MINISTERIO DE DEFENSA NACIONAL
CAJA DE RETIRO DE LAS FUERZAS MILITARES
ANEXO TECNICO

F-GRA-11/19-02-2021

ASPECTOS GENERALES

OBJETO:

CONTRATAR LA SUSCRIPCIÓN, IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN DE LICENCIAMIENTO DE SOFTWARE COMO SERVICIO (SAAS), DE UNA SOLUCIÓN DE UN NAVEGADOR SEGURO INCLUIDO SOPORTE TÉCNICO DEL FABRICANTE QUE PERMITA PROPORCIONAR ACCESO CONTROLADO A LAS APLICACIONES WEB, GARANTIZANDO LA PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN DE LA CAJA DE RETIRO DE LAS FUERZAS MILITARES.

1. ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

1. SERVICIO SSE	
ESPECIFICACION	**DETALLE**
Generalidades	La entidad requiere la implementación de una solución de Security Service Edge (SSE) bajo un modelo de servicio administrado en la nube. Este componente deberá garantizar la protección integral de las comunicaciones de los equipos institucionales frente a amenazas cibernéticas, asegurando simultáneamente el acceso remoto seguro tanto a la red local como a las aplicaciones críticas (SaaS y On-premise).
	La plataforma debe ser 100% nativa en nube del mismo fabricante de la solución ofertada, no se aceptarán tecnologías que necesiten instalar algún tipo de componente On-premise[1] para su funcionamiento y/o procesamiento.
	Con el fin de evitar brechas de seguridad por falta de visibilidad en los puntos finales, CREMIL requiere que la solución garantice una integración nativa con los sistemas operativos utilizados por sus funcionarios (Windows y macOS). Este requerimiento es esencial para materializar la política de Zero Trust, permitiendo que la entidad mantenga el control sobre la interacción con el dato misional, independientemente de la plataforma de hardware desde la cual se realice la consulta.
	Se requiere que la solución propuesta permita la integración con sistemas de autenticación robusta, soportando como mínimo el protocolo SAML 2.0 y conectividad directa con los servicios de gestión de identidades como Microsoft y Okta.
	Debe permitir crear roles de administración RBAC (Control de Acceso Basados en Roles).
	Debe proporcionar capacidad para integrarse con Active Directory y/o Azure AD, SAML, Kerberos, LDAP, RADIUS, TACACS+, MFA y Local Database
	Debe permitir crear políticas en función de Usuario de AD, Grupo de AD, IP de origen entre otros.
	La solución debe ser capaz de brindar acceso a aplicaciones internas sin necesidad de instalar máquinas virtuales en la red de destino como puente de acceso;
	La solución debe proporcionar redes remotas con rangos de direcciones exclusivos para el acceso a Internet por medio de los agentes de la solución propuesta, dejando solo las IP designadas para el fabricante de la solución SSE.

[1] *Una solución nativa en la nube garantiza alta disponibilidad (99.9%). El funcionario se conecta directamente a la nube del fabricante (navegador seguro), eliminando la dependencia de la infraestructura física de la entidad y garantizando que la operación no se detenga.*

