

INF-1030/26

INFORME SOLICITUD DE ASISTENCIA
TESORERÍA DE LA SEGURIDAD SOCIAL
TSS

SEPTIEMBRE 28, 2026.-

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **contratación de la continuidad del derecho de uso herramienta de email security**, el cual se nos ha presentado como dirección ejecutiva del gabinete de innovación y desarrollo digital.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta especificaciones técnicas

A groso modo se solicita:

- **2 Suscripción Central Email Advanced**
 - se requiere que el servicio contenga las siguientes especificaciones técnicas:
 - Requerimientos Generales y Arquitectura
 - La solución debe proteger de Ciber Amenazas para de correo electrónico en la nube Office 365 y/o Google Workspace.
 - La solución suministrada debe ser a través un servicio SaaS en nube.
 - El servicio SaaS debe contar con al menos alguna de estas certificaciones:
 - SOC 2
 - ISO 27001
 - La solución debe soportar proteger de Ciber Amenazas, en las siguientes aplicaciones SaaS de Colaboración y Almacenamiento de archivos:
 - Slack
 - Microsoft Teams
 - Microsoft OneDrive
 - Microsoft SharePoint

- Google Drive
- Box
- Dropbox
- Citrix ShareFiles
- La solución debe ser reconocida como una solución líder en seguridad de correo electrónico por analistas terceros como Forrester o Gartner en los últimos 3 años.
- La solución debe deberá proporcionar un servicio para 400 usuarios de seguridad para correo y herramientas de colaboración en el servicio de Nube.
- La solución debe proveer protección contra los siguientes Ciber ataques:
 - Prevención Ataques a Correo electrónico (Phishing, Spoofing, Spam).
 - Prevención de Malware (en correo, herramientas de colaboración y almacenamiento).
 - Prevención de Malware de día Cero con Sandboxing (en correo, herramientas de colaboración) y Limpieza de Documentos CDR.
 - Anomalías de usuarios e inicios de sesión anómalos (Indicios de robo de cuenta).
 - Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT.
 - Prevención de Fuga de Datos (DLP) en correo y herramientas de colaboración.
- La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado.
- La solución debe ser fácil y rápida de usar, con configuraciones de políticas listas para usar.
- El servicio debe ofrecer una disponibilidad de al menos 99.9%
- La solución debe Utilizar protocolos de cifrados modernos para salvaguardar la organización.

- La solución debe ser escalable y nativa de nube para soportar crecimiento a cientos de miles de usuarios.
- La plataforma deberá poder ser administrada vía HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge.
- Prevención Ataques a Correo Electrónico BEC, Phishing, Spam
 - 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 e Inteligencia Artificial (IA).
 - La solución debe proteger los correos electrónicos de entrada, salientes y proteger la comunicación interna en tiempo real para ataques laterales y amenazas internas.
 - La solución debe proveer prevención en línea (no solo detección y/o remediación), es decir interceptación de correo antes que lleguen al usuario final.
 - La solución debe permitir el despliegue automático por integración nativa de API sin requerir cambios en los registros MX de DNS para prevenir ataques por correo.
 - 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 correos (Microsoft 365 o Google).
 - 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 Workplace.
 - La solución debe contar con un periodo de aprendizaje que realice un escaneo de 13 meses de metadatos de correo electrónico (remitente, destinatario, asunto, hora) en los buzones de correo de los usuarios para determinar los patrones de comunicación y ajustar los motores de IA.

- 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 incluyan el español.
- 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 recepto del correo para de identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.
- 2.10 La solución debe etiquetar los correos electrónicos dependiendo del tipo de amenaza identificada, como mínimo:
 - Extorsión
 - Suplantación
 - Estafa Financiera
 - Ingeniería Social,
 - Facturas falsas
 - Robo de credenciales
 - Sextorsión
- 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.
- 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 evitar ataques evasivos y sofisticados.
- La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación de correo electrónico:
 - Sender Policy Framework (SPF),
 - Domain Keys Identified Mail (DKIM),
 - Domain-based Message Authentication, Reporting & Conformance (DMARC).

