MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

Requerimientos técnicos

Adquisición de herramientas informáticas de ciberseguridad.

Dirección de Ciberseguridad

2025

MARVIN MORAGA CALVO (FIRMA)

Firmado digitalmente por MARVIN MORAGA CALVO (FIRMA)
Fecha: 2025.06.09 10:38:26 -06'00'

Contenido

Especificaciones Técnicas: Solución de Protección MDR/XDR/EDR

La solución deberá cumplir, como mínimo, con las siguientes características técnicas:

I. Capacidad de Protección MDR/XDR/EDR

1.1 Plataforma XDR (Detección y respuesta extendida)

1. Plataforma y Consola de Gestión

    - La solución deberá ser una plataforma de detección y respuesta extendida (XDR) basada en la nube, con consola unificada y nativa, capaz de gestionar estaciones de trabajo, servidores, contenedores y dispositivos OT, incluso si estos se encuentran distribuidos remotamente.

2. Sensor o Agente de Protección

    - El despliegue de la solución deberá realizarse preferiblemente mediante un único sensor o agente, el cual será instalado en los distintos dispositivos protegidos (estaciones de trabajo, servidores, máquinas virtuales, contenedores o dispositivos OT).

    - El agente deberá convivir con soluciones de EPP existentes sin generar conflictos, lentitud ni requerir la desinstalación de herramientas ya instaladas.

    - Preferiblemente no deberá requerirse la creación de exclusiones para garantizar su funcionamiento efectivo.

3. Integración y Personalización

    - La solución debe permitir la integración con sistemas externos mediante API REST o mecanismos equivalentes, para facilitar la interoperabilidad con otras plataformas de ciberseguridad o gestión.

    - Deberá soportar la capacidad de cargar y gestionar Indicadores de Compromiso (IOCs) de forma personalizada, manual o automatizada mediante API, con acciones de bloqueo o exclusión definidas por la institución.

- Preferiblemente, la plataforma deberá incluir un repositorio o sistema de gestión de integraciones que permita visualizar, configurar o extender las integraciones disponibles.

4. Visibilidad y Analítica

   - La consola de gestión deberá ofrecer visibilidad completa de alertas, eventos y actividad de los dispositivos protegidos, con funcionalidades de reporte automático.

   - Preferiblemente la solución deberá contar con capacidades de análisis avanzado que utilicen inteligencia artificial y/o aprendizaje automático (AI/ML) para apoyar la detección de amenazas, la correlación de eventos y la priorización de alertas.

   - Preferiblemente la plataforma deberá contar con capacidades de orquestación y automatización de respuesta (SOAR), que permitan diseñar e implementar flujos automatizados para la contención y mitigación de incidentes de seguridad.

   - Preferiblemente estas capacidades estarán integradas de forma nativa en los distintos módulos funcionales y sin requerir licenciamiento adicional.

5. Gestión de Accesos y Roles

   - La plataforma deberá permitir la definición de roles personalizados y controles de acceso para administradores, auditores y otros perfiles autorizados.

   - El acceso a la consola deberá incluir soporte para autenticación multifactor (MFA) e integración con sistemas de autenticación única (SSO) institucionales.

6. Escalabilidad y Gestión Jerárquica

   - Preferiblemente la solución debe ser parte de un sistema de consolas para entornos multiinstancia o jerárquicos, donde pueda ser utilizada por diferentes entidades bajo un mismo entorno de gestión (padre-hijo), como parte de un CSIRT o SOC colaborativo.

- La arquitectura jerárquica no deberá afectar la independencia operativa ni administrativa de cada entidad.

7. Soporte y Capacitación

- La plataforma deberá contar con un portal de ayuda integrado, acceso a seminarios web periódicos y una base de conocimientos accesible desde la consola, orientada a fortalecer el uso efectivo de la solución.
- Preferiblemente la solución deberá incluir un mecanismo de escalamiento de casos técnicos directamente con el fabricante con atención 24/7.

8. Seguridad en el Despliegue

- La solución deberá contar con un mecanismo de protección para evitar la desinstalación no autorizada de los sensores o agentes instalados. Este mecanismo deberá requerir, al menos, una validación desde la consola central por parte de un usuario con perfil autorizado.
- Preferiblemente, este proceso debe utilizar un token de autorización de un solo uso generado de forma aleatoria.
- No se aceptarán esquemas inseguros como contraseñas fijas o reutilizables, predefinidas o compartidas

1.2 Capacidad de EDR

1. Telemetría, análisis retrospectivo y reconstrucción de eventos

- La plataforma deberá proporcionar información detallada de la telemetría relacionada con alertas y detecciones, permitiendo el análisis retrospectivo de ataques, reconstrucción de eventos, en listado y mediante líneas de tiempo.

2. Análisis forense y respuesta remota

- La solución deberá permitir la ejecución remota de comandos en los dispositivos protegidos (Windows, Linux y macOS), a través de una consola

central, para la realización de acciones como: ejecución de scripts, consulta de procesos y conexiones activas y otras funciones necesarias para agilizar el análisis forense.

3. Compatibilidad del agente

- El agente o sensor deberá ser compatible y soportar todas las funcionalidades requeridas sobre los siguientes sistemas operativos:
    - Windows (versiones soportadas oficialmente por el fabricante).
    - Windows Server (versiones soportadas oficialmente por el fabricante).
    - Linux (versiones de distribución empresarial).
    - MacOS (versiones soportadas oficialmente por el fabricante).

4. Detección y prevención de amenazas

- La solución deberá contar con mecanismos para la detección y prevención de amenazas como:
    - Malware conocido y desconocido, incluyendo amenazas de día cero.
    - Técnicas y tácticas de adversarios (TTPs), con referencia al marco MITRE ATT&CK.
    - Actividades sin archivos (fileless), mediante detección basada en comportamiento o indicadores de ataque.
    - Ejecución de scripts maliciosos, comandos sospechosos, drivers no autorizados, manipulación de registros y procesos anómalos.
    - Comportamientos asociados a ransomware: cifrado, borrado de backups o volúmenes, acceso a archivos masivo o persistente.
    - Movimientos laterales, acceso y robo de credenciales, explotación de vulnerabilidades día cero.
    - Capacidades de remediación automática frente a amenazas persistentes, como: cuarentena, liberación o eliminación de artefactos maliciosos.

