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:

ADQUISICIÓN E IMPLEMENTACIÓN DE LICENCIAS Y SERVICIOS INTEGRALES PARA SOLUCIONES DE PREVENCIÓN DE PÉRDIDA DE DATOS (DLP), ANÁLISIS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES (UEBA) Y ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA DE SEGURIDAD (SOAR)

1. ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

1.1 INFRAESTRUCTURA DE CIBERSEGURIDAD EXISTENTE EN CREMIL		
Las soluciones de DLP, UEBA y SOAR deben integrarse nativamente con los siguientes componentes ya operativos en CREMIL:		
Componente (operativo)	**Función actual**	**Capacidades disponibles para integración nativa**
Plataforma XDR	Detección y respuesta extendida en endpoints, red e identidad	Telemetría de endpoint, alertas de amenazas, respuesta automática, historial de procesos y conexiones de red
Solución de seguridad de navegación empresarial	Control y protección del tráfico de navegación web institucional en las instalaciones de la entidad.	Logs de navegación por usuario, categorías de contenido, uso de aplicaciones SaaS, intentos de acceso malicioso
Seguridad perimetral de red — NGFW (FIREWALL)	Control y protección del tráfico de red en el perímetro corporativo	Logs de tráfico, sesiones activas, aplicaciones detectadas, usuarios autenticados, amenazas bloqueadas

1.2 REQUISITO FUNDAMENTAL DE INTEGRACIÓN NATIVA

Las soluciones ofertadas deben:

a. Compartir el mismo almacén de datos y motor de correlación con los componentes existentes, sin replicación ni sincronización externa.
b. Operar bajo una única consola de administración que gestione políticas de los tres nuevos módulos (UEBA, SOAR Y DLP) y los componentes existentes desde la misma interfaz.
c. Utilizar las mismas fuentes de inteligencia de amenazas e identificadores de usuario, dispositivo y red ya enrolados en CREMIL.
d. Intercambiar eventos, alertas y acciones mediante API propietaria nativa del mismo fabricante, sin conectores SIEM intermedios.
e. Escalar bajo el mismo modelo de licenciamiento existente, sin multiplicar consolas, para lo cual el proponente deberá garantizar la incorporación de estos 3 componentes (UEBA, SOAR Y DLP) durante toda la ejecución del contrato por el termino de la vigencia de estas (12 meses)

1.3 ESPECIFICACIONES TÉCNICAS — PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

a. La herramienta deberá tener una vigencia de 12 meses, contados a partir de su activación y la implementación deberá ser respalda y ejecutada por el fabricante.
b. Inspección de tráfico de red saliente en tiempo real (HTTP/S, SMTP, FTP y protocolos empresariales) con análisis de contenido hasta capa 7.
c. Agente DLP en dispositivos de usuario final (Windows, macOS) que monitoree y controle operaciones de copia, impresión, captura de pantalla y transferencia a dispositivos USB.
d. Control de subida y descarga de datos sensibles en aplicaciones SaaS institucionales aprovechando la telemetría de navegación ya disponible en la infraestructura existente, sin agente adicional de proxy ni redirección de tráfico. La correlación usuario-sesión-dato debe realizarse de forma automática sin reautenticación adicional.
e. Clasificación de contenido mediante regex y análisis de datos sujetos a protección y regulación especial en colombianos: Cédula de Ciudadanía (con validación de dígito de verificación), NIT, tarjetas de crédito (PCI-DSS), datos de salud (HCU), información financiera, información clasificada con marcadores personalizables.
f. Enriquecimiento automático de alertas DLP con contexto de identidad, dispositivo y comportamiento de la plataforma XDR existente, sin exportación manual de eventos (logs).
g. Gestión centralizada de políticas DLP desde la misma consola de los componentes XDR y de navegación existentes.

h.	El motor DLP evalúa y hace cumplir las políticas localmente en los endpoints, protegiendo los datos incluso cuando el equipo no tiene conexión a la red o a internet.
i.	Notificación en tiempo real con contexto completo del incidente; bloqueo automático de la operación exfiltrante; copia del archivo a repositorio forense con hash criptográfico para cadena de custodia; activación automática del workflow SOAR integrado.
j.	Descubrimiento y clasificación de datos sensibles almacenados en repositorios de red, correo y nube (datos en reposo).
k.	Modelos de aprendizaje automático preentrenados para reducción de falsos positivos, ajustados al comportamiento histórico de los usuarios de CREMIL.
l.	Configuración a nivel de tenant para decidir qué hacer si el proceso DLP falla: Fail-open (permite la transferencia para no interrumpir el trabajo) o Fail-close (bloquea el archivo).
m.	Capacidad de mostrar ventanas emergentes (End User Dialogs) personalizables en el endpoint cuando una acción es bloqueada.
n.	Identifica y controla el uso de aplicaciones locales predefinidas utilizadas para transferencia de datos, tales como FileZilla, OpenSSH, WinSCP y PuTTY.
o.	Inspecciona múltiples formatos de archivo, incluyendo documentos ofimáticos (docx, xlsx, pptx), código/scripts (py, js, java, vbs) y otros formatos como pdf y csv.
p.	Capacidad de inspeccionar y bloquear subidas en aplicaciones locales de chat y colaboración que usan tecnología WebView2 (ej. WhatsApp, Microsoft Teams, Zoom) mediante la herencia de procesos padre-hijo.
q.	Integración total con playbooks de la herramienta de SOAR para automatizar la obtención de datos de Active Directory, enviar solicitudes de aprobación de excepciones, y notificar a los usuarios el resultado para cerrar el incidente.
1.4	**ESPECIFICACIONES TÉCNICAS — ANÁLISIS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES (UEBA)**
a.	La herramienta deberá tener una vigencia de 12 meses, contados a partir de su activación y la implementación deberá ser respalda y ejecutada por el fabricante.
b.	Construcción automática de perfiles de comportamiento normal por usuario, dispositivo y entidad de red durante mínimo 30 días, sin configuración manual de reglas. Actualización continua del modelo sin intervención del analista.
c.	Identificación estadística de desviaciones respecto al comportamiento histórico individual: horarios de acceso, volumen de datos manipulados, aplicaciones utilizadas, ubicación de acceso y recursos consultados.
d.	Detección de comportamientos anómalos en dispositivos, servidores, aplicaciones y cuentas de servicio: tráfico inusual, escalada de privilegios y conexiones a destinos no habituales.
e.	Puntuación de riesgo dinámica por usuario (escala 0–100) que integre señales de los componentes XDR, navegación, NGFW y DLP, con actualización en tiempo real ante cada nuevo evento.
f.	Correlación de eventos de las plataformas XDR, navegación y NGFW con el comportamiento del usuario para generar alertas contextualizadas y priorizadas.
g.	Identificación de movimiento lateral: patrones de acceso secuencial a múltiples sistemas en intervalos comprimidos.
h.	Mínimo 15 modelos de detección preconfigurados: exfiltración de datos, acceso no autorizado, compromiso de credenciales, uso de herramientas de hacking y comportamiento de ransomware.
i.	Sincronización automática con el directorio de identidades de CREMIL para enriquecer perfiles con atributos organizacionales (cargo, área, nivel de acceso).
j.	Interfaz de threat hunting para búsquedas ad-hoc sobre el historial de comportamiento de usuarios y entidades.
1.4.1.	**Criterios de puntuación de riesgo (Risk Score 0–100)**

