PROGRAMA DE INNOVACIÓN, MODERNIZACIÓN TECNOLÓGICA Y EMPRENDIMIENTO

ESPECIFICACIONES TÉCNICAS

SERVICIO DE MONITOREO Y CONTROL DE SEGURIDAD GESTIONADA - SOC

1. ANTECEDENTES

El ITP fue creado en 1979 mediante el Decreto Ley Nº 22642 con la competencia de realizar las investigaciones tecnológicas para el óptimo aprovechamiento de los productos hidrobiológicos provenientes del mar, de los ríos y de los lagos y destinados al consumo humano directo. En 1981, mediante el Decreto Legislativo Nº 92, el Gobierno Promulgó la Ley del Instituto Tecnológico Pesquero – ITP, este decreto establece que la finalidad del ITP es realizar investigaciones científicas y tecnológicas relacionadas con el manipuleo, la transformación y conservación de los recursos hidrobiológicos del mar y de las aguas continentales, con miras a lograr el racional aprovechamiento integral de los mismos y la óptima calidad de los productos que se obtengan; así como colaborar a elevar el nivel nutricional de la población, mediante la elaboración de productos de alto valor nutritivo y sin que el cumplimiento de sus fines, el ITP incide o duplique las investigaciones que realicen otras instituciones similares, con las cuales mantendrá la debida y adecuada coordinación.

En 2012, mediante la Ley Nº 29951, Ley de Presupuesto del Sector Público para el Año Fiscal 2013, se cambia la denominación por Instituto Tecnológico de la Producción (ITP) para "ampliar los servicios de investigación, desarrollo, innovación, adaptación, transformación y transferencia tecnológica, así como promover en el sector productivo el consumo de recursos hidrobiológicos, productos agroindustriales y otros productos industriales de competencia del sector producción; y, efectuar su promoción y, cuando fuera necesario, la comercialización y distribución de los mismos". Asimismo, se dispuso la adscripción al ITP de los CITE de naturaleza pública.

En 2015, mediante Decreto Legislativo Nº 1228, se establece un nuevo marco normativo para los Centros de Innovación Productiva y Transferencia Tecnológica – CITE, estableciendo determinadas funciones para el ITP y su Consejo Directivo, adicionales a las establecidas mediante el Decreto Legislativo Nº 92. Actualmente, la red CITE está conformada por 18 CITE privados, 27 CITE públicos y 2 unidades técnicas que atienden a los siguientes sectores económicos o cadenas productivas: i) agroindustrial; ii) cuero y calzado; iii) pesquero y acuícola; iv) textil-camélidos; y v) madera y forestal.

En 2018, mediante Decreto Legislativo N° 1451, se realizan precisiones en la Denominación, Competencia, Funciones y Naturaleza de diversas entidades, entre ellas el ITP, modificando los artículos 1, 2 y 4 del Decreto Legislativo N° 92, Ley del Instituto Tecnológico Pesquero.

En 2020, mediante Decreto de Urgencia N° 013-2020, que promueve el Financiamiento de la MiPyME, Emprendimientos y Startups, se realizan precisiones sobre el alcance de los servicios del ITP con la finalidad de fortalecer la prestación de servicios tecnológicos en la forma de capacitación, asistencia técnica, asesoría especializada para la adopción de nuevas tecnologías, soporte productivo, investigación, desarrollo e innovación productiva y transferencia tecnológica que brinda el Estado.

El 23 de julio de 2021, se suscribió el Contrato de Préstamo N° 5287/OC-PE entre la República del Perú y el Banco Interamericano de Desarrollo para contribuir a la financiación y ejecución del Programa de Innovación, Modernización Tecnológica y Emprendimiento, cuyo objetivo general es aumentar la productividad empresarial mediante una mayor inversión privada en actividades de innovación.

Para alcanzar el objetivo general, el Programa considera los siguientes objetivos específicos:

(a) Aumentar la inversión en innovación y el desarrollo de innovaciones en empresas establecidas beneficiarias;
(b) Aumentar el financiamiento temprano para promover el crecimiento de nuevas empresas innovadoras beneficiarias;
(c) Reducir las brechas productivas de las MIPYMEs beneficiarias
(d) Mejorar la orientación sectorial y regional de las políticas de innovación

Para ello, el Programa cuenta con tres componentes:

- Componente 1: Incentivos a la inversión privada en innovación
- Componente 2: Financiamiento temprano para capital emprendedor
- Componente 3: Modernización tecnológica de MIPYMES

Al respecto, el Componente 3 busca cerrar brechas tecnológicas de las MIPYMES a través de acciones de oferta y demanda en tres (3) áreas:

- Subcomponente 3.1. Desarrollo del mercado de servicios de digitalización para MIPYMES
- Subcomponente 3.2. Desarrollo de mercado de servicios de evaluación de la conformidad para MIPYMES
- Subcomponente 3.3. Desarrollo del mercado de servicio de extensionismo tecnológico

En el marco del Subcomponente 3.3, se encuentra prevista la actividad 3.3.2. Proyectos para la implementación Modelo de gestión de la red CITE basado en resultados, la cual prevé la implementación en el ITP y la Red CITE, de un modelo de gestión basado en resultados, a través de la implementación de un centro de coordinación optimizado por la RED CITE en el ITP para la ejecución de un nuevo modelo de gestión. Asimismo, como parte del fortalecimiento de los CITE públicos, se busca, a través de la transformación digital de los procesos centrales, automatizar su gestión con tecnologías maduras, y posteriormente desarrollar servicios digitales para las unidades productivas.

En dicho contexto, se prevé la implementación de plataformas tecnológicas para monitorear los resultados de las empresas asistidas, las cuales se integran de diversos componentes de software, como son: aplicaciones, servicios, bases de datos, reporteadores, gestores de contenidos, entre otros; algunos de ellos en código abierto y otros licenciados. Estas plataformas deben contar con una capa de seguridad que permita el funcionamiento eficiente, optimizando la gestión de incidentes de seguridad al reducir el tiempo de respuesta y minimizar la carga de trabajo manual, así como detectar y responder a amenazas en tiempo real.

La presente consultoría se financiará con cargo al Convenio de Transferencia de Recursos para "LA IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE LA RED CITE BASADO EN RESULTADOS", suscrito en el marco del Contrato de Préstamo N°5287/OC-PE, subactividad 3.3.2 ROP del Programa.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas

y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento, de conformidad con el artículo 8 de la Ley.

En tal sentido, mediante Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI, se aprueba los Lineamientos para la formulación del Plan de Gobierno Digital, estableciendo en su artículo 3 que el Plan de Gobierno Digital se constituye en el único instrumento para la gestión y planificación del Gobierno Digital de la Administración Pública, y es aprobado por el titular de la entidad para un periodo mínimo de tres (03) años, debiendo ser actualizado y evaluado anualmente.

