Grupo Social y Empresarial de la Defensa	**MINISTERIO DE DEFENSA NACIONAL** **CAJA DE RETIRO DE LAS FUERZAS MILITARES** **ANEXO TECNICO**	Servicio Justo y Oportuno

F-GRA-11/19-02-2021

ASPECTOS GENERALES

OBJETO:

CONTRATAR LA RENOVACION Y ACTIVACION DEL LICENCIAMIENTO DE LA PLATAFORMA DE SEGURIDAD CORTEX XDR CON EL SERVICIO DE SOPORTE TECNICO DE FABRICA PARA LA CAJA DE RETIRO DE LAS FUERZAS MILITARES.

1. CARACTERISTICAS TÉCNICAS

La herramienta de seguridad Cortes XDR brindan protección tanto a las aplicaciones Web, PC´s, servidores y red de datos de la entidad de la siguiente manera:

- **Modalidad de prestación del servicio**: El servicio de Cortex XDR se prestará bajo la modalidad Software como Servicio (SaaS), mediante plataforma en la nube administrada por el fabricante Palo Alto Networks, comprende el acceso al portal de administración, la actualización continua de la plataforma, el procesamiento y almacenamiento de eventos de seguridad, las capacidades de analítica avanzada, correlación de eventos, detección y respuesta ante amenazas, así como la distribución de actualizaciones de contenido y del agente.
- **Agentes de Cortex XDR**: Se mantienen instalados en los equipos y servidores objeto de protección, los cuales se comunican de manera segura con la plataforma SaaS mediante los mecanismos de conectividad soportados por el fabricante, tales como Proxy o Broker VM si es requerido por la entidad.
- **Interacción de los agentes:** Los agentes ejecutan procesos de monitoreo continuo sobre el sistema operativo, aplicaciones, procesos, archivos, memoria, conexiones de red y actividades de los usuarios.
- **Ubicación general del procedimiento y almacenamiento de la información generada por la solución:** el procesamiento, análisis, correlación y almacenamiento de la información generada por los agentes instalados en los equipos y servidores protegidos se realiza principalmente en la plataforma en la nube dispuesta por el fabricante, la información recolectada por los agentes Cortex XDR, como eventos de seguridad, telemetría de endpoints, alertas, registros de actividad, indicadores de compromiso, metadatos y resultados de análisis, es transmitida de forma segura hacia la consola central de Cortex XDR alojada en la infraestructura cloud del fabricante, utilizando canales cifrados.
- **Manejo de la información derivada de eventos, registros y reportes de seguridad:** La información derivada de los eventos, registros (logs), alertas e incidentes de seguridad generados por la solución Cortex XDR permiten la recepción, procesamiento, almacenamiento, correlación y consulta y son transmitidos de forma segura hacia la plataforma SaaS del fabricante, donde son analizados utilizando mecanismos de inteligencia artificial e inteligencia de amenazas para la detección de comportamientos anómalos y posibles incidentes de ciberseguridad.

Por los motivos mencionados, es necesario renovar las licencias, el soporte y mantenimiento para garantizar la continuidad y disponibilidad de los siguientes servicios:

- Renovar el licenciamiento de la plataforma de seguridad Cortex XDR
- Servicio de soporte técnico con fabricante

2. DESCRIPCIÓN GENERAL DE LOS SERVICIOS

El contratista deberá desarrollar el cumplimiento de las siguientes actividades para la renovación y activación de la herramienta de seguridad para garantizar la continuidad y disponibilidad del servicio así:

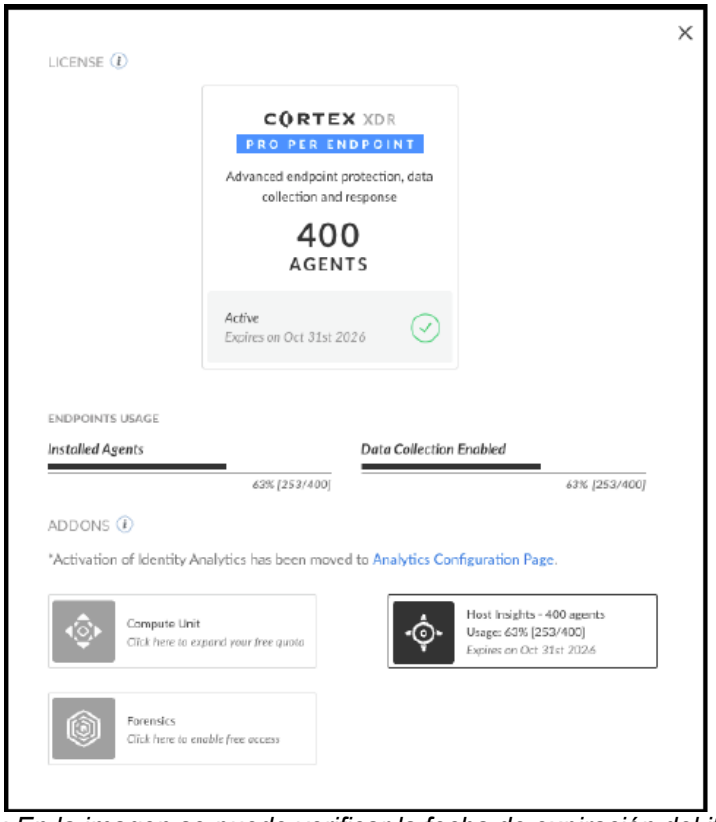
ÍTEM	DESCRIPCIÓN	CANTIDAD
1	Renovar el licenciamiento de la plataforma de seguridad Cortex XDR	400
2	Servicio de Soporte técnico con fábrica	1