	La solución debe estar optimizada para dar cumplimiento a los siguientes casos de uso: 1. Requisitos de acceso de ZTNA 2.0 2. Imponer una gobernanza[2] de datos y un cumplimiento estricto para las aplicaciones SaaS 3. Acceso seguro para dispositivos administrados y no administrados (BYOD) 4. Imponer políticas de acceso estrictas para aplicaciones privadas 5. Reducir los riesgos derivados de las vulnerabilidades de los complementos del navegador
Filtrado y categorización	La solución deberá poder soportar categorías filtrado web e idiomas y restringir acceso a contenido inapropiado.
	La solución deberá bloquear conexiones SSL no confiables, evaluando una serie de condiciones, considerando al menos en esta evaluación: SSL mal formadas, certificados root no fiables y host de SSL no coincidentes.
	La solución debe permitir la configuración de excepciones de direcciones IP/URL's exentas de análisis.
	El servicio propuesto deberá soportar la funcionalidad de Filtrado de Contenido sin necesidad de añadir hardware, procesadores ni memoria extra.
	La solución deberá contar con al menos 73+ categorías predefinidas. Así mismo, deberá contar con mecanismos de categorización en línea para sitios no conocidos.
	El servicio deberá soportar la funcionalidad de descifrado SSL.
	La solución de filtrado de contenido deberá incluir la capacidad de creación de políticas de filtrado con base en nombre de usuario o grupo de usuarios definidos en el directorio de la convocante.
	Deberá permitir configurar acciones como: ■ Permitir, el acceso a la página web. ■ Bloquear, el acceso a una página web ■ Continuar, cuando un usuario accede a una página que no cumpla con las políticas definidas, mostrando una página de advertencia y mostrando un botón para continuar. ■ Opción de override: para solicitarle al usuario una contraseña que le permita continuar navegando ■ Deberá bloquear el uso de aplicaciones tipo Proxy, ToR y Ultrasurf ■ Además de deberá permitir la funcionalidad de descifrado de SSL de acuerdo a la categoría del sitio visitado.
	Deberá contar con mecanismos de prevención de robo de credenciales en sitios de phishing e ilegítimos que intenten sustraer la información del usuario.

[2] La **Gobernanza de Datos** hace referencia a tener el control total sobre quién puede ver, mover o compartir la información de la entidad. Es decir, estas tecnologías son las que "leen" el contenido de lo que viaja hacia la nube y toman decisiones basadas en políticas de la entidad

	Configurar y mantener las políticas de control de acceso que sean aprobadas por la entidad para lo siguiente: ■ Filtrado de URLs a través de todas las categorías preconfiguradas y customizadas requeridas por la convocante. ■ Control de acceso a aplicaciones en la nube – mensajería instantánea, redes sociales y blogs , medios de streaming y compartición de archivos, webmail. ■ Control de tipo de archivos Ejecutables (.scr, .cpl, .dll, .ocx, .pif, .exe) , Java (.class, .jar), Archivos de ayuda (.chm, .hlp) y otros archivos potencialmente peligrosos .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat,Office (Word, Excel, PowerPoint)BZIP2, GZIP, ISO, RAR, Stuffit, TAR, ZIP, audio, Ejecutables (EXE), flash, .tar, codificación multi nivel, .cab, .msi, rar - cifrados y archivos zip cifrados. ■ Control de inspección de tráfico SSL. ■ Control de tráfico FTP. ■ Control de tráfico DNS para detectar y controlar exfiltración de contenido y/o exfiltración de data. ■ Control de aplicaciones indistintamente del puerto y protocolo utilizado.
	Configurar notificaciones de bloqueo, advertencia y de solicitud de revisión de políticas hacia usuarios finales que sean aprobadas por la entidad
	Realizar un monitoreo permanente sobre las actividades web de los usuarios, a través de las facilidades analíticas y de reporteo provistas por la plataforma de seguridad en la nube.
Control de Aplicaciones	Deberá incluir la capacidad de actualización para identificar nuevas aplicaciones, en cualquier puerto y protocolo.
	Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo.
	La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales.
	Deberá incluir herramientas gráficas que permitan tener la vista de aplicaciones que fluyen a través del servicio basado en nube.
Detección de Malware	La solución debe proporcionar capacidades de prevención de amenazas para todo el tráfico (todos los puertos/protocolos, web y no web, puertos no estándar, etc.) y todos los destinos (centro de datos, nube pública, SaaS, Internet), sin limitarse al tráfico web. (HTTP y HTTPS) únicamente.
	La solución debe proteger contra ataques en tiempo real.
	La solución debe tener un mecanismo para evitar la fuga de credenciales.
	La solución de SSE debe incluir Antivirus para detectar malware conocido.
	La solución de SSE debe incluir información sobre amenazas, URL maliciosas y hashes de archivos.
	La solución de SSE debe incluir machine learning automático para detectar amenazas desconocidas.
	La solución debe proteger ante amenazas que usen dominios que presenten comportamientos sospechosos o que sean parte de un ataque.
	Debe permitir la configuración de políticas de seguridad basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a las aplicaciones onpremise o nube o le otorgue acceso de mayores restricciones.
	Debe permitir aislar el dispositivo de la red y mantenerlo en cuarentena de forma dinámica, en caso se detecte alguna actividad maliciosa