5. Aislamiento remoto

- La solución deberá contar con la capacidad de aislar remotamente un dispositivo comprometido, bloqueando su comunicación con la red, excepto la necesaria para mantener el enlace con la consola de gestión. Esta función deberá estar disponible de forma integrada, sin requerir herramientas externas o intervención manual adicional

6. Mapeo de amenazas y modelos de inteligencia

- La plataforma deberá presentar alertas mapeadas conforme al marco MITRE ATT&CK para facilitar la identificación de tácticas y técnicas utilizadas en los ataques.
- Deberá permitir la integración con plataformas externas de inteligencia de amenazas para enriquecer la detección y respuesta.
- Deberá incluir capacidades de protección avanzada contra malware, utilizando tecnologías que no dependan exclusivamente de firmas tradicionales, tales como: análisis de comportamiento, detección basada en TTPs y técnicas heurísticas.

7. Capacidades avanzadas del módulo de protección

- El módulo EDR deberá incluir al menos las siguientes capacidades:
    - Bloqueo de ejecución de código malicioso, incluyendo exploits de día cero y procesos asociados a comando y control (C2).
    - Protección con conectividad o sin conectividad a la nube (Offline) para garantizar la defensa continua ante amenazas.
    - Detección basada en inteligencia artificial y machine learning, preferiblemente ejecutada localmente, especialmente en entornos Windows y macOS, sin depender exclusivamente de firmas tradicionales.

- Bloqueo de procesos y scripts maliciosos, incluyendo PowerShell, CMD, rundll32.exe, JavaScript, u otros vectores por comandos.
- Prevención de actividades maliciosas como cifrado masivo (ransomware), exfiltración de datos, robo de credenciales, movimientos laterales y escalamiento de privilegios.
- Mitigación de técnicas avanzadas de evasión, como el uso indebido de "sticky keys", ejecución desde navegadores u otros vectores no tradicionales.

8. Sandbox y cuarentena

- La solución deberá incluir un sistema de cuarentena para la contención de archivos sospechosos, con opción de análisis en sandbox, preferiblemente integrado o conectado de forma nativa a la plataforma. Esta funcionalidad podrá estar embebida en la solución o ser parte del servicio MDR provisto por el fabricante, siempre que permita el análisis seguro y detallado de muestras sin afectar los sistemas productivos.

1.3 Control de dispositivos USB y periféricos

- La solución deberá contar con capacidades de control de dispositivos USB, incluyendo al menos las siguientes funcionalidades:

  - Bloqueo o habilitación de operaciones de lectura, escritura o ejecución en dispositivos de almacenamiento extraíbles.
  - Registro detallado de archivos copiados o transferidos hacia y desde los dispositivos.
  - Definición de políticas de auditoría que permitan el monitoreo y control de la actividad relacionada con dispositivos externos.

1.4 Inteligencia de Amenazas

1. Solución integral con capacidades de protección ampliada

- Plataforma con capacidades protección de endpoints (EPP), identidades y entornos en la nube, integrando funciones de sandboxing, búsqueda de malware e inteligencia de amenazas.

2. Plataforma de inteligencia de amenazas (TIP)

- La solución deberá contar con capacidades equivalentes a una plataforma de inteligencia de amenazas tipo TIP (Threat Intelligence Platform) que permita:

    - Consultar y correlacionar indicadores de compromiso (IOCs) desde fuentes internas y externas.
    - Inyectar IOCs de forma manual o automática por medio de API.
    - Actualizar la base de IOCs y amenazas en tiempo real o en intervalos frecuentes configurables.

3. Capacidad de sandboxing en la nube

- La solución deberá incluir un entorno de análisis en sandbox, preferiblemente en la nube, con capacidad para:

    - Enviar automáticamente o por demanda muestras sospechosas desde los endpoints para su análisis dinámico.
    - Correlacionar los resultados con detecciones existentes o nuevas alertas en la consola central.

4. Reportes programados de inteligencia

- La plataforma deberá generar y entregar reportes programados de inteligencia con una periodicidad al menos semanal, que incluyan:

    - Tendencias de amenazas activas.
    - Campañas en curso a nivel regional o global.
    - Técnicas observadas y actores de amenazas relevantes.
    - Recomendaciones de mitigación y preparación.

5. Panel de inteligencia de vulnerabilidades

- La plataforma deberá incluir de forma integrada o nativa un panel de consulta de inteligencia de vulnerabilidades que proporcione información actualizada sobre nuevas vulnerabilidades detectadas, con elementos clave como:

    - Identificador CVE.
    - Clasificación de criticidad.
    - Descripción técnica del impacto.
    - Relación con los activos protegidos por la solución.
    - Recomendaciones de mitigación o actualización.

1.5 Investigación Forense y Cacería de Amenazas Proactiva

1. Monitoreo continuo y visibilidad

- La plataforma debe integrar capacidades de detección y respuesta para endpoints, identidad y entornos en la nube, brindando monitoreo continuo y visibilidad de actividad anómala para habilitar acciones de respuesta y análisis forense que mitiguen brechas potenciales o incidentes activos.

2. Detección automática desde el inicio

- La solución debe permitir la detección automática de incidentes desde su despliegue inicial, sin requerir ajustes o configuraciones adicionales previas por parte del usuario.

3. Búsqueda personalizada y rápida

- La plataforma debe permitir la ejecución de búsquedas personalizadas sobre los eventos, registros y detecciones, como parte de actividades de cacería de amenazas, y retornar los resultados de forma inmediata y eficiente para análisis interactivo.

4. Investigación forense en tiempo real y retrospectiva

- Se debe permitir la realización de investigaciones forenses en tiempo real o retrospectivas, a partir de criterios como:

    - Nombre del host o equipo.
    - Hash de archivos.
    - Direcciones IP.
    - Nombres de dominio o grupos de dominios.
    - Identificadores únicos del sensor o agente.
    - Actividades específicas como inicios de sesión, comandos de PowerShell, ejecución de tareas programadas, entre otros.
    - Sensores desplegados en sistemas operativos Windows, macOS, Linux, contenedores y entornos de Active Directory.

