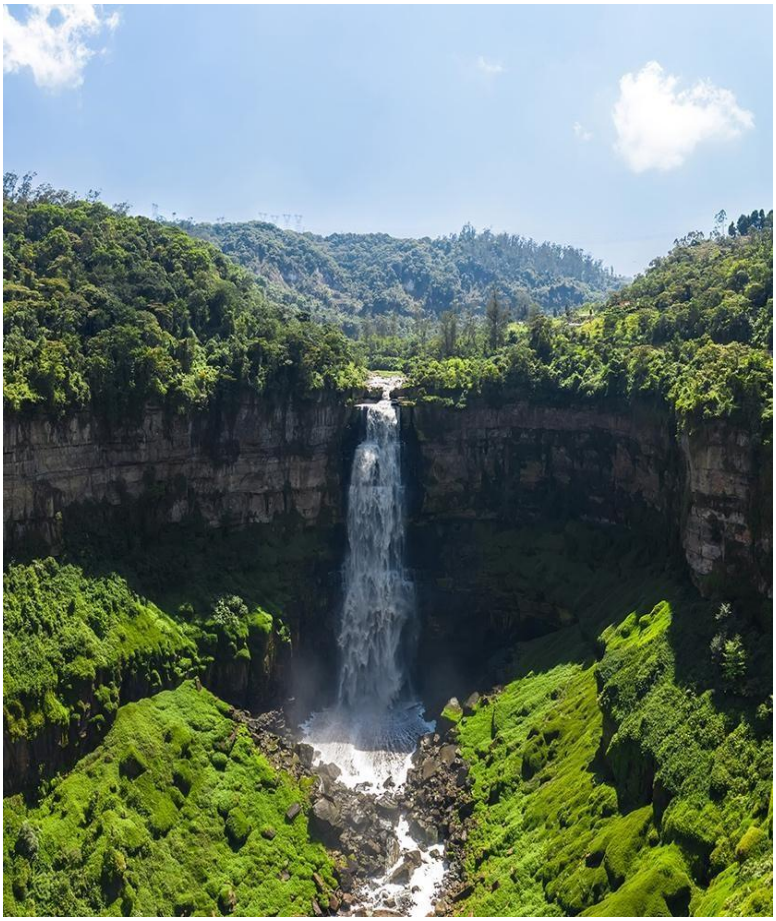
CORPORACIÓN AUTONOMA REGIONAL DE CUNDINAMARCA – CAR



ANEXO DE ESPECIFICACIONES TÉCNICAS DETALLADAS

ADQUISICIÓN DE LICENCIAMIENTO POR SUSCRIPCIÓN (SAAS), IMPLEMENTACIÓN, TRANSFERENCIA DE CONOCIMIENTO Y SOPORTE TÉCNICO DE UNA SOLUCIÓN INTEGRAL DE PROTECCIÓN AVANZADA DE END POINTS PARA ESTACIONES DE TRABAJO Y SERVIDORES, INCLUYENDO CAPACIDADES EDR Y CONSOLA CENTRALIZADA DE ADMINISTRACIÓN Y MONITOREO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA – CAR.

Bogotá D.C., 2026

1. Planteamiento del Problema (ANTECEDENTES)

En la era digital, la protección de la información se ha convertido en una prioridad para organizaciones públicas y privadas. El creciente número de amenazas informáticas, como virus, ransomware, spyware y otras, pone en riesgo la confidencialidad, integridad y disponibilidad de los sistemas y datos institucionales. Ante esta situación, la adquisición de software antivirus o solución integral de protección de endpoints (EPP, EDR y XDR) confiable y actualizado representa una necesidad fundamental dentro de cualquier estrategia de seguridad informática.

Históricamente, la Corporación Autónoma Regional de Cundinamarca (CAR), con sede principal en Bogotá y 14 Direcciones Regionales distribuidas en zonas estratégicas como Sabana Centro, Tequendama y Sumapaz, ha desempeñado un papel clave en la protección y gestión ambiental del territorio bajo su jurisdicción.

Con el paso del tiempo, la CAR ha avanzado significativamente en la adopción de infraestructura tecnológica moderna, integrando plataformas como, HyperV, Nutanix para la administración de servidores físicos y virtuales. Este proceso de transformación digital también incluye la actualización de estaciones de trabajo, equipos de escritorio, portátiles y demás dispositivos que conforman su ecosistema informático.

Dado este entorno tecnológico en constante evolución, resulta crucial fortalecer los mecanismos de protección para salvaguardar la información crítica y sensible que gestiona la entidad diariamente. Entre estos activos se encuentran:

- Solicitudes ambientales, licencias y trámites presentados por ciudadanos, empresas e instituciones.
- Estudios de impacto ambiental y datos relacionados con la gestión de los recursos naturales.
- Información almacenada en el Sistema de Información Geográfica (SIG) y en bases de datos georreferenciadas, esenciales para la toma de decisiones territoriales y ambientales.
- Datos financieros, presupuestales y contractuales, que forman parte de los procesos administrativos de la entidad.

Estos activos están expuestos permanentemente a ciberamenazas como malware, ransomware, ingeniería social, accesos no autorizados y vulnerabilidades en el software y hardware utilizado. Una falla en la seguridad podría generar consecuencias graves, no solo en la operación interna de la CAR, sino también en la confianza pública y en la protección del medio ambiente.

En la actualidad, la CAR dispone de una solución de seguridad basada en Kaspersky Endpoint Security for Business – Advanced Latin America Edition, bajo la licencia 2854000451-57738424,

con capacidad histórica para 1.798 dispositivos (incluyendo 103 servidores). Sin embargo, dicha licencia finalizó su vigencia en el año 2024, por lo cual actualmente la Entidad presenta limitaciones en la cobertura integral, soporte especializado, actualización y administración centralizada de capacidades de protección sobre la totalidad de los activos tecnológicos requeridos a nivel de endpoint, manteniendo controles complementarios de seguridad desde plataformas perimetrales institucionales.

Este escenario incrementa el nivel de exposición frente a amenazas cibernéticas, especialmente en un contexto de crecimiento sostenido de la infraestructura tecnológica y de los activos digitales de la Entidad.

Durante este periodo, la Corporación ha presentado un incremento en la cantidad de dispositivos y plataformas tecnológicas que interactúan con los sistemas institucionales, incluyendo nuevos equipos de usuario final, dispositivos fuera del dominio tradicional, esquemas de teletrabajo, expansión de servidores virtuales y crecimiento de plataformas estratégicas como IDECAR, PNUD, CDA, Sistemas de Información Geográfica (SIG), así como activos tecnológicos desplegados en sedes regionales y otros servicios institucionales.

En este contexto, el requerimiento actual de mínimo 2.400 endpoints no corresponde a un sobredimensionamiento, sino a una proyección técnica orientada a garantizar:

- La cobertura de la infraestructura tecnológica actual de la Entidad.
- La incorporación de nuevos activos digitales y plataformas tecnológicas.
- La protección de dispositivos externos que interactúan con los sistemas institucionales.
- La continuidad operativa durante la vigencia contractual de 24 meses.
- La escalabilidad necesaria para acompañar el crecimiento tecnológico de la Corporación.

Por lo anterior, se hace necesario adquirir una solución integral de protección de endpoints y servidores con capacidades EPP, EDR y XDR, administrable mediante consola centralizada en la nube, que permita la gestión unificada de servidores Windows/Linux y estaciones de trabajo de la Entidad, bajo un modelo moderno, escalable y alineado con las necesidades actuales de ciberseguridad de la CAR.

1. Cantidad de licencias disponibles: Actualmente la CAR cuenta con una licencia para 1.798 dispositivos, cuya vigencia ya finalizó y que, adicionalmente, en concordancia con el crecimiento institucional y la evolución de la infraestructura tecnológica, requiere fortalecer y ampliar las capacidades de cobertura y administración de protección sobre los endpoints de la Corporación. En este contexto, se hace necesaria una actualización y ampliación de capacidades que permita cubrir tanto los equipos de la red corporativa como dispositivos externos que interactúan con los sistemas institucionales, considerando además el crecimiento de plataformas virtuales, esquemas de teletrabajo y nuevos activos digitales de la Entidad.

2. Tipo de licenciamiento vigente: El modelo actual corresponde a licenciamiento comercial por nodos. Se requiere definir un esquema de licenciamiento actualizado, flexible y

escalable, que garantice continuidad en la protección y permita adaptarse al crecimiento tecnológico de la entidad.

3. Consola de administración: La solución actual se gestiona mediante la consola de Kaspersky. Sin embargo, debido al vencimiento de la licencia y la necesidad de mayor amplitud en el control y monitoreo, se requiere implementar una consola de administración centralizada y renovada, que permita gestionar tanto dispositivos internos como externos al dominio corporativo (se requiere en lo posible administrar los dispositivos externos mediante la consola y/o mediante agentes.

4. Consola de administración: La consola de administración de antivirus o solución integral de protección de endpoints (EPP, EDR y XDR), debe contener los equipos enrolados en la medida que se desplieguen los Jobs y políticas con control avanzado de endpoints tanto para servidores Windows a partir de 2016 y Linux, equipos de escritorio, reportes centralizados y compatibilidad con las tecnologías modernas y adoptadas por la entidad.

En conclusión, la adquisición e implementación de un antivirus o solución integral de protección de endpoints (EPP, EDR y XDR), acompañada de una consola de administración actualizada, constituye una medida indispensable para la protección integral de los activos de información de la CAR. Esta inversión no solo garantiza la continuidad de la operación institucional, sino que fortalece la seguridad digital de cara a los retos de transformación tecnológica y a la responsabilidad de proteger la información corporativa misional estructurada y no estructurada.

