

ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS

OBJETO: OTIC-I-004: Adquirir la suscripción de un software especializado tipo XDR Detección y respuestas extendidas para la protección autónoma en la nube y en la red para el fortalecimiento de la infraestructura tecnológica de la Secretaría Jurídica Distrital.

1. ALCANCE Y CONSIDERACIONES GENERALES

1.1. ALCANCE

La Secretaría Jurídica Distrital (SJD) requiere contratar la suscripción del licenciamiento bajo modelo SaaS (*Software as a Service*) y la prestación de los servicios asociados para una plataforma de ciberseguridad especializada tipo XDR (Extended Detection and Response) por un periodo de doce (12) meses para la protección autónoma de servidores virtuales en la nube, servidores físicos y virtuales on premise y estaciones de trabajo de propiedad de la Entidad distribuidos de la siguiente manera:

- 225 estaciones de trabajo (*Workstations*).
- 22 suscripciones para servidores (físicos y/o virtuales).

1.2. SERVICIOS DE IMPLEMENTACIÓN

Requiere los servicios especializados de implementación, parametrización, integración con componentes de red/nube y pruebas de funcionamiento de la plataforma XDR en la infraestructura de la SJD.

1.3. SOPORTE TÉCNICO

Requiere servicios de soporte técnico especializado bajo el esquema 8x5x4, atención 8 horas, 5 días a la semana, con tiempo de respuesta máximo de 4 horas para incidentes correctivos.

1.4. SITUACIÓN ACTUAL Y JUSTIFICACIÓN TÉCNICA

La Secretaría Jurídica Distrital opera con una infraestructura tecnológica integrada por 225 estaciones de trabajo y 22 servidores que soportan los sistemas de información jurídicos del Distrito Capital.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195



CLASIFICACIÓN DE LA INFORMACIÓN: PÚBLICA CLASIFICADA

2311600-FT-091. Versión 02

Página:

1 de 7

Actualmente, la entidad enfrenta retos operacionales que hacen indispensable dar el salto hacia una solución de protección autónoma en la nube y red:

- **Limitación de los esquemas tradicionales:** Tiempos de propagación altos para actualizar políticas de seguridad y baja integración entre eventos de red, endpoints y servicios en la nube.
- **Visibilidad fragmentada:** Falta de correlación automatizada de eventos entre dispositivos de red, servicios en la nube y endpoints.
- **Carencia de respuesta autónoma:** Necesidad de motores de Inteligencia Artificial que aislen y mitiguen amenazas de forma proactiva, incluso cuando los equipos están fuera de la red corporativa (offline).
- **Protección a estaciones de trabajo Legacy:** Actualmente la Entidad cuenta con algunos servidores y estaciones de trabajo con software legacy lo cual representa un riesgo para la protección de la información institucional.

La adquisición de la suscripción a de la solución XDR permitirá a la SJD integrar la telemetría de red, nube y endpoints bajo una misma consola con capacidades de remediación automatizada y alineada al marco MITRE ATT&CK¹.

2. CONDICIONES GENERALES DEL PROVEEDOR

1. **Plazo de entrega de la suscripción:** El proveedor deberá entregar la suscripción, máximo cinco (5) días calendario contados a partir de la reunión de *Kickoff*. La vigencia de las suscripciones XDR será de doce (12) meses a partir de su activación.
2. **Actualizaciones de versión:** La suite XDR ofertada más sus componentes de software deberán entregarse en la versión estable más reciente y recomendada por el fabricante.
3. **Activación del licenciamiento:** El proveedor deberá realizar la instalación, configuración, parametrización y puesta en operación de la solución ofertada con una suscripción en versión demo. Una vez ésta sea aprobada a satisfacción por parte de la supervisión del contrato se realizará el proceso de activación del licenciamiento con el fin de garantizar el periodo de servicio contratado.
4. **Continuidad del servicio:** El despliegue e integración en la nube/red no deberá generar indisponibilidad continua en los servicios tecnológicos que puedan afectar los servicios institucionales de la SJD.

¹ El marco **MITRE ATT&CK (MITRE ATT&CK)** es una base de conocimientos universalmente accesible y actualizada para modelar, detectar, prevenir y combatir las amenazas de ciberseguridad basadas en los comportamientos adversarios conocidos de los delincuentes cibernéticos. Las siglas ATT&CK de MITRE ATT&CK significan tácticas, técnicas y conocimiento común de adversarios.
Fuente: <https://www.ibm.com/mx-es/think/topics/mitre-attack>

5. **Acuerdo de Confidencialidad:** El representante legal del proveedor deberá suscribir un acuerdo de confidencialidad con la Entidad y suministrar los acuerdos de confidencialidad suscritos entre el personal que participará en el proyecto y la empresa que este representa.
6. **Revisión de idoneidad del recurso humano:** El contratista deberá presentar para revisión por parte del supervisor de contrato las hojas de vida del recurso humano con el fin de validar su idoneidad en la implementación del proyecto. Esta actividad deberá realizarse antes de la suscripción del acta de inicio.