Rango de score	Clasificación	Comportamiento del sistema	Acción SOAR automática recomendada
0 – 30	Riesgo bajo — dentro de la norma	Sin alertas activas. Monitoreo pasivo continuado.	Sin acción automática
31 – 59	Riesgo medio — desviación leve	Alerta informativa en el panel SOC para revisión en la siguiente sesión de trabajo.	Notificación de alertamiento si persiste más de 48h sin revisión
60 – 79	Riesgo alto — múltiples señales correlacionadas	Alerta activa con prioridad alta. Notificación inmediata al analista asignado.	De acuerdo con los Playbooks según señal dominante
80 – 100	Riesgo crítico — amenaza activa confirmada	Alerta crítica inmediata. Activación automática de playbook correspondiente.	Activación automática según contexto de la amenaza

1.4.2. Catálogo de comportamientos técnicos específicos a detectar (B01–B25)

La solución UEBA debe detectar autónomamente los siguientes comportamientos:

ID	Comportamiento / Señal a detectar	MITRE ATT&CK	Criticidad
B01	User agent sospechoso en solicitudes HTTP/S — herramientas de ataque o navegadores inusuales	T1071 — Application Layer Protocol	Alta
B02	PowerShell con parámetros de ofuscación, codificación Base64 o invocación de métodos de reflexión no habituales	T1059.001 — PowerShell	Crítica
B03	Uso inusual de herramientas Sysinternals (PsExec, PsInfo, Autoruns) por no administradores o fuera de ventanas de mantenimiento	T1569.002 — Service Execution	Alta
B04	Uso sospechoso de CURL o herramientas de transferencia HTTP desde endpoints de usuario final hacia destinos externos	T1105 — Ingress Tool Transfer	Alta
B05	Servicio remoto iniciado desde cuentas de usuario estándar o procesos padre no esperados	T1543 — Create/Modify System Process	Alta
B06	Volumen de conexiones de red significativamente superior a la línea base del dispositivo o usuario	T1571 — Non-Standard Port	Media
B07	Query LDAP que enumera usuarios, grupos, GPOs o atributos desde procesos no autorizados para operaciones de directorio	T1069 — Permission Groups Discovery	Alta
B08	Modificación del firewall local (Windows o Linux) para abrir puertos no autorizados o permitir conexiones entrantes inusuales	T1562.004 — Disable/Modify Firewall	Crítica
B09	Sesión WinRM desde equipos o cuentas sin historial de administración remota, o hacia destinos inusuales	T1021.006 — Windows Remote Management	Alta
B10	Ejecutables o scripts en rutas no estándar (Temp, AppData, ProgramData) o con nombres que imitan herramientas legítimas del sistema	T1036 — Masquerading	Crítica
B11	Escalada al contexto SYSTEM desde cuentas de usuario estándar sin justificación de tarea programada o instalador conocido	T1068 — Exploitation for Privilege Escalation	Crítica
B12	Deshabilitación de iptables, nftables o firewalld fuera de ventanas de mantenimiento autorizadas	T1562.004 — Impair Defenses	Crítica
B13	Registro de tareas programadas (Task Scheduler o cron) por procesos o usuarios no autorizados, indicativo de persistencia	T1053 — Scheduled Task/Job	Alta
B14	Ejecución de arp.exe para enumeración de la red local, indicativo de reconocimiento previo a movimiento lateral	T1018 — Remote System Discovery	Media
B15	Capturas de pantalla repetidas por proceso o usuario, especialmente combinadas con actividad de subida de archivos	T1113 — Screen Capture	Alta
B16	Sesiones RDP desde equipos o usuarios sin historial de uso de este protocolo, o en horarios fuera del patrón normal	T1021.001 — Remote Desktop Protocol	Alta

