



Proceso: OTIC-I-004:

Objeto: 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.

Respetados señores: **Secretaria Jurídica Distrital**

A continuación, enviamos Observaciones y Solicitudes de Aclaración a la ficha técnica compartida por la entidad:

1. Limitación de los esquemas tradicionales

Observación: Se identifica que los esquemas tradicionales presentan tiempos de propagación elevados para la actualización de políticas de seguridad, así como baja integración entre eventos provenientes de red, endpoints y servicios en la nube.

Solicitud de aclaración:

- ¿La entidad estaría interesada en ampliar el alcance del requerimiento incluyendo eventos de protección contra pérdida de datos (DLP) dentro del análisis y correlación de seguridad?

2. Consola de administración en la nube (SaaS)

Observación: El pliego establece que la consola de administración debe ser 100% en la nube, con arquitectura multitenant, acceso web seguro mediante SSO (SAML 2.0) y autenticación 2FA.

Solicitudes de aclaración:

- ¿La institución cuenta actualmente con un Directorio principal que permita integración mediante LDAP para el proceso de autenticación y federación?

3. Instalación y actualización sin reinicio del sistema

Observación: El pliego establece que el proceso de instalación y actualización de la solución deberá ser **transparente y sin requerir reinicio del sistema**. Sin embargo, es importante precisar que, de acuerdo con las capacidades técnicas de las plataformas de protección de endpoints, existen funcionalidades avanzadas que **sí requieren reinicio** para completar su habilitación o endurecimiento del sistema operativo.



Solicitud de aclaración:

- ¿La entidad confirma que el requerimiento de “no reinicio” aplica únicamente para la instalación y actualización estándar del agente, y que se exceptúan las funcionalidades que, por diseño, requieren reinicio para su activación? Las funcionalidades que típicamente requieren reinicio son:
 - **App Control**
 - **App Hardening**
 - **App and Device Control**

4. Posicionamiento del fabricante en Cuadrantes y pruebas de laboratorio

Observación: El pliego solicita que el fabricante se encuentre posicionado en el **Cuadrante de Líderes de Gartner**, así como en **SE Labs** y **AV-Test** para las tecnologías **EPP/EDR/XDR** durante los últimos tres (3) años. No obstante, no se especifica si este posicionamiento debe cumplirse **en todas las tecnologías** ni si debe ser **simultáneo** en todos los analistas mencionados.

Solicitud de aclaración:

- ¿La entidad requiere que el fabricante esté posicionado como líder en **todas las categorías (EPP, EDR y XDR)** y en **todos los analistas (Gartner, SE Labs y AV-Test)** de forma concurrente durante los últimos tres años?
- ¿O es suficiente que el fabricante demuestre posicionamiento relevante (líder o equivalente) en **alguna(s) de las categorías** y en **alguno(s) de los analistas**, siempre que se evidencie trayectoria y reconocimiento consistente en el periodo solicitado?

Agradecemos a la entidad analizar esta solicitud y considerar el ajuste correspondiente en la ficha técnica definitiva.

Cordialmente,

Mario Morales
Global Seis