- La solución debe contar con la opción de configuración de listas blancas y listas negras.
- La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus empleados.
- La solución debe utilizar la integración con el directorio para crear automáticamente listas de usuarios VIP para protegerlos Protección contra la suplantación de identidad.
- La solución debe inspeccionar enlaces cuando el usuario hace clic en la URL, Es decir reescribir el(los) enlace(s) en el correo.
- La solución debe emular (sandboxing) los enlaces URLs reescritos para exponer indicadores de phishing ocultos.
- 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
- La solución debe interactuar con Microsoft a través de la API, no debe generar interferencia cuando Microsoft (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.
- La solución debe reescribir enlaces en el cuerpo del correo y también en links dentro de documentos adjuntos en el correo.
- La solución debe permitir a los administradores configurar la lista de excepciones, de correos detectados mediante como maliciosos o sospechosos.
- La solución debe soportar la rescritura de URL's embebidas incluso si son códigos QR.
- 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.
- 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 puedan aprobar o no las solicitudes de restauración.

- La solución debe admitir correos electrónicos incluidos en la lista de permitidos que también son permitidos por Microsoft/Google.
- La solución debe contar con acciones automatizadas, como marcar una alertar al usuario en el correo: mover a la carpeta Spam/Junk, cuarentena el correo, y/o añadir una cabecera en el correo.
- La solución debe contar acciones automatizadas diferenciadas para phishing, malware, spam, correo de mercadeo (marketing).
- 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, si los correos electrónicos se clasifican como phishing o contienen malware, se pondrán en cuarentena.
- La solución debe permitir que el administrador personalizar las plantillas que usaría para notificar a los usuarios finales sobre las amenazas
- La solución debe tener un período de retención de correos electrónicos originales cuarentenados por al menos 180 días.
- La solución debe tener un período de retención de los metadatos de los correos electrónicos analizados maliciosos por al menos 180 días
- 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.
- La solución debe permitir opcionalmente como backup almacenar localmente los correos electrónicos/archivos en cuarentena.
- 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.

- La solución debe permitir a los usuarios y administradores proporcionar comentarios sobre correos electrónicos sospechosos para ayudar en la clasificación de phishing.
- 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.
- La solución debe integrarse con el mecanismo reporte de suplantación de identidad de MS Outlook.
- 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:
 - Solicitud de pago a través del servicio de pago.
 - Correos electrónicos con facturas / órdenes de compra.
 - Correos electrónicos con enlaces a recursos restringidos.
 - Nombre del remitente diferente a la dirección.
 - Dominio de respuesta creado recientemente y su dirección es diferente a la del remitente.
 - Error en el SPF del remitente.
 - Dominio del remitente creado recientemente.
 - Correos electrónicos entrantes de remitentes externos.
- La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones:
 - Hosts
 - Direcciones IP
 - Usuarios
 - Dominios
 - Cabeceras / Headers

- Asunto
- Links
- Adjuntos
- 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 ofertada
- 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 ofertada basada en API.
- La solución debe permitir a los administradores bloquear automáticamente las URL procedentes de las fuentes de indicadores de compromiso (IOC).
- 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
- 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).
- La solución debe permitir a los administradores enviar notificaciones sobre los usuarios que envían solicitudes de restauración a cualquier destinatario de correo.
- 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.
- La solución de permitir a los usuarios solicitar al administrador la liberación de los correos cuarentenados desde este reporte diario.

- Prevención de Malware en Correo Electrónico y herramientas de colaboración y almacenamiento SaaS
 - Debe escanear malware a través de análisis estático.
 - La solución debe tener protección antivirus/malware basado en firmas.
 - 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.
 - La solución debe detectar archivos como protegidos con contraseña al menos de las siguientes extensiones:
 - Documentos: Word, Excel, PowerPoint y PDF.
 - Archivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TB2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, IZH, RPM, WIM, ARJ, CPIO, CRAMFS, QCOW2, UDF, AR e IMG, ISO, AR.
 - Si un archivo esta 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.
 - Si no se encuentra la contraseña, el administrador debe poder seleccionar alguna de las siguientes acciones:
 - Requerir que el usuario final ingrese una contraseña
 - El usuario recibe el correo electrónico con una advertencia.
 - Cuarentena.
 - Identificar el correo como sospechoso de malware
 - Escanea todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados, por lo menos en los siguientes servicios:
 - Google Drive
 - ShareFile
 - OneDrive
 - Sharepoint