2. Objetivos

2.1. Objeto Contractual:

ADQUISICIÓN DE LICENCIAMIENTO POR SUSCRIPCIÓN (SAAS), IMPLEMENTACIÓN, TRANSFERENCIA DE CONOCIMIENTO Y SOPORTE TÉCNICO DE UNA SOLUCIÓN INTEGRAL DE PROTECCIÓN AVANZADA DE END POINTS PARA ESTACIONES DE TRABAJO Y SERVIDORES, INCLUYENDO CAPACIDADES EDR Y CONSOLA CENTRALIZADA DE ADMINISTRACIÓN Y MONITOREO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA - CAR.

- **Eje temático:** VI. SISTEMAS DE MONITOREO, TECNOLOGÍA E INNOVACIÓN.
- **Proyecto: 18.** Gestión Institucional e Interinstitucional.
- **Objetivo: 18.3.** Garantizar una plataforma tecnológica transversal moderna, que soporte los sistemas de información de apoyo, permitiendo la gestión efectiva de la Entidad.
- **Actividad 18.3.2** Disponer de los recursos tecnológicos operativos de la Entidad, mediante el mantenimiento y escalamiento del software y la infraestructura actual.
- El Plan de Acción Cuatrienal PAC se encuentra disponible para la consulta tanto de los funcionarios como de la ciudadanía en general en el link: http://www.car.gov.co/vercontenido/3868 de la página web de la entidad.

2.2. Objetivo General:

Fortalecer la postura de seguridad de la Corporación Autónoma Regional de Cundinamarca – CAR mediante la implementación de una solución de antivirus o solución integral de protección de endpoints (EPP, EDR y XDR) de protección avanzada para dispositivos finales y servidores, que permita prevenir, detectar y responder a amenazas cibernéticas, especialmente aquellas que afectan el entorno de interacción de los usuarios finales, en un contexto donde los incidentes de seguridad han incrementado por la falta de tecnologías especializadas de defensa y monitoreo.

2.3. Objetivos Específicos:

- Implementar un antivirus o solución integral de protección de endpoints (EPP, EDR y XDR), para protección para dispositivos finales, servidores y que cumpla con los estándares de seguridad exigidos por la CAR, con capacidades antimalware, detección de amenazas avanzadas y respuesta automatizada.
- Realizar la instalación de la solución en toda la infraestructura objetivo de la CAR, incluyendo estaciones de trabajo, portátiles, servidores físicos y virtuales, asegurando una cobertura integral, centralizada y escalable.
- Permitir el monitoreo continuo y la gestión de incidentes de seguridad detectados por la solución, incluyendo mecanismos de alerta, análisis forense, trazabilidad y contención.
- Garantizar la actualización continua de motores de detección, reglas, firmas y configuraciones de seguridad mediante un modelo de servicio SaaS, sin requerir intervención manual, conforme a las buenas prácticas de protección activa contra amenazas emergentes.
- Asegurar que la solución y su implementación se encuentren alineadas con las políticas del SGSI de la CAR, así como con la normatividad vigente, en especial lo dispuesto por la norma ISO/IEC 27001:2022 y la Ley 1581 de 2012.
- Transferir al personal técnico responsable de la operación de la solución, el conocimiento acerca del uso, despliegue, generación de Jobs y políticas, así como las buenas prácticas de seguridad digital y la prevención de incidentes, como parte del fortalecimiento continuo de la cultura institucional en ciberseguridad.

3. JUSTIFICACIÓN DEL PROYECTO

En la actualidad, la protección de la información constituye un pilar fundamental dentro de las estrategias tecnológicas de cualquier organización. En el contexto de la transformación digital, las amenazas cibernéticas han incrementado su frecuencia y complejidad, afectando gravemente la confidencialidad, integridad y disponibilidad de los datos institucionales. Virus, ransomware, spyware y otros ataques dirigidos se han convertido en riesgos latentes para los sistemas informáticos, tanto en el sector público como en el privado.

La Corporación Autónoma Regional de Cundinamarca (CAR), en cumplimiento de su misión de proteger y gestionar los recursos naturales del territorio bajo su jurisdicción, ha fortalecido su infraestructura tecnológica mediante la incorporación de plataformas avanzadas como, Hyper-V, Nutanix . Asimismo, ha modernizado su parque tecnológico, incluyendo estaciones de trabajo,

portátiles y otros dispositivos, lo que evidencia un claro compromiso con la eficiencia operativa y la innovación digital.

No obstante, este entorno tecnológico en constante evolución requiere de mecanismos de seguridad robustos y actualizados, capaces de enfrentar de manera efectiva los desafíos que representan las ciberamenazas. La CAR gestiona diariamente información crítica y sensible, como solicitudes ambientales, estudios técnicos, datos geoespaciales, registros financieros, presupuestales y contractuales, entre otros. Estos activos son esenciales para la toma de decisiones estratégicas, tanto administrativas como ambientales.

La exposición de estos datos a incidentes de seguridad informática puede generar consecuencias significativas, incluyendo la interrupción de servicios, pérdida de información valiosa, daños reputacionales y un impacto negativo en la confianza de los ciudadanos. Por esta razón, se hace imprescindible la adquisición de una solución antivirus o solución integral de protección de endpoints (EPP, EDR y XDR) empresarial confiable y eficiente, que permitan proteger integralmente el ecosistema digital de la entidad.

Estas herramientas no solo fortalecerán la defensa ante ciberataques, sino que también facilitarán una administración centralizada de la seguridad, asegurando la continuidad operativa y el cumplimiento de los principios de gobierno digital y buenas prácticas en la gestión pública.

En conclusión, la inversión en soluciones de seguridad informática actualizadas no es solo una medida preventiva, sino una necesidad estratégica para garantizar la protección de la información institucional, asegurar la prestación eficiente de los servicios a la ciudadanía y respaldar la misión ambiental de la CAR. Lo anterior cumpliendo lo estipulado en la norma ISO/IEC 27001:2022 en su numeral A.8.7 – Protección contra malware, incorporando desafíos actuales como ciberseguridad y cloud:

Código	**Control**
A.5.7	Inteligencia de amenazas
A.5.23	Seguridad en servicios cloud
A.5.30	Preparación de TI para continuidad de negocio
A.7.4	Monitorización de seguridad física
A.8.9	Gestión de configuración
A.8.10	Eliminación segura de información
A.8.11	Enmascaramiento de datos
A.8.12	Prevención de fuga de datos
A.8.16	Monitorización de actividades
A.8.23	Filtrado web

A.8.28	Codificación segura

4. DESARROLLO TÉCNICO

4.1. Alcance del objeto

La SOLUCIÓN INTEGRAL DE PROTECCIÓN DE ENDPOINTS para estaciones de trabajo y servidores, que incluye consola de administración, debe cumplir con los requisitos técnicos que se desarrollarán a lo largo de este numeral.

Previo a presentar las capacidades, se presentará la arquitectura en capas funcionales: protección en endpoint (EPP), capacidades de detección y respuesta (EDR) y una capa superior de correlación e inteligencia (XDR), que integrará múltiples fuentes para análisis centralizado. Esto permite asegurar que las propuestas cumplan con un enfoque moderno de ciberseguridad basado en visibilidad, prevención y respuesta.

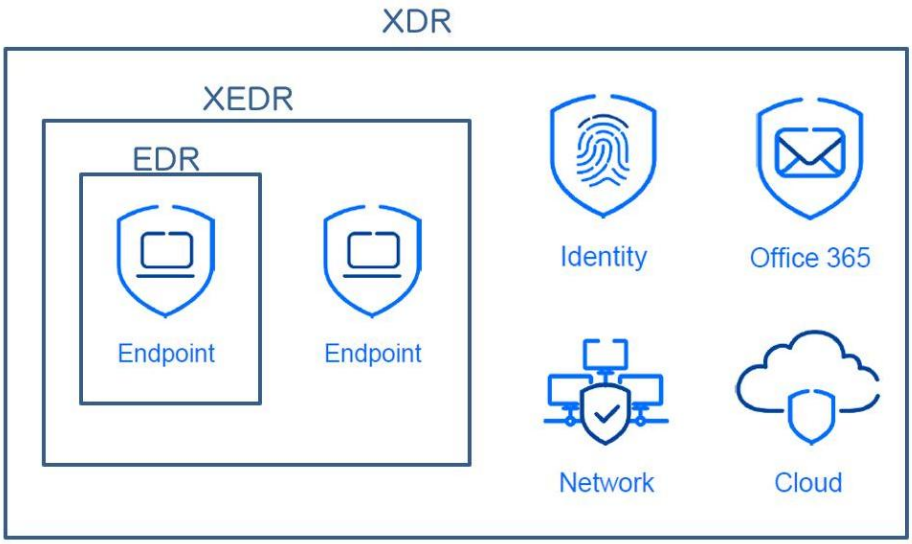


Ilustración 1 Arquitectura Gráfica de Ingesta.

Para mayor claridad, se aporta para el entendimiento del alcance del proyecto Arquitectura de Referencia EPP - EDR – XDR:



Ilustración 2 Arquitectura de Referencia

4.1.1. Consola de Administración de la solución

- Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán propuestas que incluyan consolas de administración de la plataforma de diferentes fabricantes.
- La consola de monitoreo y configuración deberá ser a través de una central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos.
- La consola deberá incluir un dashboard central con resumen del estado de seguridad de dispositivos y usuarios, así como alertas recientes, incluyendo alertas informativas, y una vista de alertas que permita filtrado por prioridad.
- Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.
- Este mecanismo de comunicación vía API deberá obtener los eventos y alertas asociados a la consola en al menos, los siguientes formatos: json, cef, or keyvalue.
- La solución deberá permitir la consulta de eventos y alertas desde la consola central mediante API para fines de integración y correlación externa.