5. Reglas personalizadas e indicadores de ataque

- La plataforma deberá permitir la creación y gestión de reglas de detección personalizadas, así como el uso de Indicadores de Ataque (IOA), con el objetivo de identificar y prevenir amenazas avanzadas, incluyendo ataques sin archivos (fileless). Estas reglas deberán permitir acciones como bloquear procesos, archivos, direcciones IP o dominios, según relaciones con comandos o procesos predecesores.

- La solución deberá contar con mecanismos que ajusten y amplíen automáticamente los indicadores integrados, con base en nuevos patrones de comportamiento malicioso observados en el entorno.

6. Hunting y exploración por telemetría

- La solución deberá permitir la búsqueda proactiva (threat hunting) de eventos o anomalías con base en la telemetría recopilada por la plataforma, utilizando rangos o períodos de tiempo definidos por el usuario.

7. Visualización contextual de incidentes

- La consola deberá ofrecer visualizaciones detalladas de los incidentes, correlacionando múltiples eventos y detecciones asociadas, presentando:
    - Evaluación del riesgo del incidente.
    - Dispositivos afectados.
    - Procesos involucrados.
    - Línea de tiempo de eventos relacionados, tanto bloqueados como observados.

8. Servicios de fábrica para MDR y threat hunting

- La solución deberá incluir servicios provistos por el fabricante (o proveedor MDR autorizado) para la ejecución de actividades de cacería de amenazas y análisis proactivo de alertas y anomalías. Estos servicios deberán formar parte de la estrategia de detección gestionada de la solución, y contribuir a la identificación oportuna de amenazas avanzadas o persistentes.

9. Consultas personalizadas y automatización de reportes

- La plataforma deberá permitir la creación de consultas personalizadas utilizando un lenguaje de consulta estándar y documentado. Estas consultas deben poder programarse y configurarse para que sus resultados

sean enviados automáticamente como reportes, incluso mediante notificación por correo electrónico.

1.6 Descubrimiento: Higiene de TI

1. Visibilidad integral desde consola central

- La solución deberá proporcionar visibilidad completa del entorno tecnológico de la organización a través de una consola de administración centralizada. Esta visibilidad debe incluir información en tiempo real e históricos sobre activos, accesos y aplicaciones, accesibles desde la consola central de la plataforma.

2. Inventario de aplicaciones y versiones

- La plataforma deberá ofrecer un inventario detallado de las aplicaciones instaladas y utilizadas en los endpoints protegidos, incluyendo sus versiones, con el fin de identificar software potencialmente no autorizado, desactualizado o sospechoso.

3. Identificación de dispositivos conectados

- La herramienta debe tener la capacidad de identificar todos los dispositivos conectados a la red institucional, estén o no gestionados por la solución de seguridad, para ofrecer una visión integral de los activos en uso.

4. Monitoreo de accesos y privilegios

La solución deberá permitir el monitoreo de los inicios de sesión de usuarios activos, diferenciando entre cuentas con privilegios locales, de dominio o de administrador. Este monitoreo debe incluir visibilidad sobre el historial de inicio de sesión, así como información sobre el estado de las credenciales (por ejemplo, fecha de última actualización de contraseña).

5. Agente unificado

- El módulo de higiene de TI deberá operar preferiblemente utilizando el mismo agente ligero implementado por la plataforma principal de protección de endpoints, evitando la necesidad de instalar software adicional y garantizando la eficiencia operativa.

6. Enriquecimiento con datos de EDR

- La funcionalidad de higiene de TI deberá estar integrada o interoperar con la plataforma EDR utilizada, aprovechando su telemetría y datos de detección para enriquecer las búsquedas, correlaciones e informes generados desde la consola de administración.

7. Control sobre cuentas privilegiadas

- La solución deberá contar con capacidades para identificar y monitorear el uso y la creación de cuentas con privilegios elevados, incluyendo administradores locales, de dominio y otras cuentas con acceso crítico. Deberá generar alertas ante comportamientos inusuales o cambios en estas cuentas, con el fin de reducir riesgos por abuso de credenciales o accesos indebidos.

1.7 Gestión de Vulnerabilidades

1. Evaluación continua y automatizada

- La solución deberá ofrecer capacidades de gestión de vulnerabilidades continua y automatizada, utilizando telemetría en tiempo real proveniente de los dispositivos protegidos. No deberá depender exclusivamente de escaneos programados para identificar exposiciones o configuraciones inseguras o desviaciones de postura.

2. Correlación unificada con amenazas

- La plataforma deberá integrar o interoperar con capacidades de gestión de vulnerabilidades, permitiendo correlacionar eventos de seguridad con información sobre exposición (CVE), nivel de criticidad y probabilidad de explotación, en un mismo flujo operativo.

3. Capacidad de análisis de CVEs

- La solución deberá permitir la consulta e investigación de vulnerabilidades documentadas como CVE (Common Vulnerabilities and Exposures), incluyendo:
    - Descripción técnica de la vulnerabilidad.
    - Criticidad asignada (por ejemplo, CVSS).
    - Activos afectados y prioridad de remediación.

4. Uso del agente EDR existente

- El módulo de gestión de vulnerabilidades deberá operar preferiblemente a través del mismo agente ligero utilizado por la solución EDR/XDR, sin requerir instalaciones adicionales en los dispositivos protegidos.

5. Supervisión continua en múltiples entornos

- La plataforma deberá permitir la supervisión continua del estado de vulnerabilidad de todos los dispositivos protegidos, independientemente de su ubicación. Esta supervisión deberá abarcar al menos:
    - Dispositivos en instalaciones físicas (on-premise).
    - Dispositivos remotos o móviles.
    - Entornos de nube pública o privada.

6. Cobertura mediante sensores en cualquier red

- El sensor o agente de la solución deberá ser capaz de monitorear dispositivos protegidos tanto dentro como fuera de la red institucional, incluyendo dispositivos físicos y virtuales.

