



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



F-GRA-11/19-02-2021

ASPECTOS GENERALES

OBJETO:

CONTRATAR ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA SOLUCIÓN DE PROTECCIÓN DE CORREO ELECTRÓNICO, CON EL FIN DE GARANTIZAR LA SEGURIDAD DE LOS CANALES DE COMUNICACIÓN DE LA CAJA DE RETIRO DE LAS FUERZAS MILITARES

1. CARACTERÍSTICAS TÉCNICAS

CREMIL requiere adquirir, instalar, configurar y poner en operación una solución de protección avanzada de correo electrónico para la plataforma Microsoft Office 365, que permita prevenir, detectar y mitigar amenazas como spam, phishing, malware, ransomware, suplantación de identidad y fuga de información, garantizando la seguridad y continuidad de la comunicación institucional.

Por los motivos mencionados, es necesario:

- **Adquirir, instalar y configurar una solución de protección de correo electrónico:** Permitirá fortalecer los mecanismos de seguridad de la plataforma institucional, garantizando la detección, prevención, mitigación y gestión de amenazas asociadas al uso del correo electrónico corporativo.

La solución debe integrar capacidades avanzadas de filtrado de spam, bloqueo de malware, análisis de adjuntos y enlaces en tiempo real, protección contra suplantación de identidad (phishing, spoofing), y herramientas de prevención de fuga de información (DLP), para lo cual se requiere lo siguiente:

ÍTEM	DESCRIPCIÓN	CANTIDAD
1	Adquirir, instalar y configurar una solución de protección de correo electrónico	400

2. ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA SOLUCIÓN DE PROTECCIÓN DE CORREO ELECTRÓNICO

La solución debe proveer la seguridad del sitio de trabajo a través de protección del correo electrónico que incluya protección contra phishing, ransomware, ataques de día cero y apropiaciones de cuentas en una sola consola.

Fabricante	Indicar
Modelo	Indicar
Cantidad usuarios:	400
Protección de correo electrónico.	



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



F-GRA-11/19-02-2021

Escaneo de correo electrónico	La solución debe analizar dinámicamente el 100% de los correos electrónicos
	La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
	La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos
	El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
	La solución debe proteger activamente contra el spam
	La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente
Identificación de amenazas	La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas.
	La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos.
	La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus.
Amenazas avanzadas	La solución debe utilizar herramientas para identificar firmas muy complejas
	La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
	La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
	La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
	La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU
Manejo de URL	La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario en Microsoft 365
	La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final
Sandbox	La solución debe contar con la tecnología Sandbox para identificar archivos maliciosos
	La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos
	La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos
	La solución debe identificar vulnerabilidades de daño en la memoria
	La solución debe detectar errores lógicos y macros dentro de los documentos



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



F-GRA-11/19-02-2021

Gestión de archivos	La solución debe escanear cientos de tipos de archivos diferentes
	La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
	La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad
	La solución debe analizar contenido protegido con contraseña al entregarse el password
	La solución debe analizar archivos comprimidos/comprimidos
Situación del mercado	La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico
	La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.
Uso	
Servicio alojado en la nube	La solución debe ser nativa de la nube y está totalmente alojada en la nube
	La solución debe actualizarse automáticamente
	La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales
Instalación	La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales
	La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en Microsoft office 365 como mínimo
	La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico
	La solución debe ser implementada automáticamente con la integración de Microsoft Office 365
integración	La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones
	La solución debe integrarse con Microsoft Office 365 a través de API sin necesidad de cambiar el registro MX.
	La solución debe poderse ajustar a las políticas y SIEM existentes y no requiere cambios en la infraestructura e integración vía REST APIs
	La solución debe estar en capacidad de exportar registros en tiempo real al correo electrónico del administrador de la solución o a un SIEM
	La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML
	Los usuarios se deben asignar automáticamente permisos a roles y grupos en función de un esquema RBAC



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



F-GRA-11/19-02-2021

	La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador
Gestión de datos	La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
	Las claves de cifrado deben estar protegidas con soluciones como AWS KMS
	La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001
	La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio
gestión	La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
	la solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.
	La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación
	El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugués
	La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto
	La solución debe enviar informes y resúmenes de acciones a los usuarios
Servicio.	
Respuesta a incidentes	La solución debe contar con un equipo interno de Incident&Response (IR) para reforzar los servicios de detección y corrección de los correos
	La solución debe proporcionar servicios complementarios de equipos Incident&Response (IR) como parte de la oferta sin cargo adicional
Soporte al cliente	La solución debe ofrecer soporte al cliente y capacitación ilimitados según sea necesario sin cargo adicional durante la duración del contrato
	El servicio de atención al cliente debe estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
Certificaciones	El oferente deberá garantizar que sus servicios basados en infraestructura en la nube cuenten con procedimientos formalmente establecidos, documentados y operativos para la gestión segura de la información en entornos cloud. Para ello, el oferente deberá contar con certificación vigente en una norma internacional que establezca buenas prácticas de



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



F-GRA-11/19-02-2021

	<p>seguridad aplicables a servicios en la nube, incluyendo aspectos como la protección de datos, la responsabilidad compartida entre proveedor y cliente, el control de accesos, la segregación lógica de entornos y el monitoreo de recursos virtualizados.</p> <p>Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de servicios en la nube, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.</p> <p>La incorporación de este requisito busca asegurar que los oferentes cuenten con las competencias y avales internacionales necesarios para garantizar la seguridad, continuidad y confiabilidad de los servicios prestados en la nube, en coherencia con las políticas de seguridad de la información aplicables al sector público.</p>
Garantía	1 año a partir de la activación de la solución

TRANSFERENCIA DE CONOCIMIENTO	
1	El Contratista deberá efectuar la transferencia de conocimiento de la solución de protección de correo electrónico a dos (2) funcionarios del Grupo de TI, con una intensidad de veinte (20) horas, modalidad virtual, durante el periodo de ejecución contractual.

INSTALAR Y CONFIGURAR LA SOLUCIÓN DE PROTECCIÓN DE CORREO ELECTRÓNICO	
1	El Contratista deberá garantizar la instalación y configuración con el siguiente perfil descrito a continuación:

PERFIL	FORMACIÓN	EXPERIENCIA PROFESIONAL
Un (1) Ingeniero certificado	<p>Ingeniero de sistemas o electrónico o telecomunicaciones</p> <p>Certificación vigente: Technical Specialist y/o una certificación equivalente</p>	<p>Acreditar experiencia profesional con mínimo dos (2) años en proyectos de soluciones de protección de correo electrónico ejecutados cuyas actividades sean relacionadas con el objeto del presente proceso.</p>



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



F-GRA-11/19-02-2021

Garantizar el soporte técnico a CREMIL (presencial o virtual), durante el tiempo que dure el licenciamiento contratado por un (1) año.

NOTA: Una vez suscrita el acta de inicio el contratista deberá allegar al supervisor del contrato la Hoja de vida del profesional asignado para la instalación de la solución y la transferencia del conocimiento.

Atentamente,

Coronel (R) JAVIER ORLANDO MEDRANO CORTES
Coordinadora Grupo Informática

Revisó:

PD JAVIER MAURICIO ESPONISA MONTUANO
Profesional de Defensa