B17	Actividad de sondeo TCP/UDP desde un endpoint corporativo hacia la red interna o externa	T1046 — Network Service Scanning	Alta
B18	Adición de equipos al dominio de Active Directory desde cuentas sin permisos habituales para esta operación	T1136 — Create Account	Alta
B19	Asignación del grupo Domain Admins fuera de procedimientos de gestión de identidades autorizados	T1098 — Account Manipulation	Crítica
B20	Volumen de impresión significativamente superior a la línea base del usuario, especialmente documentos clasificados	T1048 — Exfiltration Over Alternative Protocol	Media
B21	Ejecución de aplicaciones no pertenecientes al inventario de software autorizado de CREMIL (P2P, tunelización, anonimización)	T1072 — Software Deployment Tools	Media
B22	DNS a dominios recién registrados, con alta entropía de nombres (DGA) o con volumen anormalmente alto	T1568 — Dynamic Resolution	Alta
B23	Tráfico Kerberos o SMB desde proceso no estándar, indicativo de Pass-the-Hash o Pass-the-Ticket	T1550 — Alternate Authentication Material	Crítica
B24	Transferencia saliente de datos en volumen inusual hacia destinos en nube no categorizados, correo externo o servicios de compartición no autorizados	T1048/T1567 — Exfiltration	Crítica
B25	Consulta o descarga de documentos clasificados en un intervalo de tiempo comprimido, inusual en el patrón histórico del usuario	T1039 — Data from Network Shared Drive	Alta

NOTA 1 TÉCNICA: la detección autónoma de al menos veinte (20) de los veinticinco (25) comportamientos listados,

NOTA 2 TÉCNICA: Las reglas relacionadas corresponden a los criterios iniciales de detección definidos por la Entidad y deberán ser atendidos por la solución durante la ejecución contractual. Además de las enunciadas, el contratista durante la ejecución del contrato podrá incorporar nuevos comportamiento de acuerdo con las nuevas casuísticas y riesgos identificados mediante el análisis de logs, alertas y comportamientos de navegación de la Entidad, siempre dentro de las capacidades y alcance de la solución contratada.

1.5 ESPECIFICACIONES TÉCNICAS — ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA (SOAR)
a. La herramienta deberá tener una vigencia de 12 meses, contados a partir de su activación y la implementación deberá ser respalda y ejecutada por el fabricante.
b. Interfaz gráfica para crear, modificar y versionar playbooks sin programación: decisiones condicionales, bucles, acciones paralelas y escalación humana.
c. La solución debe ofrecer flexibilidad total en sus modelos de despliegue, soportando tanto una implementación on-premise que garantice que los datos generados por la organización permanezcan exclusivamente dentro de sus instalaciones, como arquitecturas en la nube o completamente SaaS, las cuales deberán contar con la capacidad de integrarse y conectarse de forma segura con la infraestructura local de la entidad.
d. La Solución debe ofrecer Control de Acceso Basado en Rol (RBAC por sus siglas en idioma inglés) así como también el mapeo de roles a los grupos en el Directorio Activo o SAML. Los roles se corresponden con permisos granulares con inclusión de leer/escribir, leer solamente, y acceso denegado a varias áreas de la Solución
e. La plataforma no limita el número de acciones, tareas, incidentes, indicadores, playbooks u otra acción operativa.
f. La plataforma debe realizar procesos automáticos preventivos y proactivos. Estos procesos deben ejecutarse con una frecuencia programada y sin necesidad de que un incidente se manifieste como tal.
g. Mínimo 100 playbooks preconfigurados y listos para producción: phishing, ransomware, exfiltración, compromiso de credenciales, análisis de malware y movimiento lateral.
h. La plataforma deberá permitir ejecutar playbooks frente a conjuntos de indicadores especificados por el usuario, así como ejecutar automatizaciones personalizadas ante eventos de creación, edición o eliminación de indicadores. Esta capacidad garantiza que las respuestas de seguridad se activen de manera oportuna ante cualquier cambio en el estado de los indicadores monitoreados.
i. Los playbooks deben soportar acciones totalmente automatizadas, tareas manuales, recolección de datos y tareas condicionadas, pudiendo ejecutarse automáticamente al crear un incidente, como tareas programadas o en tiempo real. Esta flexibilidad permite adaptarse a diferentes escenarios de respuesta y necesidades operativas de la organización.
j. Deberá tener un Sistema de tickets integrado para gestión del ciclo de vida completo de incidentes: asignación, priorización, SLA y trazabilidad de acciones de respuesta ejecutadas.
k. Ejecución de acciones directamente en la plataforma XDR existente (aislamiento de endpoint, terminación de proceso, bloqueo de hash) desde el playbook SOAR sin API externa.
l. Activación automática ante alertas DLP: cuarentena de archivos, bloqueo de usuario, notificación a responsables y apertura de caso de investigación.
m. Activación automática ante puntuaciones de riesgo UEBA que superen umbrales configurados, con acceso al perfil de comportamiento como contexto del incidente.
n. La Plataforma debe poder admitir formatos de código abierto estándar como STIX , CSV, JSON, Plain Text
o. Debe permitir al analista buscar indicadores en función de campos como etiquetas, estado o tipo de indicador para llevar a cabo acciones determinada o La plataforma debe automatizar la consolidación de la normalización tanto desde herramientas internas como externas para responder a los ataques en tiempo real
p. La plataforma debe realizar la des duplicación automática de indicadores
q. La plataforma debe admitir la inclusión de indicadores internos como IP y URL en la lista blanca, para garantizar que no sean marcados como maliciosos

r.	La Solución debe ser capaz de sugerir próximos pasos de acuerdo con el aprendizaje de máquina realizado durante investigaciones previas.
s.	Ejecución de acciones en el NGFW existente (bloqueo de IP/dominio, creación de reglas temporales, captura de tráfico) desde playbooks.
t.	Consulta automática de fuentes de inteligencia de amenazas (URLs, IPs, hashes, dominios) al iniciar cada caso, sin acción manual por parte de la entidad.
u.	Debe incluir la capacidad de generar informes de incidentes, informes de estadísticas (tales como MTTR – tiempo medio de reSolución) y los resúmenes o informes por incidente.
v.	Debe soportar informes programados y asociarse a una lista de distribución de correos, y el motor de informes debe ser compatible con formatos PDF, DOC y CSV.
w.	La Solución debe incluir aprendizaje dinámico de los IOCs e incidentes que se investigan y ayudar a al personal de la entidad a identificar incidentes que pueden estar relacionados.
x.	playbooks nativos de gestión de inteligencia de amenazas (Threat Intel Management) que puedan ser ejecutados directamente utilizando indicadores de compromiso (IOCs), permitiendo automatizar las tareas de investigación, enriquecimiento y respuesta.
y.	War room colaborativa digital para que múltiple personal de la entidad trabajen en tiempo real sobre un incidente.