7. Consola operativa y búsqueda en tiempo real

- La información recopilada deberá estar disponible a través de un panel o consola visual unificada, que permita:

- Visualización consolidada del estado de vulnerabilidad.
- Filtros por nivel de riesgo, ubicación o grupo.
- Búsquedas en tiempo real para análisis y priorización de remediaciones.

1.8 Cacería de Amenazas como Servicio (Threat Hunting Gestionado por el Fabricante)

1. Servicio proactivo de cacería 24/7

- La solución deberá incluir un servicio de **cacería de amenazas (threat hunting) gestionado directamente por el fabricante o proveedor del servicio MDR o un proveedor MDR autorizado**, operando por analistas expertos disponibles las 24 horas del día, los 7 días de la semana. Este servicio deberá contemplar actividades proactivas de identificación de amenazas avanzadas, análisis manual de eventos sospechosos y escalamiento oportuno de hallazgos críticos para su contención o remediación.
- La actividad de cacería de amenazas deberá apoyarse en inteligencia de amenazas actualizada, en el marco de referencia MITRE ATT&CK y telemetría recopilada desde los endpoints y otros activos protegidos.
- El servicio preferiblemente no deberá requerir la instalación de plataformas de terceros, ni el establecimiento de conexiones VPN para la recopilación o análisis de la información.

2. Actividad activa de investigación y respuesta

- El servicio deberá ir más allá de la detección automatizada y ofrecer capacidad activa de investigación e identificación de comportamientos maliciosos, intrusiones o actividades sospechosas, con el objetivo de detectar adversarios avanzados y ataques en curso.

- Como parte del servicio, se deberán emitir alertas contextualizadas, acompañadas de recomendaciones de remediación y análisis detallados que respondan a las preguntas fundamentales del incidente: ¿qué ocurrió?, ¿cómo ocurrió?, y ¿cómo contenerlo o remediarlo?

3. Investigación retroactiva y análisis de artefactos

- El equipo de cacería de amenazas deberá realizar investigaciones retroactivas, revisando datos históricos recopilados para detectar trazas o patrones de intrusión no detectados en tiempo real.
- Como parte del análisis de incidentes o actividades de investigación, se deberá permitir la recopilación de artefactos técnicos relevantes (tales como: direcciones IP, dominios, hashes de archivos, nombres de procesos, etc.) para su correlación y análisis posterior.

4. Clasificación estructurada de hallazgos

- El proceso de investigación de incidentes y alertas deberá estar basado en un playbook estructurado de análisis y clasificación de hallazgos, que permita categorizar las detecciones, como mínimo, en las siguientes clases:
  - Verdadero positivo
  - Falso positivo
  - Indeterminado
  - Sospechoso

1.9 Respuesta y Remediación de Incidentes como Servicio (Fabricante) - MDR

1. Servicio continuo y cobertura completa

- El servicio MDR deberá incluir capacidades de detección, monitoreo proactivo, análisis y remediación de amenazas 24 horas al día, los 7 días de la semana, durante todo el año (24/7/365), sin limitaciones operativas restrictivas sobre la cantidad de eventos procesados ni sobre la ejecución

razonable de acciones de respuesta. El servicio deberá garantizar cobertura para todos los dispositivos protegidos, sin importar su ubicación o tipo (local, remoto o en la nube).

2. Supervisión activa y correlación de alertas

- El servicio MDR deberá mantener una supervisión continua del software de protección instalado, abarcando estaciones de trabajo, servidores y contenedores (por ejemplo, entornos Kubernetes de producción), incluyendo la atención de alertas y el análisis constante de bitácoras (logs) generadas por el sistema de protección.
- Como parte de esta supervisión, el servicio deberá generar alertas tempranas y análisis contextualizados de amenazas, con recomendaciones y acciones destinadas a mitigar el impacto de los ataques. Estas recomendaciones deberán considerar el tipo de amenaza detectada, su criticidad, y las acciones correctivas más apropiadas según el entorno afectado.

3. Clasificación de activos y postura de seguridad

- El proveedor deberá contar con capacidades para identificar y clasificar los activos protegidos, con el fin de aplicar posturas de seguridad diferenciadas según su nivel de criticidad y condiciones de operación. Esta evaluación deberá permitir la administración de las políticas del EDR/XDR y cuando aplique, la incorporación de mecanismos adicionales como: ITDR (Identity Threat Detection and Response).

4. Contención y remediación avanzada

- Ante la detección de comportamientos anómalos como sospechas de exfiltración de datos, ransomware o intentos de compromiso interno, el servicio MDR deberá estar en capacidad de realizar de manera inmediata las siguientes acciones de contención y respuesta:

- Aislamiento remoto del dispositivo afectado.
- Remoción de archivos maliciosos.
- Envío de archivos a entornos de análisis avanzado en la nube.
- Revisión de logs de sistema y correlación de eventos.
- Terminación de procesos activos asociados a la amenaza.
- Eliminación de persistencias y mecanismos de evasión.
- Bloqueo de objetos maliciosos por hash o indicadores de compromiso.

5. Portal integrado de comunicación y gestión de casos

- El servicio MDR deberá incluir un portal de atención y colaboración que esté integrado o interoperable con la consola de gestión EDR/XDR, que permita establecer comunicación directa con el equipo de analistas del fabricante.

  Este portal deberá contar con:

  - Gestión de usuarios de contacto por roles, incluyendo:
    - Autorizador de cambios de usuarios.
    - Contacto de escalamiento para EDR.
    - Contacto de escalamiento para identidad.
    - Usuario revisor de garantía.
    - Contacto informativo.
  - Centro de mensajes con registro de comunicaciones y seguimiento de incidentes, que permita:
    - Solicitar soporte para detecciones, incidentes, configuraciones o productos.
    - Documentar acciones, recomendaciones, validaciones y cierres.

1.10 Protección de Identidades (Directorio Activo)

1. Análisis profundo de protocolos de autenticación

- La plataforma deberá contar con capacidades para inspeccionar eventos relacionados con el uso de protocolos de autenticación como (NTLM, Kerberos y LDAP), ya sea de forma nativa o a través de integración de componentes de análisis de identidad, con el fin de detectar amenazas como:
    - Reenvío de credenciales
    - Ataques Pass-the-Hash
    - Kerberoasting
    - Emisión de tickets maliciosos (Golden Ticket)
    - Validación de contraseñas contra bases de datos comprometidas.