La Oficina de Tecnologías de la Información (OTI), que tiene por función proveer soporte técnico de recursos tecnológicos necesarios a las áreas usuarias de la entidad, viene realizando actividades para modernizar sus servicios, con el propósito de simplificar e integrar la función organizacional, así como proporcionar servicios eficientes y de mayor valor para sus usuarios. Asimismo, está comprometida a proporcionar servicios que satisfacen un estándar de calidad determinado y aceptable, respondiendo efectivamente a las necesidades y requerimientos de servicios tecnológicos en la institución. Para ello, es primordial contar una solución avanzada para la gestión de la seguridad cibernética que combine las capacidades de un Security Operations Center (SOC) con la automatización y orquestación de la respuesta ante incidentes.

Esta iniciativa se enmarca dentro de las disposiciones establecidas en el Plan de Gobierno Digital, el cual tiene como objetivo fundamental promover la eficiencia, transparencia y modernización de los servicios gubernamentales a través de la integración de tecnologías de la información y comunicación. Asimismo, se alinea con las directrices y regulaciones vigentes en materia de Gobierno Electrónico y Buen Gobierno, procurando garantizar la accesibilidad, seguridad y protección de datos en todos los procesos y servicios digitales ofrecidos por la institución.

En este contexto, es necesario contar con una suscripción de plataforma de CYBER SOC tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada, que garantice la continuidad operativa y protección de los activos digitales del ITP Red CITE.

2. OBJETIVO DE LA CONTRATACIÓN

Contar con una plataforma de **Cyber SOC delegada basada en tecnología SOAR**, complementada con servicios de **XDR, seguridad gestionada y ethical hacking**, que fortalezca la postura de ciberseguridad del ITP mediante la automatización de procesos, detección avanzada, respuesta oportuna y mitigación eficiente de incidentes cibernéticos, asegurando la continuidad operativa, la protección de los activos digitales y la resiliencia institucional frente a amenazas emergentes.

2.1. OBJETIVOS ESPECÍFICOS

- Automatizar y orquestar los procesos de respuesta a incidentes de seguridad, integrando las herramientas existentes y nuevas capacidades de detección (XDR), para reducir significativamente los tiempos de respuesta y contención ante amenazas cibernéticas.
- Fortalecer la visibilidad y el monitoreo continuo en tiempo real, mediante la correlación de eventos, análisis de comportamiento y técnicas avanzadas de detección que permitan anticiparse a vulnerabilidades o ataques dirigidos.
- Delegar funciones operativas críticas de ciberseguridad a un proveedor especializado, asegurando un servicio gestionado de alta disponibilidad (24/7), que garantice

cobertura permanente ante eventos de seguridad, reduciendo la carga operativa interna.

- Capacitar al personal técnico del ITP en el uso de tecnologías SOAR y XDR, promoviendo el desarrollo de competencias en automatización de tareas, análisis de amenazas y respuesta a incidentes complejos, incrementando la eficacia operativa y la madurez en la gestión de ciberseguridad.
- Ejecutar servicios de Ethical hacking de forma anual, como mecanismo proactivo de validación de la postura de seguridad, identificando brechas y vulnerabilidades que puedan comprometer la integridad, disponibilidad o confidencialidad de los sistemas institucionales.

3. ACTIVIDADES A REALIZAR

Las actividades que, como mínimo, deberá realizar el proveedor para el logro del objetivo del presente requerimiento, son las siguientes:

3.1. GENERALES

a) El Instituto Tecnológico de la Producción (ITP) requiere contratar un centro de operaciones de ciberseguridad altamente especializado en la modalidad 24x7, conformado por infraestructura y profesionales expertos en ciberseguridad, procesos automatizados y tecnología con la capacidad de monitorear, detectar, contener, responder y automatizar frente a eventos e incidentes de ciberseguridad.

b) El CyberSOC debe contemplar la provisión de servicios como: Monitoreo Proactivo de Eventos de Seguridad, Plataforma de Correlación Extendida para la Detección y Respuesta a Incidentes, Protección de Riesgos Digitales, Equipo Respuesta ante Incidentes.

c) Las suscripciones de licencias necesarias para la operatividad de las plataformas y servicios del CyberSOC, así como el mantenimiento y soporte del fabricante y del proveedor es por el periodo de veinticuatro (24) meses contabilizados a partir del día siguiente de activado el servicio. El proveedor brindará soporte y apoyo técnico (configuraciones, alertas y reportería) por el periodo contratado.

d) El proveedor debe brindar el servicio de monitoreo y respuesta de incidentes en modalidad de 24x7x365, a través de un CyberSOC propio.

e) El proveedor debe contar con un diseño de infraestructura, procesos y personal que permitan la continuidad ante un evento de desastre.

f) El proveedor deberá contar en el SOC con certificación vigente del estándar internacional de Seguridad de la Información ISO 27001.

g) El proveedor deberá contar con otros estándares internacionales como la certificación vigente de la ISO 9001 o la ISO 37001.

h) Durante el período del servicio, el proveedor debe contar con línea de comunicación gratuita 0800 o cualquier otra propia del proveedor siempre que dicho canal garantice disponibilidad, acceso directo, y gratuidad para el usuario final, para la atención de todos las consultas e incidencias.

i) El servicio comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará “requerimiento”.

j) El servicio debe incluir el análisis, actualización, corrección y documentación de fallas en las soluciones desplegadas para brindar el servicio.

3.2. PLATAFORMA DE CORRELACIÓN EXTENDIDA PARA LA DETECCIÓN Y RESPUESTA A INCIDENTES

a) El servicio debe contar con una plataforma capaz de integrar y correlacionar logs y eventos de diferentes fuentes tecnológicas.

b) Deberá contar con soporte del fabricante durante todo el tiempo de servicio.

c) El proveedor podrá integrar tecnologías de diferentes marcas para cumplir los requerimientos mínimos solicitados en las presentes especificaciones técnicas.

d) Se deberán considerar 1600 agentes endpoint.

e) Se deberá considerar una capacidad de procesamiento de 100 GB al día o 1000 EPS (Eventos por Segundo) como mínimo para la recepción de eventos de fuentes terceras diferentes al endpoint para la integración de dos (02) Firewalls, WAF y LA plataforma Google WorkSpace del ITP.

f) La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:

- Contar con la certificación SOC2 Tipo II o SOC2 Plus de AICPA, ISO 27001, ISO 27017, ISO 27018.
- Contar con doble factor de autenticación para el login.
- Permitir el acceso solo desde un rango de IP pública. Esta información la brindará el ITP durante la ejecución del servicio.

g) La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.

h) Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.

i) Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa.

j) Tener la capacidad de generar reportes personalizados, eligiendo los tipos de gráficos a incluir y personalizando los datos, filtros y atributos a incluir en cada gráfico o tabla.

k) Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola, además de mantener un historial de los reportes que han sido generados para su posterior consulta.

l) Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.

m) Protección contra exploits:

- Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.
- El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits.
- Deberá proteger la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado.
- La protección contra vulnerabilidades deberá ser independiente al CVE identificado, la solución deberá proteger cualquier intento de explotación incluyendo a vulnerabilidades de día cero que no tengan un CVE.
- Bloquear técnicas de explotación de vulnerabilidades, como mínimo Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.
- Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel.
- Capacidad de crear un snapshot (dump) de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.

