SOC delegada la coadministración de los eventos de seguridad de la institución la deberá ejecutarse por un periodo de setecientos treinta (730) calendario garantizando el MONITOREO 24X7x360, la DETECCIÓN y RESPUESTA EFECTIVA ante ataques cibernéticos sobre un total de 100 SERVIDORES (Físicos y Virtuales), integrando las fuentes necesarias (antivirus, antispam, correo, firewalls y/o componentes de red) para mejorar la tasa de detección y respuesta.

7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA

- El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo [SOC 2](#) y [SOC 3](#)² para los productos de detección y respuesta ofertados.
- La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad [con al menos dos \(02\) de las siguientes](#)³ normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.
- La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), Centos 7 and greater, Red Hat 8 and 9.

¹ Ajuste realizado en merito a la absolución de la Consulta N°39.

² Ajuste realizado en merito a la absolución de la Consulta N°14 y 26.

³ Ajuste realizado en merito a la absolución de la Consulta N°15.

- La plataforma debe presentarse como un sistema integrado tipo SOAR integrando tecnologías y plataformas requeridas que se gobiernen desde una sola consola de orquestación automatizada con acceso basado en roles que permita la COADMINISTRACIÓN por parte del equipo del Congreso de la Republica.
- La plataforma debe proveer capacidades de detección y respuesta administrada a través del equipo del fabricante permitiendo la eficiencia y efectividad del proceso.
- La plataforma base tipo SOAR debe permitir la integración con la infraestructura de TI y seguridad existente, logrando que la plataforma administrada por el equipo de analistas de SOC del fabricante identifique rápidamente actividades maliciosas y sospechosas en los principales vectores de amenazas críticas: endpoint, red y nube, para brindar una defensa avanzada contra ciberamenazas las 24 horas, los 7 días de la semana durante el tiempo que dure la suscripción.
- La plataforma deberá trabajar preferentemente sobre un esquema basado en agente, el cual solo demande del acceso seguro a una plataforma de Cyber SOC gestionada la cual opere desde un Data Center en la nube.
- La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero, [a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva.](#)⁴
- La plataforma debe garantizar la seguridad de la información del activo protegido a través de la configuración de un agente que no pueda aceptar conexión entrante, que no sea compatible con el control remoto, ni con la capacidad de ejecutar contenido generado por el usuario en endpoints (puntos finales) o servidores.
- [La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2.](#)⁵
- La plataforma debe admitir la autenticación de dos factores (2FA) para salvaguardar el acceso a la consola.
- [La plataforma debe permitir la coadministración efectiva por parte del Congreso de la Republica a través de la integración de un sistema de acceso basado en roles, considerando como mínimo roles de administración y visualización.](#)⁶
- La plataforma debe poder definir una relación de usuarios que serán notificados a través de correo electrónico y/o vía telefónica específicamente sobre:
 - Amenazas críticas o emergencias en el momento que ocurran
 - Instrucciones de remediación y/o fortalecimiento de configuraciones
 - Advertencia y/o detección de vulnerabilidades y/o riesgos latentes
- La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral.
- La plataforma debe contar con una aplicación que brinde la posibilidad de recopilar y analizar eventos en CEF (formato de evento común) y LEEF (formato extendido de evento de registro) a través de Syslog.
- La plataforma debe tener una arquitectura multitenant que le permita crear instancias de gobierno independiente asignadas a usuarios clave dentro de la organización.
- La plataforma debe permitir crear reportes bajo demanda y programarlos para su envío automático al correo electrónico.

⁴ Ajuste realizado en merito a la absolución de la Consulta N°16 y 27.

⁵ Ajuste realizado en merito a la absolución de la Observación N°20.

⁶ Ajuste realizado en merito a la absolución de la Observación N°21.

- La plataforma debe permitir la creación de informes de inventario e informes ejecutivos hasta con una antigüedad de noventa (90) días.

7.2. CAPACIDADES DE DETECCIÓN Y RESPUESTA DE CIBERATAQUES

- La plataforma de Cyber SOC debe integrar a través del agente capacidades de detección avanzada de infracciones reconociendo tácticas, técnicas y procedimientos (TTP) del adversario de acuerdo con el marco MITRE ATT&CK.
- La plataforma de Cyber SOC deberá estar diseñada específicamente para buscar TTP sobre el dispositivo local Windows, Mac y Linux en varias categorías, incluidas mínimamente descubrimiento, persistencia, evasión de defensa, ejecución, acceso a credenciales, escalada de privilegios y movimiento lateral.
- [La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas.](#)⁷
- La plataforma deberá mapear conexiones de red entrantes y salientes las cuales deberán ser registradas y analizadas para detectar amenazas en la red. La actividad maliciosa se identificará evaluando el puerto utilizado, la reputación y la geolocalización de la dirección IP y otras atribuciones disponibles.
- La plataforma deberá detectar ransomware verificando el sistema local en busca de actividades de cifrado permitiendo a los usuarios eliminar el proceso infractor o aislar el host afectado automáticamente, deteniendo los ataques de ransomware inmediatamente después de la detección.
- La plataforma deberá contar con un monitor de registro de eventos de punto final logrando ingerir los eventos relacionados con la seguridad escritos en el registro de eventos pudiendo agregar identificadores de eventos personalizados para monitorear aplicaciones personalizadas.
- La plataforma deberá contar con la capacidad de analizar registros de firewall enviando datos a Data Center SOC a través de Syslog para monitorear los eventos de seguridad registrados, la integración deberá realizarse a nivel de API.
- La plataforma debe integrar capacidades de detección de indicadores de compromiso (IoC), esta aplicación deberá ejecutar detecciones seleccionadas por el equipo del Data Center SOC a través de su equipo de investigación de amenazas y se puede actualizar según sea necesario sin que el administrador o el usuario deban realizar ninguna acción.
- La plataforma debe presentar un entorno de trabajo colaborativo evidenciando los diferentes eventos de detección basados en múltiples fuentes de información sobre amenazas. El Data Center SOC supervisará estas detecciones y las tratará con alta prioridad, y el equipo de investigación de amenazas seguirá supervisando las métricas de detección para ajustar los falsos positivos o los falsos negativos.
- La plataforma debe contar con la capacidad de detectar archivos maliciosos a través de su propio motor de detección de malware desarrollado como parte de la solución integrada, escaneando archivos escritos en el disco o ejecutados en busca de atributos maliciosos para proporcionar redundancia sobre la solución antimalware con la que ya cuenta la institución.
- La plataforma debe contar con la capacidad de detectar servicios de red sospechosos que se ejecutan en servidores y estaciones de trabajo. Si bien existen múltiples servicios de red disponibles para uso legítimo, las detecciones sospechosas se definen como puertos y servicios conocidos que se aprovechan con fines maliciosos por lo que es de vital importancia la evaluación de cada uno de estos servicios.
- La plataforma debe contar con la posibilidad de detectar herramientas sospechosas y/o programas que puedan afectar negativamente la seguridad del sistema y la red. Las herramientas sospechosas detectadas deben investigarse y