- La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
- Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
- Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.
- La instalación debe poder realizarse de forma manual obtenido a través del cliente descargado de la consola central o también vía correo electrónico. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.
- La solución deberá proporcionar actualizaciones automáticas de producto y actualizaciones de seguridad contra nuevas amenazas, e incluir protección frente a malware y tráfico de red malicioso.
- Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
- La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros.
- Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador;
- Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
- Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
- Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración;
- La consola deberá mostrar, como mínimo, nombre del equipo, sistema operativo y versión, direcciones IP, estado de salud, última actividad, último estado de actualización del agente, grupo, productos asignados y versiones instaladas
- Capacidad de generación de informes, estadísticas o gráficos, tales como:
    - Permitir visualizar el detalle de usuarios y su estado de protección, incluyendo usuarios no protegidos"
    - Permitir visualizar el detalle de dispositivos activos e inactivos, su estado de salud, eventos recientes y condición de protección."
- La solución deberá permitir configurar el ancho de banda utilizado para la actualización del agente en estaciones Windows.
- La solución deberá permitir controlar la disponibilidad de actualizaciones y seleccionar paquetes de software por política, incluyendo despliegue piloto a subconjuntos de equipos antes del despliegue general.
- La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
- La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.

- La solución deberá contar con filtros preconfigurados y capacidades de filtrado en la consola de administración para visualizar exclusivamente los equipos que presenten eventos de seguridad, alertas o estados de salud que requieran atención, permitiendo al administrador priorizar su gestión y aplicar acciones de remediación o administración sobre dichos equipos.
- La consola deberá mostrar los equipos administrados mediante categorías, columnas configurables y filtros multiatributo, incluyendo estado de salud, sistema operativo, última actividad, IP, grupo y modo de agente.
- Una vez identificado un problema, la solución deberá permitir acciones remotas de respuesta, incluyendo al menos las siguientes:
    - Forzar una actualización en ese momento."
    - Ver los detalles de los eventos recientes."
    - Permitir iniciar un escaneo del equipo en busca de amenazas desde la consola de administración"
    - Cambio de grupo."
    - Eliminación del equipo."
    - Aislamiento de dispositivo."
    - Sesión remota de línea de comando para investigación y remediación de posibles incidentes de seguridad"
- La solución deberá permitir mover equipos entre grupos y administrar políticas aplicadas a grupos de equipos.
- La solución deberá permitir visualizar, filtrar y exportar registros de auditoría de las actividades monitoreadas en la consola de administración, incluyendo como mínimo fecha y hora, cuenta administrativa, tipo de elemento, elemento modificado, descripción de la acción e IP de origen, con capacidad de consulta histórica sobre el periodo contratado.
- Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF.
- Debe contar con varios informes para el análisis y control de los usuarios y equipos de punto final. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los para los equipos de punto final.
- La solución deberá permitir ejecutar reportes manualmente, guardarlos y enviarlos por correo electrónico bajo programación, en formatos PDF y/o CSV.
- Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.
- Deberá tener la posibilidad de instalar un servidor para reenvío de eventos en caso de que el agente no pueda comunicarse con la consola en la nube.
- La solución deberá permitir el envío de advertencias de ataque por correo electrónico a administradores registrados.

4.1.2. Características básicas del agente de protección contra malware

- La solución de protección de endpoints propuesta debe estar en el Cuadrante Mágico™ de Gartner® 2025 para Plataformas de Protección de Endpoints (EPP) como Líder, o en posiciones similares de calificación dentro de la plataforma Forrester, como *mínimo* por 3 años consecutivos incluyendo la nominación actual.

- Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
- Debe realizar verificación en tiempo real de archivos locales, remotos y medios extraíbles cuando sean accedidos o modificados, incluyendo análisis de descargas en progreso y protección frente a amenazas que afecten el inicio del sistema.
- Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente no deseadas.
- Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
- Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
- Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas.
- Debe contar con protección contra manipulación del agente impidiendo a los usuarios, incluido el administrador local, modificar la configuración, deshabilitar o desinstalar componentes sin autorización administrativa.
- Debe permitir el uso de una contraseña de protección para habilitar cambios locales controlados o la desinstalación autorizada del agente.
- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
- La solución deberá aplicar mecanismos de protección en tiempo de ejecución, mediante análisis de comportamiento y mitigación de exploits, capaces de detectar y bloquear comportamientos sospechosos o maliciosos de las aplicaciones durante su ejecución, incluyendo técnicas de explotación de memoria tales como buffer overflow, heap spray, stack execution y ROP.
- Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
- • La solución deberá contar con capacidades de Anti-Exploitation para proteger la integridad de procesos, endurecer la memoria de aplicaciones y aplicar controles de ejecución en tiempo de ejecución (runtime), incluyendo múltiples mecanismos de Capacidades técnicas avanzadas de mitigación de exploits en tiempo, sin requerir entrenamiento ni ajustes finos por parte del administrador.

4.1.3. Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas

- Protección de amenazas de día cero a través de tecnología de deep learning (signature less).
- La solución deberá contar con capacidades de Deep Learning sin firmas para la detección de malware conocido y previamente desconocido en pre-ejecución.
- La solución deberá proteger contra amenazas aún no conocidas mediante la detección y bloqueo de comportamiento malicioso o sospechoso durante la ejecución.
- Debe detectar el malware en pre-ejecución un tiempo aproximado mínimo de Capacidad de detección en tiempo real o cercano a tiempo real (20 milisegundos).
- Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.

- La solución deberá proporcionar análisis de causa raíz del incidente con visualización de la cadena de eventos y de los artefactos afectados, incluyendo procesos, archivos y claves de registro.
- Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
- Generación de excepciones ante falsos positivos.
- La solución debe tener capacidad de protección AMSI contra scripts maliciosos.
- La solución deberá contar con capacidad de prevención de tráfico malicioso en host mediante packet inspection (IPS).

4.1.4. Funcionalidad de protección contra ransomware

- La solución propuesta debe disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.
- Debe disponer de capacidad de remediación de la acción de cifrado malicioso de ransomware.
- Debe poseer protección anti-ransomware para el sector de boot.
- La solución debe incluir protección anti-ransomware basada en comportamiento en tiempo de ejecución, capaz de identificar cifrado malicioso, detener los procesos ofensivos y restaurar automáticamente los archivos afectados a su estado original.

4.1.5. Protección contra Vulnerabilidades y técnicas de explotación

- La solución propuesta debe brindar detección y protección de al menos las siguientes técnicas de explotación:
    - Enforce Data Execution Prevention;
    - Mandatory Address Space Layout Randomization;
    - Bottom-up ASLR;
    - Null Page (Null Deference Protection);
    - Heap Spray Allocation;
    - Dynamic Heap Spray;
    - Stack Pivot;
    - Stack Exec (MemProt);
    - EStack-based ROP Mitigations (Caller);
    - Branch-based ROP Mitigations (Hardware Assisted);
    - Structured Exception Handler Overwrite (SEHOP); Import Address Table Filtering (IAF)
    - Load Library;
    - Reflective DLL Injection;
    - Shellcode;
    - VBScript God Mode;
    - Wow64;
    - Syscall;
    - Hollow Process;
    - DLL Hijacking;

- Squiblydoo Applocker Bypass;
- APC Protection (Double Pulsar / AtomBombing);
- Mitigación de inyección de códigos en procesos
- Protección contra robo de credenciales
- Protección contra malware escondido en aplicaciones legitimas (code cave)
- Protección contra migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
- Protección contra escalada de privilegios y acceso elevado a recursos
- La solución deberá bloquear el abuso de aplicaciones confiables y técnicas de explotación orientadas a la ejecución de código arbitrario y a la manipulación de áreas críticas del sistema, incluyendo memoria, procesos y componentes del sistema operativo.
- Capacidad de evitar un reinicio en modo seguro para evitar que algún componente del agente sea desinstalado, modificado o vulnerado.

4.1.6. Características requeridas para la protección de punto final para servidores y estaciones de trabajo

- La protección deberá permitir el monitoreo y el control de dispositivos extraíbles en los dispositivos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo. Como mínimo de los siguientes dispositivos:
  - HD (hard disks) externos
  - Pendrives USB
  - Almacenables removibles seguras
  - CD, DVD, Blu-ray, floppy drives.
  - Interfaces de red inalámbrica
  - Módems
  - Bluetooth
  - Infrarrojo
  - MTP (Media Transfer Protocol)
  - PTP (Picture Transfer Protocol) como cámaras digitales.
- La protección deberá contar con capacidades de prevención de fuga de información (DLP) a nivel de punto final, orientadas al monitoreo y/o restricción de la transferencia de archivos que contengan información sensible desde los equipos protegidos hacia los destinos definidos por la Corporación.
- La solución deberá soportar reglas basadas en contenido y/o en archivo, e incluir listas de control de contenido preconfiguradas, así como la posibilidad de agregar reglas o listas propias de contenido. Como mínimo, deberá soportar la detección de los siguientes identificadores:
  - Números de tarjetas de crédito.
  - Números de cuentas bancarias.
  - Direcciones postales.
  - Direcciones de correo electrónico.

  - Otros identificadores sensibles requeridos mediante reglas de contenido personalizadas.
- La protección deberá contar con capacidad de monitoreo de integridad de archivos para sistemas operativos Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016 o superior, permitiendo detectar cambios tales como creación, modificación o eliminación sobre archivos y carpetas críticos del sistema, con base en una lista predefinida o línea base, y con posibilidad de personalizar los archivos, carpetas o rutas a supervisar según los requerimientos de la Entidad.
- La protección deberá permitir implementar mecanismos de control de ejecución de aplicaciones mediante política de autorización, de forma que únicamente puedan ejecutarse las aplicaciones previamente autorizadas por la Entidad, como minimo para sistemas operativos Windows Server 2016, Windows Server 2019 y Windows Server 2022.
- La solución deberá incluir capacidades de Web Control integradas en el agente y en la consola de administración y gestion que permitan restringir el acceso a sitios web por categorías, aplicar acciones de permitir, advertir o bloquear, y gestionar listas de sitios para su clasificación y aplicación de política.
- La solución deberá incluir capacidades de Application Control integradas en el agente y consola central, que permitan detectar y bloquear aplicaciones no autorizadas o no deseadas por política corporativa.
- La solución deberá incluir capacidades de protección web integradas en el agente y consola central, que permitan inspeccionar descargas en progreso, bloquear el acceso a sitios maliciosos mediante verificación de reputación y detectar archivos descargados de baja reputación.
- 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.