- Prevención de técnicas de explotación que utilizan Java Deserialization, Kernel Integrity Monitor (KIM), Local Threat Evaluation Engine (LTEE), Reverse Shell Protection, Shellcode Protection, SO Hijacking Protection, Webshell.
- Todas las capacidades de prevención de exploits deberán estar disponibles de manera offline, sin necesidad de tener una conexión a la consola.

n) Protección contra malware

- Deberá contar con funcionalidades de antimalware de siguiente generación, entiéndase antimalware de siguiente generación como plataformas que utilizan algoritmos de aprendizaje de máquina (machine learning) para detectar y bloquear el malware; no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus.
- El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.
- Deberá ser capaz de detectar y bloquear cambios sospechosos en la imagen UEFI, que intentan comprometer el proceso de arranque del host, antes de que se cargue el sistema operativo.
- Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)
- Contar con un módulo de prevención contra ransomware que podrá ser configurado en modo normal y riguroso.
- Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.
- Deberá ofrecer protección contra scripts de tipo webshell.
- Deberá ser capaz de prevenir ataques basados en el Bypass del UAC (User Account Control) que intenten escalar privilegios.
- Deberá ser capaz de analizar datos de paquetes de red para detectar comportamientos maliciosos
- Capacidad para bloquear intentos sospechosos de reiniciar el equipo en modo seguro (Safe Mode Reboot) para evadir la seguridad del agente.
- Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.
- Capacidad para bloquear ataques que permitan a un contenedor tener acceso al sistema operativo del host (container escaping) para sistemas Linux.
- Capacidad de poder colocar los malware en una carpeta de cuarentena
- Capacidad de colocar en lista permitida los archivos o directorios, para exceptuar la inspección.
- Capacidad de realizar escaneos a demanda y programados, con el objetivo de identificar malware dormido en los endpoints.

o) Plataforma de Sandboxing

- El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado. Esta capacidad deberá estar disponible para sistemas Windows, MacOS, Linux y Android.
- El sandbox podrá ser del mismo fabricante que el agente de seguridad o un fabricante tercero integrado.
- El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- El sandbox deberá soportar el análisis de al menos 500 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso o superior.
- Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con las certificaciones SOC2 Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.

p) Control de dispositivos

- Debe permitir gestionar los puertos USB que permiten conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas con conexión USB.
- Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada) y número de serie.
- Las políticas generadas deben de poder asignarse a un endpoint en particular, a un grupo de endpoints y capacidad de integrarse a Active Directory para establecer políticas en base a grupos de LDAP.
- Debe permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.
- Capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente.
- Capacidad para controlar dispositivos conectados por Bluetooth, permitiendo configuraciones granulares, que permitan diferenciar tipos de dispositivos, al menos los siguientes: Smartphones, Dispositivos de audio y video, Periféricos, Dispositivos de imágenes, Weareables.
- Capacidad para controlar el acceso a impresoras conectadas a nivel de red.

q) Telemetría y Colección de Datos y Eventos

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:
  - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
  - Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
  - Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), solicitudes DNS, conexiones y desconexiones HTTP.
  - Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.
  - Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardado de llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado; nombre del valor o llave modificado; datos del valor modificado.
  - Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Toda la telemetría recolectada de los endpoints a través del agente deberá ser almacenada por al menos 30 días en formato “hot storage”, para permitir labores de cacería de amenazas por parte del analista.
- ITP cuenta con un servicio de NGFW Palo Alto, se solicita la integración con la solución para que pueda recolectar la siguiente información de soluciones NGFW de Palo Alto:
  - IP y puerto origen y destino, nombre de la aplicación en capa 7, país origen y destino, IP NAT de origen y destino, usuario origen (cuando el Firewall se encuentre integrado al Active Directory), Bytes enviados y recibidos, Paquetes enviados y recibidos, DNS Querys, información sobre tráfico DHCP.
  - Nombre y serial number de los Firewalls.
  - Nombre, tipo, categoría y severidad de la amenaza identificada.
  - Nombre del archivo transferido a través de una política de seguridad.
  - Logs de tráfico URL, detallando URL accedida, categoría, severidad, hora, IP origen/destino, usuario, país de la URL, User-Agent de los paquetes HTTP.
  - Tipo, categoría, marca, sistema operativo, fabricante del dispositivo origen y destino que genera tráfico de red; siempre y cuando esta información se encuentre disponible.
  - Información de conexiones VPN de Global Protect, tales como IP asignada, IP Pública, País origen, Duración de la sesión VPN, Método de conexión, Estado del login (fallido, exitoso), nombre del Portal VPN.
- Capacidad de recolectar logs de Firewalls Fortinet, Palo Alto Networks, Cisco, Checkpoint, Sophos, entre otros.
- Deberá recolectar eventos de Google Workspace vía API, tales como: eventos de Google Chrome, acciones administrativas de la consola, chat, login, reglas, Google Drive, tokens, cuentas de usuarios, alertas, metadata de correos electrónicos.
- Deberá recolectar eventos de Amazon S3, Amazon Cloudwatch, Azure Event Hub, Azure Network Watcher, GCP Flow Logs, GCP DNS Logs, GCP Audit Logs, GKE.

- Deberá recolectar eventos de AWS, Azure y GCP.
- Deberá recolectar eventos de Active Directory (Window Event Logs), tales como: búsquedas de LDAP, gestión de grupos y usuarios de dominio, gestionar de computadoras del dominio.
- Deberá recolectar eventos de Netflow en sus distintas versiones (v5, v9 o IPFIX) y podrá integrarse con equipos de red de los diferentes fabricantes estándar del mercado, siempre que estos generen flujos NetFlow o sus equivalentes (por ejemplo, sFlow o J-Flow).
- Deberá recolectar eventos de otras fuentes de diferentes marcas a través del protocolo Syslog, pudiendo soportar al menos los formatos CEF, LEEF, RAW.
- Deberá permitir la recepción de logs y/o eventos en distintos formatos o protocolos, alojados Servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux, tales como: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON.
- Para los archivos alojados en carpetas compartidas, la solución debe ser capaz de colectar los eventos en línea y/o vía batch definiendo la frecuencia en base a minutos, horas o días. Se aceptará como mínimo un periodo de retención de eventos de 30 días.
- Deberá contar con conectores directos a bases de datos MySQL, MSSQL, Oracle y PostgreSQL, para poder colectar información alojada en tablas de bases de datos.
- Deberá soportar el uso de agentes para equipos Linux, capaces de recolectar los logs nativos de sistemas Red Hat, Centos, Debian, Ubuntu, así como logs de Nginx.
- Deberá contar con agentes para equipos Linux, capaces de recolectar los logs nativos de sistemas Red Hat, Centos, Debian, Ubuntu, así como logs de Nginx.
- Deberá contar con agentes para equipos Windows, capaces de recolectar los logs de DNS, logs de DHCP, logs de servidores IIS y Nginx.
- Deberá contar con agentes para equipos Windows, capaces de recolectar los logs de Eventos de Seguridad Windows (que nativamente se ven en el Event Viewer)
- Deberá poder colectar logs o eventos utilizando API, ya sea mediante el uso de HTTP Collectors o Filebeat respetivamente.
- Capacidad para subir manualmente archivos CSV o JSON a la plataforma
- Deberá ser capaz de normalizar los eventos recibidos de las diferentes fuentes, utilizando parsing rules u otro método.
- Deberá realizar la colección de información de los dispositivos en las premisas mediante la implementación de una máquina virtual (colector). El colector también podrá ser desplegado en entornos nube.
- Los colectores deberán tener la capacidad de ser desplegados en Alta Disponibilidad.
- La plataforma deberá poder almacenar la información recolectada en formato raw log (log crudo) por al menos 30 días.
- La plataforma debe permitir el almacenamiento de información por cada tipo de fuente, con el fin de poder gestionar métricas y parámetros de almacenamiento.
- La plataforma debe permitir el indexado de los eventos colectados en un esquema de tablas que permitan la búsqueda y uso de estadísticas/métricas de cada campo normalizado.
- La plataforma debe permitir visualizar las métricas de espacio, promedio de ingesta diaria, promedio de ingesta total, fecha de última vez de colección, etc.
- La plataforma debe soportar un mínimo de 1000 datasets, asociados a cada fuente de datos.