⁷ Ajuste realizado en merito a la absolución de la Observación N°19

clasificarse como utilidades de piratería, descifradores de contraseñas u otras herramientas utilizadas por atacantes con fines maliciosos.

- La plataforma debe poder configurarse para habilitar la monitorización de registros de unidades USB (Medios extraíbles) para mapear cuando un dispositivo USB se conecta y se desconecta.
- La plataforma debe contar con capacidades de respuesta ante ataques en curso, aislando dispositivos en la red que tengan instalado un agente, el aislamiento del host se realizará como consecuencia de un análisis y/o activación automática de un playbook de respuesta a incidentes para evitar la propagación de código malicioso al impedir que una máquina vulnerada se comunice con otros dispositivos de red en internet o la red del cliente. La máquina aislada mantendrá la conectividad con la plataforma correspondiente y permitirá que el Data Center SOC o equipo responsable en la institución reconecten el dispositivo.
- La plataforma debe contar con capacidades de respuesta y remediación a través del agente, logrando ejecutar la eliminación de archivos, eliminación de claves y valores del registro, terminación de procesos, desinstalación de software, parada de servicios, eliminación de tareas programadas.
- La plataforma deberá mostrar por cada activo protegido el detalle de las potencias brechas de seguridad en función a la cantidad de eventos maliciosos y eventos sospechosos especificando la telemetría y detalle de cada evento analizado.
- La plataforma deberá mostrar todos los eventos detectados en orden cronológico permitiendo visualizar objetivos, tácticas y técnicas previstas por los atacantes ayudando a interrumpir rápidamente un proceso de ataque reduciendo el tiempo de permanencia, cada evento en el tiempo deberá de mostrar la fecha y hora exacta de la detección, la IP local, el puerto, IP remota el puerto remoto el país y el detalle de la conexión o telemetría del evento.
- La plataforma deberá mostrar información detallada del servidor y/o estación custodiada en línea con información detallada del inventario del activo permitiendo conocer:
 - Configuración del sistema y configuración de red
 - Detalle de los servicios (Nombre, tipo, estado y ubicación)
 - Software instalado (Fabricante, usuario, versión, tamaño y fecha de instalación)
 - Usuarios y sesiones activas
 - Status de aplicación de políticas de contraseñas
 - Recursos compartidos
 - Estado de la red (Netstat) y tabla ARP
 - Status de Update y Upgrade

7.3. CAPACIDADES DE PREVENCIÓN Y REDUCCIÓN DE SUPERFICIE DE ATAQUE CIBERNETICO

- La solución propuesta para este escenario tiene por objetivo añadir capacidades de prevención proactiva contra ataques cibernéticos a la plataforma de Cyber SOC delegada a través de la reducción proactiva y continua de la superficie de ataque externa e interna en la entidad.

7.3.1. GESTIÓN COLABORATIVA Y PRESENTACIÓN DE RESULTADOS DE POSTURA DE SEGURIDAD EN EL TIEMPO

- La reducción de la superficie de ataque se hará efectiva a través de la ejecución de ejercicios de hacking ético, pentesting y la priorización de vulnerabilidades, configuraciones débiles y anomalías, [la cantidad de ejercicios solicitados anualmente son: Hacking Ético: 2 ejercicios completos por año, Pentesting: 2 ejercicios completos por año y priorización de Vulnerabilidades: 4 evaluaciones \(una cada trimestre\).](#)⁸

⁸ Ajuste realizado en merito a la absolución de la Consulta N°30

- La reducción de la superficie de ataque interna y externa deberá ser presentada a través de una plataforma web de entorno colaborativo que permita documentar e interactuar a todos los integrantes del equipo del POSTOR y a los del equipo del Congreso de la República en las tareas de remediación de vulnerabilidades y riesgos, mapeando fechas, tareas y asignaciones.
- La plataforma web utilizada para ejecutar las actividades de reducción de superficie de ataque deberá presentarse en modalidad cloud (SaaS).
- La plataforma deberá permitir documentar la actividad sobre cada vulnerabilidad y/o riesgo cibernético identificado, permitiendo ingresar y actualizar información referida a la descripción, solución, tipo de vulnerabilidad, nivel de severidad, información adicional, relación con el activo específico afectado, relación con otras vulnerabilidades, actividades realizadas, usuarios responsables de cada actividad, captura de pantalla y/o evidencia de remediación aplicada y cierre o mitigación formal de riesgo.
- La plataforma web utilizada para ejecutar las actividades de reducción de superficie de ataque deberá poder modelar el siguiente proceso para la remediación de las vulnerabilidades detectadas empezando desde la detección de la vulnerabilidad, documentando el informe en la plataforma, asignando tareas específicas de corrección de la vulnerabilidad al equipo del Congreso de la República, soportando consultas, preguntas y soporte a incidentes del equipo del congreso de la República, documentando la corrección y/o remediación aplicada en ambiente de producción, para finalmente cerrar el caso.