- Debe proporcionar puntajes de riesgo para usuarios y dispositivos, mediante análisis de comportamiento, nivel de privilegio, actividad reciente, detecciones asociadas.

2. Perfilado de comportamiento y análisis de riesgo

   La solución deberá:

   - Identificar cuentas privilegiadas, de servicio, regulares y obsoletas.
   - Detectar cambios sospechosos en usuarios, credenciales, privilegios o actividad.
   - Correlacionar eventos relacionados con sesiones de usuario, autenticación y acciones.

3. Descubrimiento continuo de usuarios y cuentas

   La solución deberá contar con capacidades para identificar, de forma continua:

   - Cuentas activas en el directorio

- Cuentas privilegiadas y de servicio
- Cuentas regulares
- Cuentas obsoletas o inactivas

4. Reducción de superficie de ataque

- La solución deberá contribuir con la reducción de la superficie de ataque mediante:
  - Detección de administradores ocultos o no autorizados
  - Identificación de cuentas de servicio con configuraciones inseguras o comportamientos inusuales
  - Análisis de comportamientos anómalos asociados a usuarios o cuentas privilegiadas

5. Integración con agente EDR/XDR

- Preferiblemente la solución deberá permitir el mismo sensor o agente utilizado por el EDR/XDR para activar funciones de monitoreo e inspección de identidad en los controladores de dominio, evitando duplicidad de software o sobrecarga operativa.
- La plataforma deberá integrar datos de identidad con la detección de amenazas en endpoint y vulnerabilidades, desde una **consola unificada.**
- Las respuestas automáticas deberán poder activarse según políticas, incluyendo:
  - Reforzamiento de autenticación (por ejemplo, MFA).
  - Bloqueo temporal o suspensión de cuentas.
  - Forzado de cambio de contraseñas.

6. Respuesta automática y basada en riesgo

- La plataforma deberá tener la capacidad de:
    - Responder en tiempo real a eventos o amenazas relacionadas con la identidad, siguiendo políticas preestablecidas.
    - Tomar medidas preventivas según umbrales de puntuación de riesgo definidos por la organización, sin interrumpir el acceso legítimo de usuarios válidos.

7. Correlación, auditoría y cacería

   La solución deberá contar con capacidades como:

    - Correlación automatizada de eventos dentro del contexto de sesión de un usuario
    - Registro y retención de telemetría de usuario (accesos, acciones, dispositivos)
    - Permitir la consulta avanzada de eventos y datos de telemetría ya sea mediante lenguaje de consulta estructurado nativo o funcionalidad equivalente.

8. Detección de anomalías en el comportamiento de usuarios

   La plataforma deberá ser compatible con entornos de Active Directory en múltiples dominios o bosques y contar con capacidades para identificar comportamientos inusuales de usuarios o cuentas privilegiadas, incluyendo:

    - Cambios de credenciales fuera de comportamiento habitual
    - Inicios de sesión desde múltiples ubicaciones geográficas
    - Inicios de sesión desde ubicaciones inusuales o sospechosas
    - Uso atípico de cuentas de servicio
    - Seguimiento de sesiones completas desde inicio hasta cierre
    - Cambios de credenciales o creación/eliminación de cuentas por acceso remoto
    - Logins sospechosos en controladores de dominio

1.11 Capacidad XDR y Nueva Generación de SIEM

1. Ingesta y análisis en una única plataforma

- La plataforma deberá permitir la ingesta de múltiples tipos de datos y registros (logs) desde diversas fuentes internas o externas, incluyendo: endpoints, nube, identidad, red, navegación web, dispositivos de seguridad, correo electrónico y aplicaciones corporativas.

- Esta funcionalidad deberá estar integrada en la misma plataforma de gestión del EDR/XDR y protección de identidades, permitiendo el análisis de datos en una sola consola, sin requerir consolas adicionales.

2. Funcionalidades clave del SIEM

- La plataforma deberá contar con al menos las siguientes capacidades:

    - Monitoreo y gestión de incidentes mediante análisis automatizado con inteligencia artificial o aprendizaje automático (AI/ML), sin depender exclusivamente de reglas preconfiguradas.
    - Creación y personalización de reglas de correlación, con posibilidad de clasificar eventos y detecciones conforme al marco MITRE ATT&CK (Enterprise o Mobile).
    - Consultas avanzadas sobre eventos y datos, así como la creación de dashboards personalizables para soportar procesos de threat hunting y monitoreo continuo.
    - Ingesta de datos mediante conectores configurables o personalizables, que permitan parametrizar fuentes diversas.
    - Capacidad de respuesta orquestada para múltiples vectores (EDR, nube, identidad, correo, navegación web, red y firewall), activada automáticamente o por demanda.

3. Activación de detecciones sin configuración manual

- La plataforma debe incluir capacidades nativas de detección y respuesta que puedan activarse sin requerir configuración o desarrollo adicional, siempre que la fuente de datos haya sido integrada.

4. Capacidades nativas requeridas

- La solución deberá tener capacidad de integrar de manera nativa los siguientes componentes:
    - Plataforma de inteligencia de amenazas (TIP) reconocida en el mercado.
    - Gestión y retención de registros (Log Management).
    - Capacidades de investigación basadas en telemetría enriquecida.
    - Correlación avanzada y reglas personalizadas basadas en condiciones lógicas o patrones de comportamiento.
    - Casos de uso de cumplimiento normativo, con reglas personalizables e ingesta de datos específica para auditoría.
    - Módulos XDR para correlación de múltiples vectores.

5. Integración abierta

- La solución deberá contar con capacidad de integración mediante API REST documentada, que permita la interoperabilidad con sistemas externos de gestión, orquestación, respuesta o cumplimiento.