r) Capacidades de Analítica y Detección de Amenazas

- Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia

gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.

- Deberá mostrar información de los procesos correlacionados en la secuencia gráfica, mostrando los siguientes datos: ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.
- Por cada proceso correlacionado en la secuencia gráfica del incidente se deberá mostrar lo siguiente:
  - Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso.
  - Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.
  - Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.
  - Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista.
  - Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.
  - Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.
  - Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado.
  - Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente.
  - Si el endpoint genera tráfico malicioso o sospechoso que pase por el Firewall de la Entidad, la solución deberá mostrar en la secuencia gráfica dicha correlación de eventos, especificando qué proceso del endpoint gatilló ese tráfico sospechoso o malicioso.
- Deberá tener más de 500 casos de uso automáticos de detección de amenazas complejas basadas en comportamiento y procesadas con inteligencia artificial.
- Deberá permitir crear reglas personalizadas de detección de amenazas, las cuales deberán estar basados en comportamientos de los usuarios y hosts, para ello deberá ser posible especificar en la regla uno o varios de los siguientes atributos: actividad de archivos (lectura, borrado, modificación, escritura); ejecución de procesos y línea de comando ejecutada; cambios en las claves de registro de Windows, especificando el nombre, valor de la clave de registro y tipo de operación (creación, lectura, edición); acceso a DLL de Windows; eventos de login o logout; interacción del endpoint con cualquier IP privada o pública, especificando el puerto origen y/o destino.
- Deberá permitir enriquecer las reglas de correlación con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad.
- Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.
- Deberá contar con capacidades de UEBA (User and Entity Behavior Analytics), siendo capaz de retener los eventos recolectados durante al menos 30 días y aprender una línea base o perfil de comportamiento de cada dispositivo y usuario.

- Los perfiles de comportamiento deberán de ser generados mediante el uso de algoritmos de aprendizaje de máquina no supervisado.
- A partir del comportamiento aprendido, el módulo de UEBA deberá ser capaz de alertar los siguientes comportamientos inusuales, que estén fuera del perfil base aprendido:
  - User agent sospechoso
  - Ejecución de comando Powershell sospechoso
  - Uso inusual de herramientas Systernals
  - Uso sospechoso de CURL
  - Servicio remoto iniciado desde una fuente inusual
  - Cantidad de interacciones de red inusuales
  - Query LDAP inusual
  - Creación de reglas de firewall inusuales
  - Sesión WinRM anómala
  - Proceso raro ejecutado en la institución
  - Elevación de privilegios con usuario SYSTEM de manera anómala
  - Firewall de Linux desactivado de manera anómala
  - Tarea programada creada de forma inusual
  - Ejecución de arp.exe anómala
  - Cantidad inusual de screenshots tomados
  - Conexión RDP inusual
  - Escaneo de puertos sospechoso
  - Creación de una máquina en el dominio
  - Creación de usuario con permisos de domain admin
  - Usuario imprime una cantidad inusual de archivos
  - Uso de aplicación no habitual
  - Cantidad inusual de solicitudes DNS generadas
  - Tráfico Kerberos y/o SMB generado desde un proceso no estándar
  - Subida de información anómala hacia internet
- El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.
- Todas las alertas de seguridad, asociadas a ataques y anomalías, deberán almacenarse en la consola por al menos 180 días.

s) Capacidades de Investigación y Threat Hunting

- Deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints:
  - Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
  - Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.
  - Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.
  - Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.
  - Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.
  - Actividad de autenticación al endpoint
  - Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.

        - Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
        - Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pye, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador.
        - Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
    - Deberá contar con un lenguaje propio para realizar consultas de la telemetría almacenada, deberá incluir al menos los siguientes criterios: Filtros por cada atributo recolectado del endpoint (procesos, archivos interacciones de red, login/logut, actividad en claves de registro y DLLs) con coincidencia total o parcial de cada atributo; uso operadores booleanos (and, or, not); operadores de comparación (igual, no igual, mayor que, menor que, mayor o igual que, menor o igual que); capacidad para especificar un límite de resultados (top 10, 20, 100, 500, 1000, personalización en general); operadores de comparación de datos; operadores matemáticos (promedio, contar, contar-distinto, máximo, mínimo, sumar); uso de expresiones regulares.
    - Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.
    - Deberá permitir realizar labores de cacería de amenazas permitiendo la búsqueda de información de los diferentes logs y eventos recolectados de otras fuentes externas al endpoint.
    - Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
    - La solución debe contar con columnas de los dashboards de visualización de datos y deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
    - Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
    - Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
    - Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando exista alguna coincidencia en el log (o logs) recolectados con la regla de búsqueda.

t) Capacidades de Gestión de Incidentes

- Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática.
- Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP.
- Deberá mostrar los hosts y usuarios asociados al incidente.
- Las alertas e incidentes de seguridad deberán tener una valoración cualitativa de al menos 4 niveles de severidad: bajo, medio, alto y crítico. Estos niveles de severidad podrán ser modificados de manera manual o automática.
- Tener la capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto de este.
- Debe tener la capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.