3. ESPECIFICACIONES TÉCNICAS MÍNIMAS (XDR)

3.1. Consola Central XDR y Protección en la Nube (SaaS)

1. La consola de administración deberá operar bajo modalidad SaaS (Software as a Service) provista directamente por el fabricante, garantizando la segregación lógica, confidencialidad, integridad y aislamiento de la información de la Entidad, mediante arquitectura multitenant o arquitectura cloud equivalente, con controles verificables de aislamiento, gestión de acceso basada en roles (RBAC) y separación segura de datos entre clientes. El oferente deberá describir y documentar la arquitectura ofrecida y sus mecanismos de aislamiento.
2. La consola deberá permitir acceso web seguro y soportar autenticación multifactor (MFA/2FA) e inicio de sesión único (SSO) mediante SAML 2.0, OpenID Connect, OAuth 2.0 o protocolos empresariales equivalentes. Estas capacidades podrán ser nativas de la plataforma o implementarse mediante integración de identidad de la Entidad, y deberán quedar configuradas y operativas durante la fase de implementación, previo a aprobación por parte del supervisor de contrato.
3. Deberá contar con la capacidad de correlacionar eventos de ciberseguridad en tiempo real combinando fuentes de datos de red, nube, servidores y estaciones de trabajo.
4. La solución deberá contar con Integración con fuentes de datos de terceros (SIEM, Firewalls, OCI, Azure, AWS) mediante conectores como APIs, RESTful documentadas, syslog y marketplaces propios del fabricante.
5. La solución ofertada deberá acreditar, dentro de los últimos tres (3) años, al menos una (1) de las siguientes condiciones: (i) posicionamiento como Líder ("Leader") en el Cuadrante de Líderes del Gartner Magic Quadrant for Endpoint Protection Platforms; (ii) certificación vigente expedida por SE Labs para soluciones EPP, EDR y/o XDR; o (iii) certificación vigente expedida por AV-TEST para soluciones EPP, EDR y/o XDR. No se aceptará el reconocimiento o la certificación obtenidos en informes o pruebas referidos a categorías de mercado distintas al EPP/EDR/XDR (p. ej., Gestión Unificada de Endpoints/UEM).

3.2. Agente Unificado y Compatibilidad

1. La solución Agente único y ligero para sistemas operativos Windows 11 y 10; Server 2016, 2019, 2022 y 2025 y Linux (Oracle Linux 7, 8 y 9).
2. Deberá contar con una protección de manipulación (*Anti-tamper*) a nivel de Kernel en sistemas operativos Windows.
3. La instalación y las actualizaciones ordinarias del agente deberán realizarse de manera transparente y, generalmente, sin requerir reinicio del sistema. En caso de que el sistema operativo, una actualización de componentes, controladores o prerrequisitos técnicos requiera reinicio, este deberá ser informado y coordinado con la supervisión del contrato.

3.3. Protección Autónoma y Respuesta Automatizada (SOAR/XDR)

1. La solución deberá contar con una detección avanzada basada en comportamiento y motores de Inteligencia Artificial / Machine Learning alineados con MITRE ATT&CK.
2. Deberá tener la capacidad de aislar endpoints de la red, cancelar procesos maliciosos, revertir cambios (rollback) y bloquear tráfico malicioso en la red o nube de forma automática.
3. La solución instalada en los dispositivos deberá contar con la capacidad de prevención y mitigación de amenazas en estado desconectado (offline).

4. SERVICIOS ASOCIADOS Y SOPORTE TÉCNICO

4.1. Servicios de Implementación

1. El proveedor deberá realizar el despliegue del 50% de las suscripciones con acompañamiento por parte de la SJD, el restante lo desarrollará la entidad.
2. El proveedor deberá adelantar Parametrización de reglas de detección e integración con plataformas externas de red/nube y el Active Directory/SSO de la SJD.
3. El proveedor deberá realizar pruebas de funcionamiento en ambientes controlados sin afectación del servicio.

4.2. Esquema de Soporte Técnico y Mantenimiento

1. El Proveedor deberá prestar Soporte especializado 5x8x4: Atención de fallas correctivas las 8 horas del día, 5 días a la semana, con tiempo máximo de respuesta e inicio de atención en sitio/remoto de 4 horas.
2. Para los incidentes valorados por la entidad como críticos el proveedor tendrá máximo 2 horas para la atención y solución en máximo 12 horas calendario.
3. El proveedor deberá suministrar una matriz de comunicaciones, escalamiento donde se evidencie el contacto con fábrica en caso de requerir soporte con este.
4. El Proveedor deberá contar con canales de comunicaciones propios para la gestión de requerimientos e incidentes que requiera la entidad. Adicionalmente, deberá contar con una herramienta de gestión que permita validar el estado de los casos registrados.