1.12 Capacidades de Analítica, Detección y Prevención Extendida XDR y SIEM

1. Detección y prevención a través de SIEM

- El módulo de analítica de la plataforma deberá identificar amenazas a través de los principales vectores, empleando correlación de eventos, inteligencia de amenazas e indicadores de ataque (IOA). Las capacidades mínimas deben incluir:
    - Detección de malware conocido, desconocido y amenazas de día cero, ya sea por firmas, heurística o análisis de comportamiento.
    - Identificación de TTPs con referencia al marco MITRE ATT&CK.
    - Detección de ataques sin archivos (fileless) mediante análisis conductual e indicadores de ataque.

- Identificación de actividades sospechosas como ejecución de scripts, procesos anómalos, comandos maliciosos y modificaciones del registro.
- Detección de comportamientos asociados a ransomware: cifrado, borrado de backups, o acceso masivo a archivos.
- Capacidad para identificar movimientos laterales, abuso de credenciales y explotación activa de vulnerabilidades.

2. Correlación avanzada y reglas personalizadas

- La plataforma deberá permitir la creación o personalización de reglas de correlación basadas en eventos provenientes de múltiples fuentes y condiciones lógicas definibles por el administrador, incluyendo tipificación de incidentes detectados con base en el marco de referencia MITRE ATT&CK o equivalentes.

3. Capacidades de análisis forense

- La plataforma deberá habilitar funciones de análisis forense sobre dispositivos protegidos incluyendo capacidades como:

  - Exploración de archivos, procesos y actividad del sistema.
  - Consulta y exportación de registros de eventos logs relevantes.
  - Extracción de memoria de procesos (preferiblemente mediante funcionalidades de memory dump).
  - Recolección de datos específicos (scripted forensic capture).
  - Ejecución remota de comandos y scripts.
  - Comandos de remediación: eliminación de archivos, detención de procesos, edición de registro, transferencia de artefactos.

1.13 INGESTA DE DATOS DEL XDR Y SIEM

1. Conectividad e integración de fuentes

- La plataforma deberá contar con capacidades de conectividad que permitan la integración de datos desde múltiples fuentes relevantes, mediante conectores nativos, APIs o colectores de logs. Deberá soportar, al menos, la ingesta de información proveniente de: endpoints, servidores, servicios

en la nube, redes, sistemas de identidad, correo electrónico, dispositivos de seguridad, aplicaciones corporativas y otros sistemas críticos para la organización.

- La plataforma deberá incluir un tablero operativo de seguimiento del consumo de eventos provenientes de las distintas fuentes de datos conectadas al sistema de gestión (XDR, SIEM).

2. Parsers personalizados para fuentes no estándar

- La plataforma deberá ofrecer la capacidad de crear parsers personalizados para fuentes de datos no estandarizadas, utilizando herramientas como scripts, expresiones regulares (regex) o funciones nativas que faciliten la transformación, enriquecimiento y clasificación de eventos para su posterior análisis.

3. Compatibilidad con entornos diversos

- El componente de recolección de datos deberá ser desplegable en múltiples entornos (físico, virtual o nube) y ser compatible, al menos, con los siguientes sistemas operativos:
    - Windows (versiones soportadas oficialmente por el fabricante).
    - Windows Server (versiones soportadas oficialmente por el fabricante).
    - Linux (versiones de distribución empresarial).
    - MacOS (versiones soportadas oficialmente por el fabricante).

4. Integraciones y extensibilidad

- La plataforma deberá contar con capacidades de integración con herramientas de terceros mediante API REST u otros mecanismos estándar. Además, deberá permitir la validación operativa de las integraciones activas, ya sea mediante paneles integrados, bitácoras de

funcionamiento, o mecanismos equivalentes que garanticen trazabilidad y visibilidad de dichas integraciones.

5. Visualización y análisis operacional

- La plataforma deberá permitir la creación o utilización de tableros de control personalizables que faciliten el seguimiento de tendencias de seguridad, identificación de Indicadores de Compromiso (IOCs) y monitoreo de métricas clave del proceso de respuesta.

  Estos tableros deberán incluir al menos los siguientes indicadores:

  - Tiempo promedio de detección de amenazas.
  - Tiempo promedio de diagnóstico.
  - Tiempo promedio de cierre de incidentes.

1.14 Automatización y Respuesta Orquestada SOAR

1. Integración del módulo SOAR

- La solución deberá integrar capacidades de orquestación y automatización (SOAR) que funcionen de forma interoperable con la consola de administración del SIEM, permitiendo la ejecución de acciones desde un entorno operativo unificado. Preferiblemente, esta integración deberá realizarse sin depender de herramientas o interfaces externas, a fin de garantizar una experiencia coherente para el usuario.

2. Desarrollo y uso de playbooks

- La plataforma debe permitir la creación de playbooks de automatización, que definan flujos de trabajo de respuesta ante eventos de seguridad.
- Debe incluir una biblioteca de playbooks predefinidos, listos para ser utilizados o adaptados, sin necesidad de desarrollarlos desde cero.
- El módulo debe permitir la creación de playbooks en los siguientes escenarios:

- Basados en eventos automáticos: alertas, detecciones, incidentes, cambios en dispositivos o políticas.
- Activados por demanda: mediante acción manual de un administrador para ejecutar tareas programadas.

3. Registro y auditoría de ejecuciones

- Cada playbook ejecutado debe generar un registro detallado que incluya las actividades realizadas, decisiones tomadas, resultados obtenidos y cualquier error encontrado, para facilitar la auditoría y la mejora continua.

4. Acciones automatizadas de remediación

- El módulo de SOAR debe tener la capacidad de ejecutar acciones correctivas automáticas y personalizables, tales como:
    - Aislamiento de dispositivos comprometidos.
    - Bloqueo de autenticaciones o usuarios.
    - Deshabilitación de cuentas.
    - envió de artefactos a entornos de sandboxing.
    - Captura de información para análisis forense.

Especificaciones Técnicas: Solución de Protección DNS

II. Capacidad de Protección DNS

La solución deberá cumplir, como mínimo, con las siguientes características técnicas:

2.1. Capacidad de Protección y Funcionalidad General

I. Protección DNS a nivel global:

- La solución debe inspeccionar y analizar todas las solicitudes DNS realizadas por los dispositivos institucionales, mediante una red de infraestructura global que asegure alta disponibilidad, baja latencia y enrutamiento óptimo mediante tecnología Anycast o equivalente.