- Debe contar con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad (clasificados por su plataforma, etc.)
- Debe permitir asignar cada alerta de seguridad a un analista administrador de la consola, esta asignación se puede hacer de forma manual o automática en base a ciertos criterios de la alerta. Por cada asignación que se realicé se deberá notificar vía correo al analista.
- Cada incidente de seguridad debe tener un estado, tales como abierto, en proceso, cerrado, resuelto, o estados equivalentes.
- Debe permitir colocar un comentario por cada incidente, con el objetivo de llevar un seguimiento de este durante la investigación.
- Debe contar con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente.
- Debe tener un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- Deberá tener un motor automático de scoring de incidentes, que permitan dar una valoración cuantitativa en un puntaje de 0 a 100 en base a determinados criterios de cada alerta de seguridad, éste deberá de funcionar de manera paralela a la valoración cualitativa de los incidentes y alertas de seguridad.

u) Capacidades de Threat Intelligence

- Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API
- Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.
- Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)
- Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.
- Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.
- Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.
- Capacidad para integrarse a Google Maps vía API y extraer información contextual de la ubicación física de una dirección IP
- Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.

v) Capacidades de respuesta

- Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes.
- Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática.
- Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada.
- Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador

- Deberá ser capaz de hacer una búsqueda masiva en todos los endpoints en base al hash de un archivo o el path, con el objetivo de borrar dichos archivos de todos los endpoints.
- Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
- Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base al tipo de amenaza, como mínimo estas reglas deberán permitir las siguientes acciones: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint, ejecutar un script en el endpoint.
- Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
  - Listar procesos y archivos
  - Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux y MacOS).
  - Ejecutar scripts basados en Python
- Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrente.
- Deberá contar con una librería de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python.
- Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.
- Mostrar sugerencias para las remediaciones de un equipo comprometido.
- Capacidad de integración con un SIEM vía Syslog y plataformas SOAR.

w) Descubrimiento de activos

- Deberá contar con un mecanismo para descubrir dispositivos de la red sin el agente instalado.
- Permitir exceptuar los segmentos de red que no se desea escanear.
- Deberá contar con el licenciamiento adecuado para el descubrimiento de dispositivos en las diferentes sedes de la entidad.

x) Capacidades de visibilidad del endpoint

- Deberá poder generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS y Linux
- Deberá generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura.
- Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo)
- Deberá poder listar los autoruns, servicios y unidades o carpetas compartidas para el caso de Windows.
- Deberá mostrar los daemons para el caso de MacOS y Linux
- Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días.

y) Capacidades de Análisis de Vulnerabilidades

- Deberá mostrar las vulnerabilidades de los sistemas operativos de los endpoints, ofreciendo detalles de los CVEs, incluyendo el nivel de severidad y métricas según la base de datos de vulnerabilidades de NIST.
- Deberá mostrar los KB instalados por cada endpoint.
- Deberá mostrar las vulnerabilidades a nivel de las aplicaciones instaladas en sistemas Linux y Windows.

- Deberá permitir exportar en un archivo leíble en Excel todas las vulnerabilidades identificadas en cada endpoint.

z) Características del agente

- Deberá ser un agente ligero que incluso pueda convivir con cualquier otro software instalado en el endpoint.
- Soporte para las siguientes versiones de sistemas operativos:
  - Windows 10 y versiones superiores
  - Windows Server 2012 y superior
  - MacOS 12.x y superior
  - Linux, distribuciones: CentOS 6.7 y superior, Debian 8 y superior, Red Hat Enterprise Linux 6.7 y superior, Suse for Enterprise 12.1 y superior, Ubuntu Server 12 y superior, Amazon Linux 2017 y 2018, Oracle Linux 6 y superior.
  - Android y iOS.
- No debe requerir el reinicio del equipo para que el agente se encuentre operativo.
- Deberá estar protegido ante intentos de desinstalación o manipulación del agente.
- Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.

3.3. PLATAFORMA DE AUTOMATIZACIÓN, ORQUESTACIÓN Y RESPUESTA (SOAR)

a) Debe estar licenciada para un (01) analista por un periodo de veinticuatro (24) meses contabilizados a partir del día siguiente de activado el servicio.

b) Debe incluir una tecnología SOAR para la automatización de respuesta ante incidentes. Esta tecnología deberá ser totalmente integrable con soluciones SIEM.

c) Debe soportar investigaciones interactivas que permitan la colaboración, la revisión histórica y la documentación en tiempo real de todas las acciones.

d) Debe soportar flujos de trabajo y secuencias de comandos modulares.

e) Debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.

f) Debe soportar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones.

g) Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar o manualmente ejecutar en tiempo real según los requisitos del caso de uso.

h) La automatización se debe lograr utilizando flujos de trabajo modulares y scripts.

i) Las tareas automatizadas se deben visualizar en flujos de trabajo basados en interfaz gráfica y ser impulsadas por scripts de automatización en el backend.

j) Cualquier script puede ser adjunto a una tarea automatizada dentro de flujos o playbooks visuales. La cantidad de playbooks a configurar será de 10 aparte de los que vienen por defecto en la solución y las tecnologías a integrarse con el SOAR son las siguientes:

- Solución de Correlación Extendida para la Detección y Respuesta a Incidentes
- Solución de Firewall Perimetral.
- Solución de Firewall de Aplicaciones (WAF).
- Solución de Correo Electrónico.

k) Debe incluir una función "BYOI" o similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard.

l) Debe incluir nuevas integraciones de productos y automatizaciones automáticas como parte de actualizaciones de contenido.

m) La herramienta debe contar con un mínimo de 100 casos de usos o playbooks de respuesta a incidentes

n) Los playbooks deben ser de código abierto.

o) Debe permitir crear playbooks copiando flujos existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks

p) Debe permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente.

q) Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de collection de datos o tareas condicionadas.

r) Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociado al playbook correspondiente

s) Los playbooks también pueden ser ejecutados como tareas y ejecutados en tiempo real para casos de uso como health checks.

t) La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad.

u) La herramienta debe de tener la capacidad de ejecutar flujos/playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario.

v) Las acciones de los playbooks deben ser totalmente personalizables por el usuario y deben poder utilizarse para adherirse a cualquier requisito de proceso organizacional o industrial.

w) La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica.

x) Debe incluir una instancia donde los usuarios puedan ver evidencia y documentación de incidentes anteriores, la herramienta debe agregar información de investigaciones pasadas.

y) Debe detectar alertas redundantes y agregar incidentes duplicados en uno solo, desplegando los datos de la agregación realizada.

z) Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parte del incidente, tareas terminadas, comandos de interacción, evidencia, chats (opcional), notas y tareas de playblooks.

aa) Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook.

bb) Toda la información a recolectar debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia.

cc) Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos deben estar asociados a las distintas fases del ataque o kill chain.

dd) Los analistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque.

ee) El producto debe proveer herramientas de colaboración entre usuarios, debe agrupar a todos los usuarios asociados a un incidente dentro del mismo o en un cuarto de guerra.

ff) Los analistas deberán poder colaborar uno con otro usando la línea de comando dentro de la investigación de un incidente.

gg) La colaboración puede ser extendida a grupos o equipos de trabajo terceros, como usuarios internos, grupos de recursos humanos, PR, o terceros.

hh) Las tareas realizadas dentro de incidentes deben de ser respaldadas para que sirvan de documentación para entrenar a nuevos analistas

ii) La herramienta debe incluir un Canvas de investigación dentro de la solución ofertada o como componente adicional que pueda integrarse, el cual mediante machine learning pueda crear un mapa de ataques en tiempo real.

jj) Los resultados de los canvas deben ser exportados y compartidos por equipos ejecutivos e interesados.

kk) El producto debe correlacionar bidireccionalmente indicadores e incidentes. Los usuarios deben poder ver todos los indicadores de un incidente y viceversa.

ll) Debe ser posible importar y exportar indicadores en archivos STIX.