4.1.7. Despliegue Agente

- La solución debe soportar máquinas con arquitectura de 64 bits y contemplar soporte para arquitecturas de 32 bits en aquellas plataformas que el fabricante mantenga bajo su política de ciclo de vida, incluyendo esquemas de soporte legacy o extendido cuando aplique.
- El agente para estaciones de trabajo deberá ser compatible con macOS 13, macOS 14, macOS 15 y macOS 26, en equipos Intel de 64 bits y Apple Silicon (ARM64)
- El agente para estaciones de trabajo deberá ser compatible con Windows 10 de 64 bits y Windows 11.
- El agente para servidores Windows deberá ser compatible con Windows Server 2016, Windows Server 2019, Windows Server 2022 y Windows Server 2025.
- La solución deberá contemplar soporte para plataformas Windows legacy, conforme a la política de ciclo de vida del fabricante. Como mínimo, deberá incluir Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8.1 y Windows 10 de 32 bits, con el alcance de soporte que corresponda según la clasificación de ciclo de vida definida por el fabricante.

- La solución deberá ser compatible para su instalación en servidores con los sistemas operativos:
  - Amazon Linux 2
  - Amazon Linux 2023
  - CentOS
  - Debian 11
  - Debian 12
  - Debian 13
  - Oracle 8
  - Oracle 9
  - Oracle 10
  - RHEL 8
  - RHEL 9
  - RHEL 10
  - Suse Linux Enterprise Server 15
  - Ubuntu 22.04 (LTS)
  - Ubuntu 24.04 (LTS)
- Para las plataformas y versiones de sistema operativo relacionadas a continuación, clasificadas por el fabricante dentro de esquemas de soporte legacy, extendido o equivalente, la solución deberá contar con cobertura de soporte conforme a la política de ciclo de vida publicada por el fabricante:
  - CentOS 7 (3.10.0-1062 o posterior)
  - Debian 10
  - Oracle 7 (UEK 4.14 o posterior, RHCK 3.10.0-1062 or later)
  - RHEL 7 (3.10.0-1062 o posterior)
  - SUSE Linux Enterprise Server 12
  - Ubuntu 18.04 (LTS) (4.15 o posterior)
  - Ubuntu 20.04 (LTS)

4.1.8. Capacidades de EDR

- La solución deberá identificar y presentar actividades inusuales o sospechosas en los dispositivos protegidos.
- La solución deberá mapear las detecciones a tácticas y técnicas de MITRE ATT&CK.
- La solución deberá identificar dispositivos Windows cuyo sistema operativo no se haya actualizado por 30 días o más.
- La solución deberá ofrecer una vista gráfica de investigación que muestre cómo se desarrolló el ataque y los procesos, archivos, claves y otros artefactos afectados.
- La solución deberá permitir aislamiento automático del dispositivo comprometido, manteniendo su administración desde la consola central.
- La solución deberá proporcionar acceso remoto seguro por la línea de comandos desde la misma consola de gestión para investigación y remediación.
- La solución deberá permitir búsquedas proactivas sobre endpoints administrados para identificar indicios de amenazas no detectadas previamente.

- La solución deberá permitir consultas orientadas a revisión de postura de seguridad y validación de cumplimiento técnico en los endpoints protegidos.
- La solución deberá incluir consultas predefinidas editables por el analista.
- La solución deberá permitir crear consultas personalizadas para investigación y caza de amenazas.
- La solución deberá soportar consultas de eventos sobre información de endpoint en el repositorio histórico centralizado en nube.
- La solución deberá permitir programar consultas periódicas sobre el repositorio histórico.
- La solución deberá permitir controlar el acceso mediante roles administrativos predefinidos y personalizados.
- La solución deberá soportar autenticación multifactor para el acceso a la consola administrativa, ya sea mediante MFA nativa de la plataforma o mediante autenticación federada.
- La solución deberá permitir generar capturas forenses bajo demanda sobre endpoints investigados.
- La solución deberá permitir convertir las capturas forenses generadas a formatos aptos para consultas, incluyendo base de datos SQLite y archivo con formato JSON.
- La solución deberá permitir solicitar análisis adicional de archivos sospechosos desde el flujo de investigación.
- La solución deberá aplicar análisis estático a archivos sospechosos mediante reputación, escaneo y modelos de aprendizaje automático.
- La solución deberá aplicar análisis dinámico de archivos sospechosos en un entorno aislado para observar su comportamiento.
- 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.
- La solución EDR deberá contar con mecanismos para la detección y protección frente a amenazas como:
    - Malware conocido y desconocido, incluyendo amenazas de día cero.
    - Técnicas y tácticas de adversarios (TTPs), con mapeo de las detecciones a tácticas y técnicas del marco MITRE ATT&CK.
    - Actividades sin archivos (fileless), mediante detección basada en comportamiento, AMSI y protección frente a shellcode dinámico y amenazas basadas en scripts.
    - Ejecución de scripts maliciosos, comandos sospechosos, abuso de APIs de drivers, cambios inusuales en el registro y procesos anómalos, mediante capacidades de runtime protection, detección de comportamiento malicioso y telemetría para investigación.
    - Comportamientos asociados a ransomware, incluyendo protección frente a cifrado malicioso, ransomware ejecutado de forma remota, ataques contra el Sistema de archivos cifrados de Windows (Encrypting File System) y ransomware dirigido al Registro de arranque maestro (Master Boot Record), con capacidad de reversión automática de los archivos afectados.
    - Robo de credenciales, escalamiento de privilegios y explotación de aplicaciones vulnerables.

- Capacidades para realizar la investigación y respuesta remota para remediación de amenazas, incluyendo finalización de procesos sospechosos y eliminación de archivos maliciosos desde la consola de gestión.

4.1.9. Capacidades de IA

- La solución deberá permitir búsquedas en lenguaje natural sobre datos históricos de seguridad para localizar indicadores de compromiso y otros artefactos relevantes, como IP, usuarios, archivos y actividad de endpoint.
- La solución deberá proporcionar sugerencias de consulta, mostrar la consulta técnica generada, y permitir guardar la consulta resultante para reutilización posterior.
- La solución deberá generar resúmenes automáticos de casos, incluyendo hechos observados, entidades impactadas, tácticas MITRE ATT&CK identificadas y siguientes pasos sugeridos.
- La solución deberá analizar líneas de comando sospechosas para explicar su intención y posible impacto de seguridad.

4.1.10. Gestión de casos

- La solución deberá agrupar eventos y hallazgos relacionados en casos de investigación para facilitar su análisis y respuesta.
- La solución deberá permitir administrar cada caso con severidad, estado y responsable asignado.
- La solución deberá permitir registrar en cada caso una bitácora de investigación con hallazgos y seguimiento.

4.1.11. Capacidades de detección y respuesta XDR

- La solución XDR propuesta deberá ser tipo SaaS y cloud-native, y permitir la gestión centralizada, normalización y correlación de eventos de seguridad provenientes de múltiples fuentes.
- La plataforma XDR propuesta deberá permitir la integración de datos desde múltiples fuentes, 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 y otros sistemas críticos para la organización.
- La suscripción de la plataforma propuesta deberá tener una vigencia mínima de 24 meses e incluir el licenciamiento para mínimo, 2400 endpoints (estaciones de trabajo y servidores) definidos por la Entidad.
- La plataforma propuesta debe contar con capacidades de análisis avanzadas, incluyendo aprendizaje automático y modelos de comportamiento, para identificar amenazas conocidas y desconocidas, reducir falsos positivos y priorizar alertas relevantes para su investigación.
- La plataforma deberá contar con un repositorio centralizado de datos en nube capacidad suficiente para la ingesta, procesamiento y retención de telemetría acorde al volumen de

la Entidad, estimado en al menos 9 TB mensuales, sin degradación del servicio (endpoint, red, nube, identidad, entre otros), ni la disponibilidad de consultas.