1.5.1. Catálogo de integraciones requeridas

Sistema por integrar	Acciones requeridas desde SOAR	Prioridad
Plataforma XDR existente	Aislamiento de endpoint, consulta de historial de procesos, terminación de proceso, bloqueo de hash, adición a grupos de políticas	Crítica
Solución DLP existente	Consulta de alertas activas, modificación de políticas de usuario, cuarentena de archivos, solicitud de evidencias forenses	Crítica
Módulo UEBA existente	Consulta de puntuación de riesgo, historial de anomalías, snapshot de comportamiento del usuario	Crítica
NGFW — seguridad perimetral de red	Bloqueo de IP/dominio, creación de reglas de política temporal, consulta de sesiones activas	Crítica
Directorio de identidades corporativo	Deshabilitación de cuenta, restablecimiento de contraseña, consulta de atributos, adición a grupos de cuarentena	Crítica
Correo electrónico corporativo	Envío de notificaciones, recuperación de mensajes de phishing, consulta de metadatos de correo	Alta
Sistema de tickets / ITSM	Creación de tickets, actualización de estado, escalación a segunda línea con SLA	Alta
Fuentes de inteligencia de amenazas	Consulta de reputación de IP, URL, dominio y hash; ingesta de IOC	Alta
Plataforma SIEM Googlr SecOps (si aplica)	Búsqueda de eventos históricos relacionados con el incidente	Media

1.5.2. Playbooks obligatorios (*operacionales en el primer mes de ejecución*)

ID	Nombre	Secuencia lógica mínima de ejecución

PB01	Respuesta a phishing	Recepción → extracción de URLs, adjuntos y remitente → consulta de reputación en inteligencia → análisis de hash de adjuntos → si malicioso: bloqueo de dominio/IP en NGFW y navegación → búsqueda de otros usuarios expuestos → notificación individualizada → cierre con informe de alcance
PB02	Respuesta a exfiltración DLP	Alerta DLP crítica → cuarentena de archivo en repositorio forense → consulta de perfil de riesgo UEBA en tiempo real → si score UEBA > umbral: aislamiento preventivo del endpoint → notificación al supervisor del contrato y CISO → registro forense con hash → apertura de caso de investigación
PB03	Anomalía UEBA de insider	Score UEBA ≥ 80 → snapshot de actividad de las últimas 24h → verificación de alertas DLP activas del usuario → consulta de accesos a recursos críticos en 48h → verificación de sesiones activas → apertura automática de caso → notificación al CISO con resumen ejecutivo
PB04	Compromiso de credenciales	Alerta de acceso anómalo o fuerza bruta → deshabilitación preventiva en directorio → cierre de todas las sesiones activas → forzado de restablecimiento de contraseña → notificación al usuario por canal alternativo → notificación a supervisor → apertura de ticket con evidencias
PB05	Respuesta a ransomware	Comportamiento de cifrado masivo → aislamiento inmediato del endpoint (sin acceso a red) → bloqueo de IP C2 en NGFW → búsqueda de otros endpoints con actividad similar en las últimas 2h → consulta de backups disponibles → notificación de emergencia al equipo de respuesta → apertura de incidente mayor con clasificación de impacto
PB06	Investigación de malware	Detección XDR → extracción del hash del archivo → consulta en fuentes de inteligencia → búsqueda del hash en todos los endpoints monitoreados → bloqueo del hash en todos los endpoints y en navegación → análisis de procesos padre-hijo → generación de informe con IOC identificados
PB07	Vulnerabilidades críticas	Resultado de escaneo con severidad crítica/alta → priorización de dispositivos con exposición a internet → verificación de exploits públicos conocidos → clasificación por criticidad del activo → ticket de remediación con SLA (crítico 24h, alto 72h) → seguimiento automático y verificación de cierre
PB08	Escalación de incidente	Verificación de casos con SLA vencido → actualización automática de prioridad → notificación a segunda línea con contexto completo → notificación a supervisor de turno SOC → registro del evento de escalación en el historial del caso → reinicio del contador de SLA de segunda línea
PB09	Reporte diario SOC	Ejecución 06:00 diario → recopilación de métricas del día anterior (volumen de alertas por módulo, casos abiertos/cerrados, MTTD/MTTR, tasa de automatización, ANS) → comparación con día anterior y semana anterior → generación de informe HTML/PDF → envío a lista de distribución (supervisor del contrato, gerencia TI)
PB10	Integridad de infraestructura	Ejecución semanal lunes 07:00 → verificación de estado de cada componente del ecosistema (XDR, DLP, UEBA, SOAR, navegación, NGFW) → verificación de agentes activos y versionados → alerta inmediata si hay degradación → verificación de integridad de políticas críticas → reporte semanal de salud del ecosistema

1.6 Acuerdos de Niveles de Servicio (ANS)

Categoría	Criterio de clasificación	Tiempo de respuesta	Tiempo de resolución
Crítico — P1	Indisponibilidad total de cualquier componente en producción o incidente de seguridad activo	30 minutos	4 horas

Alto — P2	Degradación significativa de funcionalidades o configuración incorrecta de políticas críticas	2 horas	8 horas hábiles
Medio — P3	Funcionalidad afectada con workaround disponible o consulta técnica compleja	4 horas hábiles	3 días hábiles
Bajo — P4	Consultas, optimizaciones y solicitudes de nuevas configuraciones	1 día hábil	5 días hábiles
Disponibilidad mensual (SLA)	Componentes en la nube del fabricante, excluyendo mantenimientos programados con 72h de anticipación	≥ 99.5% mensual	—

1.7 UNIDADES DE VISUALIZACIÓN DIGITAL ESTACIONARIA DE GRAN FORMATO Y MATRIZ ACTIVA PARA ENTORNOS DE MISIÓN CRÍTICA (SOC).