3.4. SEGURIDAD GESTIONADA

a) El servicio de seguridad gestionada deberá contemplar de forma integral la gestión proactiva de toda la plataforma de Cyber SOC delegada.

b) 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.

c) 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 al Cybersecurity Framework (CSF) de la NIST.

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

3.4.1. MONITOREO PROACTIVO DE EVENTOS DE SEGURIDAD

b) El proveedor a través del CyberSOC se encargará de la monitorización y análisis de información permanente de los eventos e incidentes de seguridad registrados en la plataforma de detección, así como las alertas de incidentes, creación y seguimiento de los tickets de atención.

c) El proveedor será el encargado de la administración de la plataforma Extendida de Detección y Respuesta a Incidentes.

d) El proveedor deberá alertar ante un evento que sea catalogado como crítico al área o persona encargada por parte de ITP para tomar las medidas respectivas, ya sea mediante llamada o correo.

e) El proveedor del servicio CyberSOC debe notificar sobre:

- Alertas en las que se requieran investigaciones internas para su confirmación.
- Incidentes de seguridad confirmados que requieren tratamiento.
- Las alertas y los incidentes deben calificarse por su gravedad y prioridad de tratamiento, entendiéndose que puede haber incidentes de baja gravedad, pero

cuyo tratamiento puede ser prioritario, por ejemplo, debido a la volatilidad de la información de que se trate.

3.4.2. ESPECIALISTA TECNICO RESIDENTE

a) Durante la vigencia de las suscripciones se deberá incluir un Especialista Técnico Residente para el análisis técnico, uso de metodología, corrección y solución a las vulnerabilidades en sistemas operativos, servidores, red en layer 2, layer 3, NGFW, malware, ransomware, Active Directory, DNS, ambientes en desarrollo y producción, siendo el horario de las actividades del especialista residente de manera presencial, el horario laboral es de 08:00 a 18:00 horas de lunes a viernes en la sede Callao ubicada en Carretera a Ventanilla KM 5.2 Callao. El Especialista Técnico Residente iniciará sus actividades al día hábil siguiente de firmada el acta de activación del servicio.

b) Deberá realizar ejercicios de hacking ético, pentesting y la priorización de vulnerabilidades, amenaza persistente avanzada(APT), tácticas técnicas y procedimiento(TTP), configuraciones débiles y anomalías. Estas actividades se deberán realizar de manera continua por parte del contratista.

c) Deberá realizarlas siguientes actividades:

- 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.

3.4.3. NIVELES DE SERVICIOS ESTABLECIDOS (SLA)

a) Los acuerdos de nivel de servicio establecidos tienen por finalidad asegurar la calidad en la ejecución del servicio. Para tal efecto, se establecerán los tiempos de notificación y tiempo de entrega de acciones correctivas, que el proveedor debe cumplir como parte del servicio.

b) Será considerado un incidente de seguridad: “un evento que afecte negativamente la seguridad de la información y/o genera algún impacto en los servicios de TI preexistentes.

c) No serán considerados incidentes de seguridad aquellos relacionados a componentes externos al servicio y/o aplicación web bajo monitoreo, tales como: problemas de hardware, problemas de energía, problemas de plataforma de virtualización u otros no relacionados a la seguridad informática.

d) En la tabla N° 01 se muestra los tiempos empleados por nivel de criticidad del incidente:

Nivel de criticidad del incidente	*Notificaciones de incidentes*	*Entrega de Acciones Correctivas*
Crítica	=< 30 minutos	=< 60 minutos
Alta	=< 60 minutos	=< 120 minutos
Media	=< 120 minutos	=< 240 minutos
Baja	=< 240 minutos	=< 360 minutos

Tabla N° 01: Tiempos para resolución de incidente de seguridad por nivel de criticidad

e) En la tabla N° 02 se muestra la definición de los niveles de criticidad del incidente empleados en la tabla N° 01.

Nivel de criticidad del incidente	*Descripción*
Crítica	Incidente que genera afectación total y/o parcial a la operación del negocio. Este tipo de incidente ha dejado inoperativo y tiene un alto impacto de compromiso en la seguridad de algun servicio.
Alta	Incidente que genera afectación de servicios de TI. Este tipo de incidente ha dejado inoperativo total o parcialmente algún servicio.
Media	Incidente que pueda generar un nivel de afectación de alguno de los activos de TI.
Baja	Incidente que no afecta alguno de los activos de TI, pero debe ser tratado y/o mitigado en una ventana de mantenimiento programado.

Tabla N° 02: Definición de los niveles de criticidad del incidente

f) En la tabla N° 03 se muestra la definición de los tipos de tiempos empleados en la tabla N° 01.

Nivel de criticidad del incidente	*Descripción*
Notificación de incidentes	Tiempo transcurrido desde que se identifica un incidente y el proveedor, previa evaluación de criticidad e impacto, alerta o comunica el incidente a ITP
Entrega de acciones correctivas	Tiempo transcurrido entre la notificación del incidente por parte del proveedor hasta la entrega de manera verbal y/o correo electrónico, de las acciones necesarias para la correcta resolución y/o mitigación del incidente en curso.

Tabla N° 03: Definición de los tipos de tiempos

g) Cada vez que ocurra un incidente de seguridad y finaliza la atención del mismo, el proveedor debe entregar un informe técnico detallado en formato físico o electrónico. El informe se entregará en un plazo no mayor de cinco (05) días calendario, luego de

finalizada la atención. Dicho informe debe contener como mínimo lo siguientes puntos:

- Causas del origen del incidente de seguridad y/o avería(s).
- Diagnósticos, escalamiento, solución y tiempos empleados.
- Recomendaciones para mejora de la postura de seguridad.
- Lecciones aprendidas.
- En caso se superen las métricas señaladas en la tabla N° 01, el proveedor debe incorporar el plan de acción a desplegar para optimizar este tiempo en casos similares.

3.5. CAPACITACIÓN

El CONTRATISTA deberá efectuar un programa de capacitación para un mínimo de cinco (05) personas de la OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN durante la ejecución del servicio, en los siguientes cursos:

Detalle de Capacitación	Tipo
Curso de gestión de la plataforma de correlación extendida para la detección y respuesta a incidentes de la marca ofertada.	Tipo Oficial
Curso de gestión de la plataforma de automatización, orquestación y respuesta (SOAR)	Tipo Oficial
Curso de Certificación en Systems Security Certified Practitioner (SSCP)	Tipo oficial
Taller de Transferencia de Información de la plataforma instalada	Tipo no oficial

El curso oficial será dictado en las instalaciones del CONTRATISTA o centros autorizados o de manera remota previa coordinación con la Oficina de Tecnologías de la Información, con una duración mínima de 24 horas por cada curso; siendo los capacitadores, personal certificado por el fabricante, se deberá considerar los siguientes participantes:

Para cinco (05) personas de la Oficina de Tecnologías de la Información

- Curso de gestión de la plataforma de correlación extendida para la detección y respuesta a incidentes de la marca ofertada.
- Curso de gestión de la plataforma de automatización, orquestación y respuesta (SOAR)
- Curso de Certificación en Systems Security Certified Practitioner (SSCP)

Para cinco (05) personas de la Oficina de Tecnologías de la Información

- Taller de Transferencia de Información de la plataforma instalada

El certificado del curso oficial debe contener las horas lectivas y las fechas que se realizó la capacitación firmado por el instructor certificado por la marca ofertada.