	La solución debe proporcionar funciones de inspección del tráfico entrante y saliente para detectar malware desconocido o de tipo APT con filtrado de amenazas avanzado y análisis de ejecución en tiempo real;
Interfaz y Uso	La gestión de la solución deberá basarse en una plataforma WEB, con acceso a través de un navegador estándar del mercado, utilizando comunicación cifrada.
	La solución deberá tener la capacidad de utilizar cuentas de usuario del AD interno para la autenticación en la consola de administración, a través de la integración con Azure Active Directory;
	La solución debe permitir el uso de autenticación de doble factor (2FA o MFA) para acceder a la consola de administración de la solución.
	Poder visualizar, directamente en la solución, las aplicaciones más utilizadas, los usuarios que más utilizan estos recursos.
	Habilitar la generación de informes de amenazas con evaluación y gestión de riesgos e información detallada sobre el entorno, ayudando a identificar el tráfico de archivos maliciosos, entre otras amenazas.
	Deberá contar con un portal para validar el estado de los servicios con el objetivo de brindar transparencia sobre el cumplimiento del SLA.
	La disponibilidad del servicio debe estar garantizada por un acuerdo de nivel de servicio (SLA) de 99,999% para los servicios en línea.

2. Navegador seguro - Browser Corporativo	
ESPECIFICACIÓN	**DETALLE**
Generalidades	Debe estar diseñada para cubrir los siguientes casos de uso: 1. Proporcionar un espacio de trabajo seguro basado en navegador para proveedores externos, y colaboradores de la entidad. 2. Proporcionar un espacio de trabajo seguro para los funcionarios de la entidad cuando intenten usar características tipo VDI. 3. Proporcionar un espacio de trabajo seguro basado en navegador para BYOD y acceso a dispositivos no administrados.
	El Browser corporativo debe tener una función que permita a los usuarios acceder de forma segura a aplicaciones internas desde cualquier ubicación sin la necesidad de una solución VPN o VDI adicional, ofreciendo una alternativa optimizada y más segura en comparación con las soluciones VPN tradicionales.
	El navegador debe contar con una función que permita denegar el acceso a aplicaciones web según características o acciones del usuario, como la posición de seguridad del dispositivo, la hora, la dirección IP, la versión del sistema operativo y otras.
Integración simplificada	UX basada en Chromium, Interfaz compatible con extensiones nativas de Chrome.
	La solución no debe requerir privilegios de administrador para una instalación sencilla como Chrome.
	La solución deberá tener la capacidad de Importa marcadores, historial, extensiones y credenciales de otros navegadores.
	La solución deberá tener integración de SSO y sincronización de perfiles
	La solución deberá ser mínimo compatible con Windows 10,11, macOS 11,12,13,14, android 11 y superior, iOS 17 y superior
Entorno Seguro	La solución deberá poder aislar el espacio de trabajo del dispositivo, lo que permite a los usuarios trabajar de forma segura en puntos finales comprometidos.
	La solución deberá tener resistencia a la manipulación, reforzando la integridad del navegador con técnicas de fijación y endurecimiento de certificados.