Para garantizar la efectividad de la *War Room* colaborativa digital y permitir que el Grupo de Infraestructura Tecnológica de la Oficina TICS audite en tiempo real los tableros de control unificados de DLP, UEBA y SOAR, se requiere la incorporación de hardware especializado de salida visual de gran formato, con las siguientes características:

1. Cantidad: Cuatro (4).
2. Dimensión Diagonal del Panel: Mínimo de 152,4 centímetros.
3. Resolución y Densidad de Píxeles: Reproducción de video en resolución original de 3840×2160 píxeles.
4. Capacidad de Interfaz e Integración: Mínimo tres (3) puertos HDMI de alta velocidad, compatibilidad con protocolos de transmisión de datos inalámbricos empresariales y puerto RJ-45 de red.
5. Tasa de Refresco y Ciclo de Trabajo: Optimizado para operación continua (mínimo 16/7) con tecnología de reducción de fatiga visual.
6. Instalación de todos componentes contemplada a todo costo para que quede funcional
7. Un (1) Equipo de cómputo que va a soportar la visualización de los tablero:
    a. **Procesamiento, memoria y almacenamiento.** El equipo deberá contar con procesador de mínimo 6 núcleos físicos, frecuencia base ≥3.0 GHz y soporte para virtualización hardware; memoria RAM de 32 GB DDR4/DDR5 a 3200 MHz en configuración dual-channel, expandible a 64 GB; almacenamiento principal SSD NVMe PCIe Gen3 de 512 GB con lectura secuencial ≥3000 MB/s, más disco secundario de 2 TB HDD o 1 TB SSD para almacenamiento de evidencias.
    b. **Subsistema gráfico para matriz de 4 monitores.** Deberá incorporar tarjeta gráfica dedicada con 6 GB VRAM GDDR6 mínimo, mínimo cuatro (4) salidas de video nativas DisplayPort 1.4 o HDMI 2.0, soporte para resolución 2560x1440@60Hz por pantalla, drivers certificados para entornos empresariales y capacidad de renderizar interfaces de consolas de ciberseguridad sin latencia perceptible ni pérdida de foco en ventanas activas durante sesiones prolongadas de operación SOC.
    c. **Conectividad, expansión y gestión remota.** El equipo deberá integrar controlador Ethernet Gigabit con soporte PXE/Wake-on-LAN, módulo Wi-Fi 6 (802.11ax) y Bluetooth 5.0+, mínimo cuatro puertos USB 3.2 Gen1 y un puerto USB-C con soporte de video; fuente de poder ≥550W; módulo TPM 2.0 y soporte para Secure Boot.

NOTA: Estos bienes deberán ser entregados a la Entidad al inicio de la ejecución contractual, debidamente instalados y en condiciones óptimas de funcionamiento, y serán recibidos a satisfacción mediante la correspondiente acta de entrega. Una vez efectuada su recepción, los bienes harán parte de los activos de la Entidad, de conformidad con los procedimientos internos aplicables. El Contratista será responsable de garantizar su correcta instalación, puesta en marcha y funcionamiento, conforme a las especificaciones técnicas establecidas en el presente Anexo Técnico.

1.8 OTROS REQUERIMIENTOS

1. **Alcance de la Implementación**
   El CONTRATISTA deberá ejecutar la implementación de las soluciones de DLP, UEBA y SOAR bajo la modalidad **"llave en mano"**, asumiendo la responsabilidad integral de:

Actividad	Descripción Detallada	Entregable
Suministro	Provisión de licencias, agentes, conectores, módulos de software y componentes de infraestructura necesarios para el funcionamiento completo de la solución	Certificado de licenciamiento vigente a nombre de la Entidad
Instalación	Despliegue de componentes en la arquitectura tecnológica de la Entidad (on-premise, nube híbrida o SaaS), incluyendo configuración de alta disponibilidad si aplica	Acta de instalación técnica firmada por los intervinientes.
Configuración	Parametrización de políticas DLP, modelos de comportamiento UEBA, playbooks SOAR e integraciones nativas con la infraestructura existente (XDR, NGFW, Navegador Seguro)	Documento de arquitectura de integración y matriz de configuraciones
Pruebas de Aceptación	Ejecución de PoC funcional que valide: (i) integración nativa sin conectores externos, (ii) cumplimiento de casos de uso obligatorios DLP/UEBA/SOAR, (iii) métricas de rendimiento acordadas	Informe de PoC con resultados cuantitativos y acta de aceptación
Puesta en Producción	Migración controlada desde entorno de pruebas a producción, con plan de rollback documentado y ventana de mantenimiento aprobada por la Entidad	Acta de puesta en producción y plan de continuidad operativa
Documentación Técnica	Manuales de administración, guías de operación para el personal técnico de la entidad, catálogo de playbooks, diagramas de flujo de datos y procedimientos de recuperación ante desastres	Repositorio documental en formato editable y en español

2. **Integración Nativa con Infraestructura Existente**
   El CONTRATISTA deberá garantizar que la solución ofertada cumpla con los siguientes criterios de integración, so pena de incumplimiento contractual:

   - Compartir el mismo data lake y motor de correlación con los componentes XDR, Secure Web Gateway y NGFW ya operativos en la Entidad.
   - Operar bajo una única consola de administración (single pane of glass) que permita gestionar políticas de DLP, UEBA y SOAR desde la misma interfaz utilizada para los componentes existentes.
   - Utilizar las mismas fuentes de inteligencia de amenazas y los mismos identificadores de usuario, dispositivo y red ya enrolados en la infraestructura vigente.
   - Intercambiar eventos, alertas y acciones de respuesta mediante API propietaria nativa del mismo ecosistema, sin necesidad de conectores SIEM intermedios, middleware de integración o replicación externa de datos.