II. Bloqueo de amenazas en tiempo real:

- Debe bloquear de forma inmediata solicitudes de resolución de nombres de dominio hacia sitios maliciosos identificados en listas dinámicas de amenazas que incluyan malware, phishing, ransomware, botnets, cryptomining y otros vectores de ataque relacionados.

III. Detección y bloqueo de tráfico de comando y control (C2):

- La solución debe identificar y bloquear conexiones de comando y control utilizadas por redes de botnets o malware para exfiltración de datos, callbacks o control remoto, incluyendo intentos que eludan las consultas DNS tradicionales.

IV. Filtrado de aplicaciones por categorías:

- Capacidad para identificar y controlar el uso de aplicaciones basadas en web mediante políticas configurables que permitan o bloqueen categorías específicas de aplicaciones (por ejemplo, mensajería, redes sociales, almacenamiento en la nube, etc.).

V. Descubrimiento de aplicaciones no autorizadas (Shadow IT):

- La solución debe permitir identificar aplicaciones en la nube utilizadas por los usuarios que no han sido aprobadas formalmente, brindando visibilidad de riesgos asociados y permitiendo aplicar políticas de bloqueo o restricción.

VI. Proxy selectivo inteligente:

- Preferiblemente, la solución debe incluir un proxy en la nube con capacidad de inspeccionar el tráfico HTTP y HTTPS únicamente para dominios considerados de riesgo, evitando impactar la latencia y el rendimiento del tráfico legítimo. Este proxy debe integrar análisis de reputación de archivos y motores antivirus en la inspección.

VII. Inteligencia de amenazas integrada:

- La solución deberá contar con mecanismos de inteligencia de amenazas para identifica dominios maliciosos conocidos y emergentes, basados de fuentes globales y capacidades como aprendizaje automático, análisis predictivo y correlación histórica de eventos.

VIII. Sin necesidad de infraestructura local:

- La solución no debe requerir implementación de hardware adicional en la institución ni la instalación de dispositivos on-premise para su operación. La solución debe integrarse fácilmente con los servidores DNS existentes o mecanismos de integración con los dispositivos o servidores NDS existentes.

IX. Trazabilidad a nivel de LAN:

- La solución preferiblemente deberá contar con la capacidad que permita recopilar y correlacionar información de tráfico DNS y actividad de red de los dispositivos internos, proporcionando trazabilidad y visibilidad granular de usuarios y equipos en la red LAN corporativa, sin requerir la instalación de agentes individuales en cada dispositivo final, mediante mecanismos como la integración con servicios de directorio, el uso de sensores virtuales, registros de red o componentes equivalentes.

X. Extensión de protección fuera del perímetro:

- La solución debe extender su cobertura a usuarios móviles o en teletrabajo sin requerir el uso exclusivo de VPN, utilizando agentes ligeros o

integraciones con el sistema operativo o mecanismos equivalentes que permitan aplicar las políticas de seguridad DNS fuera de la red institucional.

XI. Soporte para múltiples plataformas:

- Capacidad para proteger dispositivos con sistemas operativos Windows, MacOS, iOS, Android y Chromebook, tanto administrados (MDM) como no administrados.

XII. Control de acceso por tenant en la nube:

- Preferiblemente, la solución deberá contar con capacidades de aplicar políticas que restrinjan el acceso a cuentas personales en servicios de almacenamiento y colaboración en la nube, asegurando que únicamente se permita el acceso a los entornos corporativos autorizados, con capacidad para definir acciones específicas sobre dicho tráfico y garantizar el cumplimiento de las políticas institucionales.

XIII. Control de descargas y cargas de archivos:

- Posibilidad de bloquear descargas y cargas de archivos en función de su tipo o categoría (ejecutables, comprimidos, imágenes, etc.) y restringir acciones en aplicaciones web como WhatsApp, Facebook, Messenger, entre otras.

XIV. Visualización de servicios en la nube (autorizados y no autorizados):

- La solución deberá permitir identificar los servicios en la nube en uso, quién los utiliza y el riesgo asociado.

XV. Optimización del proxy:

- La solución preferiblemente deberá incluir mecanismos de optimización que permitan enrutar mediante proxy únicamente las solicitudes dirigidas a dominios categorizados como de riesgo o no clasificados, con el fin de minimizar el impacto en el rendimiento de la red y mejorar la experiencia del usuario final

XVI. Extensión de protección sin agentes adicionales:

- Aprovechar clientes existentes para aplicar protección DNS, sin necesidad de instalar nuevos agentes ni requerir intervención del usuario.

XVII. Compatibilidad con clientes ligeros:

La solución deberá contar, preferiblemente con un cliente ligero para sistemas operativos Windows y MacOS que permita aplicar políticas de seguridad DNS sin depender de red o ubicación.

XVIII. Protección para invitados:

- La solución deberá permitir aplicar políticas de seguridad DNS en redes Wi-Fi corporativas y de invitados, a fin de garantizar una navegación segura sin requerir instalación de agentes en los dispositivos conectados.

XIX. Compatibilidad sin conflictos:

- La solución deberá operar de manera transparente y sin generar conflictos con otras tecnologías de seguridad existentes, tales como: antivirus, sandbox u otros sistemas, ni requerir firewall, NGIPS, proxy ni DPI para bloquear amenazas en tiempo real.

XX. Integración con plataforma de almacenamiento cloud:

- Preferiblemente, la solución deberá tener la capacidad de integrarse con aplicaciones de almacenamiento en la nube y realizar escaneos automáticos para detectar y eliminar archivos maliciosos presentes en dichas aplicaciones, garantizando la protección activa del entorno de almacenamiento y evitando la propagación de malware.

2.2 Administración y Gestión

I. Consola de administración centralizada:

- La solución debe ofrecer una única consola web segura accesible meditante conexión segura (HTTPS) para administración, configuración, monitoreo y generación de reportes, accesible desde cualquier ubicación sin requerir VPN.