- La plataforma propuesta debe incluir una funcionalidad de chat para asistencia experta directa del fabricante, integrada en la misma consola, que permita a la Entidad contactar en tiempo real, 24x7, con los analistas de seguridad del fabricante. Esta asistencia debe estar orientada a la atención de consultas asociadas a alertas, apoyo en procesos de investigación. Debe incluir como mínimo 100 casos mensuales de asistencia vía chat.
- La plataforma XDR propuesta deberá conservar, dentro de su repositorio de datos en la nube, los datos de eventos y detecciones por un período mínimo de 12 meses, permitiendo su consulta desde la consola para investigaciones históricas durante todo ese período.
- La plataforma XDR propuesta debe conservar el mensaje original (raw data) y permitir búsquedas sobre el contenido original del evento dentro del mismo período de retención de 12 meses.
- La plataforma XDR propuesta debe ser capaz de reconocer a los adversarios por su comportamiento, incluso si no están utilizando malware, y permitir la detección de amenazas desconocidas y avanzadas.
- La solución debe incluir una herramienta visual e interactiva que represente de manera gráfica las relaciones entre entidades involucradas en un incidente de seguridad (como usuarios, direcciones IP, endpoints y archivos). Esta funcionalidad debe facilitar la comprensión del alcance de la amenaza, identificar la causa raíz y apoyar el análisis contextual durante las investigaciones, permitiendo a los analistas visualizar el flujo de eventos y sus correlaciones.
- "La plataforma XDR propuesta deberá proveer un mecanismo de enriquecimiento automatizado de alertas que, al identificar entidades como direcciones IP, hashes de archivos, hashes de programas, dominios o URLs, incorpore información de inteligencia adicional obtenida de fuentes internas y externas.
- La plataforma propuesta debe proporcionar cobertura y análisis de amenazas alineados con el framework MITRE ATT&CK®, permitiendo identificar y analizar software malicioso y actores adversarios junto con las tácticas y técnicas asociadas.
- La solución debe permitir la exploración y consulta de dicha cobertura, mostrando cómo la plataforma detecta y protege frente a software adversario específico, facilitando la comprensión de los TTPs utilizados por los actores de amenaza.
- La solución debe permitir la replicación automática de los datos de eventos hacia un bucket de Amazon S3 que sea propiedad y esté bajo control exclusivo de la Entidad, en caso de que esta lo requiera.
- La solución debe soportar la ingestión y normalización de telemetría mediante Syslog, HTTP Ingest y File Upload API. Asimismo, debe soportar el procesamiento de fuentes en formatos JSON, CEF, LEEF, CSV, entre otros.
- La solución debe ofrecer tableros de control (dashboards) con vistas multifocales que faciliten la identificación rápida de posibles amenazas activas o actividades sospechosas.
- La solución debe permitir la descarga de paneles o visualizaciones en formato de imagen PNG, así como la exportación de datos a archivos en formatos CSV y JSON.
- La plataforma debe permitir definir reglas de detección personalizadas para los distintos casos de uso de la organización.

- La plataforma propuesta debe permitir el acceso a registros de auditoría que documenten todas las acciones realizadas por los usuarios dentro del sistema.
- La solución debe ofrecer capacidades de análisis asistido por inteligencia artificial generativa para apoyar la investigación de detecciones, casos e incidentes, incluyendo la generación de resúmenes, contexto y explicaciones técnicas. Adicionalmente, debe soportar el enriquecimiento de investigaciones mediante playbooks incluyendo integración con OpenAI, entre otros.
- La solución deberá ofrecer una arquitectura multitenant nativa, permitiendo la segmentación lógica de múltiples entidades o áreas bajo una misma consola de administración, con control de acceso granular y aislamiento de datos.
- La solución deberá permitir la gestión de IoC mediante API y/o TAXII 2.1, soportando como mínimo indicadores tipo IP, dominio, URL y hash de archivo en formatos MD5, SHA1 y SHA256.
- La plataforma debe permitir la integración con múltiples soluciones de seguridad ampliamente utilizadas en el mercado, habilitando la visualización y extensión de las integraciones disponibles con equipos y tecnologías de seguridad como Firewalls, cloud, WAF, Seguridad de correo, NDR y OT, entre otros.
- La solución deberá incorporar capacidades de análisis avanzado basadas en inteligencia artificial y aprendizaje automático que permitan fortalecer los procesos de detección de amenazas, la correlación de eventos de seguridad y la priorización de alertas.
- 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 SSO.
- La plataforma deberá ser compatible con los estándares abiertos STIX (Structured Threat Information Expression) y TAXII (Trusted Automated Exchange of Intelligence Information), con el fin de permitir el consumo automatizado de indicadores estructurados de amenaza.
- La solución debe permitir la detección automática de posibles incidentes desde su despliegue inicial, sin requerir ajustes o configuraciones adicionales previas por parte del usuario.
- 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.
- El proceso de desinstalación de sensores o agentes deberá estar protegido mediante un mecanismo seguro de autorización previa.
- La plataforma deberá permitir la creación de reglas de detección personalizadas basadas en consultas de búsqueda avanzada sobre eventos normalizados, incluyendo criterios sobre campos de telemetría como línea de comando, identificador de proceso y relación con proceso padre.
- La solución deberá soportar integraciones de ingesta de datos para integrar telemetría de productos del mismo fabricante y de terceros hacia el repositorio centralizado para ampliar la detección e investigación.
- La solución deberá admitir integraciones basadas en colector de logs para recibir eventos syslog de las fuentes que defina la Entidad.

- La plataforma deberá soportar integración con tecnologías de terceros para ingestión de telemetría y eventos de seguridad, incluyendo como mínimo: AWS, Microsoft Azure, Microsoft 365/Office 365, GCP, OCI, Abnormal, Akamai, Cisco, Citrix, Cloudflare, Corelight, CyberArk, Darktrace, F5, Forcepoint, Fortinet, Google Workspace, Imperva, Infoblox, Ivanti Pulse Secure, Juniper, Linux Servers, Microsoft DHCP, Microsoft DNS, Microsoft Entra Risk Detection, Microsoft Graph Security API v1/v2, Microsoft IIS, Windows Event Log, Mimecast, Netskope, Okta, OPNsense,, pfSense, Salesforce Real-Time Event Monitoring, Skyhigh Secure Web Gateway, Snowflake, Suricata, Symantec Endpoint Protection, VMware vCenter y Zscaler.
- La solución deberá incluir capacidades de parsing personalizado para fuentes no estándar, permitiendo la normalización de eventos, de modo que dicha información quede disponible para análisis, búsqueda, correlación y reglas personalizadas.
- La plataforma debe contar con sensores desplegables en entornos de red, endpoint y nube, que permitan detectar actividades asociadas a múltiples vectores de ataque.
- La plataforma XDR propuesta deberá disponer de una API con mecanismos seguros para la consulta automatizada de inteligencia de amenazas incluyendo indicadores de compromiso (IoCs) y reportes de inteligencia.

4.1.12. Requerimientos de Detección y Análisis

- La plataforma Propuesta debe incluir capacidades nativas de detección y respuesta que puedan activarse sin requerir configuración o desarrollo adicional.
- La solución XDR propuesta deberá cumplir como mínimo con:
    - Correlación de eventos de múltiples vectores.
    - Plataforma de inteligencia de amenazas (TIP) reconocida en el mercado.
    - Gestión y retención de registros en caliente por 12 meses.
    - Capacidades de investigación basadas en telemetría enriquecida.
    - Capacidad para crear reglas personalizadas en base a consultas, expresiones regulares, severidad, categorías MITRE e información histórica, entre otros.
    - Capacidad para crear supresión de alertas basadas en entidades específicas como direcciones IP, endpoints, dominios y usuarios, con capacidad de búsqueda posterior de alertas suprimidas.
- La plataforma propuesta debe permitir la colaboración interna entre analistas y equipos mediante casos investigativos, donde múltiples analistas de seguridad pueden comentar y manejar evidencia conjunta.
- La plataforma deberá soportar el enriquecimiento y análisis de archivos sospechosos mediante integraciones con servicios de inteligencia y análisis de programa maligno (MALWARE), incluyendo análisis estático y dinámico de indicadores observados por la solución.
- La plataforma propuesta deberá incluir un tablero operativo de seguimiento del consumo de eventos provenientes de las distintas fuentes de datos conectadas a la plataforma.
- El módulo de analítica de la plataforma XDR propuesta deberá identificar amenazas empleando correlación de eventos, detección comportamental e inteligencia de amenazas.

- La plataforma deberá habilitar funciones de análisis forense sobre dispositivos protegidos incluyendo capacidades como:
    - Aislamiento
    - Terminación de Procesos.
    - Borrado de archivos
    - Ejecución remota
    - Captura Forense
    - Exportación de logs y transferencia de artefactos
- 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.
- 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.
- 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.
- La plataforma deberá permitir la creación o utilización de tableros de control personalizables que faciliten el seguimiento de tendencias de seguridad.
- 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.
- La plataforma deberá permitir la creación de consultas personalizadas, así como la generación de tableros y reportes configurables. Estas consultas o reportes deberán poder programarse y notificar su disponibilidad automáticamente por correo electrónico a usuarios autorizados.
- La solución deberá proporcionar visibilidad a través de una consola de administración centralizada. Esta visibilidad debe incluir información casi en tiempo real e históricos.
- La plataforma deberá incluir una herramienta de análisis y manipulación de datos, accesible directamente desde la consola XDR que permita, como mínimo:
    - Decodificación de datos en múltiples formatos, entre los cuales se resalta base64 y XOR.
    - Conversión de datos y formatos de zonas horarias, entre otros.
    - Descifrado y desensamblado de shellcode.
    - Compresión y descompresión de información.
    - Cálculo de hashes y checksums."
- Se debe permitir la realización de investigaciones y búsquedas sobre la telemetría recolectada por la plataforma a partir de criterios como:
    - Nombre del host o equipo.
    - Direcciones IP

  - Nombres de dominio o patrones de dominio.
  - Identificadores únicos del sensor, host o agente soportados por la plataforma.
  - Actividades específicas como eventos de autenticación, comandos y líneas de ejecución de procesos, incluyendo PowerShell, así como ejecución de tareas programadas, entre otros.
  - Recolección e investigación sobre endpoints con agentes en Windows, macOS y Linux.
  - Ingesta e investigación de eventos de autenticación y registros de Microsoft Windows Event Log relacionados con entornos Active Directory.
- La plataforma debe contar con un mecanismo automatizado de triaje inicial de alertas, que permita filtrar, clasificar y priorizar eventos de seguridad de forma inteligente, con el fin de optimizar el tiempo de análisis y reducir la carga operativa del equipo de ciberseguridad.
- La plataforma debe incorporar mecanismos de detección que analicen los eventos normalizados para generar alertas.
- La solución propuesta deberá incluir sin costo adicional para la Entidad, el software de los colectores de datos requerido para la integración de las fuentes de telemetría syslog definidas por la Entidad.
- La plataforma propuesta debe incluir búsquedas contextuales (pivot) entre eventos y alertas con capacidades para seleccionar campos, indicadores y ventanas de tiempo.