3. **Documentación necesaria para iniciar la implementación**
   El CONTRATISTA deberá entregar, dentro de los **cinco (5) días hábiles** siguientes a la suscripción del acta de inicio, un documento técnico que especifique de manera exhaustiva:

Categoría	Información Requerida	Formato de Entrega

Sistema Operativo	Versiones soportadas, parches mínimos requeridos, compatibilidad con distribuciones Linux/Windows Server de la Entidad	Matriz de compatibilidad
Base de Datos (Si aplica)	Motor requerido (si aplica), versión, configuración de alta disponibilidad, esquema de almacenamiento estimado	Diagrama ER y especificaciones técnicas
Licenciamiento de Terceros (Si aplica)	Licencias de SO, BD, virtualización o middleware necesarias no incluidas en la oferta	Listado con costos estimados y proveedor recomendado
Hardware / Máquinas Virtuales (Si aplica)	Especificaciones de CPU, RAM, almacenamiento, IOPS, redundancia para cada componente de la solución	Tabla de dimensionamiento por escenario (mínimo, esperado, máximo)
Networking	Puertos requeridos, protocolos, reglas de firewall, configuración de load balancer, requisitos de latencia entre componentes	Diagrama de flujo de tráfico y matriz de puertos
Alta Disponibilidad (Si aplica)	Arquitectura propuesta para HA, RTO/RPO esperados, procedimientos de failover y recuperación	Documento de diseño de resiliencia
Escalabilidad (Si aplica)	Capacidad máxima de la configuración base, procedimiento para escalar horizontal/verticalmente, impacto en licenciamiento	Modelo de crecimiento y curva de costos

4. **Validación de Compatibilidad**

   Antes del inicio de la implementación en producción, el CONTRATISTA deberá realizar un análisis de compatibilidad con la infraestructura actual de la Entidad, entregando:

   - Informe de brechas técnicas (si las hubiera) y plan de mitigación.
   - Certificación escrita del fabricante al inicio del proyecto que avale la compatibilidad de la solución ofertada con los componentes XDR, NGFW y Navegador seguro ya desplegados.

5. **Cronograma a definir con el acta de inicio**

   El Contratista deberá presentar como entregables contractuales de cumplimiento obligatorio: un cronograma detallado que especifique recursos, tiempos de ejecución, hitos medibles, responsables, riesgos y plan de continuidad operativa; un documento de arquitectura de integración que describa el diseño técnico de la integración nativa, incluyendo diagramas de flujo de datos entre los seis componentes del ecosistema y el listado de APIs empleadas; y un informe final de implementación que contenga la documentación técnica completa, la línea base de métricas, las guías operativas y las lecciones aprendidas. Estos documentos se anexarán formalmente al contrato y cualquier retraso imputable al Contratista dará lugar a la aplicación de penalidades.

   Tiempos de entrega con la suscripción del acta de inicio siguientes a la suscripción del acta de inicio, plazo máximo del cronograma para despliegue y puesta en marcha, no mayor a **UN MES y medio o en su defecto 45 dias.**

6. **Soporte, Mantenimiento y Acompañamiento de la Solución**
   El CONTRATISTA deberá garantizar un esquema integral de soporte y mantenimiento para la solución ofertada, el cual incluirá los siguientes componentes:

a. Soporte del Fabricante

La solución deberá contar con soporte directo del fabricante durante toda la vigencia del servicio, el cual incluirá acceso telefónico y a través de portal en línea en modalidad 24x7. Este soporte deberá contemplar actualizaciones de software, parches de seguridad, inteligencia de amenazas, optimización de playbooks, revisiones de arquitectura y, cuando se requiera, servicios de configuración y afinamiento de la herramienta. Las métricas de cumplimiento asociadas estarán sujetas a las penalidades contractuales establecidas.

b. Servicio Soporte del fabricante

El soporte del fabricante deberá incluir un servicio orientado a maximizar la adopción de la tecnología y el fortalecimiento de la postura de seguridad de la organización, con asistencia y orientación continua. Este servicio tendrá como mínimo los siguientes alcances:

- Verificar el estado de los componentes de la solución.
- Proveer recomendaciones para la adopción de configuraciones alineadas con buenas prácticas.
- Realizar *workshops* y demostraciones sobre nuevas capacidades publicadas a lo largo del servicio.
- Asistir a la Entidad en el afinamiento de alertas e incidentes.
- Asistir a la Entidad en la optimización de los *playbooks* de automatización.
- Proveer *workshops* a la medida, acorde con los objetivos de la Entidad.

1.9 TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá garantizar la ejecución de actividades de transferencia de conocimiento dirigidas a los funcionarios de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC), conforme a las siguientes condiciones:

1. Transferencia de conocimiento: El contratista deberá realizar una transferencia de conocimiento dirigida a mínimo tres (3) funcionarios o contratistas designados por la Entidad coordinados por el supervisor del contrato, con el propósito de fortalecer sus capacidades para la operación, administración y monitoreo del servicio objeto del contrato.