5. EQUIPO DE TRABAJO MÍNIMO REQUERIDO

Rol	Cantidad	Formación Académica Requerida	Experiencia Mínima Exigida	% Dedicación
Líder-Implementador XDR	1	Profesional en Ingeniería de Sistemas, Electrónica, Telemática o afines.	General: 5 años. Específica: 3 años en instalación e implementación de soluciones EDR/XDR. EDR. Certificado en la solución ofertada por el oferente	100%

6. FICHA DE VERIFICACIÓN CUMPLIMIENTO

ESPECIFICACIONES TÉCNICAS HERRAMIENTA XDR		CUMPLIMIENTO	
ÍTEM	DETALLE DEL REQUERIMIENTO	SI	NO
1.0 ALCANCE Y CANTIDADES DE LICENCIAMIENTO			
1.1	Suscripción de licenciamiento bajo modelo SaaS (Software as a Service) por un periodo de doce (12) meses para una plataforma tipo XDR, con cobertura total para 247 activos tecnológicos distribuidos en: 225 estaciones de trabajo (Workstations) y 22 suscripciones para servidores (físicos y/o virtuales). Entrega máxima dentro de los cinco (5) días calendario contados a partir de la reunión de Kickoff.		
2.0 CONSOLA CENTRAL Y ARQUITECTURA EN LA NUBE (SaaS)			
2.1	Consola de administración 100% en la nube (SaaS) con arquitectura multitenant y acceso web seguro mediante SSO (SAML 2.0) y autenticación de doble factor (2FA).		
2.2	Capacidad de correlacionar eventos de ciberseguridad en tiempo real combinando fuentes de datos de red, nube, servidores y estaciones de trabajo. Integración nativa con fuentes de datos de terceros (SIEM, Firewalls, OCI, Azure, AWS) mediante conectores nativos y APIs RESTful documentadas.		
2.3	Posicionamiento del fabricante en el Cuadrante de Líderes de Gartner, SE Labs o AV-Test para soluciones EPP/EDR/XDR en los últimos tres (3) años.		
3.0 AGENTE UNIFICADO Y COMPATIBILIDAD			
3.1	La solución Agente único y ligero para sistemas operativos Windows 11 y 10; Server 2016, 2019 y 2025 y Linux (Oracle Linux 7, 8 y 9). Con protección de manipulación (Anti-tamper) a nivel de Kernel en SO Windows. Instalación y actualización transparente sin requerir reinicio del sistema.		
4.0 PROTECCIÓN AUTÓNOMA Y RESPUESTA AUTOMATIZADA (SOAR/XDR)			
4.1	Detección avanzada basada en comportamiento y motores de IA / Machine Learning alineados con el marco MITRE ATT&CK. Capacidad de prevención y mitigación de amenazas en estado desconectado (offline).		
4.2	Respuesta autónoma con capacidad de aislar endpoints de la red, cancelar procesos maliciosos, revertir cambios (rollback) y bloquear tráfico malicioso en la red o nube de forma automática.		
5.0 SERVICIOS DE IMPLEMENTACIÓN Y CONFIGURACIÓN			
5.1	Despliegue e instalación del 50% de las suscripciones por parte del proveedor con acompañamiento del personal de la SJD. Incluye parametrización de reglas de detección, integración con Active Directory/SSO y plataformas externas, así como pruebas de funcionamiento en ambientes controlados.		
6.0 SOPORTE TÉCNICO, MANTENIMIENTO Y NIVELES DE SERVICIO (SLA)			
6.1	Servicio de soporte técnico especializado bajo el esquema 8x5x4 (atención 8 horas, 5 días a la semana, con tiempo máximo de respuesta e inicio de atención remoto/sitio de 4 horas). Para incidentes críticos: máximo 2 horas para atención y solución en máximo 12 horas calendario.		

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195



CLASIFICACIÓN DE LA INFORMACIÓN: PÚBLICA CLASIFICADA

2311600-FT-091. Versión 02

Página: 6 de 7

6.2	Suministro de matriz de comunicaciones y escalamiento con contacto directo con fábrica. Canales de comunicación propios y herramienta de gestión de casos para seguimiento de incidentes. Realización de mínimo dos (2) mantenimientos preventivos durante la vigencia del servicio.		
7.0 EQUIPO DE TRABAJO MÍNIMO REQUERIDO			
7.1	Líder Implementador XDR (1 recurso, 100% dedicación): Profesional en Ing. de Sistemas, Electrónica, Telemática o afines. Experiencia general min. 5 años, específico min. 3 años en instalación e implementación de soluciones EDR/XDR. Certificado en la solución ofertada.		