- Box
- Dropbox: de malware, ransomware, ataques laterales
- La solución debe escanear y analizar cada archivo en busca de enlaces maliciosos que luego bloquear en todas sus aplicaciones para compartir archivos.
- La solución debe detectar directamente el comportamiento malicioso y poner en cuarentena los archivos antes de que la amenaza se propague.
- Brindar protección contra enlaces de phishing, código o archivos maliciosos y fuga de datos en plataformas de chat empresarial.
- La solución debe habilitar a los administradores permitir o bloquear direcciones URL exactas y dominios completos en mensajes de Teams y Slack.
- Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Folder (Carpeta bóveda).
- Prevención de Malware de día Cero (sandboxing) en Correo y herramientas de colaboración y almacenamiento SaaS y Limpieza de Documentos
 - La solución debe incluir capacidades de "Sanboxing" 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.
 - 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 vídeo del resultante de la emulación.
 - 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.
 - 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.

- 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, .js/.jse), VBS, scripts y archivos PowerShell (.ps1).
- La solución debe permitir a los administradores puedan seleccionar los sistemas operativos que utilizará el sandbox del Anti-Malware para emular archivos.
- La Emulación debe soportar hacerlo en Win7, Win8.1, Win10 o inclusive Win11.
- 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.
- La Solución CDR debe ser capaz de gestionar al menos los siguientes tipos de archivos:
 - PDF, DF, XLSX, XLSB, XLSM, XLTX, XLTM, XLAM, XLSB, XLS, PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM, PPT, PPS, POT, PPA, DOCX, DOCM, DOTX, DOTM, DOC, DOT.
- Anomalías de usuarios y Detección de Cuentas comprometidas
 - 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
 - La solución debe contar con un motor analiza el comportamiento 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.
 - La solución debe detectar comportamientos y acciones que parecen anormales cuando se observan en el contexto de una organización y la actividad histórica de un usuario.
 - 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:

- Borrado de todos los correos electrónicos del buzón.
- Usuarios que envían correos electrónicos maliciosos.
- Mover todos los correos electrónicos a una subcarpeta.
- Detección basada en Inteligencia artificial de inicios de sesión anómalos.
- Iniciar la sesión desde una dirección IP maliciosa.
- Primera vez en un nuevo país.
- Reenvío automático a una dirección de correo electrónico externa.
- Acceso inusual desde un país.
- Acceso desde una geográfica sospechosa (viaje imposible).
- Error de inicio de sesión sospechoso en MFA.
- El cliente es un navegador vulnerable.
- La solución debe un evento de seguridad que brinda el contexto e información necesaria para la investigación, debe clasificar como crítica o sospechosa.
- La solución debe tener la capacidad de tomar las siguientes acciones de respuesta cuando detecte cuentas potencialmente comprometidas o cuentas secuestradas:
 - Bloquear la cuenta.
 - Restablecer la contraseña.
- Las Anomalías Críticas y de inicio de sesión identificados de los usuarios comprometidos podrán ser bloqueadas automáticamente.
- La solución debe permitir a los administradores configurar un buzón dedicado al que se enviarán alertas sobre cuentas comprometidas.
- Bloqueo de cuentas que inicien se sesión desde direcciones IPs conocidas como maliciosas por una base de inteligencia del fabricante (TIP)
- Entre los eventos que la solución debe analizar para identificar cuentas secuestradas (“account takeover”) deben incluirse:
 - El inicio de sesión.
 - La ubicación desde donde se hizo el inicio de sesión.
 - Anomalías recientes.

- Correos recientes.
- Acciones del usuario recientes.
- Shadow IT & Application Control
 - La solución basada en el análisis de correos electrónicos (Office 365 y/o Gmail), debe identificar las aplicaciones en las que se ha estado haciendo uso del correo institucional, para brindar visibilidad de dichas aplicaciones en la nube y que se utilizan en nombre del dominio de la empresa.
 - La solución detectará y proporcionará informes de aplicaciones de Shadow IT y top de usuarios.
 - La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.
 - La solución debe indicar el uso de las aplicaciones a lo largo del tiempo.
 - La solución debe presentar las aplicaciones usadas según su categoría.
 - La solución debe permitir a probar una aplicación o crear lista blanca la aplicación.
- Gestión de Eventos, Tableros, Reportes y Auditoria
 - La solución debe permitir gestionar los eventos de seguridad, ya sea que se detecten/prevenan automáticamente o que los administradores/usuarios finales encuentren después de no haber sido prevenidos.
 - 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.
 - La solución debe contar comuna vista centrada en las amenazas de correo electrónico con información como
 - Categorías de phishing detectadas.
 - Acción sobre el correo electrónico malicioso, si está en cuarentena, en la bandeja de entrada, o en la carpeta de no deseado.

