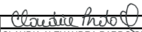


 Función Pública Función Pública DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA - DAFP OFICINA DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES			
Objeto: Adquirir, instalar, configurar, implementar y soportar una solución integral de ciberseguridad compuesta por: (i) un Firewall de Nueva Generación (NGFW) con prevención avanzada de amenazas, sandboxing y acceso remoto seguro; (ii) una solución de protección de correo electrónico y plataformas de colaboración en la nube; y (iii) una plataforma de gestión centralizada de seguridad en la nube; para fortalecer la seguridad perimetral y la protección de los sistemas de información y usuarios del Departamento Administrativo de la Función Pública. Códigos UNSPSC: 43222500,43232800,43233200,43201500,81111800			
Fecha:		[Empresa coligante: _____]	
ESPECIFICACIONES TÉCNICAS			
ITEM	CARACTERÍSTICAS	CUMPLE	NO CUMPLE
DESCRIPCIÓN			
1. ESPECIFICACIONES TÉCNICAS FIREWALL			
1	Adquisición de una solución de protección de red con características de Next Generation Firewall y Prevención avanzada de amenazas para la seguridad de la información de Departamento Administrativo de la Función Pública – DAFP.	X	
2	Los componentes objeto de la solución a ofertar deben ser interoperables entre sí y compatibles con la infraestructura existente. Podrán provenir del mismo fabricante o de fabricantes distintos que cuenten con integración nativa demostrable o equivalente cien por ciento funcional, garantizando soporte unificado por parte del oferente.	X	
3	La solución debe ofertar servicios de soporte, licencias por un periodo de 1 año.	X	
4	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el sitio del fabricante en listas de end-of-life y end-of-sale.	X	
5	La solución ofertada debe incluir todos los componentes o elementos necesarios para: el montaje, instalación, energización, conexión de red, etc., para la puesta en operación de todas las funcionalidades que brindan los equipos ofertados según las buenas prácticas del fabricante.	X	
6	Se deberá incluir los módulos de fibra, patch cords de fibra y cobre necesarios para la conectividad de cada una de las soluciones requeridas por la institución.	X	
7	Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, sistemas de prevención de intrusiones, identificación de usuarios y control granular de permisos.	X	
8	Por funcionalidades de Prevención avanzada de amenazas se entiende: protección de malware conocido (antivirus), prevención de comando y control (Anti-Bot), protección anti-phishing avanzada, seguridad DNS y prevención de malware de día cero con Sandboxing.	X	
9	Todos los equipamientos ofertados deben ser adecuados para montaje en rack 19".	X	
10	Para fines de tener un mejor control sobre los cambios en la política de seguridad la solución debe soportar la instalación o control de las políticas de control de acceso (Firewall, VPN, Control de aplicaciones y URL filtering) de manera independiente de las políticas de prevención de amenazas (Anti-Virus, Anti-Bot, Sandboxing, extracción de amenazas (CDR)).	X	
11	El fabricante de la solución debe contar con evaluaciones independientes de eficacia de seguridad realizadas por laboratorios reconocidos del sector, con resultados publicados en los últimos 2 años que certifiquen la solución como recomendada. No se aceptarán soluciones con categorización de precaución. No se aceptarán cartas o documentos no públicos como soporte.	X	
	La plataforma de seguridad debe contar con evaluaciones de eficiencia de seguridad y experiencia de usuario realizadas por laboratorios de pruebas independientes reconocidos del sector, con resultados publicados en los últimos 2 años que demuestren desempeño igual o superior a la media del sector.	X	
12	La plataforma de seguridad debe contar con evaluaciones independientes de eficacia en entornos de firewall híbrido o perimetral, realizadas por laboratorios reconocidos del sector, con resultados publicados en los últimos 2 años que la posicionen como solución destacada o líder en eficacia de seguridad real.	X	
13	La solución de cluster debe soportar una configuración de cluster utilizando un único objeto de administración que automáticamente sincronice las configuraciones y software a todos los miembros del cluster.	X	
14	La configuración de clusterización debe ser escalable en arquitectura que permita añadir hardware on-the-fly logrando que la configuración y los paquetes de software se denoren automáticamente del único objeto de administración.	X	
2. CARACTERÍSTICAS DEL HARDWARE Y REDIMIENTO DE LA SOLUCIÓN			
1	La plataforma de seguridad debe poseer las capacidades y características siguientes:	X	
2	Throughput Enterprise de Next Generation Firewall 20 Gbps con todas las siguientes funcionalidades habilitadas simultáneamente (Firewall, Application Control e IPS).	X	
3	Throughput Enterprise de Prevención Avanzada de Amenazas 7 Gbps con todas las siguientes funcionalidades habilitadas simultáneamente (Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, protección anti-phishing, Seguridad DNS y Sandboxing).	X	
4	TLS Inspection para la totalidad del tráfico saliente y entrante de Internet con IPS habilitado, con un rendimiento mínimo de 1.5 Gbps, documentado en la hoja técnica oficial pública del fabricante. No se aceptarán cartas o documentos no públicos.	X	
6	Soporte a, como mínimo, 7.2M conexiones de conexiones simultáneas.	X	
7	Soporte a, como mínimo, 195.000 conexiones por segundo.	X	
8	Tasa de rendimiento de VPN IPSec de al menos 23 Gbps.	X	
9	Fuente 100(240) AC o DC, redundante.	X	
10	mínimo 480 GB NVMe SSD M.2	X	
11	mínimo 16 interfaces de red 1 GbE Cobre RJ-45	X	
13	2x interfaces de red 2.5 GbE Cobre RJ-45	X	
14	8x interfaces de red 1 GbE SFP	X	
15	4x interfaces de red 10 GbE	X	
16	Soporte Modo Activo/Activo	X	
3. REQUERIMIENTOS DEL SOFTWARE DE LA SOLUCIÓN			
1	Firewall	X	
2	Geo-localización y objetos dinámicos actualizables	X	
3	Funcionalidades de red	X	
4	Funcionalidades de geo	X	
5	Https inspection	X	
6	Ssh inspection	X	
7	Identificación de usuarios	X	
8	Control o filtro de datos	X	
9	Vpn site-to-site	X	
10	Vpn client-to-site de tipo ipsec y ssl	X	
11	Control de aplicaciones	X	
12	Filtrado de url	X	
13	Sistema de prevención de intrusiones (IPS)	X	
14	Análisis de malware (antivirus y antibot)	X	
15	Análisis de malware modernos – sandboxing (zero day)	X	
16	Protección anti-phishing avanzada	X	
17	Disa security	X	
18	Content Disarm and Reconstruction (CDR)	X	
1	El Firewall debe soportar el control de políticas por zonas, puertos o servicios, direcciones IP, segmentos y/o rangos de red, país y/o región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos URL y/o aplicaciones, categorías de aplicaciones y URL, tipo de datos.	X	
2	La solución de Firewall debe implementar una arquitectura de procesamiento que garantice el aislamiento entre el plano de datos y el plano de control, con el fin de incrementar la estabilidad y seguridad operativa, o equivalente funcional.	X	
3	Soportar objetos para Reglas IPv6.	X	
4	Soportar objetos para Reglas multicast.	X	
5	Soportar objetos para NAT.	X	
6	Soportar HI count para reglas NAT.	X	
7	Soportar objetos para Vpn.	X	
8	Soportar habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	X	
9	Soportar objetos con Etiquetas para ser identificados o agrupados según la etiqueta.	X	
10	Debe tener la opción de negar los objetos de origen o destino, es decir que para una regla dada permite todas las conexiones de origen/destino excepto la especificada en la regla.	X	
11	Soportar enviar logs para sistemas de monitoreo externos, simultáneamente.	X	
12	Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y TLS.	X	
13	Debe permitir configurar certificados en caso necesario para autenticación del sistema de monitoreo externo de logs.	X	
14	Soporte configuración de alta disponibilidad Activo/Pasivo o Activo/Activo. En modo transparente (Bridge/L2) en Capa 3 (L3).	X	
15	Las funcionalidades de Firewall, VPN, QoS, NATs, Identificación de usuarios, Geo-localización, deben de estar embebido en el sistema operativo de manera permanente sin necesidad de una licencia que active las mismas.	X	
16	Protección contra flujos de alto ancho de banda y larga duración (large flows); debe detectar conexiones intensivas y reasignar automáticamente más núcleos de CPU para su procesamiento, sin impactar el rendimiento del resto del tráfico.	X	
17	Aceleración de flujos de alto volumen sobre protocolos SMB/CIFS y QUIC (RFC 9000), con capacidad de inspección de seguridad sobre tráfico QUIC/UDP.	X	
18	Debe contar con una vista consolidada en CLI de todas las conexiones que están atravesando el Firewall.	X	
1	La solución debe soportar VPNs IPsec Site-to-Site.	X	
2	La solución de VPNs IPsec debe soportar: Algoritmo Internet Key Exchange (IKEv1 & IKEv2).	X	
3	La solución debe soportar descripción con AES-128, AES-256 (Advanced Encryption Standard), 3DES.	X	
4	La solución debe soportar integridad de los datos con MD5, SHA-1, SHA-256.	X	
5	Soportar Diffie-Hellman Group 1, Group 2, Group 5 y Group 14.	X	