	La solución deberá tener aislamiento contra amenazas de endpoints comprometidos, protegiendo contra eyloggers, screen scrapers y amenazas de red como MitM.
	La solución deberá tener controles de sesión, permitiendo el bloqueo automático de sesiones y la eliminación automática de datos al iniciar o en inactividad.
	La solución deberá tener comprobación de la postura del dispositivo, evaluar la seguridad de los endpoints mínimo cada 90 segundos y bloquear el acceso en caso de incumplimiento.
Protección web	La solución deberá tener prevención de malware basado en Sandboxing
	La solución deberá permitir a los administradores controlar el acceso a URL específicas, aplicaciones web o categorías de sitios web según las credenciales de inicio de sesión del usuario.
	La solución deberá tener defensa contra phishing utilizando filtrado avanzado de URL, aplicando el modo de solo lectura o aísla el acceso a sitios de alto riesgo.
	La solución deberá tener aislamiento del navegador para sitios no confiables; deshabilitando las funciones vulnerables del navegador para reducir la superficie de ataque.
	La solución deberá tener control de extensiones maliciosas bloqueando extensiones de riesgo según permisos, comportamiento y puntuaciones de riesgo.
	La solución deberá tener implementar búsquedas seguras de contenido en los principales motores de búsqueda.
Información de Seguridad	La solución deberá tener capacidad de auditoría y análisis Forense, recopilar datos de eventos enriquecidos y grabaciones completas de las sesiones de usuario. Así mismo, la integración con un SIEM es admitida como funcionalidad complementaria que refuerza, pero no sustituye, la capacidad de grabación forense.
	La solución deberá tener monitoreo de usuarios y dispositivos rastreando el comportamiento del usuario, el estado del dispositivo y el uso de las aplicaciones.
	La solución deberá tener descubrimiento de Shadow IT, detectando y monitoreando el uso de aplicaciones no autorizadas.
	La solución deberá tener visibilidad de extensiones informando sobre los niveles de riesgo, el origen y los permisos de las extensiones.
	La solución deberá poder generar la grabación completa de las acciones del usuario en las aplicaciones web antes y después del evento para investigaciones forenses y cumplimiento normativo.
Controles	La solución deberá tener controles granulares para permitir/denegar por acción, acceso web, inicio de sesión, descarga/subida, copiar/pegar, imprimir, captura de pantalla, escritura, enmascaramiento, marca de agua, uso de cámara/micrófono.
	El navegador deberá tener la función que permite mostrar una marca de agua semitransparente en la pantalla del navegador para evitar el robo de datos o la violación de derechos de autor al identificar los detalles de la sesión cuando los usuarios capturan o fotografían la pantalla.
	Los administradores deben poder usar la solución para evitar que los empleados accedan a sus cuentas personales en el trabajo. Por ejemplo, se podría impedir que los usuarios copien datos empresariales a una cuenta personal de almacenamiento en la nube (p. ej., permitir que el usuario acceda a Dropbox solo cuando use sus credenciales corporativas).
	El navegador debe tener una función que impida la descarga o carga de archivos. Esta protección es esencial cuando una aplicación web aloja datos confidenciales que podrían ser exfiltrados, intencional o involuntariamente.
	El navegador deberá tener una función que permita proteger contra ataques de phishing y robo de credenciales otorgando a los usuarios acceso de "solo lectura" a sitios web que no son confiables y evitando que ingresen sus credenciales.

	El navegador debe tener una función que permita habilitar o bloquear extensiones del navegador dentro de la sesión. Es fundamental permitir a los usuarios agregar extensiones seguras según sea necesario y bloquear las extensiones maliciosas conocidas.
	La solución debe bloquear el acceso si intentan iniciar sesión en Dropbox con sus credenciales personales.
	La solución deberá tener controles de archivo para aplica reglas por tamaño de archivo, tipo y hash.
	La solución deber ser compatible mínimo con los siguiente IdP: Microsoft Azure Active Directory, Okta, PingID OneLogin, Google Workspace.

3. IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN

a. Fase de Implementación:

- Configuración de Políticas: Creación de reglas de acceso, perfiles de filtrado web y políticas de prevención de fuga de datos (DLP).
- Despliegue de Agentes: Instalación del software en los endpoints (Windows).

b. Fase de Puesta en Operación:

- Acompañamiento: Soporte técnico presencial o remoto durante los primeros 30 días hábiles tras la salida a producción.

c. Pruebas de Funcionamiento

Para recibir el servicio a satisfacción, se deben incluir Pruebas de Aceptación de Usuario final, de acuerdo con los siguientes aspectos técnicos:

- Prueba de Conectividad: Verificar que el tráfico fluye por el túnel SSE sin latencia excesiva.
- Prueba de Seguridad: Intentar descargar un malware de prueba (tipo EICAR) y verificar que el Sandboxing lo bloquee.
- Prueba de Identidad: Validar que el inicio de sesión único (SSO) con Microsoft/Okta funcione correctamente.

La vigencia de las suscripciones y el soporte técnico deberá ser por 12 meses.