4.1.13. Requerimientos de acceso móvil

- La plataforma XDR propuesta debe contar con una aplicación web accesible desde navegadores móviles, que permita la gestión básica del entorno desde dispositivos móviles.
- La aplicación web móvil deberá permitir la gestión de casos de investigación, incluyendo consultar casos en curso y añadir comentarios.
- La aplicación web móvil deberá permitir visibilidad de agentes de endpoint.

4.1.14. Requerimientos de Inteligencia de Amenazas

- La plataforma XDR propuesta debe incluir el servicio de inteligencia de amenazas que analice a nivel global actores adversarios y campañas, colabore con autoridades y fuerzas del orden, y utilice dicha inteligencia para fortalecer de forma continua las capacidades de detección, prevención y respuesta de la plataforma XDR.
- La plataforma XDR propuesta deberá incorporar un módulo de inteligencia de amenazas que permita consultar y visualizar de forma periódica información especializada de ciberinteligencia, incluyendo como mínimo reportes técnicos con recomendaciones de seguridad, alertas sobre amenazas emergentes, análisis de actores de amenaza y reportes de actividades maliciosas relevantes para la operación de seguridad global.
- La plataforma XDR propuesta deberá contar con capacidades de inteligencia de amenazas que permitan como mínimo:
  - Consultar indicadores de compromiso (IoCs), malware, grupos de amenaza y reportes de inteligencia

  - Correlacionar automáticamente indicadores de compromiso contra la telemetría, eventos y detecciones de la plataforma.
  - La plataforma XDR propuesta debe integrarse con fuentes externas de inteligencia, tales como VirusTotal y APIVoid, para validar la reputación de los indicadores observados.
- El servicio de Inteligencia de Amenazas deberá disponer de un equipo especializado a nivel global que soporte los procesos de investigación, análisis y contextualización de amenazas cibernéticas, contribuyendo al fortalecimiento continuo de la detección y respuesta
- Se deberá realizar monitoreo de al menos 200 grupos de amenazas globalmente reconocidos (Threat Groups), con visibilidad sobre la actividad en fuentes como la deep web y dark web, directamente desde la plataforma.

4.1.15. Automatizaciones

- La plataforma XDR propuesta deberá incorporar capacidades de automatización que permita ejecutar, gestionar y dar seguimiento a acciones y flujos de respuesta desde el contexto de análisis, triage e investigación sin requerir módulos adicionales o integraciones externas.
- La plataforma XDR debe permitir la creación de playbooks de automatización, que definan flujos de trabajo de respuesta ante eventos de seguridad.
- La plataforma XDR debe permitir la ejecución de playbooks en los siguientes escenarios:
  - Por eventos que ocurren dentro de XDR.
  - Como acción iniciada por el usuario dentro de XDR.
  - Manual o programada.
- El módulo de automatizaciones debe tener la capacidad para configurar y ejecutar acciones correctivas automáticas. Como mínimo, deberá soportar capacidades de contención y respuesta tales como:
  - Aislamiento y restauración de hosts
  - Des habilitación y habilitación de usuarios
  - Des habilitación de cuentas.
  - Revocación de sesiones de inicio de sesión
  - Bloqueo o desbloqueo de indicadores como direcciones IP, dominios y hashes de archivo.

5. IMPLEMENTACION

El proyecto se estructurará aplicando principios de gestión definidos con la supervisión del contrato.

5.1. Configuración del licenciamiento y la solución:

- Activación de consola y configuración inicial de parámetros de seguridad.
- Despliegue inicial en ambientes controlados.

- Validación técnica de la solución con el equipo de la CAR y ajustes.
- Definición de estrategias de despliegue eficientes:
- Uso de GPOs u otras herramientas automatizadas de distribución masiva.
- Segmentación por sedes, grupos, áreas críticas o niveles de riesgo.
- Generación de informes de avance técnico con trazabilidad del proceso.
- La implementación y configuración de la solución deberá ser realizada integralmente por el proponente siguiendo mejores prácticas del fabricante, complementándose con servicios profesionales de fabricante para garantizar despliegue correcto.
- El CONTRATISTA es responsable del despliegue, configuración, operación y validación de los agentes de seguridad requeridos por la plataforma, en todos los dispositivos definidos en el alcance del contrato (endpoints, servidores, recursos en nube y on-premise).
- La Entidad suministrará la infraestructura de cómputo requerida para el despliegue de los colectores de datos. Sobre dicha infraestructura, el contratista deberá ejecutar la instalación, configuración, validación operativa y puesta en marcha de los colectores necesarios para la integración de las fuentes de telemetría syslog definidas en el alcance del proyecto, asegurando su correcto funcionamiento, conectividad y envío de eventos hacia la plataforma XDR.

5.2. Servicios profesionales de fábrica

- El proponente debe contemplar una sesión de descubrimiento de hasta 2 horas con servicios profesionales directo de fabrica para priorizar integraciones de activos y APIs, identificar ubicaciones recomendadas para colectores de datos y confirmar la matriz de contactos.
- El proponente debe contemplar una (1) capacitación para administradores de la plataforma dictada directamente por el fabricante de hasta 4 horas orientada a acelerar la familiarización con la plataforma.
- El proponente debe contemplar una (1) capacitación para analistas de seguridad dictada directamente por el fabricante de hasta 4 horas orientada a acelerar la familiarización con la plataforma.
- El proponente debe contemplar la creación y despliegue de (3) automatizaciones estándar alineados a las integraciones estándar existentes en la plataforma.
- El proponente debe contemplar la creación de (5) reglas personalizadas para soportar casos de uso de monitoreo orientados al negocio.
- El proponente debe contemplar una bolsa de (10) horas de servicios profesionales directos de fábrica, que pueden ser utilizados en el despliegue de data collectors, soporte de integración de fuentes de datos y nube, soporte de despliegue de agentes, validación de nueva fuente de datos y creación automática de casos.

6. EQUIPO DE TRABAJO

Los servicios profesionales requeridos para la implementación, configuración, soporte y acompañamiento deberán estar incluidos dentro del valor total de la solución ofertada, no siendo objeto de cotización independiente.

Los perfiles anteriormente definidos participarán durante la vigencia del plazo de ejecución contractual, exclusivamente en las actividades relacionadas con la implementación, configuración, parametrización, despliegue y estabilización de la solución.

Una vez culminadas las etapas de implementación y puesta en operación, las actividades de soporte técnico, actualización, garantía y atención especializada de la plataforma se regirán conforme a las condiciones de soporte del fabricante y del licenciamiento adquirido, de acuerdo con lo establecido en el numeral 11 “Garantías y Soporte” del presente documento.

PERFIL REQUERIDO	CANTIDAD	FORMACIÓN ACADÉMICA	EXPERIENCIA GENERAL/ESPECIFICA
PROFESIONAL No. 1 **GERENTE DE PROYECTO**	1	Título profesional en **INGENIERÍA DE SISTEMAS; O INGENIERÍA ELECTRÓNICA; O INGENIERÍA DE SOFTWARE; O INGENIERÍA DE TELECOMUNICACIONES;** en cualquiera de los casos deberá contar con título de **posgrado** en **GERENCIA DE PROYECTOS; O GERENCIA DE PROYECTOS DE INGENIERÍA; O EN SEGURIDAD DE LA INFORMACIÓN; O EN GERENCIA DE PROYECTOS DE TELEINFORMÁTICA; O SIMILARES SEGÚN NBC DEL SNIES.**	**EXPERIENCIA GENERAL:** De **OCHO (08) AÑOS** contada a partir de la expedición de la matricula profesional; y **EXPERIENCIA ESPECÍFICA:** Mínima certificada de **CUATRO (04) AÑOS EN CARGOS O ROLES O FUNCIONES DE LIDERAZGO, COORDINACIÓN O GERENCIA DE PROYECTOS** relacionados con Sistemas de protección o seguridad informática o seguridad de la Información o Ciberseguridad.
PROFESIONAL No. 2 **INGENIERO SEGURIDAD**	1	Título profesional en **INGENIERÍA DE SISTEMAS; O INGENIERÍA INFORMÁTICA; O INGENIERÍA DE SISTEMAS INFORMÁTICOS; O INGENIERÍA ELECTRÓNICA; O INGENIERÍA DE SOFTWARE; O INGENIERÍA DE TELECOMUNICACIONES; O SIMILARES SEGÚN NBC DEL SNIES;** en cualquiera de los casos deberá contar con título de **posgrado** en **GESTIÓN DE PROYECTOS; O GESTIÓN DE SERVICIOS DE TI; O SIMILARES SEGÚN NBC DEL SNIES.**	**EXPERIENCIA GENERAL**: De **SIETE (07) AÑOS** contada a partir de la expedición de la matricula profesional; y **EXPERIENCIA ESPECÍFICA:** Mínima certificada de **CINCO (5) AÑOS** en **CARGOS O ROLES O FUNCIONES** como **IMPLEMENTADOR DE PROYECTOS; O CISO; O INGENIERO DE SEGURIDAD EN EMPRESAS PÚBLICAS O PRIVADAS.**

		***** Deberá contar con certificación o Formación como Auditor ISO 27001:2022 o ISO 20000 o CTIA u Oficial de protección de datos, emitida por entidad certificadora reconocida.	
PROFESIONAL No. 3 **INGENIERO DE SERVICIOS Y SOPORTE**	1	Título profesional en **INGENIERÍA DE SISTEMAS, O INGENIERÍA DE SISTEMAS INFORMÁTICOS, O INGENIERÍA ELECTRÓNICA, O INGENIERÍA DE TELECOMUNICACIONES O SIMILARES SEGÚN NBC DEL SNIES;** en cualquiera de los casos deberá contar con título de **posgrado** en **SEGURIDAD INFORMÁTICA O CIBERSEGURIDAD**; y acreditar Certificación técnica vigente emitida por el fabricante de la solución ofertada que lo faculte para realizar la instalación, configuración y soporte técnico especializado de la solución de Protección de Endpoint ofertada.	**EXPERIENCIA GENERAL:** De **TRES (3) AÑOS** contada a partir de la expedición de la matricula profesional; y **EXPERIENCIA ESPECÍFICA:** Mínima certificada de **TRES (3) AÑOS EN CARGOS O ROLES O FUNCIONES** relacionados con análisis de seguridad de la información.
***** Se aclara que, la certificación ISO requerida al **Profesional No. 2 - INGENIERO SEGURIDAD** corresponde exclusivamente a las competencias, idoneidad técnica y formación del talento humano propuesto para la ejecución del contrato.			