7.3.2.MONITOREO Y REDUCCIÓN CONTINUA DEL NIVEL DE EXPOSICIÓN AL RIESGO EXTERNO

- La plataforma utilizada deberá permitir la automatización de las pruebas de penetración e identificación de riesgos sobre los activos publicados.
- La plataforma debe estar desarrollada sobre un marco de mejora continua en el tiempo, brindando detalles de las remediaciones a aplicar por cada vulnerabilidad o riesgo asociado al activo.
- La plataforma deberá realizar automáticamente el filtrado de salida para garantizar que la organización esté restringiendo efectivamente el tráfico de salida innecesario, evitando de esta manera que un determinado acceso pueda permitir que un actor malicioso exfiltre datos del sistema de la organización.
- La plataforma deberá auditar los intentos de autenticación para detectar el uso de credenciales de usuario comprometidas. El objetivo es que, de manera automática, se intente validar dichas credenciales para identificar los accesos y sistemas en los que puedan ser explotadas. Este es un proceso comúnmente utilizado por atacantes y probadores de penetración durante la escalada de privilegios, por lo que resulta crucial que la plataforma ejecute esta validación en primera instancia.
- La plataforma deberá auditar y validar la escalada de privilegios y movimiento lateral usando un conjunto válido de credenciales identificando áreas valiosas dentro de su organización. Esto es llevado a cabo a través de una variedad de métodos y herramientas a fin de poder ejecutar netstat de forma recursiva en múltiples hosts, proporcionando salida y representación visual del flujo de datos (o conexiones de red) dentro del entorno.
- La plataforma deberá poder detectar y documentar la exfiltración de datos a través de la simulación y registro de esta actividad para ayudar al equipo de informática del Congreso de la República para ajustar configuraciones y cerrar brechas de seguridad.
- La plataforma deberá poder hacer uso de acceso elevado e intentar cargar código malicioso en sistemas remotos en un intento de probar la protección de punto final de la organización a fin de afinar los controles antimalware.

- La plataforma deberá poder generar un informe ejecutivo y un informe técnico acerca de una vulnerabilidad y automatizar la prueba de penetración documentando la capacidad de respuesta que se tuvo frente a esta.
- La plataforma deberá poder configurarse para analizar objetivos externos publicados a internet u objetivos internos como servidores y/o aplicaciones.
- La plataforma deberá presentar informes de penetración y remediación de forma trimestral evidenciando la evolución de los ejercicios.

7.3.3. MONITOREO Y REDUCCIÓN CONTINUA DEL NIVEL DE EXPOSICIÓN AL RIESGO INTERNO

- La plataforma deberá ser de tipo SaaS con una arquitectura basada en agente ligero el cual no supere los 20 MB de tamaño para su óptimo desempeño.
- La plataforma deberá implementar una gestión avanzada de vulnerabilidades, configuraciones alineadas a cumplimiento normativo como ISO y NIST además los activos en busca de anomalías.
- La plataforma deberá estar basada en la gestión avanzada de vulnerabilidades internas trabajando sobre una metodología de priorización de riesgos SSVC la cual consiste en un sistema que ayuda a analizar las vulnerabilidades para tomar decisiones que contribuyan a prevenir incidentes de seguridad y contener sus consecuencias.
- La plataforma deberá presentar la priorización de vulnerabilidades según su nivel de explotabilidad mínimamente con los siguientes criterios: fácilmente explotable, explotable en la red, explotación pública disponible, explotación con alto movimiento lateral.
- La plataforma deberá tener la capacidad de relacionar las vulnerabilidades con ataques de alta fidelidad, las vulnerabilidades de los kits de explotación que se pueden utilizar para explotar la debilidad. Esto debe permitir predecir un ataque específico arrojando las coordenadas exactas para mitigarlo.
- La plataforma deberá contemplar el descubrimiento de activos de TI de forma automática y permitir generar alertas de uso indebido de aplicaciones o software a los responsables.
- La plataforma deberá gestionar de forma integral la corrección de errores de configuración y controles de seguridad para fortalecer los sistemas.
- La plataforma deberá identificar, clasificar, distribuir e instalar parches de actualización para mitigar los riesgos de seguridad considerando parches sobre Windows, Linux, macOS y todas las aplicaciones instaladas sobre los hosts tales como navegadores, bases de datos, componentes, etc.
- La plataforma deberá evaluar el cumplimiento normativo mínimamente de [NIST CSF](#), [ISO](#), [STIG](#) y/o [SOC-2⁹](#) a través de la validación que realice el agente instalado sobre los servidores y/o estaciones seleccionadas.
- La plataforma debe cubrir mínimamente la siguiente lista de puntos de referencia para su módulo de cumplimiento:
 - Tiempo mínimo de la contraseña.
 - Permitir estados de espera cuando el equipo o servidor inicie sesión.
 - Requerir una contraseña cuando una computadora se activa.
 - Criptografía del sistema para el forzado de una fuerte protección de claves para las claves de usuario almacenadas en la computadora.
 - La clave debe cumplir los requerimientos de complejidad.
 - Desactivar la prevención de ejecución de datos para el ejecutable de ayuda HTML.
 - Requerir contraseña al conectarse.
 - Habilitar la autenticación del cliente del asignador de extremos de RPC.
 - Requerir autenticación de usuario para conexiones remotas mediante autenticación de nivel de red.