El taller no oficial será dictado en las instalaciones del CONTRATISTA o en el ITP o de manera remota, previa coordinación con la Oficina de Tecnologías de la Información, estará dirigido a cinco (05) personas, con una duración mínima de 24 horas por cada curso. Los certificados del curso deben contener las horas lectivas y las fechas que se realizó la capacitación.

El CONTRATISTA al inicio de cada curso debe entregar al personal asistente, todo el material necesario para el desarrollo de este tales como: syllabus, guías o separatas del curso, entre otros. Asimismo, debe contar con todos los recursos informáticos para desarrollar el temario del curso dictado.

El CONTRATISTA al finalizar las capacitaciones en conjunto con la Oficina de Tecnologías de la información emitirá las actas de conformidad correspondientes.

3.6. PRESENTACIÓN OBLIGATORIA DENTRO DE LA PROPUESTA:

El Postor dentro de su propuesta, deberá acreditar fehacientemente el cumplimiento de las características técnicas solicitadas en los numerales 3.3 y 3.4 incluyendo al lado derecho de cada especificación técnica solicitada, el link del fabricante en donde se demuestre que cumple con cada especificación técnica solicitada. El link del fabricante se refiere a toda información y/o publicación del fabricante a través de su página web, tales como 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 y/o cartas de cumplimiento.

4. PRODUCTOS A OBTENER

Los productos a obtener en el presente servicio son los siguientes:

PAGO	PRODUCTO	DESCRIPCIÓN	PLAZO DE ENTREGA
1	Producto 1	Activación de las suscripciones por el periodo de 24 meses, correspondientes a: ● 1600 suscripciones de licencias del producto XDR ● 1 Suscripción de SOAR para 1600 nodos. Dicha activación se sustenta con un acta suscrita por las partes, siendo este el producto 1	Como máximo a los 40 días calendario, contados desde el día siguiente de firmado el contrato.
2	Producto 2	Deberá presentarse la siguiente documentación: 1. **Informe de Resultados de Seguridad Gestionada**, el cual debe contener lo siguiente:	Como máximo a los 240 días calendario, contados desde el día siguiente de firmado el contrato.

PAGO	PRODUCTO	DESCRIPCIÓN	PLAZO DE ENTREGA
		● Vulnerabilidades detectadas al inicio del servicio. ● Vulnerabilidades detectadas a los 240 días posteriores a la firma del contrato. ● Comparación entre vulnerabilidades detectadas al inicio del servicio y a los 240 días posteriores a la firma del contrato. ● Remediaciones aplicadas. ● Recomendaciones. ● . ● Casos de soporte técnico atendidos ● Tiempos de respuesta y solución ante incidentes ● Mejores prácticas implementadas 2. **Informe de Funcionamiento de la Plataforma,** el cual debe contener lo siguiente: ● Estado actual de operación. ● Servicios habilitados. ● Paneles de control, monitoreo y alertas. ● Recomendaciones de uso avanzado. 3. **Informe de Resultados de Capacitación,** el cual debe contener lo siguiente: ● Temario aplicado ● Relación de participantes ● Certificados de Capacitación emitidos ● Actas de asistencia de la capacitación y las firmas correspondientes. 4. **Informe de Oportunidades de Mejora Finales** y sugerencias para la evolución del SGSI.	

5. PLAZO DE EJECUCIÓN Y FORMA DE PAGO

5.1.- PLAZO DE EJECUCIÓN

El plazo de ejecución del servicio es de doscientos cuarenta (240) días calendario, contabilizado a partir del día siguiente de suscrito el contrato., de acuerdo al siguiente detalle:

- El plazo para la activación del servicio es de hasta sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato. Esta actividad considera la entrega, instalación, configuración y puesta en marcha, por 24 meses, de 1600 suscripciones de licencias producto XDR y 1 suscripción de SOAR para 1600 nodos, así como el inicio del servicio de Ethical hacking y soporte técnico en el marco de Seguridad Gestionada. La

activación de las suscripciones se sustenta con la firma del acta de activación del servicio.

- El plazo de ejecución es de doscientos cuarenta (240) días calendarios, contados a partir del día siguiente de suscrito el contrato..

5.2.- FORMA DE PAGO

El pago de la contraprestación, a favor del PROVEEDOR, será en 2 armadas; cada pago se realizará de acuerdo a la presentación de los productos, conforme a lo establecido en los numerales 3 y 4), a la presentación del informe y del comprobante de pago correspondiente a cargo del Proveedor, previa conformidad emitida por parte del jefe de la Oficina de Tecnologías de la Información del Instituto Tecnológico de la Producción, en su calidad de área usuaria, de acuerdo al siguiente detalle :

Producto	Porcentaje de pago
01	54% del monto total del contrato.
02	46% del monto total del contrato.

El monto referencial del servicio es de **S/ 2,319,520.00** (dos millones trescientos diecinueve mil quinientos veinte y 00/100 soles) a todo costo, incluido los impuestos de Ley.

6. LUGAR Y FORMA DE ENTREGA

Se deberá proporcionar mediante mesa de partes, el impreso del correo electrónico enviado a oti-licencias@itp.gob.pe donde se pueda validar el acceso a la suscripción del producto por el periodo de 24 meses.

7. CONFORMIDAD DE LOS PRODUCTOS DEL PROVEEDOR

La conformidad del servicio será emitida por el jefe de la Oficina de Tecnologías de la Información del Instituto Tecnológico de la Producción, la cual deberá comprobar el cumplimiento de lo estipulado en el presente documento.

La Oficina de Tecnologías de la Información dispondrá de siete (7) días calendario para dar conformidad o efectuar observaciones a los productos, contados a partir del día siguiente de recibido el producto por mesa de partes virtual del ITP.

El proveedor dispondrá de siete (7) días calendario para levantar dichas observaciones, contados a partir del día siguiente de recibida la comunicación electrónica por parte del contratante. Sólo se podrá realizar dos observaciones a cada producto, si las observaciones persisten se aplicará una penalidad.

Se aplicará penalidad en los casos de retraso en la entrega de los productos, levantamiento de observaciones, en caso se presenten más de dos observaciones. El cálculo de la aplicación de las penalidades se realizará según lo indicado en el numeral “Penalidad” del presente documento.

8. PERFIL DE LA FIRMA CONSULTORA

8.1. Generales:

Los requisitos que debe cumplir el proveedor, debido a la naturaleza de la contratación, son los siguientes:

a) Ser una persona jurídica.
b) Estar habilitado para contratar con el Estado.
c) Contar con Registro Nacional de Proveedores activo.
d) Contar con RUC activo.
e) Contar con un centro de Atención al Cliente o mesa de ayuda 24x7.
f) El postor deberá ser distribuidor autorizado de la solución ofertada.