6	La VPN deben soportar autenticación vía certificado IKE con PKI (Public Key Infrastructure).	X	
7	La VPN debe poseer interoperabilidad con terceros fabricantes.	X	
8	La VPN debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los límites VPN.	X	
9	Debe soportar redundancia con configuración de múltiples puntos de entrada usando Dead Peer Detection (DPD) con los peers de terceros.	X	
10	Soportar la configuración de cifrados múltiples para Gateways externos en una única comunidad de VPN. Usar métodos de encriptación granular entre 2 peers específicos.	X	
11	Soporte para VPN de alta escala (Large Scale VPN), permitiendo la conexión automática de peers dentro de la comunidad VPN sin requerir configuración individual ni aplicación de políticas por cada peer.	X	

	VPN SITE-TO-SITE	Soportar como mínimo el protocolo IKEv2/IPsec conforme al estándar FIPS 203 del NIST, para la implementación de criptografía post-clásica (PQC) en las negociaciones de VPN site-to-site (fases IKE).	X
13		Detectar automáticamente cambios en la configuración de las nubes públicas AWS, Azure y GCP, ajustando los parámetros de VPN para garantizar la estabilidad de la conexión.	X
14		Proveer una herramienta avanzada de monitoreo de VPN que muestre información detallada sobre cada túnel VPN, incluyendo métricas de salud y rendimiento.	X
15		Permitir selección de enlace mejorada con capacidades de interoperabilidad, redundancia y granularidad.	X
16		Utilizar direcciones IP públicas como identificadores de túnel para establecer túneles separados por cada enlace.	X
17		Implementar Dead Peer Detection (DPD) como protocolo estándar de sondas de enlaces, en lugar de protocolos propietarios del fabricante, garantizando la interoperabilidad con equipos de terceros.	X
18		Habilitar redundancia para líneas VPN, incluyendo compatibilidad con peers VPN de terceros o ruidos de la nube.	X
19		Configurar un Security Gateway para utilizar diferentes interfaces VPN en distintas comunidades VPN, proporcionando mayor flexibilidad y control.	X
20		El fabricante de la solución debe soportar como mínimo el algoritmo Mc-KEM (Kyber/768) conforme al estándar FIPS 203 del NIST, para la fase 1 y la fase 2 de la negociación IKEv2 y VPN site-to-site.	X
1		La solución debe prevenir sobre el tráfico la transferencia de archivos maliciosos	X
2		Permitir el bloqueo de virus, por lo menos de los siguientes protocolos: HTTP, HTTPS, FTP, SMB/CIFS, SMTP.	X
3		Debe soportar la inspección de malware en protocolos SMB/CIFS incluyendo versión 2 y versión 3.	X
4		Soportar inspección o prevención de archivos por tipo de archivos, para al menos 70 (setenta) tipos de archivos.	X
5	ANÁLISIS DE MALWARE (ANTI-VIRUS, ANTI-BOT)	Permitir la inspección en archivos comprimidos (ZIP, RAR, etc.).	X
6		La solución debe tener la capacidad de detectar y prevenir comunicaciones de comando y control (C&C) de bots informáticos.	X
7		Permitir el detectar y prevenir comunicaciones de comando y control (anti-bot), basado en dominios, URL, dirección IP que sean maliciosas.	X
8		Búsqueda patrones de tráfico C&C, no solo en su destino DNS.	X
9		Los eventos deben identificar el país de donde originó la amenaza.	X
10		Debe soportar la captura de paquetes (PCAP) para virus y bot / capturar información para un análisis forense.	X
11		Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques considerando usuarios, grupos de usuarios, origen, destino, zona de seguridad, etc.	X
1		La solución debe poseer la capacidad de análisis de amenazas y prevención de malware no conocido, mediante emulación de archivos (sandboxing), antes de que firmas de protección estáticas sean creadas.	X
2		El dispositivo de seguridad debe ser capaz de enviar archivos para análisis de forma automática a la Nube del fabricante, donde el archivo será ejecutado y emulado en un ambiente controlado (sandboxing).	X
3		Seleccionar a través de la política que tipos de archivos se enviarán a este análisis.	X
4		Soportar el análisis como por lo menos 50 tipos de comportamientos maliciosos para el análisis de la amenaza no conocida.	X
5		Soportar el análisis de archivos en el ambiente controlado (sandboxing) del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos Java (.jar), archivos ejecutables, DLLs, ZIP y HTSPS.	X
6		Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7, Windows 8.1 y Windows 10 y Windows 11.	X
7		Debe soportar sandboxing de archivos de al menos 10 MB para todos los archivos reportados y la capacidad de incrementalmente al menos hasta 100MB.	X
8		Debe soportar el análisis de archivos transferidos por internet (HTTP, FTP, HTTPS, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB/CIFS.	X
9		El motor de sandboxing debe analizar, cambios en el Sistema de archivos, cambios en el registro, conexiones de red y procesos del sistema y proveer informaciones sobre el usuario infectado.	X
10		Debe ofrecer prevención en tiempo real para el paciente cero en malware desconocido para la navegación web, es decir, debe estar en capacidad de detener el archivo y analizarlo antes de entregarlo. De modo que pueda bloquear un malware de día cero incluso si es la primera vez que se detecta.	X
11	ANÁLISIS DE MALWARES MODERNOS - SANDBOXING (ZERO DAY)	Debe ofrecer prevención en tiempo real para paciente cero en malware desconocido en correo electrónico SMTP, de modo que pueda bloquear un malware de día cero incluso si es la primera vez que se recibe vía correo electrónico.	X
12		La solución debe soportar la implementación en modo MTA para correo electrónico.	X
13		La solución de sandboxing debe estar en capacidad de detectar ROP y otras técnicas de explotación mediante el monitoreo de los flujos del CPU.	X
14		Permitir el envío de archivos para análisis en el ambiente controlado (sandboxing) via web o de forma automática via API.	X
15		Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.	X
16		Debe generar reportes detallados de la emulación que incluyan como mínimo detalles de la actividad anterior, capturas de pantalla y grabaciones de video del comportamiento del archivo emulado, mostrando la ejecución real en el entorno de sandboxing.	X
17		Debe permitir la descarga de los malware identificados.	X
18		El reporte debe permitir visualizar los resultados de los análisis de malware de día zero en los diferentes sistemas operacionales soportados.	X
19		Debe permitir reportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración y a terceros, SIEM.	X
20		Debe entregar reportes forenses de la emulación en formato del MITRE ATT&CK que incluya la matriz con las tácticas y técnicas adversarias detectadas para cada archivo que se considere malicioso.	X
21		Soporte para la inspección de tráfico HTTP/S sobre transporte QUIC/UDP (RFC 9000 y RFC 9114), incluyendo como mínimo capacidades de prevención de amenazas y sandboxing sobre este protocolo.	X
22		Inspecciona el comportamiento a lo largo del tiempo con IA y algoritmos de procesamiento de señales para detectar actividad maliciosa, previniendo C2 (Comando y Control) de día cero, campañas de zero day/shifting y otras amenazas avanzadas.	X
1		La solución debe incluir mecanismos de filtrado y extracción de amenazas sobre documentos, de modo que los documentos de Microsoft Office y PDFs puedan ser reconstruidos en el mismo dispositivo de seguridad, eliminando así cualquier malware en estos.	X
2		Debe estar en capacidad de reconstruir los archivos sólo con los elementos benignos conocidos.	X
3		Debe soportar al menos documentos Microsoft Office 2013 o superior y PDFs.	X
4		Debe soportar remover contenido malicioso de distintas partes de un documento, como mínimo: macros, objetos y archivos embebidos, y accesos URL (links) a sitios externos.	X
5		Debe poder entregar documentos libres de malware.	X
6		Debe permitir configurar una política que convierta los documentos reconstruidos a PDF para mayor seguridad.	X
7	COR - LIMPIEZA DE DOCUMENTOS	A pesar de la conversión, debe permitir mecanismos para acceder al archivo original en caso de ser necesario.	X
8		Se debe operar sin interferir con otros recursos ya sea en memoria o almacenamiento o incluso que se lean sea realicen en paralelo y solo se le permita acceso al usuario al archivo original (si así lo solicita) si no fue encontrado como malicioso por la emulación de documentos.	X
9		Debe permitir configuración de seleccionar a cuáles partes del documento se le debe aplicar la política de extracción de amenazas.	X
10		Debe soportar documentos con lenguaje latín.	X
11		Debe soportar ser configurado como gateway MTA (mail transfer agent) para la protección del correo electrónico.	X
12		La solución de extracción de amenazas o COR debe ser capaz además opciones de extraer las amenazas y convertir a PDF los siguientes tipos de archivos pdf, .xlsx, .docx, .pptx, .doc, .ppt, .xls, .pptm, .xlsm, .pptm, .docm, .dotm, .dot, .dotxm, .dotl, .dtd, .psd, .tif, .tiff, .tif, .tiff, .png, .bmp.	X
13		La solución de extracción de amenazas debe ser capaz de convertir a PDF los siguientes tipos de archivos: .mp3, .flc, .dls, .eps, .pdf, .tss, .psd, .tif, .tiff, .png, .bmp.	X