⁹ Ajuste realizado en mérito a la absolución de la Consulta N°32

- Requerir el uso de inicio rápido.
- Desactivar la prevención de ejecución de datos para Explorer.
- Hacer cumplir el historial de contraseñas.
- Seguridad de la red: nivel de autenticación de LAN Manager.
- Control del comportamiento del Registro de eventos cuando el archivo de registro alcanza su tamaño máximo (Seguridad).
- Inicio de sesión interactivo: límite de inactividad de la máquina.
- Desactiva las notificaciones de aplicaciones en la pantalla de bloqueo.
- Permitir el acceso remoto a la interfaz Plug and Play.
- No procesar la lista de ejecutar una vez para la configuración del equipo.
- No enumerar usuarios conectados en equipos unidos a un dominio.
- Umbral de bloqueo de cuenta.
- Seguridad de red: seguridad de sesión mínima para clientes basados en NTLM SSP (incluido RPC seguro).
- Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM.
- No procesar la lista de ejecución heredada para la configuración del equipo.
- Impedir la instalación de dispositivos extraíbles.
- Longitud mínima de la contraseña.
- Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash y la firma.
- Control de cuentas de usuario: eleve solo las aplicaciones de UIAccess que están instaladas en ubicaciones seguras.
- Acceso a la red: rutas y subrutas de registro accesibles de forma remota.
- Miembro del dominio: cifre o firme digitalmente los datos del canal seguro (siempre).
- Control de cuentas de usuario: Comportamiento del aviso de elevación para usuarios estándar.
- Control de cuentas de usuario: detecte instalaciones de aplicaciones y solicite la elevación.
- Cuentas: estado de la cuenta de invitado
- Acceso a la red: restrinja el acceso anónimo a canalizaciones con nombre y recursos compartidos.
- Acceso a la red: no permitir la enumeración anónima de cuentas SAM.
- Acceso a la red: no permitir aplicar permisos a usuarios anónimos.
- Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador.
- Control de cuentas de usuario: eleve solo los ejecutables que estén firmados y validados
- La plataforma deberá consolidar y presentar el análisis y búsqueda de vulnerabilidades, configuraciones erróneas alineadas a cumplimiento NIST, anomalías de postura que deriven del uso de procesador, red, memoria, puertos, servicios, usuarios, perfiles, etc. y otros riesgos de seguridad.
- La plataforma debe integrar un módulo que ejecute acciones para alinear políticas de uso de los activos tales como:
 - Bloquear una aplicación por determinado tiempo.
 - Permitir la ejecución de aplicaciones en determinados intervalos de tiempo.
 - Bloquear y determinar el acceso a dispositivos por determinado intervalo de tiempo.
 - Enviar un script.
 - Gestionar un proceso.
 - Gestionar el status de un servicio.
 - Gestionar un registro.
 - Instalar o desinstalar una aplicación por determinados periodos de tiempo.
 - Evaluar la actividad de la red.

- Evaluar la transferencia de archivos.
 - Validar que programas inician sesión.
 - Borrar un archivo.
 - Mover un archivo a cuarentena.
- La plataforma deberá automatizar la creación de informes completamente personalizables y listos para auditorías, presentando mínimamente informe de inventario o exposición de activos, informes de incumplimiento de políticas de uso de software, informes de vulnerabilidades con su respectivo nivel de riesgo basado en múltiples criterios, informes de aplicación de parches sobre sistemas operativos y aplicaciones instaladas, informes de anomalías con indicadores de ataque (IoA) e indicadores de compromiso (IoC) e informes de cumplimiento de la NIST y/o ISO, evidenciando la reducción del riesgo en el tiempo.

7.4. CAPACIDADES DE PREDICTIBILIDAD DE ATAQUES

El servicio ofertado deberá incluir el acceso, administración y reportes a una plataforma de Cyber Threat Intelligence capaz de poder implementar capacidades de predictibilidad de ataques cibernéticos dirigidos y no dirigidos a través del monitoreo continuo de dark web y diversos canales utilizados por hackers y ciberdelincuentes.

- La plataforma deberá ser presentada en modalidad de Software as a Service (SaaS) sin requerir de infraestructura física adicional para su normal desempeño.
- La plataforma deberá detectar credenciales comprometidas de la institución, las credenciales que se recuperan pueden estar relacionadas con clientes externos, afiliados de terceros, aplicaciones comerciales y aplicaciones de TI internas.
- La plataforma deberá reconocer robo de credenciales de botnets las cuales han sido robadas por los servidores de crime logrando determinar el origen de la fuente, ya sea por configuraciones incorrectas y/o robo a través de herramientas de malware identificando el nombre de la botnet responsable y técnicas de ingeniería social utilizadas.
- La plataforma deberá reconocer credenciales de hacktivismo las cuales han sido filtradas en fuentes de cibercrimen y hacktivistas como foros, sitios de pegado, P2P, sitios web oscuros, etc.
- La plataforma deberá monitorear la actividad de hacktivismo en redes sociales, sitios de pegado, chats IRC, etc. para saber si existen grupos de hacktivismo que buscan atacar activos tecnológicos de la institución.
- La plataforma debe permitir identificar y detectar vulnerabilidades y ataques de día 0/1 día que afectan el software y hardware utilizado por la institución.
- La plataforma deberá integrar capacidades de predictibilidad basada en la recopilación de datos de fuentes abiertas, cerradas y privadas a través del acceso a una base de datos con el cual los especialistas en inteligencia realizarán búsquedas en la Darknet profunda y redes relacionadas (Contenido Darknet, Contenido Deepweb, Plataformas de chat encriptado (Telegram y otros), Hacker fóruns, FTP servers, Marketplaces y otros lugares no divulgados) para encontrar indicios o evidencias de amenazas existentes o emergentes que puedan atentar contra el Congreso de la Republica.
- La plataforma deberá presentar detalles de los hallazgos del módulo de credenciales, entregando mínimamente los siguientes datos:
 - Categorización según el nivel de criticidad y/o prioridad de las credenciales encontradas.
 - Usuario y contraseña comprometida.
 - Tipo de botnet relacionada.
 - URL afectada y/o plataforma o servicio afectado.
 - Palabras clave utilizadas para la captura.
 - Tipo de credencial.
 - Clasificación.
 - Relación con plataforma de correo.
 - Última actualización.