NOTA: Para la renovación de la licencia y el soporte técnico con fábrica deberán activarse a partir del día siguiente al vencimiento indicado por la Entidad, esto es, desde el 31 de octubre de 2026, garantizando la continuidad del servicio sin interrupciones.

1. RENOVAR EL LICENCIAMIENTO DE LA PLATAFORMA DE SEGURIDAD CORTEX XDR

CREMIL cuenta actualmente con la siguiente herramienta de seguridad, a la cual se debe renovar su licenciamiento por un (1) año.

CANTIDAD	P/N	DESCRIPCION	SERIALES	FECHA DE EXPIRACIÓN
400	PAN-XDR-ADV-EP	Cortex XDR Pro for 1 endpoint, includes 30 days of date retention and standard success	0220980000030125	10/31/2026
	PAN-XDR-HOST-INST	Host Insights add-on for Cortex XDR		



NOTA: En la imagen se puede verificar la fecha de expiración del item 1.

2. SERVICIO DE SOPORTE TÉCNICO CON FABRICANTE

El contratista debe cumplir con lo siguiente durante la vigencia de las licencias:

ASISTENCIA TECNICA	
1	El contratista deberá prestar el servicio de soporte técnico con fabrica durante el tiempo de vigencia de las licencias a partir del acta de inicio, responder a los requerimientos o solicitudes realizados por CREMIL, en un esquema 7x24 con un tiempo de respuesta de 2 horas a partir de la solicitud, para soportar el primer nivel de atención de manera remota o presencial, el tiempo máximo para la atención y solución de un incidente o problema debe ser de cuatro (4) horas, contadas a partir del reporte de la novedad.
2	En coordinación con el supervisor del contrato, el contratista revisará y afinará la herramienta de administración de Cortex XDR durante la ejecución del contrato.
3	En el caso de actualización de versiones, el contratista deberá programar esta actualización con anterioridad y con aprobación del Supervisor del contrato, así mismo, deberá programar la socialización de las nuevas funcionalidades de administración de las plataformas para los funcionarios que gestionen la solución.
4	El contratista deberá realizar la respectiva configuración, actualización y soporte técnico con fabrica durante la vigencia del licenciamiento, deberá incluir la puesta en marcha de nuevas versiones firmware, reléase, parches y demás productos a la última versión

	probada del fabricante necesarios para corregir problemas y efectuar mejoras sobre los productos licenciados.
5	El contratista deberá instalar los componentes dentro de la infraestructura del cliente, PC, Portatiles y Servidores durante la ejecución del contrato.
6	El contratista deberá definir alertas basadas en el análisis de vulnerabilidades o los resultados de la auditoría de configuración las cuales deberán sincronizarse con el correo institucional del supervisor del contrato.
7	El contratista será en encargado de instalar las actualizaciones y uso de la última versión estable, por el fabricante durante la vigencia del Licenciamiento adquirido.
8	Entregar un reporte trimestral al correo del supervisor del contrato detallado de la trayectoria de todos los sistemas protegidos y permitir identificar archivos de malware descargados, archivos que estén descargando malware y/o cualquier tipo de aplicaciones dañinas.
9	El contratista deberá entregar un informe del diagnóstico del estado actual de la solución de seguridad generando las recomendaciones de las mejores prácticas de administración y configuración para un mejor rendimiento y desempeño de la infraestructura de seguridad de Cremil a los 15 días de iniciado el contrato.
11	Monitoreo permanente para el escaneo de vulnerabilidades, entrega de un informe trimestral al correo del supervisor del contrato para realizar las remediaciones pertinentes.

TRANSFERENCIA DE CONOCIMIENTO	
1	El Contratista deberá efectuar la transferencia de conocimiento de la herramienta **Cortex XDR** a tres (3) funcionarios del Grupo de Infraestructura Tecnológica de la Oficina TIC, con una intensidad de diez (10) horas, modalidad virtual, durante el periodo de ejecución contractual.