   Esta actividad deberá cumplir con las siguientes condiciones:

   - Modalidad: Híbrida (Presencial o Virtual (sincrónica)).
   - Intensidad horaria: mínimo Cuarenta y ocho (48) horas.
   - Lugar de ejecución: Ciudad de Bogotá D.C. (Deberá coordinarse el horario y disponibilidad con el supervisor).
   - Periodo de ejecución: Durante el plazo de ejecución del contrato, conforme a cronograma previamente aprobado por el supervisor.

   El CONTRATISTA deberá abarcar los siguiente temas: enfoque en arquitectura, integración nativa, gestión de políticas y mantenimiento operativo, énfasis en investigación de incidentes DLP, correlación de anomalías UEBA, ejecución y personalización de playbooks SOAR, y uso de la consola unificada. La trasferencia de conocimiento deberá ser impartidas por instructores con certificaciones vigentes del fabricante y/o experiencia acreditada en las herramientas, .. Todos los materiales, presentaciones, guías de laboratorio y grabaciones quedarán en propiedad de la Entidad, en formato editable y en español, sin costo adicional.

1.10 CANTIDADES Y VIGENCIA DEL LICENCIAMIENTO Y BIENES REQUERIDOS

Las cantidades objeto de la presente contratación se determinan a partir del inventario de equipos de cómputo institucionales y de la planta de personal reportada por el área competente con corte del jueves 6 de agosto de 2026, correspondiente a doscientos setenta y tres (273) servidores públicos con equipo de cómputo asignado, más una proyección de ochenta y siete (87) usuarios adicionales para la vigencia 2026 derivada de las dinámicas del proceso de Talento Humano, para un total de trescientos sesenta (360)

usuarios, y un margen operativo de quince (15) licencias destinado a cuentas de servicio, equipos de contingencia y usuarios temporales, para un total de trescientas setenta y cinco (375) licencias por módulo.

Ítem	Descripción	Unidad de medida	Cantidad	Vigencia
1	Licencias módulo de Prevención de Pérdida de Datos (DLP), numeral 1.3	Licencia por usuario / endpoint	375	Doce (12) meses contados a partir de la activación
2	Licencias módulo de Análisis de Comportamiento de Usuarios y Entidades (UEBA), numeral 1.4	Licencia por usuario / entidad	375	Doce (12) meses contados a partir de la activación
3	Plataforma de Orquestación, Automatización y Respuesta (SOAR), numeral 1.5	Solución	1	Doce (12) meses contados a partir de la activación
4	Unidades de visualización digital de gran formato para el SOC, numeral 1.7	Unidad	4	Garantía de fabricante no inferior a doce (12) meses
5	Equipo de cómputo de soporte a la visualización de tableros, numeral 1.7	Unidad	1	Garantía de fabricante no inferior a doce (12) meses
6	Servicios de implementación, configuración, integración nativa y puesta en producción, numeral 1.8	Servicio integral	1	Conforme al cronograma del numeral 1.12
7	Transferencia de conocimiento, numeral 1.9	Horas	48	Dentro del plazo de ejecución del contrato
8	Soporte técnico, mantenimiento y acompañamiento, numeral 1.8	Servicio	1	Doce (12) meses contados a partir de la activación

Notas sobre las cantidades:
a. Las licencias de los módulos DLP y UEBA deberán corresponder al mismo ecosistema tecnológico y al mismo modelo de licenciamiento, conforme al literal e) del numeral 1.2 del presente Anexo.
b. La plataforma SOAR no podrá licenciarse ni limitarse por número de acciones, tareas, incidentes, indicadores o playbooks, conforme a las especificaciones del numeral 1.5.
c. Todo crecimiento de usuarios que se presente durante la vigencia del licenciamiento deberá poder absorberse bajo el mismo modelo de licenciamiento, sin multiplicar consolas ni celebrar contratos adicionales, conforme al literal e) del numeral 1.2.
d. El licenciamiento deberá quedar registrado a nombre de la CAJA DE RETIRO DE LAS FUERZAS MILITARES – CREMIL, y así constar en el certificado de licenciamiento exigido como entregable en el numeral 1.8.

1.11 PERFILES Y EXPERIENCIA DEL EQUIPO DE TRABAJO

El proponente deberá acreditar, como requisito habilitante, el siguiente equipo mínimo de trabajo. Los perfiles deberán mantenerse durante toda la ejecución del contrato; cualquier reemplazo requerirá aprobación previa del supervisor y la acreditación de condiciones iguales o superiores a las aquí exigidas.

Perfil	Cant.	Formación académica	Experiencia general	Experiencia específica
Perfil 1 — Líder de Proyecto	1	Título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software o Ingeniería de Telecomunicaciones. En cualquiera de las carreras acreditadas deberá contar con título de posgrado, según Núcleo Básico de Conocimiento (NBC) del SNIES, en Gerencia de Proyectos, Dirección y Gestión de Proyectos, Gerencia de Proyectos de Ingeniería, Seguridad de la Información o Gerencia de Proyectos de Teleinformática.	Mínimo ocho (8) años, contados a partir de la expedición de la tarjeta profesional o del título profesional, según corresponda.	Mínimo cuatro (4) años en roles de liderazgo, coordinación o gerencia de proyectos, contados a partir de la obtención del título profesional, en proyectos relacionados con sistemas de protección o seguridad informática, seguridad de la información o ciberseguridad.
Perfil 2 — Ingeniero de Seguridad	1	Título profesional en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Sistemas Informáticos, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de Telecomunicaciones o similares según NBC del SNIES. Deberá contar con título de posgrado, según NBC del SNIES, en gestión de proyectos, gestión de servicios de TI o afines.	Mínimo siete (7) años, contados a partir de la expedición de la tarjeta profesional o del título profesional, según corresponda.	Mínimo cinco (5) años como implementador de proyectos, CISO o analista de seguridad en empresas públicas o privadas.
Perfil 3 — Ingeniero de Servicios y Soporte	1	Título profesional en Ingeniería de Sistemas, Ingeniería de Sistemas Informáticos, Ingeniería Electrónica o Ingeniería de Telecomunicaciones. Deberá contar con título de posgrado, según NBC del SNIES, en Seguridad Informática o Ciberseguridad.	Mínimo tres (3) años en el sector TI, contados a partir de la obtención de la tarjeta profesional o del título profesional, según corresponda	Mínimo tres (3) años en cargos relacionados con análisis de seguridad de la información.