- Fecha de reporte.
- Fecha de violación o captura
- La plataforma deberá permitir la creación de alertas para todos sus módulos.
- La plataforma deberá poder afinar la búsqueda a través de filtros, parámetros y clasificación por dominio, IP o palabra para todos sus módulos.
- La plataforma deberá poder integrar datos de amenazas STIX/TAXII e intercambio de información con el SIEM o SOAR que la institución implemente.
- ¹⁰
- La plataforma deberá presentar complementos disponibles para SIEM, XSOAR y TIP.
- La plataforma deberá administrar un sistema dinámico de puntuación de riesgos para alimentar programas de gestión de vulnerabilidades a través de API.
- La plataforma deberá integrar puntuación y clasificación de amenazas de malware.
- La plataforma deberá integrar en sus procesos la entrega verificada por humanos a fin de minimizar falsos positivos.
- La plataforma deberá integrar una asociación continua con Cyber Threat Alliance (CTA).
- La plataforma deberá de tener una arquitectura modular que permita activar diferentes funcionalidades en el tiempo según los requerimientos de profundización e investigación a medida, estas funcionalidades deberán comprender mínimamente el compromiso de credenciales, protección de dominio, fuga de datos, hacktivismo, tarjetas de crédito, monitoreo de la organización en la dark web, exploración de amenazas, monitoreo de la organización en redes sociales e indicadores de ataque.

7.5. PRESENTACION OBLIGATORIA DENTRO DE LA PROPUESTA:

El Postor dentro de su propuesta, deberá acreditar mediante la presentación de catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, el cumplimiento de los siguientes componentes:¹¹

Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG).

7.6. CARACTERISITICAS DE LA SEGURIDAD GESTIONADA

- El servicio de seguridad gestionada deberá contemplar de forma integral la gestión proactiva de toda la plataforma de Cyber SOC delegada, incluyendo la gestión tipo MDR correlacionando los eventos de equipos, servidores, componentes de red,

¹⁰ Se suprime en merito a la Consulta N° 34

¹¹ Ajuste realizado en merito a la absolución de la Consulta N° 12

antivirus y firewall, correo electrónico, directorio activo y demás plataforma de seguridad convenientes.

- El servicio de seguridad gestionada deberá contemplar la gestión proactiva de todas las capacidades de prevención, detección, respuesta y predictibilidad que oferte la plataforma Cyber SOC delegada.
- El servicio de seguridad gestionada deberá presentar un plan de acción con las salvaguardas y estrategias recomendadas para el cumplimiento progresivo de los controles de seguridad idóneos alineados a la NIST.
- El servicio de seguridad gestionada deberá destinar un recurso (Operador de servicio) local en las instalaciones del Congreso o remota que se comunicará por correo electrónico y otros medios para coordinar las siguientes actividades:¹²
 - Consolidar y presentar los resultados obtenidos de la plataforma tipo SOAR (Cyber SOC) para brindar capacidades de detección y respuesta ante ataques cibernéticos, mostrando evidencia del correlacionamiento de eventos de múltiples fuentes, alertas sobre servicios o aplicaciones sospechosas, conexiones con redes ciberterroristas e infracciones de seguridad revisadas en el tiempo con su respectiva telemetría.
 - Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para las capacidades de prevención con respecto al hacking, pentesting y reducción de superficie de ataque interna y externa, adjuntando información sobre la gestión de riesgos basado en vulnerabilidades, configuraciones débiles y anomalías.
 - Absolución de consultas técnicas y soporte a incidentes reportados en la institución.
 - Elaboración e implementación de directivas y estrategias de concienciación en ciberseguridad a través de webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la institución, la cantidad de los webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la organización deberán ser mínimo tres (03) veces al año.¹³
 - Para el desarrollo de sus actividades del especialista u operador deberá contar con un equipo de cómputo el cual deberá ser proporcionado por el postor que lo presente como integrante del personal clave propuesto.¹⁴
- El servicio de seguridad gestionada deberá considerar actividades de reducción de superficie de ataque interna y externa a fin de mitigar los riesgos y reducir rápidamente su superficie de ataque por lo que el servicio debe considerar una gestión continua de vulnerabilidades con capacidad de detectar, evaluar, priorizar y remediar riesgos de seguridad más allá de las vulnerabilidades y exposiciones comunes (CVE) evidenciando:
 - Detección y clasificación de vulnerabilidades por Host y por aplicaciones con detalle de antigüedad, grupos específicos, ataques relacionados, Explotabilidad, vulnerabilidades remediadas, mitigadas, excluidas y programadas para remediación.
 - Detalles de los activos expuestos (Programas instalados).
 - El servicio de seguridad gestionada asumirá la remediación integral de los riesgos, aplicando parches, corrigiendo configuraciones, anomalías y definiendo políticas de uso de software a través de la desinstalación y/o bloqueo efectivo de aplicaciones, toda actividad deberá quedar documentada en la plataforma que corresponda para futuras auditorías. Todas las actividades que no se alcance a realizar deberán estar

¹² Ajuste realizado en merito a la absolución de la Consulta N°36

¹³ Ajuste realizado en merito a la absolución de la Consulta N°37

¹⁴ Ajuste realizado en merito a la absolución de la Consulta N°36

debidamente justificadas con la aprobación de los responsables de la institución y cogerán prioridad en el siguiente mes de objetivos.