4. CONSOLA DE ADMINISTRACIÓN Y MONITOREO, LOGS, REPORTES			
1		La solución debe centralizar la administración de gateways de seguridad, políticas, y objetos usando una única interfaz de administración.	X
2		La solución debe soportar la gestión de al menos 01 gateway de seguridad red requeridos por la organización.	X
3		La Consola debe permitir administración basada en roles. Debe permitir roles granulares para: acceso de escritura, acceso de lectura, creación de usuarios, delimitar las funciones de configuraciones.	X
4		La administración de la consola de la solución debe soportar acceso por un cliente GUI o via Web, via SSH y API abierta.	X
5		Debe permitir el acceso de administradores concurrentes; que trabaje en la vez sobre la misma política sin que el trabajo del uno interfiera en el otro.	X
6		La solución deberá ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.	X
7		Debe permitir la autenticación integrada con servidor Radius/TACACS.	X
8		Debe permitir autenticación de los administradores con proveedor de identidad SAML 2.0.	X
9		Permitir enviar los cambios en políticas dentro de un flujo de autorización y reclutamiento antes de aplicación.	X
10		La solución debe incluir un canal de comunicaciones seguro cifrado entre todos los componentes.	X
11		La plataforma de seguridad debe permitir realizar tareas de gestión a través del API.	X
12	MONITOREO CENTRAL, MONITOREO Y GESTION LAS POLITICAS DE SEGURIDAD	La solución debe incluir una CA \$500 interno (Autoridad de certificación) que pueda generar certificados para las puertas de enlace y los usuarios para permitia una autenticación feroz.	X
13		La solución debe incluir la capacidad de utilizar CA externas, que sea compatible con las normas PKCS #12, CAP, o Entrust.	X
14		La solución debe reportar alta disponibilidad de administración, utilizando un servidor de administración en espera que se sincroniza automáticamente con el activo.	X
15		La solución debe incluir la capacidad de administrar centralmente las acciones de todos los dispositivos de seguridad.	X
16		La solución debe incluir la capacidad de distribuir de forma centralizada y aplicar las acciones, versiones de software via parches en los dispositivos de seguridad, red.	X
17		La administración de la solución debe proporcionar un conjunto de estadísticas históricas y en tiempo real de los gateways y el tráfico que pasa por los gateways de seguridad: como CPU, Memoria, Disco, Throughput, Conexiones Conocidas, Conexiones por Segundo.	X
18		Debe posibilitar la integración con soluciones de SIEM del mercado.	X
19		La solución de Administración debe ofrecer como un servicio en la nube (Cloud), permitiendo la gestión centralizada de la seguridad desde una plataforma cloud, sin necesidad de infraestructura física o virtual ubicada en el centro de datos del Departamento Administrativo de la Función Pública – DAEP.	X
20		La solución debe ofrecer unificar operaciones, esto es en una regla incluyendo usuarios, direcciones IP, aplicaciones, tipos de datos.	X
21		La solución debe poder conectar dispositivos IPv4 e IPv6 en una misma regla.	X

22		La solución debe incluir la capacidad de administrar centralmente las licencias de todos los gateways de seguridad, incluyendo Firewalls virtualizados Datacenter, Firewall AWS y Firewall Azure	X	
23		Debe permitir instalar paquetes de parches sin conexión a Internet y distribuirlos de forma centralizada	X	
24		La solución debe contar con la opción de revisar y aprobar los cambios de configuración realizados por otros administradores antes de publicarlos o instalarlos	X	
1	GESTIÓN DE IDENTIDADES DE USUARIOS Y DISPOSITIVOS CENTRALIZADOS	La consola debe permitir integrar de manera fluida con proveedores de identidad externos para recopilar datos de usuario y dispositivo durante el inicio de sesión	X	
2		Obtener la información sobre todas las identidades de sesión, su origen de proveedor de identidad (IDP) y una lista de dispositivos donde cada identidad ha iniciado sesión	X	
3		Validación granular de usuarios para la implementación de Zero Trust en entornos locales, nube y endpoints	X	
1	VALIDACIÓN CONTINUA DE POLÍTICAS AUTOMATIZADA	La solución/consola de administración debe cumplir con los siguientes requisitos:	X	
2		Visibilidad de las políticas en diferentes segmentos de red, con información detallada por unidad de negocio, población de usuarios y ubicación	X	
3		Recibir advertencias preventivas sobre violaciones que están a punto de ocurrir con cualquier cambio de política	X	
4		Garantizar que las políticas estén alineadas de manera constante con las reglas de seguridad de la organización	X	
5		Eliminar accesos excesivamente permisivos, políticas superpuestas o en conflicto, y vulnerabilidades	X	
6		Obtener información continua sobre todas las políticas con recomendaciones para una limpieza eficiente	X	
7		Aprovechar alertas accionables sobre reglas u objetos sin coincidencia, con sugerencias para ajustar reglas y reemplazar políticas no utilizadas	X	
1	PREVENCIÓN DE AMENAZAS COLABORATIVA	La solución o consola de administración debe cumplir con los siguientes requisitos:	X	
2		Proveer contención y prevención automática mediante flujos de respuesta automatizados (playbooks), evitando la propagación de ataques en todo el entorno de seguridad a través de la ejecución de acciones preventivas, incluyendo el aislamiento de hosts, la finalización de procesos y la notificación a los administradores	X	
3		Ofrecer integración fluida con soluciones propias y con soluciones líderes de terceros reconocidas en el mercado, para una cobertura integral en todo el ecosistema de seguridad, garantizando el más alto nivel de protección en cada punto de aplicación	X	
4		Permitir la implementación rápida de procesos para lograr mayor seguridad y eficiencia operativa, sin requerir de un especialista en automatización. Se deben agregar nuevas secuencias de automatización de forma regular	X	
5		Contar con una interfaz unificada para gestionar y monitorear el estado de prevención en todas las dimensiones de seguridad, garantizando una supervisión integral y operaciones simplificadas	X	
6		Incluir como mínimo herramientas de asistencia basadas en inteligencia artificial que permitan crear o personalizar flujos de trabajo de seguridad en lenguaje natural, sin necesidad de un ingeniero de automatización	X	
7		La activación debe realizarse en cuestión de minutos. Los playbooks listos para usar deben ponerse en marcha automáticamente, incluyendo la capacidad de bloquear un dispositivo o dirección IP en todos los puntos de aplicación, notificar a los administradores sobre instalaciones de políticas en dispositivos de seguridad, poner en cuarentena direcciones IP internas, archivos, entre otros	X	
1	SIMPLICIDAD EN LA OPERACIÓN Y MONITOREO	La solución o consola de administración debe cumplir con los siguientes requisitos:	X	
2		Debe permitir obtener el estado de salud operativo histórico y en tiempo real, con monitoreo y alertas de todos los Firewalls en una sola plataforma	X	
3		Debe permitir responder y resolver incidentes automáticamente basándose en patrones aprendidos, reglas predefinidas e información	X	
4		Aprovechar la analítica predictiva con IA para identificar y abordar proactivamente posibles problemas antes de que afecten las operaciones, reduciendo el tiempo de inactividad	X	
5		Debe incluir un asistente digital (agente IA) para reducir el tiempo necesario para tareas de seguridad, incluyendo la creación e implementación de políticas y la resolución de tickets de soporte	X	
6		Recibir orientación para crear nuevos controles de prevención de amenazas o actualizar los existentes, como reglas de protección de datos, firewall o firmas IPS	X	
7		Aprovechar las capacidades del asistente de IA en la búsqueda, análisis y resolución de amenazas	X	
5. SERVICIOS PROFESIONALES				
9	Servicio Profesional	Servicio profesional orientado al diseño, implementación, validación y migración de las políticas de la solución actual, así como al soporte integral durante la puesta en marcha de la nueva plataforma que reemplazará los equipos existentes	X	

FIRMA	
Representante Legal:	CLAUDIA ALEXANDRA PARDO BUITRAGO
Nombre:	S3 SIMPLE SMART SPEEDY SAS
C.G.:	30394928
Teléfono:	5214708289
Contacto:	NATALIA DORADO GAVIRIA
Dirección:	CR 49 A NO 86 40
Correo:	licilaciones@s3.com.co

 Función Pública Función Pública		DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA DAFP OFICINA DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES		
Adquirir, instalar, configurar, implementar y soportar una solución integral de ciberseguridad compuesta por: (i) un Firewall de Nueva Generación (NGFW) con prevención avanzada de amenazas, sandboxing y acceso remoto seguro; (ii) una solución de protección de correo electrónico y plataformas de colaboración en la nube; y (iii) una plataforma de gestión centralizada de seguridad en la nube; para fortalecer la seguridad perimetral y la protección de los sistemas de información y usuarios del Departamento Administrativo de la Función Pública.				