II. Gestión basada en roles:

- La solución deberá soportar una administración basada en roles dentro de la consola web, permitiendo asignar perfiles diferenciados tales como administrador, auditor, lectura o generación de reportes. Esta capacidad debe facilitar la delegación de funciones, asegurar el principio de mínimo privilegio y permitir una gestión segmentada conforme a las necesidades operativas de la institución.

III. Bitácora de cambios:

- La solución debe registrar todas las modificaciones realizadas en la configuración, indicando fecha, hora, usuario y detalle del cambio, para auditoría y cumplimiento.

IV. Creación de políticas granulares:

- La solución deberá permitir crear políticas de seguridad basadas en combinación de usuarios, grupos, direcciones IP, nombres de dominio, aplicaciones y categorías de contenido.

V. API de integración:

- La solución deberá contar con una interfaz de programación de aplicaciones (API), preferiblemente de tipo REST, que permita integrar funciones como consulta de reportes, acceso a logs y administración de políticas con otras plataformas institucionales. Esta integración deberá facilitar el intercambio de información con soluciones como SIEM, herramientas de respuesta a incidentes (SOAR) o portales corporativos, y deberá estar debidamente documentada.

VI. Exportación de registros:

- Capacidad de exportar registros de consulta DNS, actividad de navegación web a formatos estándar como CSV. Asimismo, deberá permitir la exportación a plataformas de almacenamiento externo (por ejemplo, Amazon S3) y la integración con sistemas SIEM o soluciones de análisis de seguridad, a través de conectores nativos o mediante API, syslog..

VII. Personalización de páginas de bloqueo:

- La solución deberá permitir, preferiblemente, la personalización de las páginas de bloqueo mostradas a los usuarios cuando se impida el acceso a sitios o servicios no autorizados. Esta personalización debe incluir la posibilidad de incorporar elementos de identidad institucional (como logotipo y colores) y mensajes adaptados según el contexto de la política aplicada.

VIII. Integración con directorios corporativos:

- Integración con Active Directory u otros directorios LDAP para aplicar políticas basadas en identidad (usuario o grupo), sin requerir sincronización manual de usuarios.

IX. Asistente de políticas:

- La solución deberá contar, preferiblemente, con un asistente integrado que facilite la creación de políticas de seguridad DNS mediante un proceso guiado paso a paso. Esta funcionalidad deberá permitir validar o simular el impacto de las políticas antes de su aplicación definitiva, con el objetivo de evitar configuraciones incorrectas y facilitar la administración.

X. Políticas unificadas en interfaz integrada:

- La solución deberá permitir crear y gestionar políticas DNS, web y firewall desde una sola interfaz.

XI. Panel web de generación de informes:

- La solución deberá contar con un panel web para crear y generar informes centralizados.

XII. Soporte de arquitectura multitenant:

- La solución preferiblemente deberá permitir gestionar múltiples organizaciones o entidades de forma independiente dentro de la consola de administración. Esto incluirá la capacidad de definir políticas, visualizar registros, generar reportes y administrar configuraciones por separado para cada tenant o grupo definido, sin comprometer la seguridad ni la autonomía operativa entre ellos.

XIII. Integración avanzada:

- La solución deberá permitir establecer integraciones con sistemas externos, incluyendo plataformas SIEM, herramientas de respuesta a incidentes u otras soluciones corporativas. Preferiblemente, deberá permitir configurar al menos diez (10) integraciones personalizadas adicionales con sistemas internos mediante API, conectores o mecanismos de exportación compatibles, facilitando la interoperabilidad y el enriquecimiento de datos de seguridad.

2.3. Infraestructura y Desempeño

I. Infraestructura cloud global y redundante:

- La solución debe operar mediante una red de centros de datos distribuidos globalmente, utilizando balanceo de carga geográfico utilizando preferiblemente tecnología Anycast u otro mecanismo equivalente para garantizar baja latencia y alta disponibilidad.

II. Escalabilidad automática:

- Arquitectura basada en microservicios o equivalente con capacidad de escalado automático para mantener el rendimiento sin intervención manual.

III. Procesamiento de grandes volúmenes:

- Capacidad de procesar grandes solicitudes DNS diarias a nivel global, asegurando que las consultas de la institución sean procesadas sin afectación de rendimiento.

IV. Optimización Anycast y geo balanceo:

- Redirigir solicitudes DNS al nodo más rápido mediante Anycast o equivalente, con balanceo geo-consciente para SWG.

V. Alta escalabilidad:

- La solución deberá contar con una arquitectura moderna basada en microservicios u otros mecanismos equivalentes, que permita el escalado automático de recursos y capacidades en función de la demanda, garantizando un rendimiento óptimo sin necesidad de intervención manual.

VI. Retención ilimitada de registros:

- La solución deberá permitir la retención de registros de consulta DNS y actividad relacionada durante el período que la institución defina, incluyendo la posibilidad de retención prolongada o indefinida, ya sea de forma nativa o mediante integración con servicios de almacenamiento externo

2.4. Inteligencia de Amenazas y Análisis

I. Modelos predictivos avanzados:

- La solución deberá utilizar modelos de análisis e inteligencia para puntuar y clasificar datos, detectar anomalías y amenazas emergentes, empleando técnicas como aprendizaje automático (machine learning), análisis conductual o modelos de puntuación de riesgo.

II. Predicción de amenazas y análisis contextual:

- La solución deberá contar con capacidades de predicción de amenazas y análisis contextual, que permitan anticipar destinos potencialmente maliciosos y comprender la infraestructura utilizada por los atacantes, mediante la correlación de datos históricos y en tiempo real provenientes de múltiples fuentes de inteligencia.

III. Análisis enriquecido con datos públicos y privados:

- Obtener inteligencia de amenazas alimentada por diversas fuentes (públicas y privadas) accesible vía consola o API.

IV. Optimización de tráfico SWG:

- La solución deberá contar con mecanismos de optimización que permitan minimizar el tráfico inspeccionado a profundidad, priorizando únicamente las solicitudes hacia dominios o destinos considerados de riesgo, con el objetivo de mantener un alto rendimiento y baja latencia en el resto del tráfico legítimo.