8.2. Experiencia:

El POSTOR debe demostrar experiencia máxima de diez (10) ventas de servicios y/o bienes de soluciones de ciberseguridad en general, como: servicios de suscripción de plataforma de CYBER SOC delegada tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada o soluciones de Correlación de Eventos de Seguridad (SIEM) o sistema de protección y seguridad para red o XDR, o EDR, en los últimos 07 años. El monto facturado acumulado deberá ser por un monto superior a S/ 4,000,000.00 (Cuatro millones de Soles).

8.3. Acreditación:

La experiencia del PROVEEDOR en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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 pago.

Cuando los contratos, órdenes de compra o comprobantes de pago indiquen un monto facturado expresado en moneda extranjera, deberá especificarse el tipo de cambio de venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

8.4. PERSONAL CLAVE

La firma consultora debe acreditar que cuenta con el personal necesario para la ejecución del servicio, para lo cual debe presentar en su propuesta el siguiente personal:

- **Un (01) jefe de Proyectos**

  Formación Académica:
  - Ingeniero titulado en computación o sistemas o electrónica o redes o informática o telecomunicaciones o sistemas de información o seguridad informática.
  - Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.

  Experiencia:
  - Experiencia general no menor de ocho (8) años en el sector público o privado.
  - Experiencia no menor de cinco (05) años como Jefe o Gestor de Proyectos de soluciones de Ciberseguridad.

- **Un (01) Personal Técnico Residente**
  Formación Académica:
  - Técnico profesional o bachiller en computación o sistemas o electrónica o redes o informática o telecomunicaciones o redes y comunicaciones de datos o sistemas de información.
  - Certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC) y/o Certificación en CEH V12 - Certified Ethical Hacker o similar.

  Experiencia:
  - Experiencia general no menor de tres (3) años en el sector público o privado.
  - Experiencia no menor de dos (2) años como especialista en soluciones de ciberseguridad.

  Acreditación:

  Los requisitos de experiencia y formación se acreditan mediante la presentación de documentos como diplomas, certificados y/o constancias de trabajo o participación de proyectos, y/o contratos con conformidad, u otro documento que demuestre en forma fehaciente la experiencia en el servicio a realizar. En el caso que el profesional haya realizado dichos proyectos como personal de planta de la firma consultora, la experiencia podrá ser certificada por esta. En el caso de los títulos de grado académico, estos deberán estar inscritos en la SUNEDU o en su defecto podrán acreditarse con copia del diploma respectivo.

  Toda documentación necesaria para el sustento, será presentada por la firma consultora ganadora durante la formalización del contrato.

9. ASPECTOS COMPLEMENTARIOS

I. Confidencialidad

Se deberá mantener en forma reservada toda la información suministrada por el ITP o los CITE. Asimismo, el proveedor se compromete a no divulgar las actividades materia del presente servicio. Esta obligación permanecerá vigente no obstante el vencimiento o la terminación del servicio prestado.

II. Propiedad intelectual

El proveedor acepta expresamente que los derechos patrimoniales y conexos de propiedad intelectual sobre los productos y documentación generada que se entreguen al amparo del presente servicio corresponden únicamente al ITP, con exclusividad y a todos los efectos. Siendo responsable el proveedor de mantener la confidencialidad de la información frente a sí y ante terceros.

III. Vicios ocultos

La conformidad del servicio por parte del ITP no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. El plazo máximo de responsabilidad del proveedor es de un (01) año contado a partir de la conformidad otorgada por el ITP.

10. ANTICORRUPCIÓN

Los participantes se obligan a conducirse en todo momento, durante la postulación al concurso, 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, participantes, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

Además, los participantes se comprometen 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.

11. PENALIDAD

Las penalidades a aplicar son las siguientes:

<table>
<tr><th>Supuestos de aplicación de penalidad</th><th>Forma de cálculo</th><th>Indicaciones</th></tr>
<tr><td>En caso de retraso injustificado en la ejecución de las prestaciones objeto del presente contrato, se aplicará al proveedor una penalidad por cada día calendario de atraso.</td><td rowspan="3">Penalidad = penalidad diaria x cantidad de días de retraso
Penalidad diaria =
0.10 x monto
F x plazo en días
Donde:
F = Factor de 0.40 para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras

F = Factor de 0.25 para plazos mayores a sesenta (60) días, para bienes, servicios en general y consultorías:</td><td>La cantidad de días de retraso, se considerará desde el día siguiente de la fecha en que el proveedor debió presentar el producto, hasta la fecha de presentación del producto.
Si el día de entrega del producto establecido en el presente TdR, coincide con un día no laborable, se correrá la fecha de entrega hasta el siguiente primer día hábil, sin que sea sujeto de penalidad.</td></tr>
<tr><td>En caso el proveedor no subsane las observaciones en el plazo establecido, se aplicará penalidad por cada día calendario de atraso.</td><td>La cantidad de días de retraso, se considerará desde el día siguiente calendario de la fecha en que el proveedor debió presentar el producto con las observaciones subsanadas, hasta la fecha de presentación de la subsanación.</td></tr>
<tr><td>En caso se presenten más de dos (2) observaciones por producto sin obtener conformidad, se aplicará penalidad hasta la subsanación del producto.</td><td>La cantidad de días de retraso se considerarán desde el día siguiente establecido para levantar las observaciones del producto correspondiente hasta la fecha de presentación de la última subsanación de observaciones.</td></tr>
</table>

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o, en caso de que estos involucran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

Las penalidades en su conjunto serán aplicadas hasta por un monto máximo equivalente al diez por ciento (10%) del monto contractual. Cuando se alcance el monto máximo de penalidad, la entidad contratante podrá resolver el contrato por incumplimiento.

Las penalidades establecidas en la presente cláusula se aplicarán sin perjuicio de la obligación del proveedor de responder por los daños y perjuicios que pudieran derivarse de su incumplimiento o de las demás sanciones que pudieran corresponder.

Las penalidades se aplicarán de los pagos pendientes previa comunicación.

En caso de retraso injustificado en la ejecución de las prestaciones objeto del presente contrato.

ANEXO 01
ESTRUCTURA DE COSTOS

HONORARIOS	UNIDAD DE MEDIDA	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Un (01) JEFE DE PROYECTOS	MES	8	S/ 12,000.00	S/ 96,000.00
Un (01) ESPECIALISTA RESIDENTE	MES	8	S/ 10,000.00	S/ 80,000.00
GASTOS ADMINISTRATIVOS	MES	8	S/ 1,000.00	S/ 8,000.00
PLATAFORMA DE CORRELACIÓN EXTENDIDA PARA LA DETECCIÓN Y RESPUESTA A INCIDENTES	MES	24	S/ 30,000.00	S/ 720,000.00
PLATAFORMA DE AUTOMATIZACIÓN, ORQUESTACIÓN Y RESPUESTA	MES	24	S/ 30,000.00	S/ 720,000.00
SEGURIDAD GESTIONADA Y ETHICAL HACKING	MES	24	S/ 5,000.00	S/ 120,000.00
UTILIDAD (15%)	PORCENTAJE	15		S/ 261,600.00
IGV (18%)	PORCENTAJE	18		S/ 313,920.00
TOTAL				**S/ 2,319,520.00**