Códigos UNSPSC: 43222600, 43231600, 43233200, 8112600				
Fecha:		Empresa cotizante:		
ESPECIFICACIONES TÉCNICAS				
ITEM	CARACTERÍSTICAS		CUMPLE	NO CUMPLE
DESCRIPCIÓN				
2. ESPECIFICACIONES TÉCNICAS SOFTWARE				
1	REQUERIMIENTO GENERALES Y ARQUITECTURA	La solución suministrada debe ser a través un servicio SaaS en nube.	X	
		El servicio SaaS debe contar con al menos alguna de estas certificaciones:		
		SOC 2	X	
		ISO 27001	X	
		La solución debe ser reconocida como una solución líder en seguridad de correo electrónico por analistas terceros en los últimos 3 años	X	
		La disponibilidad del servicio SaaS debe ser de al menos 99.9%	X	
		La solución debe usar protocolos de cifrados modernos para salvaguardar la organización.	X	
		La solución debe ser escalable y nativa de nube para soportar crecimiento a cientos de miles de usuarios	X	
		La solución debe proteger de Ciber Amenazas para de correo electrónico en la nube Office 365 y Google Workspace.	X	
		La solución debe soportar proteger de Ciber Amenazas, en las siguientes aplicaciones SaaS de Colaboración y Almacenamiento de archivos:	X	
		Stack	X	
		Microsoft Teams	X	
		Microsoft OneDrive	X	
		Microsoft SharePoint	X	
		Google Drive	X	
		Box	X	
		Dropbox	X	
		Citrix Sharefiles	X	
		La solución debe deberá proporcionar un servicio para quinientos treinta (530) usuarios y buzones	X	
		La solución debe proveer protección contra los siguientes Ciber ataques:	X	
		Prevención ataques a Correo electrónico (Phishing, Spoofing, Spam)	X	
		Prevención de Malware (en correo, herramientas de colaboración y almacenamiento)	X	
		Prevención de Malware de día Cero con Sandboxing (en correo, herramientas de colaboración) y Limpieza de Documentos CDR	X	
		Análisis de usuarios e índices de sesión anómalos (Índices de robo de cuentas)	X	
		Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT	X	
		La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado	X	
		La plataforma deberá poder ser administrada via HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge	X	
		La solución debe ser fácil y rápida de usar, con configuraciones de políticas listas para usar.	X	
		La solución debe bloquear sofisticados ataques de ingeniería social, como la suplantación de identidad, spam, phishing de día cero y Business Email Compromise (BEC) usando motores de machine learning(ML), Deep Learning y de Inteligencia Artificial (IA)	X	
		La solución debe proteger los correos electrónicos de entrada, salientes y proteger la comunicación interna en tiempo real para ataques laterales y amenazas internas.	X	
		La solución debe proveer prevención en línea (no solo detección y/o remediación), es decir intercepción de correo antes que lleguen al usuario final.	X	
		La solución debe permitir el despliegue automático por integración nativa de API sin requerir cambios en los registros MX de DNS para prevent ataques por correo.	X	
		La integración por API debe ser automática y sencilla de gestionar, debe permitir reglas granulares por usuarios y/o grupos que pueden estar en prevención y/o remediación y no requerir de configuraciones manuales del lado del servicio de correo (Microsoft 365 o Google)	X	
		La solución debe ser invisible para los atacantes y debe aplicar seguridad en profundidad siendo una capa de seguridad como última línea de defensa y no desactivar la seguridad nativa de las soluciones de Correo de Nube de Office 365 y/o Google Workspace.	X	
		La solución debe contar con un periodo de aprendizaje histórico que realice como mínimo un análisis de 13 meses de metadatos de correo electrónico (remite, destinatario, asunto, hora) en los buzones de correo de los usuarios, con el fin de determinar patrones de comunicación y ajustar los motores de detección.	X	
		La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico utilizando Inteligencia Artificial, incluyendo al menos 100 idiomas que incluyen el español.	X	
		La solución debe inspeccionar los metadatos, archivos adjuntos, enlaces e idioma de la comunicación, dominios, OCR, QR codes, así como todas comunicaciones históricas, para determinar relaciones de confianza previas entre el emisor y el receptor del correo para de identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.	X	
		La solución debe etiquetar los correos electrónicos dependiendo del tipo de amenaza identificada, como mínimo:	X	
		Extorsión	X	
		Suplantación	X	
		Estafa Financiera	X	
		Ingeniería Social	X	
		Facturas falsas	X	
		Robo de credenciales	X	
		Seducción	X	
		La solución debe analizar cada correo electrónico como un todo y no de manera individual, permitiendo establecer al menos los siguientes puntos:	X	
		A nivel de contenido del correo analizado:	X	
		¿Este remitente ha escrito antes a la organización?	X	
		¿Algunos de los usuarios internos han estado en contacto previo con esta dirección o dominio?	X	
		¿Relación entre la dirección externa o dominio externo y la organización?	X	
		¿Qué tan común es para estos destinatarios de la organización recibir el mismo correo?	X	
		¿Ha sido mencionado este remitente por los usuarios internos en algún correo previo?	X	
		La dirección del remitente se parece a alguna dirección interna o externa conocida (dirección/dominio)?	X	
		A nivel de Contexto del correo analizado:	X	
		¿La estructura del link es sospechosa?	X	
		¿Los enlaces contenidos en el correo son similares a los correos de Phishing?	X	
		¿El enlace se encuentra ofuscado a través de algún método conocido?	X	
		¿El enlace está diseñado para redirigir al destinatario a un dominio diferente del supuesto por enlace original?	X	
		¿El contenido contiene contenido potencialmente malicioso como enlaces o imágenes o	X	
		¿Hay signos de intento de extorsión en el cuerpo de este correo?	X	
		¿El lenguaje del correo sugiere que es un correo típico de Phishing o Spam?	X	
		La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre.	X	
		La solución debe realizar la verificación de más de 200 de indicadores de ataque sobre el correo electrónico como la verificación DMARC, SPF o DKIM para verificar que un correo electrónico se origina en el supuesto dominio de origen, a través de inteligencia artificial para detectar ataques maliciosos y sofisticados.	X	
		La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación de correo electrónico:	X	
		Sender Policy Framework (SPF)	X	
		Domain Keys Identified Mail (DKIM)	X	
		Domain-based Message Authentication, Reporting & Conformance (DMARC)	X	
		La solución debe contar con la opción de configuración de listas blancas y listas negras.	X	
		La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus empleados.	X	
		La solución debe utilizar la integración con el directorio para crear automáticamente listas de usuarios VIP para protegerlos Protección contra la suplantación de identidad.	X	
		La solución debe inspeccionar enlaces cuando el usuario hace clic en la URL. Es decir re-escribir enlaces en el correo.	X	
		La solución debe emular (sandboxing) los enlaces URL re-escritos para exponer indicadores de phishing ocultos.	X	
		La solución debe permitir a los administradores detectar a los usuarios que hicieron clic en los enlaces que resultaron maliciosos y que requieren mayor educación y capacitación para evitar hacer clic en enlaces maliciosos.	X	
		La solución debe Interactuar con Microsoft a través de la API, no debe generar interferencia cuando MS ATP o Defender inspecciona la URL antes que se reescriba la URL. Por lo tanto, puede usarse con MS ATP o Defender, como una capa adicional de protección.	X	
		La solución debe re-escribir enlaces en el cuerpo del correo y también en links dentro de documentos adjuntos en el correo	X	
		La solución debe permitir a los administradores configurar la lista de excepciones, de correos detectados mediante como maliciosos o sospechosos	X	

La solución debe soportar la recritura de URLs embebidas incluso si son códigos QR, reemplazado la imagen del código QR en el cuerpo del correo con un nuevo código QR que apunta a un enlace resuelto.	X	
La recritura de enlaces de la solución debe tener la opción de permitir ofuscar la ruta completa de la URL, dejando solo visible el dominio de la URL, de esta manera, los usuarios pueden comprender aproximadamente a dónde apunta el enlace, sin permitirles eludir la seguridad.	X	