La dedicación del personal deberá ser conforme a los roles y responsabilidades dentro de su perfil. En esa medida, el contratista deberá garantizar durante la ejecución del contrato, el cumplimiento integral del objeto contractual, así como la atención oportuna a los requerimientos de los supervisores del contrato.

Notas generales que los proponentes deben tener en cuenta:

Nota 1	Cuando el personal propuesto acredite títulos académicos obtenidos en el exterior, estos deberán estar debidamente convalidados en Colombia cuando así lo exija la normatividad aplicable para el ejercicio profesional correspondiente. Para efectos de evaluación de la formación académica, el proponente deberá aportar copia del título, certificado, diploma o documento equivalente, acompañado de su respectiva traducción oficial al idioma español cuando se encuentre en otro idioma. La experiencia profesional o específica obtenida en el exterior será válida para el presente proceso, siempre que sea acreditada mediante certificaciones expedidas por la entidad contratante, empleador o beneficiario del servicio, en las cuales se indique como mínimo: nombre de la entidad o empresa, identificación o datos de contacto, objeto o descripción de las actividades realizadas, rol

	desempeñado, fecha de inicio, fecha de finalización, dedicación cuando aplique y firma o medio verificable de expedición. Las certificaciones expedidas en idioma diferente al español deberán presentarse con traducción oficial. CREMIL podrá solicitar aclaraciones, documentos complementarios o mecanismos de verificación cuando lo considere necesario, con el fin de validar la equivalencia, autenticidad, pertinencia y suficiencia de la formación o experiencia presentada.
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, solo con dicha aprobación operará el cambio sin necesidad de suscribir un contrato modificatorio.
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	En caso de resultar adjudicatario, deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato.
Nota 6	Que en caso de resultar adjudicatario 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 CREMIL, no adquiere ninguna relación civil o laboral con los trabajadores del contratista, sin embargo, en el pago de seguridad social se debe evidenciar el personal que hace parte del proyecto.
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
Nota 10	Debido a la naturaleza del objeto contractual y al tratamiento de información institucional y datos personales administrados por CREMIL, el contratista deberá garantizar que todo el personal asignado a la ejecución del contrato suscriba, previamente al inicio de sus actividades, el Acuerdo de Confidencialidad dispuesto por la Entidad. Ningún integrante del equipo de trabajo podrá acceder a ambientes tecnológicos, bases de datos, sistemas de información o información institucional sin haber suscrito dicho acuerdo. Esta obligación será igualmente exigible respecto del personal que sea incorporado o reemplazado durante la ejecución contractual

1.12 CONTROLES DE SEGURIDAD DE LA PLATAFORMA UNIFICADA DLP, UEBA Y SOAR

Con el fin de garantizar la operación segura, trazabilidad, integridad y administración de la plataforma unificada conformada por los módulos DLP, UEBA y SOAR, el contratista deberá implementar y dejar operativas las siguientes capacidades técnicas de seguridad:

- Autenticación multifactor (MFA) para perfiles administrativos.
- Control de acceso basado en roles (RBAC).

- Permitir la segregación de funciones entre administradores, operadores, analistas y auditores.
- Registro centralizado de auditoría para acciones administrativas y operativas.
- Trazabilidad de modificaciones y acciones automatizadas sobre políticas DLP, modelos UEBA, integraciones y playbooks SOAR.
- Cifrado de comunicaciones mediante TLS 1.2 o superior.
- Gestión segura de credenciales, tokens y llaves API utilizadas por las integraciones.
- Sincronización horaria mediante servicios NTP.
- Respaldo y recuperación de configuraciones críticas.
- Conservación e integridad de evidencias generadas en incidentes de seguridad.
- Trazabilidad de acciones automáticas ejecutadas por playbooks SOAR.
- Exportación de registros para actividades de auditoría e investigación forense.
- Protección de sesiones administrativas mediante controles de expiración y cierre de sesión.
- Gestión centralizada y correlacionada de eventos de seguridad en la consola unificada.

Atentamente,

Iván Gómez Maldonado.

Ing. IVÁN MAURICIO GÓMEZ MALDONADO
Coordinador Grupo de Infraestructura Tecnológica – Oficina TICS
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 TICS[	Iván Gómez Maldonado.
Apoyo a la estructuración técnica del proceso	ANDRES DAVID CARDOZO Contratista responsable de Seguridad Técnica de Oficina TIC	
NOMBRE Cargo	COMITÉ ECONÓMICO ESTRUCTURADOR	
NOMBRE Cargo	COMITÉ JURÍDICO ESTRUCTURADOR	

VoBo.

PD. 3-1-15. CAMILA ANDREA CABRERA RODRIGUEZ.
SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST).
GRUPO DE TALENTO HUMANO – SST.

PD. 3-1-15. NATALIA FLOR ARIZA
SISTEMA DE GESTIÓN AMBIENTAL
SUBDIRECCIÓN DE GESTIÓN DE ACTIVOS

PS. LORENA SUAREZ SIERRA
Oficial de seguridad de la Información CREMIL