4. SOPORTE TÉCNICO 24x7

El contratista deberá garantizar la disponibilidad, actualización y asistencia técnica de la solución conforme a los siguientes parámetros:

1. Disponibilidad de la Plataforma (Uptime)

Dado que la operación misional de CREMIL depende del navegador, la plataforma en la nube deberá garantizar una disponibilidad mínima del 99.7% (*tiempo de actividad mensual*). Los mantenimientos programados deberán ser notificados con al menos 48 horas de antelación y realizados fuera de la jornada laboral institucional.

2. Tiempos de Respuesta y Solución:

a) Tiempo de Respuesta:

Es el compromiso de "reacción inicial". Se cuenta desde el momento en que se reporta un problema hasta que una persona especializado toma contacto, reconoce el fallo y comienza a trabajar en él.

b) Tiempo de Solución:

Es el tiempo total que transcurre desde que se reporta el incidente hasta que el problema queda completamente resuelto o se entrega una alternativa funcional que permita continuar trabajando.

Nivel de Severidad	Descripción	Tiempo de Respuesta	Tiempo de Solución
Crítico (S1)	Falla total que impide el acceso a las aplicaciones de CREMIL (Nómina, Prestaciones) a nivel general.	< 1 hora	< 4 horas
Alto (S2)	Vulnerabilidad de seguridad detectada (Zero-Day) o fallo en políticas de bloqueo de datos sensibles.	< 2 horas	< 8 horas
Medio (S3)	Fallas parciales que afectan a un grupo de funcionarios o problemas de lentitud no crítica.	< 4 horas	< 24 horas
Bajo (S4)	Consultas técnicas, cambios en configuración de políticas o dudas de administración.	< 8 horas	< 48 horas

Consideraciones acerca del Soporte Técnico:

- El soporte técnico especializado deberá incluir la actualización constante del motor del navegador (mantenimiento preventivo) y la asistencia en caso de incidentes (mantenimiento correctivo). El respaldo debe ser directo del fabricante (actualizaciones y escalamiento a tercer nivel) para garantizar la calidad del software, pero operado a través del contratista.

- En soluciones de ciberseguridad bajo modelo de suscripción, la licencia de uso y el soporte técnico constituyen componentes integrales e inseparables del servicio. La disponibilidad de la licencia sin el correspondiente soporte técnico limita la capacidad de respuesta ante incidentes o vulnerabilidades emergentes, como las de tipo “Zero Day”. En ausencia de soporte para la aplicación oportuna de parches, actualizaciones y acciones de mitigación, la herramienta pierde efectividad en el cumplimiento de su propósito de protección. En consecuencia, el servicio de soporte técnico debe garantizarse durante el mismo periodo de vigencia de la licencia, es decir, por los doce (12) meses correspondientes a la activación de la solución.

5. TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá garantizar la ejecución de actividades de transferencia de conocimiento y sensibilización 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 dos (2) funcionarios designados por la Entidad, 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: Virtual (sincrónica).
- Intensidad horaria: Veinte (20) horas.
- Lugar de ejecución: Ciudad de Bogotá D.C. (aunque se realice de manera virtual, deberá coordinarse el horario y disponibilidad).
- Periodo de ejecución: Durante el plazo de ejecución del contrato, conforme a cronograma previamente aprobado por el supervisor.

2. Sesión de sensibilización: El contratista deberá realizar una (1) sesión virtual de sensibilización dirigida a los funcionarios de la Entidad, orientada al fortalecimiento de la cultura de seguridad digital.

Esta actividad deberá cumplir con las siguientes condiciones:

- Modalidad: Virtual.
- Cantidad: Una (1) sesión.
- Duración mínima: Definida en coordinación con el supervisor (se recomienda mínimo 2 horas).
- Contenido mínimo:
  - Uso adecuado del navegador seguro.
  - Principios básicos de ciberseguridad.
  - Protección de datos personales y responsabilidad de los usuarios.
  - Riesgos comunes (phishing, malware, accesos no autorizados, entre otros).
  - Recomendaciones prácticas para el manejo seguro de la información.

Atentamente,



Coronel (R) JAVIER ORLANDO MEDRANO CORTES
Jefe Oficina TICS

Revisó:

Iván Gómez Maldonado.

PD IVÁN MAURICIO GÓMEZ MALDONADO
Profesional de Defensa Oficina TICS