La solución debe ser capaz de poner en cuarentena los correos electrónicos, los archivos y los mensajes según las políticas de seguridad y la configuración de los motores de seguridad.	X	
La solución de acuerdo con la política debe permitir a los usuarios finales enviar solicitudes de restauración para correos electrónicos en cuarentena, seleccionar administradores autorizados pueden aprobar o no las solicitudes de restauración.	X	
La solución debe permitir a los administradores configurar enviar notificaciones sobre solicitudes de restauración de correos en cuarentena a cualquier dirección de correo electrónico, así como parte del equipo de soporte o el SOC, este equipo recibe notificaciones de las solicitudes y las gestiona según su SLA.	X	
La solución debe permitir a los administradores configurar un remitente personalizado para las notificaciones enviadas a los usuarios finales sobre la aprobación o rechazo de solicitudes de restauración de correos en cuarentena y los reportes sobre correos de phishing, siendo posible configurar al menos los siguientes parámetros:	X	
Dirección del remitente	X	
Nombre del remitente	X	
Dirección de respuesta	X	
Cuando las organizaciones utilicen soluciones de Simulación y Entrenamiento de Phishing, en las que envían campañas de phishing falsas para evaluar la respuesta de los usuarios y educarlos, la solución de seguridad de correo electrónico debe detectar automáticamente estos reportes y los distingue de otros correos, y cuando los usuarios reporten estos correos simulados, pueden enviar una respuesta automatizada para reconocer su conciencia.	X	
Para el caso de spam al ser una amenaza que principalmente desperdicia el tiempo y/o el impacto en la productividad de usuario. Mas, sin embargo, el spam podría para un empleado ser valioso y para otro no, para evitar genera frustración del usuarios final cuarentenando algo innecesario o moverlo al carpeta de spam y/o carga adicional para el soporte técnico debido a la necesidad de crear excepciones manuales, la solución debe tener la opción de permitir a los administradores que los usuarios finales pueden marcar remitentes y dominios como confiables, asegurando que los correos electrónicos de estos remitentes lleguen a su bandeja de entrada, incluso si son clasificados como spam. Los correos clasificados como phishing o que contienen malware deben seguir puestos en cuarentena.	X	
Al revisar los correos electrónicos de resumen de cuarentena diarios o visitar el portal de cuarentena del usuario final, los usuarios finales pueden confiar en los remitentes.	X	
De esta manera, los correos electrónicos que les envíen estos remitentes y se marquen como Spam o Graymail, llegarán a su buzón y no a la carpeta de correo no deseado o cuarentena.	X	
La solución debe permitir a los administradores monitorear y gestionar la lista de remitentes confiables desde el portal de gestión de Excepciones de Anti-Spam.	X	
Los administradores pueden confiar en los remitentes globalmente para toda la organización.	X	
Los administradores de la solución deben poder editar o agregar remitentes de confianza para destinatarios específicos a través del portal de la solución.	X	
Los administradores pueden asignar remitentes de confianza no solo para un destinatario específico, sino para toda la organización.	X	
De esta manera, los correos electrónicos de ese remitente de confianza, si se encuentran como spam o Graymail, llegarán al buzón del destinatario, independientemente de quién sea el destinatario.	X	
Para los correos electrónicos de Graymail están en algún lugar entre el spam y los correos electrónicos profesionales del día a día.	X	
La solución debe permitir a las organizaciones que utilizan Microsoft 365 Exchange Online mover automáticamente estos correos electrónicos a una carpeta dedicada.	X	
La solución debe crear y mantener la carpeta debajo de la bandeja de entrada de todos los usuarios finales, para que todos los empleados sepan exactamente dónde encontrar los correos electrónicos de Graymail.	X	
La solución debe permitir correos electrónicos incluidos en la lista de permitidos de la solución también en sean permitidos por Microsoft/Google.	X	
La solución debe contar acciones automatizadas como marcar como alertar al usuario en el correo, mover a la carpeta Spam/Junk, Cuarentena el correo, y/o añadir una cabecera en el correo.	X	
La solución debe contar acciones automatizadas como marcar como alertar al usuario en el correo, mover a la carpeta Spam/Junk, Cuarentena el correo, y/o añadir una cabecera en el correo.	X	
La solución debe contar acciones automatizadas diferenciadas para phishing, malware, spam, correo de mercado (marketing).	X	
La solución debe contar acciones automatizadas como marcar como alertar al usuario en el correo, mover a la carpeta Spam/Junk, Cuarentena el correo, y/o añadir una cabecera en el correo.	X	
La solución debe permitir al administrador que los usuarios finales confíen en los remitentes para que los correos electrónicos clasificados como spam y entreguen en su buzón, en cambio, a los correos electrónicos se clasifican como phishing o contienen malware, se pondrán en cuarentena.	X	
La solución debe permitir que el administrador personalizar las plantillas que usaría para notificar a los usuarios finales sobre las amenazas.	X	
La solución debe tener un periodo de retención de correos electrónicos originales cuarentenados por al menos 180 días.	X	
La solución debe tener un periodo de retención de los metadatos de los correos electrónicos analizados maliciosos por al menos 180 días.	X	
La solución debe permitir conservar los correos electrónicos puestos en cuarentena por Microsoft, por un periodo de tiempo más largo que la retención de Microsoft y esta duración se puede configurar hasta 180 días.	X	
La solución debe tener un periodo de retención de todos los correos electrónicos originales analizados por al menos 14 días, aun si son clasificados como limpios.	X	
La solución debe permitir opcionalmente como backup almacenar localmente los correos electrónicos/archivos en cuarentena.	X	
La solución debe tener la capacidad de remediación las amenazas que llegan a las bandejas de entrada de los usuarios, desde la interfaz de gestión debe poder realizar la identificación, el análisis y la corrección. Si llega un correo electrónico o un archivo, y se pueden tomar medidas inmediatas en miles de bandejas de entrada con unos pocos clics, sin PowerShell ni codificación de ningún tipo.	X	
La solución debe permitir a los usuarios y administradores proporcionar comentarios sobre correos electrónicos sospechosos para ayudar en la clasificación de phishing.	X	
La solución debe permitir que los usuarios puedan ayudar a detectar ataques perdidos y permitir que los administradores de seguridad bloqueen los ataques detectados y prevenir ataques similares en el futuro.	X	
La solución debe integrarse con el este mecanismo reporte de suplantación de identidad de MS Outlook.	X	
La solución debe permitir la adición de Banners de correo electrónico educativos usando inteligencia artificial para los correos electrónicos entrantes, que permita a la organización concienciación sobre ciberseguridad y recordar a los usuarios que sigan la política, los banners deben ser totalmente personalizables para el color que represente la gravedad y el texto, e informar al destinatario sobre correos con contenido como:	X	
Solicitud de pago a través del servicio de pago	X	
Correos electrónicos con facturas / ordenes de compra	X	
Correos electrónicos con enlaces a recursos restringidos	X	
Nombre del remitente diferente a la dirección	X	
Dominio de respuesta creado recientemente y su dirección es diferente a la del remitente	X	
Error en el SPF del remitente	X	
Dominio del remitente creado recientemente	X	
Correos electrónicos entrantes de remitentes externos.	X	
La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones:	X	
Hosts	X	
direcciones IP	X	
Usuarios	X	
Dominios	X	
Cabeceras / Headers	X	
Asunto	X	
Links	X	
Adjuntos	X	
El diagrama de flujo de seguridad del correo electrónico en el tablero principal que muestra cuántos correos electrónicos envió Microsoft a la bandeja de entrada, cuarentena, correo no deseado y detectados y cuarentenados por la solución de seguridad ofrecida.	X	