MESA DE SERVICIO	
1	El oferente para la prestación del servicio debe incluir el soporte técnico a través de una mesa de ayuda cuyo alcance se relacione en certificar servicios administrados, soporte y prestación de servicios, a través de esta mesa de servicio será la encargada de gestionar todos los incidentes y requerimientos reportados, garantizando calidad de la asistencia brindada.
2	El oferente deberá garantizar la prestación de asistencia no programada sin límite de solicitudes incluidos durante el tiempo que dure las licencias.

Equipo de trabajo

Garantizar la prestación del servicio del objeto contractual, a través del personal solicitado en “Roles del equipo de trabajo requerido” del presente anexo técnico, a CREMIL (presencial o virtual), durante el tiempo que dure el licenciamiento contratado por un (1) año.

PERFIL	FORMACIÓN	EXPERIENCIA PROFESIONAL
Dos (2) Ingenieros certificados	Ingeniero de sistemas o electrónico o telecomunicaciones Certificaciones vigentes en: Palo Alto Networks Certified Network Security Professional	Acreditar experiencia profesional con mínimo dos (2) años y máximo cinco (5) años en proyectos de seguridad informática ejecutados en contratos mediante la presentación de certificaciones cuyas actividades sean relacionadas con el objeto del presente proceso.

	y/o PCNSC Palo Alto Networks Certified Network Security Consultant	

Con el fin de acreditar las calidades y experiencia académica y laboral del personal arriba mencionado, el proponente debe allegar los siguientes documentos con la oferta así:

- Hoja de vida firmada.
- Fotocopia de la cédula de ciudadanía.
- Copia de los títulos o acta de grado de pregrado, y/o postgrado expedido por una universidad con registro calificado ante el M.E.N vigente.
- Certificaciones de experiencia. Las certificaciones deberán contener la siguiente información: nombre, dirección y teléfono de quien suscribe la certificación, plazo de duración del contrato, fecha de inicio y fecha de finalización, descripción de las funciones realizadas por el contratante.

NOTA: Para efectos de contabilización de tiempo de experiencia profesional no se aceptarán certificaciones de actividades realizadas en tiempos simultáneos con diferentes empleadores (traslapo de tiempo).

Notas generales que los proponentes deben tener en cuenta:

Nota 1	Cuando se trate de estudios realizados en el exterior, el título deberá estar convalidado de acuerdo con la legislación colombiana.
Nota 2	El desarrollo del objeto contractual debe ser realizado por el personal ofertado y anteriormente descrito, en caso de requerirse cambio del personal, el contratista deberá entregar los documentos soporte que cumplan con los perfiles y presenten iguales o superiores características a las estipuladas en las condiciones técnicas al supervisor para que éste los apruebe
Nota 3	La experiencia será contada a partir de la expedición de la tarjeta profesional (Según Aplique).
Nota 4	Para las profesiones afines al personal mínimo requerido se tomará en cuenta lo publicado por SNIES – (Sistema Nacional de Información de Educación Superior)
Nota 5	El contratista, deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato.
Nota 6	El contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de esta.
Nota 7	Que, en caso de resultar adjudicatario, se compromete a cambiar al personal designado en caso de presentarse inconformidades, previa solicitud del supervisor sin generar costo alguno para la entidad. El personal deberá cumplir con las mismas o superiores características aquí descritas de acuerdo con el perfil y para ello el contratista deberá entregar la hoja de vida al supervisor para su verificación y aceptación. sin necesidad de suscribir un contrato modificatorio.
Nota 8	Todo el personal que sea empleado por el contratista para el cumplimiento de las obligaciones que adquiera en virtud de la ejecución del contrato, será de su exclusiva cuenta y riesgo y se entenderán directamente con el contratista para efectos de pago de salarios, prestaciones sociales, indemnizaciones y demás costos inherentes a que haya lugar, puesto que la Entidad, no adquiere ninguna relación civil o laboral con los trabajadores del contratista
Nota 9	Dentro de los 5 días calendario siguientes a la firma del contrato, el contratista deberá presentar al supervisor del contrato, fotocopia del carné de afiliación al sistema de seguridad social de todo el personal.

Atentamente,

Iván Gómez Maldonado.

Ing. Iván Mauricio Gómez Maldonado
Profesional de Defensa Oficina TIC
Coordinador(a) o responsable del proceso

COMITÉS ESTRUCTURADORES

COMITE TECNICO	CARGO Y NOMBRES	FIRMA
Estructurador técnico del proceso	Ing. IVÁN MAURICIO GÓMEZ MALDONADO Profesional de Defensa Oficina TIC	Iván Gómez Maldonado.