



Señores
SECRETARIA JURIDICA DISTRITAL
Bogotá D.C.

Referencia: 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

Observaciones

Numeral: Situación actual / Contexto general

Texto actual: El Anexo describe la infraestructura tecnológica actual de la Entidad sin detallar el inventario completo de sistemas en operación.

Observación/justificación: Para garantizar un soporte adecuado y evitar brechas de cobertura, es necesario conocer si existen sistemas legacy o fuera de soporte por parte del fabricante/distribuidor dentro del alcance del contrato.

Solicitud: Se solicita amablemente a la Entidad su apoyo con la lista completa de los sistemas con los que opera actualmente, incluyendo aquellos en condición de legacy o fuera de soporte del distribuidor, con el fin de garantizar el soporte adecuado de estos.

Numeral 2.2

Texto actual: El Anexo exige integración nativa con SIEM, firewall perimetral y servicios de nube, sin especificar marca ni plataforma.

Observación/justificación: El dimensionamiento del alcance y del valor de la oferta depende de las marcas y plataformas específicas que deban integrarse.

Solicitud: Se solicita a la Entidad precisar las marcas y plataformas específicas de SIEM, firewall perimetral y servicios de nube efectivamente en uso, que deberán integrarse durante la ejecución del contrato, con el fin de dimensionar correctamente el alcance y el valor de la oferta.

Numeral 4.2

Texto actual: "Deberá tener la capacidad de... revertir cambios (rollback)... de forma automática."

Observación/justificación: La solución ofertada revierte de forma automática los cambios producidos por procesos maliciosos: restauración de los archivos cifrados por ransomware a su estado previo y eliminación automática de los artefactos, archivos y modificaciones de registro asociados a la detección. Es necesario precisar si este alcance satisface el requerimiento, dado que existen mecanismos de reversión de naturaleza distinta (restauración de imagen o instantánea del sistema operativo completo).



Solicitud: Se solicita a la Entidad confirmar que el requerimiento del ítem 4.2 se entiende satisfecho con esta capacidad de reversión automática de cambios maliciosos, y no con un mecanismo de restauración de imagen o instantánea del sistema operativo completo.