La solución debe ser permitir a los administradores desde la misma consola de gestión de seguridad de correo electrónico ver y restaurar todos los correos electrónicos en cuarentena, ya sea que hayan sido puestos en cuarentena por Microsoft o por la solución de seguridad ofrecida basada en API.	X	
La solución debe permitir a los administradores bloquear automáticamente las URL procedentes de las fuentes de indicadores de compromiso (IOC).	X	
Revisión de correos electrónicos de phishing reportados por el usuario	X	
Los usuarios pueden ayudar a detectar ataques perdidos, permitir que los administradores de seguridad corrijan los ataques detectados y ajustar las políticas para evitar ataques similares en el futuro.	X	
La solución debe ingerir automáticamente estos informes, alertar a los administradores sobre ellos y los presentar un panel dedicado que permita a los administradores investigar y tomar las medidas necesarias.	X	
La solución se debe poder integrar con el complemento nativo Report Message para Microsoft 365, para marcar como phishing en Outlook. Cuando un usuario hace clic en esta opción.	X	
Responder automáticamente y corregir los informes de los usuarios finales sobre correos electrónicos de phishing.	X	
Para reducir la carga de trabajo de los equipos de SOC y Help Desk se reduce significativamente.	X	
Cada vez que un usuario envíe un reporte de correo de phishing, la solución debe volver a evaluar el correo electrónico, utilizando la reputación actualizada, los motores de seguridad actualizados y con el informe como un indicador adicional para la IA. El resultado es un veredicto reevaluado: limpio, phishing o no concluyente.	X	

3	PREVENCIÓN DE MALWARE EN DÍA CERO (SANDBOXING) EN CORREO Y HERRAMIENTAS DE COLABORACIÓN Y ALMACENAMIENTO SAAS Y LIMPIEZA DE DOCUMENTOS	Para cada veredicto reevaluado, los administradores ahora pueden configurar un flujo de trabajo (poner en cuarentena el correo electrónico o mantener el correo electrónico en el buzón), así como definir notificaciones personalizables tanto para los administradores como para los usuarios finales.	X	
		La solución debe permitir a los administradores configurar un comentario automatizado para que se envíe a los usuarios finales cuando informen de correos electrónicos de entrenamiento de phishing.	X	
		La solución debe permitir a los administradores configurar un remitente personalizado para las notificaciones enviadas a los usuarios finales sobre las solicitudes de restauración de cuarentena aprobadas o rechazadas y los informes sobre correos electrónicos de suplantación de identidad (phishing).	X	
		La solución debe permitir a los administradores pueden enviar notificaciones sobre los usuarios que envían solicitudes de restauración a cualquier destinatario de correo.	X	
		La solución debe permitir enviar un reporte diario por correo electrónico a los usuarios finales sobre los correos electrónicos en cuarentena y basura/spam en las últimas 24 horas.	X	
		La solución debe permitir a los administradores configurar la liberación automática de correos electrónicos de la cuarentena de Microsoft si son clasificados como limpios por el sistema de seguridad, es decir falsos positivos en las detecciones de Phishing de Alta Confianza evitando que los administradores dediquen mucho tiempo a liberar estos correos de la cuarentena, como una última línea de defensa y capa de seguridad la solución debe poder configurarse para liberar automáticamente los correos en cuarentena por Microsoft como Phishing de Alta Confianza si el sistema los clasifica como limpios.	X	
		Los correos electrónicos que Microsoft / Google entregan falsamente a la carpeta de correo no deseado pueden redirigirse a la bandeja de entrada del usuario.	X	
		La solución permite corregir sus detecciones de falsos positivos, para que los equipos de SOC no dediquen tiempo a acudir a los usuarios finales a localizar sus correos electrónicos legítimos perdidos.	X	
		Portal Dedicado para la Gestión de Correos en Cuarentena por los Usuarios Finales	X	
		Las organizaciones necesitan que sus usuarios finales tengan acceso a sus correos para mantener el funcionamiento del negocio. En casos raros en los que un correo es puesto en cuarentena erroneamente por el sistema de seguridad o por Microsoft, y no es liberado automáticamente, es crucial que el usuario pueda recuperarlo rápidamente.	X	
		El Portal de Seguridad de Correos Electrónicos para Usuarios Finales, debe permitir a los usuarios ver todos sus correos en cuarentena, filtrarlos, previsualizarlos y restaurarlos o enviar solicitudes de restauración, todo conforme a las políticas organizacionales definidas.	X	
		Los usuarios pueden iniciar sesión en el portal de cuarentena de usuario final a través de Microsoft, aplicando los mismos controles de seguridad, incluido el inicio de sesión único, a través de su cuenta corporativa de Microsoft.	X	
		La solución de permitir a los usuarios solicitar al administrador la liberación de los correos cuarentenados desde este reporte diario.	X	
		Prevención de Malware en Correo Electrónico y herramientas de colaboración y almacenamiento Saas	X	
		Debe escanear malware a través de análisis estático	X	
		La solución debe tener protección antivirus/malware basado en firmas.	X	
		La solución debe permitir a los administradores configurar la lista de bloqueo cualquier tipo de archivo y marcado como malware y para los tipos de archivos (PDF, EML, HTML) optar por bloquear estos archivos en función de si contienen enlaces o no.	X	
		La solución debe detectar archivos como protegidos con contraseña al menos de las siguientes extensiones	X	
		Documentos: Word, Excel, PowerPoint y PDF	X	
		Archivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, LZH, RPM, WIM, ARJ, CPIO, CROMFS, QCOWZ, UDF, AIO e IMG, ISO, AR	X	
		Si un archivo está como protegido con contraseña, la solución debe intentar extraer la contraseña mediante varias técnicas, como buscar la contraseña en el cuerpo del correo electrónico y si se encuentra la contraseña, debe usar la contraseña para descifrar el archivo e inspeccionarlo en busca de malware.	X	
		Si no se encuentra la contraseña, el administrador debe poder seleccionar alguna de las siguientes acciones:	X	
		Requerir que el usuario final ingrese una contraseña	X	
		El usuario recibe el correo electrónico con una advertencia.	X	
		Cuarentena.	X	
		Identificar el correo como sospechoso de malware	X	
		La solución debe permitir a los administradores pueden excluir remitentes externos del flujo de trabajo predeterminado para el manejo de correos con archivos adjuntos protegidos por contraseña, para evitar solicitar contraseñas repetidamente de sistemas automatizados o dominios confiables que envían muchos correos con archivos adjuntos protegidos, las exclusiones deben permitir las direcciones de remitente o dominios específicos pueden ser excluidos del flujo de trabajo, permitiendo que sus correos sigan siendo inspeccionados para malware. Si el sistema no puede entender las contraseñas, los archivos adjuntos se considerarán como permitidos (limpios).	X	
		Escanea todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados". Google Drive, SharePoint, OneDrive, Dropbox, de malware, ransomware, ataques laterales	X	
		La solución debe escanear y analizar cada archivo en busca de enlaces maliciosos que luego bloquear en todos sus aplicaciones para compartir archivos.	X	
		La solución debe detectar directamente el comportamiento malicioso y pone en cuarentena los archivos antes de que la amenaza se propague.	X	
		Brinda protección contra enlaces de phishing, código o archivos maliciosos y fuga de datos en plataformas de chat empresarial.	X	
		La solución debe a los administradores permitir y bloquear direcciones URL exactas y dominios completos en mensajes de Teams y Slack.	X	
		Para Aplicaciones como OneDrive, SharePoint debe permitir por políticas dos tipos de acciones de remediación Cuarentena y Vault Feder(Carpeta bóveda)	X	
4	ANOMALÍAS DE USUARIOS Y DETECCIÓN DE CUENTAS COMPROMETIDAS	La solución debe incluir capacidades de "Sandboxing" resistente a la evasión para bloquear el malware de día cero, con un análisis dinámico en un entorno virtual aislado y escalable basado en la nube	X	
		La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes. Incluso debe tener la capacidad de ver un video del resultante de la emulación.	X	