6.1. Soporte y operación:

- Prestación de soporte técnico proactivo, e incidencias por parte del fabricante.
- Validación de integridad y disponibilidad de servicios.
- Aplicación de parches o cambios de configuración recomendados por Microsoft.
- Acceso a reportes periódicos de amenazas (globales y locales) y a materiales del fabricante (webinars, boletines).
- Elaboración y firma del Acta de cierre técnico y funcional del proyecto, con aprobación expresa por parte del supervisor del contrato.

7. CERTIFICACIONES

- Se deberá acreditar la relación comercial y técnica activa y vigente con el fabricante de la solución ofertada, en uno de los dos niveles más altos del programa oficial de canales de dicho fabricante. Esta condición debe estar soportada mediante certificado emitido directamente por el fabricante, con fecha de expedición no superior a 30 días anteriores a la presentación de la oferta, en el que conste de forma explícita el nivel de membresía otorgado y su período de vigencia. No se aceptan certificaciones emitidas por distribuidores, mayoristas o terceros distintos al fabricante, ni documentos sin fecha de vigencia definida.

8. MARCO TEÓRICO, NORMATIVO Y ESPACIAL

Marco Teórico: La evolución de las amenazas digitales ha superado la capacidad de los antivirus tradicionales, haciendo necesaria la implementación de plataformas de seguridad con capacidades de detección y respuesta avanzada y extendida. Estas soluciones permiten identificar, contener y responder de manera proactiva a ataques sofisticados como ransomware, malware, explotación de vulnerabilidades.

Los componentes principales son:

8.1. Problemática de las Amenazas Cibernéticas:

- **Tipos de Malware:** Definir y clasificar virus, gusanos, troyanos, spyware, ransomware, etc.
- **Vectores de Infección:** Analizar cómo se propagan estas amenazas (archivos adjuntos descargas, exploits, etc.).
- **Impacto de las Infecciones:** Evaluar los daños que puede causar el malware (pérdida de datos, robo de identidad, interrupción de servicios, etc.).
- **Crecimiento de las Amenazas:** Investigar el aumento en el volumen y la sofisticación de las amenazas cibernéticas.

8.2. Software Antivirus:

- **Definición y Funciones:** Explicar qué es un antivirus y sus funciones principales (detección, eliminación, prevención).
- **Tipos de Antivirus:** Clasificar los antivirus según su enfoque (firmas, heurística, comportamiento).
- **Componentes de un Antivirus:** Describir los módulos clave (motor de análisis, base de datos de firmas, cortafuegos, etc.).
- **Funcionamiento del Antivirus:** Explicar cómo el antivirus analiza archivos, detecta amenazas y actúa para proteger el sistema.

8.3. Tendencias Futuras en Seguridad Informática:

- **Inteligencia Artificial y Machine Learning:** Analizar cómo estas tecnologías se están utilizando para mejorar la detección y prevención de amenazas.

- **Criptografía Cuántica:** Considerar el impacto potencial de la computación cuántica en la seguridad informática.
- **Blockchain y Ciberseguridad:** Investigar cómo la tecnología blockchain puede mejorar la confianza y la seguridad en línea.
- **Desarrollo de Antivirus Más Avanzados:** Explorar las nuevas técnicas y tecnologías que se están utilizando para proteger los sistemas contra las amenazas emergentes.

9. MARCO NORMATIVO

Este requerimiento se sustenta en las siguientes disposiciones legales vigentes:

- **Ley 80 de 1993 y Ley 1150 de 2007**, artículos sobre planeación y transparencia en la contratación pública.
- **Ley 1581 de 2012** sobre protección de datos personales.
- **Ley 1266 de 2008** y normas sectoriales de ciberseguridad.
- **ISO/IEC 27001:2022**, como referente técnico de buenas prácticas en seguridad de la información.
- **Plan de Acción Cuatrienal 2024-2027 de la CAR**, línea estratégica 6, proyecto 18.3.

9.1. Marco Espacial:

La CAR cuenta con presencia en 104 municipios del departamento de Cundinamarca y una sede central en Bogotá D.C. La infraestructura tecnológica está distribuida en sedes físicas, centros de datos, servicios en la nube, y dispositivos conectados por redes seguras o acceso remoto.

10. METODOLOGÍA

- Reunión de apertura
- Cronograma
- Instalación y configuración de licenciamiento
- Configuración de despliegue y políticas diferenciadas para servidores y estaciones de trabajo.

11. GARANTÍAS Y OBLIGACIONES DEL PROVEEDOR

- Garantizar la disponibilidad y activación de licencias por mínimo 24 meses.
- Brindar soporte técnico en español durante la ejecución.
- Asegurar la protección frente a amenazas locales y globales.
- Cumplimiento de niveles de servicio y seguridad de la información.
- Configurar informes técnicos y acceso a consola administrativa.
- Debe contar con un sistema de soporte técnico directo con el fabricante para registro de incidencias.

- La instalación las realizará el contratista con el acompañamiento de los ingenieros del área de servicios tecnológicos que serán los administradores del software.
- El servicio de incidencias se realizará mediante tickets a petición mediante incidencia o requerimiento.
- Las garantías del licenciamiento deberán incluir ANS asociados a la atención de incidentes y/o requerimientos realizados por la Entidad cuando se requiera, contemplando soporte remoto, telefónico y, de ser necesario, presencial, bajo esquema 5x8 durante la vigencia de veinticuatro (24) meses del licenciamiento, con trazabilidad mediante número de ticket.

  El soporte técnico asociado a la solución deberá ser provisto directamente por el fabricante de la plataforma ofertada, garantizando acceso a actualización, atención especializada, escalamiento de incidentes y acompañamiento técnico durante toda la vigencia contractual.
- Se debe entregar totalmente documentada la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.

11.1. De la entidad:

- Facilitar acceso local y remoto seguro a infraestructura para instalación.
- Disponer de servidor físico o virtual para pruebas.
- Acompañar técnicamente el proceso de despliegue completo.

12. ALCANCE DEL PROYECTO

Las licencias contempladas dentro del alcance del objeto del contrato deberán ser emitidas en su totalidad directamente por el fabricante, a nombre de la CAR Cundinamarca, garantizando una vigencia mínima de veinticuatro (24) meses contados a partir de la fecha de activación, y deberán estar plenamente habilitadas para su uso conforme a los términos y condiciones del fabricante.

Lugar de ejecución: Sede central CAR en Bogotá D.C., con cobertura remota para todas las dependencias a nivel de la jurisdicción.

Plazo de ejecución: Tres (3) meses a partir del acta de inicio

Cobertura requerida Licenciamiento:

Producto	Modalidad	Cantidad
Licenciamiento de software de seguridad para **servidores** (Antivirus / Antimalware) por 24 meses	Licencias Cloud – SaaS	250
Licenciamiento de software de seguridad para **estaciones de trabajo** (Endpoint Security) por 24 meses.	Licencias Cloud – SaaS	2400

La desagregación en el formato de cotización tiene fines exclusivamente económicos y de comparabilidad, sin que esto implique la fragmentación de la solución, la cual deberá operar de manera integrada bajo una arquitectura unificada.

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANTIDAD (A)
1	Licenciamiento de software de seguridad para servidores (EPP/Antimalware y EDR) bajo modalidad de computación en la nube (SaaS) por 24 meses.	UN	250
2	Licenciamiento de software de seguridad para estaciones de trabajo (EPP/Antimalware y EDR – Endpoint Security) bajo modalidad de computación en la nube (SaaS) por 24 meses.	UN	2400
3	Licenciamiento de plataforma de detección y respuesta extendida (XDR) para servidores, bajo modalidad de computación en la nube (SaaS) por 24 meses.	UN	250
4	Licenciamiento de plataforma de detección y respuesta extendida (XDR) para estaciones de trabajo (endpoints), bajo modalidad de computación en la nube (SaaS) por 24 meses.	UN	2400

La consola de administración en la nube del antivirus, al ser un componente integral de la solución, deberá estar contemplada dentro del valor total ofertado.

Las licencias Antivirus / Antimalware (consola de administración, Software Seguridad Endpoint y Server), deberán ser entregadoas a nombre de la Corporación por documento tipo carta u otro, que sea emitido desde el fabricante que constate la vigencia de 24 meses. El licenciamiento deberá corresponder a una suscripción con vigencia continua de 24 meses, sin requerir renovaciones intermedias durante dicho periodo.

El proveedor se encargará de la configuración y/o parametrización de las herramientas (Antivirus) así como de brindar líneas de atención y soporte del fabricante durante el licenciamiento. La totalidad de las licencias requeridas, incluyendo la consola de administración y gestión centralizada, deberá ser provista directamente por el fabricante como parte integral de la solución ofertada.
Al momento del ingreso al almacén institucional, estas licencias se registran como **bienes intangibles**, dado que no constituyen un activo físico, sino un derecho de uso por un período determinado (24 meses de vigencia) otorgado por el proveedor.