7.7. NIVELES DE SERVICIOS ESTABLECIDOS (SLA)

- El Cyber SOC escalará un evento de interés a un incidente de forma automática o manual; los incidentes generarán una notificación por EMAIL o un ticket de mesa de ayuda cuando la integración esté habilitada.
- El Cyber SOC escalará aún más un incidente mediante una llamada telefónica al usuario o, si es necesario, aislando el dispositivo y notificando al usuario. Cuando se detecte una ejecución potencialmente maliciosa en un dispositivo, el Cyber SOC lo gestionará como un incidente de Gravedad 1 hasta que la organización indique lo contrario
- Después de que el primer evento sospechoso/malicioso se convierta en un incidente, los analistas buscan otros eventos e incidentes inusuales y que lo corroboren. No recomendamos archivar los eventos.
- Las aplicaciones sirven como recopiladores de eventos; el Cyber SOC evalúa regularmente los eventos en las aplicaciones para buscar cualquier instancia que deba escalar a un incidente o crear una regla lógica para generar notificaciones automáticamente.
- El tiempo de detección, los patrones de telemetría y la zona horaria del usuario son elementos clave para los analistas del Cyber SOC y afectan la acción que tomarán. El Cyber SOC considera la zona horaria de la organización y las ejecuciones fuera del horario laboral en su proceso de toma de decisiones.
- El Cyber SOC iniciará una investigación en profundidad luego de cualquier incidente/evento de Gravedad 1 para determinar si el historial de incidentes y los eventos en las aplicaciones presentan algún otro indicio de un entorno violado. Según lo que encuentre, el SOC aislará los dispositivos si:
 - El cliente no responde la llamada para confirmar que las acciones están autorizadas.
 - El SOC no puede determinar con 100 % de certeza que alguna etapa de un ataque no está en curso en función de los incidentes y eventos encontrados en el panel del cliente en ese momento.

NIVELES DE GRAVEDAD – EVENTOS / INCIDENTES				
SEVERIDAD	IMPACTO	DESCRIPCIÓN	RESPUESTA TÍPICA (DETECCIÓN/ NOTIFICACIÓN/ ACCIÓN)	SLA (ACUERDO DE NIVEL DE SERVICIO)
SEV1	CRÍTICA URGENTE	Compromiso del sistema confirmado; ataque en curso.	2 min. / 5 min. / 10 min.	60 min.
SEV1	CRÍTICA	Fallo en cuarentena del antivirus; actividad maliciosa o sospechosa detectada en ejecución de archivos inusuales, conexiones con IPs de mala reputación o países monitoreados.	2 min. / 5 min. / 20 min.	60 min.
SEV2	IMPORTANTE	Actividad inusual detectada sin compromiso confirmado de	2 min. / 10 min. / según sea necesario	No aplica

		sistemas, se detectó una alerta y ningún componente de los sistemas están comprometidos.		
SEV3	MENOR	El sistema muestra intentos de inicio de sesión fallidos u otros eventos generados por la red del cliente sistemas o usuarios y no forman parte de una amenaza de ciberseguridad.	2 min. / 10 min. / según sea necesario	No aplica
SEV4	INFORMATIVA	No se observa ningún efecto malicioso en el sistema.	2 min. / según sea necesario / según sea necesario	No aplica
CONEXIONES DE RED TERRORISTA CIBERNÉTICA				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
Cyber SOC	Cyber SOC	Cyber SOC	Cyber SOC Local	Cyber SOC
Conexión RDP sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros Eventos sospechosos.	Si se detecta un inicio de sesión exitoso, notifique al socio de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios, contraseñas con acceso al dispositivo. Ejecute un escaneo de antivirus completo. Investigar raíz causa. Aplicar políticas de acceso estrictas.	EMAIL/TICKET LLAMADA AISLAR
		Si se detecta fuerza bruta pero no inicio de sesión exitoso detectado, notificar Socio de TI.	Coloque RDP detrás de VPN. Actualizar sistema. Aplicar políticas de acceso estrictas.	EMAIL/TICKET
Conexión SQL sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos sospechosos.	Si la conexión es exitosa, notifique al socio de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios contraseñas con acceso al dispositivo. Ejecute un escaneo antivirus completo. Aplicar estrictas políticas de acceso.	EMAIL/TICKET LLAMADA AISLAR
		Si la conexión está autorizada, notifique al socio de TI.	Ejecute un escaneo antivirus completo. aplicar estricto políticas de acceso.	EMAIL/TICKET LLAMADA

Conexiones entrantes sospechosas en 445 o 25 (SMB/SAMBA/Usos compartido de archivos de Windows) o 139 Servicio de sesión NetBIOS	Analizar detalles. Revisar la línea de tiempo. Identifica cualquier otro evento sospechoso.	Si la conexión es exitosa, notifique al personal de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios contraseñas con acceso a la dispositivo. Ejecute un escaneo antivirus completo. Investigar la causa raíz de compromiso. Aplicar políticas de acceso estrictas.	EMAIL/TICKET LLAMADA AISLAR
		Si la conexión está autorizada, notifique al socio de TI.	Si el Socio responde a nuestra llamada y confirma autorizado, o actual incidente o incidentes anteriores son resueltos antes de la convocatoria el SOC no aislará el dispositivo.	EMAIL/TICKET LLAMADA

SERVICIOS DE CYBERSOC					
Servicio		SLA		Reportes y Accesos	
Monitoreo de salud de la plataforma		Disponibilidad diaria 24x7x365		Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.	
Monitoreo avanzado tiempo real y correlación de eventos de seguridad		Disponibilidad diaria 24x7x365		Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.	
Cyber Threat Intelligence (Inteligencia de Ciberseguridad)		Disponibilidad diaria 24x7x365		Informe de Inteligencia periódico.	
Threat Hunting		Disponibilidad diaria 24x7x365		Atención de casos de seguridad avanzados	
Alerta Temprana		Disponibilidad diaria 24x7x365		Envío de alertas de acuerdo con la matriz de comunicación.	
Portal de Supervisión		Disponibilidad diaria 24x7x365		Acceso al Dashboard personalizado de reporte.	
Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Preparación	Tiempo promedio de	Tiempo promedio de contención	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de repercusiones

	detección e inicio del análisis				
Permanente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.
Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365 2 horas de atención como plazo máximo en Lima Metropolitana					
Registro de tickets de mesa de ayuda					
Tiempo máximo de registro del incidente, desde que son reportados		15 minutos			

8. OTRAS CONSIDERACIONES

Es responsabilidad del contratista adoptar todas las medidas de seguridad para la ejecución del servicio, no siendo responsabilidad de la Entidad cualquier accidente que pudiera presentarse por la no observancia de lo que norma al respecto.