		El análisis de sandboxing debe obtener un veredicto respecto de un archivo adjunto o del recurso web asociado a un hipervínculo en un lapso no mayor a 5 minutos.	X	
		La solución debe contar con una página de bloqueo para impedir el acceso de los usuarios a los sitios web maliciosos asociados a los hipervínculos contenidos en los mensajes de correo analizados.	X	
		La solución debe ser capaz de sandboxing al menos los siguientes tipos de archivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, SWF, JAVA (jar, .jar, .jar), VBS, scripts y archivos PowerShell (.ps1)	X	
		La solución debe permitir a los administradores puedan seleccionar los sistemas operativos que utilizará el sandbox del Anti-Malware para emular archivos.	X	
		La Emulación debe soportar hacerlo en Win7, Win8.1, Win10 o inclusive Win11.	X	
		La solución debe admitir capacidades CDR (Content disarm and Reconstruction) es decir, podrá limpiar los documentos o imágenes adjuntos en los correos electrónicos de contenido malicioso.	X	
		La solución CDR debe ser capaz al menos los siguientes tipos de archivos: PDF, FOF, XLSX, XLSB, XLSM, XLTX, XLTM, XLAM, XLSB, XLS, PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM, PPT, PPS, POT, PPA, DOCX, DOOM, DOTX, DOTM, DOC, DOT	X	
		La solución en los correos electrónicos para archivos detrás de enlaces de descarga directa debe emular los archivos(sandbox) para extender la protección contra archivos desconocidos que se ocultan detrás de enlaces, antes de ser entregados a los usuarios finales.	X	
		Además, debe prevenir ataques en los que el archivo detrás del enlace se altera después de que se envía el correo aplicando la protección de reescritura del enlace, así la a inspección se realizara cuando los usuarios hagan clic en estos enlaces después de ser reescritos, y si se detecta que el archivo es malicioso, el acceso al archivo deberá ser bloqueado.	X	
		La solución debe evitar ataques avanzados de apropiación de cuentas aumentando los procesos de autenticación, evitar usuarios no autorizados y los dispositivos comprometidos accedan a su correo electrónico en la nube o a las aplicaciones SaaS	X	
		La solución debe contar con un motor analiza el comportamiento utilizando un algoritmo de aprendizaje automático utilizando un algoritmo de aprendizaje automático que crea un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.	X	
		La solución debe contar detecta comportamientos y acciones que parecen anómalas cuando se observan en el contexto de una organización y la actividad histórica de un usuario.	X	
		Para identificar cuentas potencialmente comprometidas. Debe incluir un motor de inteligencia artificial para inspeccionar todos los parámetros de los eventos de inicio de sesión para identificar los realizados por actores malintencionados.	X	
		Borrado de todos los correos electrónicos del buzón	X	
4	ANOMALÍAS DE USUARIOS Y DETECCIÓN DE CUENTAS COMPROMETIDAS	Usuarios que envían correos electrónicos maliciosos	X	
		Mover todos los correos electrónicos a una subcarpeta	X	
		Detección basada en Inteligencia artificial de inicios de sesión anómalos	X	
		Iniciar la sesión desde una dirección IP maliciosa	X	
		Primera vez en un nuevo país	X	
		Reenvío automático a una dirección de correo electrónico externa	X	
		Acceso intenal desde un país	X	
		Acceso desde una geográfica sospechosa (viaje imposible)	X	
		Error de inicio de sesión sospechoso en MFA	X	
		El cliente es un navegador vulnerable.	X	
		La solución debe un evento de seguridad que brinda el contexto e información necesaria para la investigación, debe clasificar como crítica o sospechosa.	X	
		La solución debe tener la capacidad de tomar las siguientes acciones de respuesta cuando detecte cuentas potencialmente comprometidas o cuentas secuestradas:	X	
		Bloquea la cuenta.	X	
		Restablecer la contraseña.	X	
		Las Anomalías Críticas y de inicio de sesión identificados de los usuarios comprometidos podrán ser bloqueados automáticamente.	X	
		La solución debe permitir a los administradores configurar un buzón dedicado al que se enviarán alertas sobre cuentas comprometidas.	X	
		Bloqueo de cuentas que inicien sesión desde direcciones IPs conocidas como maliciosas por una base de inteligencia del fabricante (TIP)	X	

5	SHADOW IT & APPLICATION CONTROL	Entre los eventos que la solución debe analizar para identificar cuentas secuestradas ("account takeover") deben incluirse:	X	
		El inicio de sesión:	X	
		La ubicación desde donde se hizo el inicio de sesión:	X	
		Anomalias recientes	X	
		Correos recientes	X	
		Acciones del usuario recientes	X	
		Los administradores pueden configurar agregar automáticamente una lista de bloqueo para todo el tráfico saliente de las cuentas detectadas como comprometidas o sospechosas de estar comprometidas, como un capa agregada de seguridad en escomarios como:	X	
		Mensajes maliciosos programados: el atacante puede programar el envío de correos electrónicos en una etapa posterior que se adapte a su ataque, sabiendo que el usuario que comprometió puede ser bloqueado en cualquier momento.	X	
		Entornos híbridos: en los casos en los que el Active Directory local invalida el Azure Active Directory, es posible que se desbloqueen los usuarios bloqueados. En este caso, todos los correos electrónicos salientes de este usuario comprometido seguirán bloqueados.	X	
		La solución basada en el análisis de correos electrónicos (Office 365 y/o Gmail). Debe identificar los correos electrónicos de las aplicaciones en la nube para los usuarios que supieren que han estado usando, para brindar visibilidad de las aplicaciones en la nube que se utilizan en su empresa.	X	
		La solución detectará y proporcionará informes de aplicaciones de Shadow IT y top de usuarios.	X	
		La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.	X	
		La solución debe indicar el uso de las aplicaciones a lo largo del tiempo	X	
		La solución debe Presentar las aplicaciones usadas según su categoría	X	
		La solución debe permitir a probar una aplicación o crear lista blanca la aplicación	X	
		La solución debe permitir gestionar los eventos de seguridad, ya sea que se detecten/prevengan automáticamente o que los administradores/usuarios finales encuentren después de no haber sido prevenidos de diversas amenazas, desde correos maliciosos y spam hasta cuentas comprometidas y socios riesgosos.	X	
		La solución debe contar con una vista detallada de todos los eventos de seguridad en tiempo real. Mediante la búsqueda y los filtros, puede ver eventos relacionados con cualquier período de tiempo, estado, nivel de gravedad y SaaS.	X	
		La solución debe contar con una vista centrada en las amenazas de correo electrónico con información como:	X	
		Categorías de phishing detectadas	X	
		Acción sobre el correo electrónico malicioso, si está en cuarentena, en la bandeja de entrada, o en la carpeta de no deseado	X	
		Usuarios involucrados en el evento (destinatarios, remitentes, propietarios de archivos compartidos)	X	
		Información de quien remedió la amenaza que puede ser el administrador, por la herramienta de seguridad o por el proveedor de correo en nube	X	
		La solución debe proporcionar tableros análisis de eventos maliciosos detallados para cada aplicación SaaS	X	
		Los Tableros (Dashboards) detallados de los eventos de seguridad por cada aplicación SaaS de almacenamiento y/o colaboración.	X	
		Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.	X	
		La solución deberá proveer reportes ejecutivos de eventos de seguridad de los última semana, dos semanas y últimos 30 días.	X	
		La solución debe permitir a los administradores programar informes de seguridad se envíen con diferentes zonas horarias y a diferentes destinatarios.	X	
		Debe proveer capacidades de investigación que apoyen los procesos de cacería de amenazas de la organización, poder realizar consultas a toda la metadata (correos electrónicos, archivos, inicios de sesión de usuario, etc.) capturada y almacenados en el tenant	X	
		La capacidades de investigación deben permitir los siguientes tipos de filtro:	X	
		Múltiples Valores en una Consulta: listas extensas de hasta 200 valores en un solo campo de búsqueda que acepta texto libre, con condiciones disponibles (Contiene Cualquiera, Coincide con Cualquiera, Excluir Cualquiera, Excluir Coincide).	X	