13. OBLIGACIONES ESPECÍFICAS CONTRACTUALES Y TÉCNICAS

Durante la ejecución contractual y en cumplimiento del objeto descrito, se considera necesario el desarrollo de las siguientes actividades por parte del contratista:

- Suministrar y habilitar la solución contratada a la CAR, conforme a las indicaciones del supervisor del contrato.
- Cumplir con el Anexo de Especificaciones Técnicas, de acuerdo con los lineamientos impartidos por la supervisión del contrato y las mejores prácticas del fabricante.
- Habilitar y configurar la consola de administración en la nube, clientes, despliegues, Jobs, tanto del nivel central como de los 14 sitios regionales.
- Presentar a la supervisión del contrato las opciones de configuración disponibles de la solución tecnológica adquirida, y asesorar técnicamente sobre aquella(s) que mejor se adapten a las necesidades de la Corporación y permitan un mejor desempeño.
- Cumplir con el Anexo de Especificaciones Técnicas, de acuerdo con los lineamientos impartidos por la supervisión del contrato y las mejores prácticas del fabricante.
- Habilitar y configurar la consola de administración en la nube del fabricante.
- Presentar a la supervisión del contrato las opciones de configuración disponibles de la solución tecnológica adquirida, y asesorar técnicamente sobre aquella(s) que mejor se adapten a las necesidades de la Corporación y permitan un mejor desempeño.
- Entregar al supervisor informes sobre incidentes, recomendaciones técnicas y acciones tomadas, que se presenten durante la implementación, operación o soporte de las soluciones.
- Entregar al supervisor informe de configuración, incidentes, recomendaciones técnicas y acciones tomadas, que se presenten durante la implementación, operación o soporte de las soluciones.
- Firmar el Acuerdo de Confidencialidad que garantice la no divulgación ni uso indebido de la información a la que se acceda durante la ejecución del contrato.
- Entregar formalmente al finalizar la ejecución del contrato toda la documentación técnica generada o actualizada, manuales de administración, configuraciones aplicadas, y un informe final sobre el estado de la solución.
- Suministrar la solución de seguridad para endpoints y servidores en modalidad SaaS, instalar, configurar, parametrizar, poner en marcha y realizar pruebas de funcionamiento de la solución en los ambientes requeridos.
- Dar estricto cumplimiento a las especificaciones técnicas de los bienes o servicios contratados, de acuerdo con las fichas técnicas, licencias y documentación incluida en el contrato.
- Brindar soporte técnico a la solución ofertada, incluyendo resolución de incidentes, ajustes de configuración, atención remota y en sitio cuando la CAR lo requiera, durante todo el tiempo de vigencia del contrato y sus garantías.
- Dar estricto cumplimiento a las políticas de seguridad de la información vigentes en la Corporación Autónoma Regional de Cundinamarca – CAR, en el marco de su Sistema de Gestión de Seguridad de la Información (SGSI), y actuar conforme a los lineamientos establecidos por la norma ISO/IEC 27001:2022
- Configurar la consola de administración en la nube y las licencias de antivirus por personal calificado, incluyendo la transferencia de conocimiento por parte del fabricante y/o canal autorizado cuando aplique.

- Brindar atención de incidentes o consultas mediante múltiples canales, llamadas telefónicas y sesiones remotas, de acuerdo con el nivel de criticidad y las condiciones del contrato.
- Asumir las demás obligaciones que, por la naturaleza del contrato, le correspondan al contratista, de acuerdo con la Ley 80 de 1993, Ley 1150 de 2007 y las disposiciones contractuales suscritas.

NOTA 1. Los informes deberán ser presentados en medio magnético en formato PDF, debidamente firmados.

14. PRODUCTOS DEL CONTRATO

Como resultado de la ejecución del presente contrato, el contratista deberá entregar a satisfacción de la supervisión los siguientes productos:

1) Licencias activas de la solución antivirus protección contratadas, en número y vigencia conforme al alcance técnico a nombre de la Corporación.
2) Consola de administración operativa y accesible, con las configuraciones básicas validadas por el equipo técnico de la CAR, cumpliendo con el alcance y administración de equipos.
3) Manual de instalación, configuración, operación y recuperación de la solución, incluyendo las directrices específicas para entornos de servidores, estaciones y usuarios móviles.
4) Informe técnico final de despliegue y validación, con lista de dispositivos protegidos, configuraciones aplicadas y verificación de conectividad con la consola.
5) Plan de soporte técnico y matriz de escalamiento, incluyendo SLA, canales, responsables y tiempo de atención por nivel de severidad.
6) Registro documental de incidentes de seguridad atendidos y gestionados durante la ejecución del contrato (si los hubiera).

15. SUPERVISIÓN Y ANEXOS

La supervisión será realizada por la Oficina de Gobernanza Digital y Analítica de Datos Comunicaciones (OGDA), que validará:

- Instalación y operación de la solución.
- Generación de alertas y cumplimiento funcional.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y NIVELES DE SERVICIO (ANS)

En el desarrollo del servicio contratado, y en concordancia con los principios del Sistema de Gestión de Seguridad de la Información (SGSI) de la CAR Cundinamarca, el contratista deberá cumplir con las siguientes directrices frente a incidentes de seguridad de la información que

afecten la continuidad, integridad o disponibilidad de los sistemas de información, plataformas tecnológicas o servicios administrados.

17. ALCANCE DE LA OBLIGACIÓN

El contratista será responsable de implementar, mantener y operar procedimientos efectivos de detección, análisis, clasificación y respuesta ante incidentes de seguridad, de acuerdo con niveles de criticidad previamente definidos. Esta obligación se aplicará durante toda la vigencia del contrato, incluyendo etapas de despliegue, soporte y operación.

Los incidentes contemplan, entre otros:

- Acceso no autorizado.
- Modificación de recursos no autorizada.
- Uso inapropiado de recursos tecnológicos.
- No disponibilidad de recursos.
- Ataques multicomponente o amenazas combinadas.
- Cualquier incidente que altere la operación o genere riesgos para la información institucional.

18. ESTÁNDARES Y CLASIFICACIÓN

El software se clasificará en el estándar del catálogo de servicios de la CAR.

18.1. Registro, análisis y evaluación de incidentes

El contratista deberá:

- Centralizar toda la información relevante para el análisis de incidentes (logs, consolas, tráfico, etc.).
- Garantizar la sincronización horaria de todos los equipos gestionados, con la hora legal colombiana.
- Realizar correlaciones de eventos y detecciones basadas en comportamiento.
- Informe de incidentes conforme a su impacto: o **Alto impacto**: Afecta misionalidad, reputación o aspectos legales. o **Medio impacto**: Afecta procesos específicos. o **Bajo impacto**: Impacto menor o monitoreo preventivo.

18.2. Tiempos de respuesta y niveles de criticidad funcional

Se deberá determinar el nivel de prioridad de atención basado en:

- Criticidad del activo afectado.
- Impacto actual y proyectado.
- Riesgo sobre los objetivos institucionales.

La siguiente tabla se adopta como referencia para clasificar la severidad dentro de la consola.

Nivel de Criticidad	Valor	Definición
Inferior	0,10	Estaciones de trabajo sin funciones críticas
Bajo	0,25	Sistemas que apoyan una sola dependencia
Medio	0,50	Sistemas transversales a más de una dependencia
Alto	0,75	Infraestructura TI o usuarios críticos
Superior	1,00	Sistemas críticos para la operación institucional

18.3. Informes:

- Informe de Configuración, plataformas y herramientas utilizadas para la gestión de incidentes junto con la política de tratamiento de incidentes, matriz de severidad y criterios de activación.
- Flujo de atención con responsables, canales y escalamiento (link de soporte).
- Suministrar link de soporte y/o línea de atención suministrando usuario y contraseña.

19. Clasificador de bienes y servicios

43231500 – Software funcional
43233200 - Software de seguridad y protección
81112200 - Mantenimiento y soporte de software
81112500 - Servicios de alquiler o arrendamiento de licencias de software de computador

20. Instrumento de Agregación de Demanda / Sistema Dinámico de Adquisición (IAD/SDA) para adquirir licencias, software como servicio (SaaS) y servicios conexos.

La solución requerida por la Entidad contempla capacidades integrales de protección de endpoints y servidores bajo una arquitectura unificada EPP, EDR y XDR, incluyendo funcionalidades avanzadas de correlación, telemetría, analítica, investigación y respuesta centralizada frente a eventos e incidentes de ciberseguridad.

Así mismo, el alcance funcional incluye integración de múltiples fuentes de información, capacidades de administración centralizada en la nube, automatización, trazabilidad, monitoreo avanzado, generación de alertas, threat hunting y soporte especializado del fabricante durante toda la vigencia del licenciamiento.

En este contexto, aunque dentro del Instrumento de Agregación de Demanda (IAD/SDA) de Software por Catálogo II pueden existir productos asociados a esquemas tradicionales de Antivirus, Antimalware o Endpoint Security, las capacidades funcionales, técnicas y operativas requeridas para el presente proyecto exceden el alcance estándar de licenciamiento individual disponible en dicho instrumento.

Por lo anterior, la necesidad planteada por la Entidad requiere una solución integral de ciberseguridad con componentes y servicios especializados que no se encuentran cubiertos integralmente dentro del Acuerdo Marco de Precios de Software por Catálogo II.



NELSON JOSE OROZCO SALGADO
Jefe Oficina de Gobernanza Digital y Analítica de Datos.

Proyectó: Jeison Jair González Vargas – Profesional Especializado DGEN. 

Revisó: Mateo Andrés Sánchez Ortega – Contratista DGC 

Revisó: Hector Junior Vega Arias – Contratista OGDAD 