- Usuarios involucrados en el evento (destinatarios, remitentes, propietarios de archivos compartidos).
- Información de quien remedio la amenaza que puede ser el administrador, por la herramienta de seguridad o por el proveedor de correo en nube.
- La solución debe proporcionar tableros análisis de eventos maliciosos detallados para cada aplicación SaaS.
- Los Tableros (Dashboards) debe detallar los eventos de seguridad por cada aplicación SaaS de almacenamiento y/o colaboración.
- Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.
- La solución deberá proveer reportes ejecutivos de eventos de seguridad de los última semana, dos semanas y últimos 30 días.
- La solución debe permitir a los administradores programar informes de seguridad se envíen con diferentes zonas horarias y a diferentes destinatarios.
- 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.
- La solución debe tener la posibilidad de exportar eventos a archivos CSV, json, xlsx.
- La solución deberá proveer reportes de los eventos por hasta 180 días, en formato csv o xlsx.
- La solución debe permitir filtrar los correos electrónicos en función de su dirección, entrante, saliente e interno.
- La solución debe permitir que los administradores deben tener capacidad de filtrar correos por el campo de Message ID.
- 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.

- 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.
- 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.
- 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
- Los administradores de la solución deben tener visibilidad en tiempo real de como Microsoft 365 clasificó cada correo electrónico y qué acción que tomó son sus soluciones de EOP o Defender, es decir, la solución debe trabajar con seguridad en profundidad y en capas.
- Los eventos y en cada correo electrónico, deben tener la clasificación de (SCL, BCL) y que acción de cumplimiento (cuarentena, mover a junk folder) que tomó sobre el correo electrónico de acuerdo con la clasificación.
- La solución debe permite filtrar correos electrónicos basado en las acciones tomadas por las herramientas o para las decisiones de cumplimiento de Microsoft.
- 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.
- 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.
- La solución debe permite filtrar correos electrónicos por esta y las decisiones de cumplimiento de Microsoft.

- Los usuarios finales pueden generar un nuevo informe de cuarentena (resumen) para las últimas 24 horas en cualquier momento.
- La solución debe permitir a los administradores personalizar:
 - Cuando y cuántas veces al día sus usuarios finales reciben el informe de cuarentena (resumen).
 - La dirección de respuesta del informe de cuarentena diario enviado a los usuarios finales.
 - Los textos en el cuerpo y el asunto del informe diario de cuarentena del usuario final (resumen).
 - El texto del enlace en el que los usuarios hacen clic para generar un reporte.
- 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.
- Todas las solicitudes de restauración enviadas por los usuarios finales estarán disponibles para los administradores en el panel Solicitudes de restauración
- 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.
- 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.
- La solución debe permitir a los administradores puedan restringir el acceso al portal de la organización a una dirección IP o CIDR específica.

- La solución debe permitir desde portal de gestión que los administradores se mantengan actualizados sobre las actividades de mantenimiento y el estado del servicio.
- La solución debe permitir a los administradores puedan definir buzones dedicados para recibir alertas sobre el estado del servicio.
- Integraciones a SIEMs y API
 - La solución ofertada debe permitir integrarse con soluciones SIEM mediante Syslog vía TCP, o JSON vía HTTP.
 - La solución debe soportar API Rest para administrar y actuar sobre los eventos de seguridad detectados.

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030, esta aprobación tiene vigencia hasta el 31 de diciembre 2026.

Mario Adames

Encargado departamento Asistencia Técnica Especializada
Oficina Gubernamental de Tecnologías de la Información y Comunicación
(OGTIC)

MF/ma



Oficina Gubernamental de Tecnologías de la Información y Comunicación
Manuel Mayrele - Director de Servicios Digitales Institucionales (29/09/2026 08:10 AST)
Mario Adames - Encargado/a de Departamento de Asistencia Técnica Especializada (29/09/2026 08:44 AST)
Edgar Batista Carrasco - Director General (29/09/2026 11:48 AST)
Documento firmado digitalmente, para validar en medio electrónico:
<https://buzon.firmagob.gob.do/inbox/app/ogtic/v/043b471e-8e22-4303-8e27-cdcafb2012f0>