		Múltiples Condiciones de Búsqueda para el mismo Campo: aplicar filtros a un campo, definir múltiples condiciones para ajustar la búsqueda de manera más precisa, gestionar el operador (Y/O) entre cada condición.	X	
		La solución debe proveer un tablero de resumen que proporcione a los administradores una visibilidad instantánea de todas las tareas pendientes de revisión, incluyendo:	X	
		Usuarios comprometidos	X	
		Socios riesgosos	X	
		Solicitudes abiertas de restauración de cuarentena por parte de usuarios finales	X	
		Reportes abiertos de phishing por parte de usuarios finales	X	
		Ataques BEC incluye un indicador que muestra si las cuentas comprometidas se bloquean automáticamente o no.	X	
		La solución debe tener la posibilidad de exportar eventos a archivos CSV, json, stax	X	
		La solución deberá proveer reportes de los eventos por hasta 180 días, en formato csv o stax.	X	
		La solución debe permitir filtrar los correos electrónicos en función de su dirección, entrante, saliente e interno.	X	
		La solución debe permitir que los administradores deben tener capacidad de filtrar correos por el campo de Message ID	X	
		Los administradores de la solución deben poder filtrar los correos electrónicos utilizando indicaciones en el idioma nativo, utilizando la IA generativa, el Asistente de IA.	X	
		Con el Asistente de IA, puede buscar correos electrónicos utilizando indicaciones en el idioma nativo y obtener resultados instantáneos, debe permitir búsqueda se base en muchos campos.	X	
		La solución debe contar con un tablero con el número de reportes phishing de los usuarios, solicitudes de restauración y socios de riesgo, así como una indicación de si las cuentas comprometidas se bloquean automáticamente o no.	X	
		La solución debe permitir a los administradores tener visibilidad del riesgo de los socios con los que comunican utilizando un motor de IA y recibir alertas sobre los socios que pueden estar comprometidos.	X	
La solución debe permitir a los administradores puedan desencadenar una acción específica cuando el dominio del remitente se parece mucho al dominio de un socio, o evitar ataques de socios comprometidos	X			
La solución debe permitir a los administradores puedan ver la justificación de los usuarios finales antes de aprobar / rechazar las solicitudes antes de liberar un correo de cuarentena	X			
Los administradores de la solución deben tener visibilidad en tiempo real cómo Microsoft 365 clasificó cada correo electrónico y qué acción que tomo son sus soluciones de EOP o Defender, es decir la solución debe trabajar con seguridad en profundidad y en capas.	X			
Los eventos y en cada correo electrónico, deben tener la clasificación de (SC, BC, I) y que acción de cumplimiento (cuarentena, mover a junk folder) que tomo sobre el correo electrónico de acuerdo con la clasificación.	X			
La solución debe permitir filtrar correos electrónicos basado en las acciones tomadas por las herramientas o para las decisiones de cumplimiento de Microsoft	X			
La solución debe brindar el detalle del análisis de un archivo identificado como malicioso incluyendo los comportamientos riesgosos que fueron identificados y las técnicas identificadas. El resultado de la emulación de un archivo malicioso debe incluir un video indicando el resultado de emulación.	X			
El panel principal debe proporcionar una descripción general de cómo la solución clasificó los correos electrónicos que Microsoft decidió dejar pasar a los usuarios finales.	X			
La solución debe permitir filtrar correos electrónicos por esta y las decisiones de cumplimiento de Microsoft	X			
La solución debe incluir un informe diario de cuarentena (Resumen) le permite enviar un informe por correo electrónico diariamente a los usuarios finales sobre los correos electrónicos en cuarentena y no deseados/spam. Los usuarios finales obtienen un informe detallado que contiene información sobre los correos electrónicos que se les enviaron y se pusieron en cuarentena en las últimas 24 horas.	X			
Los usuarios finales pueden generar un nuevo informe de cuarentena (resumen) para las últimas 24 horas en cualquier momento.	X			
La solución debe permitir a los administradores pueden personalizar:	X			
Cuándo y cuántas veces al día sus usuarios finales reciben el informe de cuarentena (resumen)	X			
La dirección de respuesta del informe de cuarentena diario enviado a los usuarios finales.	X			
Los textos en el cuerpo y el asunto del informe diario de cuarentena del usuario final (resumen).	X			
El texto del enlace en el que los usuarios hacen clic para generar un reporte.	X			
La solución debe permitir a los administradores puedan configurar, para cada detección de Microsoft 365, si los usuarios finales pueden solicitar una restauración, restaurar por su cuenta o no pueden restaurar los correos electrónicos en absoluto.	X			
Todas las solicitudes de restauración enviadas por los usuarios finales estarán disponibles para los administradores en el panel Solicitudes de restauración	X			
La solución debe permitir a los administradores puedan cargar un logotipo personalizado para agregarlo a las notificaciones por correo electrónico, las páginas del navegador y los informes.	X			
La solución debe permitir a los administradores que puedan buscar en la consola de seguridad de correo electrónico ofertado los correos electrónicos detectados debido a una regla de transporte de Microsoft, ya sea que se entreguen al usuario final, en la carpeta de correo no deseado o que la solución de seguridad o Microsoft los pongan en cuarentena.	X			
La solución debe permitir desde portal de gestión que los administradores se mantengan actualizados sobre las actividades de mantenimiento y el estado del servicio.	X			
La solución debe permitir a los administradores puedan definir buzones dedicados para recibir alertas sobre el estado del servicio.	X			
Portal de Gestión	X			
Control de acceso granular basado en roles al portal web de gestión, al menos para Administrador, Solo Lectura, Help desk.	X			
Los usuarios del Help Desk y los usuarios de solo lectura pueden recibir permisos de solo visualización para la sección de Políticas.	X			
Los usuarios del Help Desk y los usuarios de solo lectura pueden recibir permisos para ver y editar la sección de Políticas.	X			
Por defecto, los usuarios del Help Desk y de solo lectura no tienen permiso para ver ni editar las reglas de políticas. Anteriormente, se había anunciado la capacidad de otorgar permisos de solo visualización para esta sección.	X			
La solución debe permitir a los administradores puedan restringir el acceso al portal de la organización a una dirección IP o CIDR específica	X			
Integraciones a SIEMs y API	X			
La solución ofertada debe permitir integrarse con soluciones SIEM via syslog via TCP o json via HTTP	X			
La solución debe soportar API Rest para administrar y actuar sobre los eventos de seguridad detectados	X			
SERVICIOS PROFESIONALES				

1	Servicio Profesional	Servicio profesional orientado al diseño, implementación, validación y migración de las políticas de la solución actual, así como al soporte integral durante la puesta en marcha de la nueva plataforma que reemplazará los equipos existentes.	X	
1	Personal requerido			
	El contratista deberá: Acreditar el personal requerido en la ficha técnica respecto de perfiles, formación académica, certificaciones y experiencia, mediante la entrega de la documentación y soportes correspondientes con la presentación de la oferta. En caso de requerir el reemplazo de algún profesional o técnico, informar al supervisor con mínimo cinco (5) días hábiles de anticipación y garantizar que la persona propuesta acredite igual o mayor nivel de formación, experiencia y certificaciones que las exigidas en la ficha técnica para el respectivo rol. El reemplazo solo podrá efectuarse previa aprobación escrita del supervisor, so pena de requerimiento y aplicación de las medidas previstas en el contrato por incumplimiento de obligaciones contractuales.		X	

FIRMA	
Representante Legal:	CLAUDIA ALEXANDRA PARDO OÑEROGA
Nombre:	S3 SIMPLE SMART SPEEDY SAS
C.C:	30394928
Teléfono:	3214708289
Contacto:	NATALIA DORADO GAVIRIA
Dirección:	CR 48 A NO 86 40
Correo:	licitaciones@s3.com.co