9. REQUISITOS DEL PROVEEDOR Y SU PERSONAL

9.1. Requisitos del proveedor

- ✓ El postor deberá tener su Registro Nacional de Proveedores (RNP) vigente, a fin de poder contratar con el estado.
- ✓ El postor deberá tener Registro Único de Contribuyente (R.U.C.)
- ✓ El postor deberá contar con al menos 2 certificaciones de soluciones de Ciberseguridad.
- ✓ El postor deberá tener un centro de Atención al Cliente 24x7 de tipo call center.
- ✓ El postor adjudicado deberá ser **socio, partner o distribuidor autorizado**¹⁵ de la solución ofertada.
- ✓ La empresa deberá disponer de todos los equipos y herramientas de trabajo necesarios a ser utilizadas durante la prestación del servicio.
- ✓ El ejecutor deberá de contar con un sólido equipo de trabajo, el mismo que deberá garantizar el desarrollo del trabajo solicitado en el plazo y horarios establecidos.

16

Acreditación centro de atención al cliente:

Para acreditar certificaciones de soluciones de ciberseguridad se aceptarán: i) copias simples de los certificados oficiales emitidos por la entidad autorizada o documentos de designación formal o, ii) carta del fabricante o representante local de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado y se precise las certificaciones de soluciones de ciberseguridad con las que cuenta.¹⁶

Para acreditar ser socio, partner o distribuidor autorizado por el fabricante, deberá presentar copia de carta del fabricante o representante local del fabricante de las de soluciones de ciberseguridad en donde se acredite al postor como socio, partner o distribuidor autorizado.¹⁷

Para acreditar el centro de atención al cliente 24x7, el postor deberá presentar una declaración jurada que certifique la disponibilidad de un centro de atención al cliente con servicio continuo (24x7).

Estos documentos deberán ser presentados para el perfeccionamiento del contrato.¹⁸

9.2. Requisitos del Personal propuesto:

El proveedor debe acreditar que cuenta con los siguientes especialistas:

- **Un (01) jefe de Proyectos.**
Formación Académica, capacitación y otros:
 - Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio.

¹⁵ Ajuste realizado en merito a la absolución de la Consulta N°5 y 9

¹⁶ Ajuste realizado en merito a la absolución de la Consulta N°4

¹⁷ Ajuste realizado en merito a la absolución de la Consulta N°9

¹⁸ Ajuste realizado en merito a la absolución de la Consulta N°5

- Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.
- Certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC) y/o Certified Cyber Security Management Professional ISO 27032 (La presentación de cualquiera de los certificados mencionados es opcional)¹⁹
- Participación en curso o taller "Gestión de Ciber Crisis" con un mínimo de 08 horas lectivas.

Experiencia:

- Experiencia no menor de tres (03) años como Jefe o Gestor de Proyectos de soluciones de Ciberseguridad.

17

- **Un (01) Operador de Servicio**

Formación Académica, capacitación y otros:

- Técnico profesional Titulado y/o Título o Bachiller profesional en ingeniería en redes y comunicaciones y/o telecomunicaciones y/o sistemas y/o informática.²⁰
- Certificación técnica vigente en CEH V12 - Certified Ethical Hacker y/o Ethical Hacking Professional Certification (CEHPC)²¹.
- Participación en curso o taller "Gestión de Ciber Crisis" con un mínimo de 08 horas lectivas.

Experiencia:

- Experiencia no menor de tres (03) años como especialista en soluciones de Ciberseguridad.

El jefe de Proyectos será el responsable para realizar las coordinaciones con el Área de Infraestructura Tecnológica de la institución.

El jefe de Proyectos participará en la ejecución del servicio, y realizará las coordinaciones necesarias para que los operarios u otro personal operativo pueda ingresar a la entidad en forma adicional.

Acreditación:

Los documentos que acrediten el perfil señalado corresponden a lo siguiente:

- La formación académica se acreditará con copia simple del título profesional.
- La experiencia se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- En el caso de la colegiatura y la experiencia del personal, solo será acreditada al momento del inicio de la participación efectiva del profesional en la ejecución del contrato.
- Las acreditaciones de las certificaciones solicitadas para el personal propuesto deberán ser presentadas como parte de los documentos requeridos para el perfeccionamiento del contrato.

En caso de reemplazo del personal, éste deberá tener un perfil igual o superior al previsto en los términos de referencia, el mismo que deberá ser aprobado por el área usuaria del servicio. Asimismo, este evento deberá ser comunicado previamente y de manera formal por mesa de partes del Congreso de la República.

¹⁹ Ajuste realizado en merito a la absolución de la Observación N°2 y 10 y Consulta N°22.

²⁰ Ajuste realizado en merito a la absolución de la Consulta N°24

²¹ Ajuste realizado en merito a la absolución de la Consulta N°23

10. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo para la ejecución del servicio es de setecientos treinta (730) días calendarios, contados a partir del día siguiente de la implementación del servicio.

El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la firma del contrato. Este proceso deberá concluir con la suscripción de un acta de culminación de implementación, documento que marcará el inicio oficial del período de ejecución del servicio, conforme a los plazos establecidos.

11. PLAN DE TRABAJO

El contratista deberá entregar en un plazo máximo de quince (15) días calendario contados a partir del día siguiente de la firma del contrato, el plan de trabajo que incluya el cronograma de actividades para la implementación del “Servicio de suscripción de plataforma de Cyber SOC delegada tipo Soar para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la Republica”.

12. ENTREGABLES

ENTREGABLE	PLAZO DE ENTREGA
Primer Entregable: Informe de Implementación de la Solución	Como máximo a los 7 días calendarios contados a partir de suscrita el acta de culminación de la implementación del servicio.
Segundo Entregable: Informe anual del servicio -1er año	Como máximo a los 7 días calendario culminado los 365 días calendarios de iniciado el servicio.
Tercer Entregable: Informe anual del servicio – 2do año	Como máximo a los 7 días calendario culminado los 730 días calendarios de iniciado el servicio.

19

13. FORMA DE PAGO

El pago se efectuará en tres (03) armadas después de emitida la conformidad por parte del Área de Infraestructura Tecnológica y refrendado por el Departamento de Tecnologías de la Información, efectuándose según siguiente detalle:

Entregable	Porcentaje de pago	Condición de pago
01	40% del monto total de la prestación	A la conformidad del Primer Entregable.
02	30% del monto total de la prestación	A la conformidad del Segundo Entregable.
03	30% del monto total de la prestación	A la conformidad del Tercer Entregable.

Asimismo, para el pago el contratista deberá presentar:

- comprobante de pago

14. CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información luego de la recepción y revisión de los entregables.

14.1. DEL PRIMER ENTREGABLE.

La conformidad será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información luego de:

- La entrega del Acuerdo de Nivel de Servicios - ANS.
- La entrega del Plan de Trabajo y Cronograma de Actividades.
- La verificación del cumplimiento de las actividades correspondientes a la prestación principal.
- La recepción y validación del informe técnico correspondiente a la etapa de instalación, configuración y pruebas de la solución.

14.2. DEL SEGUNDO Y TERCER ENTREGABLE.

La conformidad del segundo y tercer entregable será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información previa recepción y validación del informe anual del servicio.

15. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad le aplicará automáticamente una penalidad por mora por cada día de retraso. La penalidad se considerará de acuerdo a lo estipulado en el Artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo vigente en días}}$$

Donde F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F: 0.40.
- Para plazos mayores a sesenta (60) días:
 - Para bienes, servicio y consultorías: F = 0.25.
 - Para obras: F = 0.15.

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso. Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En calificación del retraso como justificado, no da lugar al pago de gastos generales de ningún tipo.

16. OTRAS PENALIDADES

En caso se incurra en el incumplimiento de las prestaciones relacionadas al servicio, las penalidades se considerarán de acuerdo a lo estipulado en el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

- De acuerdo con el artículo 163 del Reglamento se pueden establecer penalidades distintas al retraso o mora en la ejecución de la prestación, las cuales deben ser objetivas, razonables, congruentes y proporcionales con el objeto de la contratación.
- Para dicho efecto, se debe incluir un listado detallado de los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Por día de atraso en la entrega del Informe de Implementación de la Solución.	1 % de una UIT por cada día de atraso.	Mediante acta de culminación de la implementación del servicio.
2	Por día de atraso en la entrega del Acuerdo de Nivel de Servicio – ANS (Service Level Agreement - SLA)	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
3	Por día de atraso en la entrega del Plan de trabajo	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria.
4	Por día de atraso en la entrega Informe anual del servicio.	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria.

17. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.

18. CONFIDENCIALIDAD

El contratista se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita del Congreso de la República, toda información que le sea suministrada por ésta última y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del presente Contrato.

El contratista deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida revelar a terceros.

Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución del contrato, durante su ejecución y la producida una vez que se haya concluido el contrato.

Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista.

Asimismo, aun cuando sea de índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del Congreso de la República.

19. ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios,

accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

22

20. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

21. LUGAR DE EJECUCIÓN

Jirón Huallaga 358 - Cercado de Lima - Lima. Horario de atención desde las 9:00 hasta las 17:00 horas.

22. SISTEMA DE CONTRATACION

El sistema de contratación es de suma alzada.

23. REQUISITOS DE CALIFICACIÓN

B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<u>Requisitos:</u> <u>Jefe de Proyectos:</u> <ul style="list-style-type: none"> Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio. <u>Operador de Servicio:</u> <ul style="list-style-type: none"> Técnico profesional Titulado y/o Título o Bachiller profesional en ingeniería en redes y

	<p>comunicaciones y/o telecomunicaciones y/o sistemas y/o informática.²²</p> <p><u>Acreditación:</u></p> <p>El título será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <div> <p>Importante para la Entidad</p> <p><i>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.</i></p> <p><i>Incluir o eliminar, según corresponda. Sólo deberá incluirse esta nota cuando la formación académica sea el único requisito referido a las calificaciones del personal clave que se haya previsto. Ello a fin que la Entidad pueda verificar los grados o títulos requeridos en los portales web respectivos.</i></p> </div> <p>En caso de títulos no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p><u>Jefe de Proyectos:</u></p> <p>Mínimo de ocho (08) horas lectivas, en participación en curso o taller “Gestión de Ciber Crisis.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias o certificados según corresponda</p> <p><u>Operador de Servicio:</u></p> <p>Mínimo de ocho (08) horas lectivas, en participación en curso o taller “Gestión de Ciber Crisis</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias o certificados según corresponda</p> <div> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p><u>Jefe de Proyectos:</u></p> <ul style="list-style-type: none"> Experiencia no menor de tres (03) años como jefe o gestor de proyectos de soluciones de Ciberseguridad. <p><u>Operador de Servicio:</u></p> <ul style="list-style-type: none"> Experiencia no menor de tres (03) años como especialista en soluciones de

²² Ajuste realizado en merito a la absolución de la Consulta N°24

	<p>Ciberseguridad.</p> <p><u>Acreditación:</u> La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div> <p>Importante</p> <ul style="list-style-type: none"> Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases. </div>
C	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'500,000.00 (Un Millón Quinientos Mil con 00/100 Soles), por servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: servicios de soluciones y/o implementación de soluciones de seguridad y ciberseguridad (antivirus y/o antispam y/o XDR y/o EDR), soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática y/o soluciones de respaldo y restauración de información para entornos físicos o virtualizados y/o servicio de hackeo ético y/o servicio de ethical hacking y/o servicio de ejecución de ethical hacking y/o servicio para el análisis de vulnerabilidades y/o servicio de análisis de vulnerabilidades y/o servicio de pruebas de penetración y/o servicio para el análisis de ciberseguridad.²³</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago²⁴, correspondientes a un máximo</p>

²³ Ajuste realizado en merito a la absolución de la Consulta N°1, 3 y 38

²⁴ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

“... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”
(...)

	<p>de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo correspondiente, referido a la Experiencia del Postor en la Especialidad</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo correspondiente.</p> <p>Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad</p>
--	--

“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.