Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

DG-0677-25

Santo Domingo, D.N.
22 de mayo de 2025

Sr. Francisco A. Torres
Superintendente
Superintendencia de Pensiones
Su Despacho. –

Distinguido Sr.:

Respetuosamente, nos dirigimos a usted en atención a su requerimiento marcado con fecha 09/05/2025, donde nos solicitan la asistencia para llevar a cabo el siguiente proceso: **"adquisición de hardware y servicios de ciberseguridad".**

En ese sentido, tenemos a bien comunicarle que luego de analizar su expediente determinamos que su solicitud ha sido aprobada, esta aprobación tiene vigencia hasta el 20 de agosto 2025, según consta en el informe técnico INF-0373/25, el cual se encuentra adjunto.

Con sentimientos de alta estima y consideración, se despide,

Atentamente,

Mario Adames
Elaborado por

Manuel Mayrele
Revisado por

Edgar Batista Carrasco
Aprobado por

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

INF-0373/25

INFORME SOLICITUD DE ASISTENCIA

SUPERINTENDENCIA DE PENSIONES

SIPEN

MAYO 22, 2025.-

GOBIERNO DE LA
REPÚBLICA DOMINICANA
ADMINISTRACIÓN PÚBLICA

ogtic
Oficina Gubernamental de Tecnologías de la Información y Comunicación

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

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 **adquisición de hardware y servicios de ciberseguridad,** 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 ficha técnica

A groso modo se solicita:

- 1 Servicios Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad
  - Monitoreo en tiempo real de la infraestructura crítica de la Superintendencia de Pensiones (SIPEN)
  - Análisis de bitácoras y comportamientos anómalos.
  - Monitoreo en tiempo real de la infraestructura crítica de la Superintendencia de Pensiones (SIPEN)
  - El servicio debe hacer una revisión e interpretación de logs y alarmas
  - El servicio debe hacer una Revisión e interpretación de bloqueos, patrones y alertas
  - El servicio debe proveer apoyo para la mitigación de los eventos de seguridad encontrados.
  - El servicio debe hacer las Actualizaciones del Contenido de Seguridad
  - La solución debe alertar automáticamente sobre las actividades inusuales y anómalas en la red
  - El servicio debe hacer un monitoreo de las vulnerabilidades.

GOBIERNO DE LA REPÚBLICA DOMINICANA
ADMINISTRACIÓN PÚBLICA

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- El servicio debe hacer una notificación temprana de las vulnerabilidades detectadas
- El servicio debe hacer una Detección y Notificación de eventos de seguridad
- El servicio debe hacer una Detección, Análisis y Notificación de Comportamiento Anómalo
- El servicio debe hacer un escalamiento de solicitudes de remediaciones
- El servicio debe hacer un Monitoreo de Perímetro de Seguridad
- El servicio debe hacer un Historial de amenazas de seguridad experimentadas por la institución
- El servicio debe hacer un análisis de aplicaciones publicadas en tiendas oficiales
- El servicio debe hacer un monitoreo de cuentas en redes sociales.
- El servicio debe hacer una revisión de los dominios propiedad de la institución.
- El servicio debe hacer una Investigación mediante el uso de inteligencia derivada de la información recogida y proporcionada por fuentes humanas
- El servicio debe hacer un monitoreo constante de las redes sociales populares.
- El servicio debe identificar filtraciones en foros, en red abierta y Darknet (Red Onion/ToR), Deep Web.
- El servicio deberá identificar la venta de información confidencial del cliente en mercados negros y abiertos.
- El servicio debe hacer una investigación e identificar y dar seguimiento de actividad en grupos de hackers y del cibercrimen que puedan representar una amenaza a la institución.
- El servicio deberá identificar en foros y comunidades tanto de redes abiertas como de la Red Onion/ToR donde se planeen y difundan campañas de ataques informáticos que pudieran representar un riesgo.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Apoyar la madurez del sistema de gestión de seguridad de la información (SGSI) institucional.
- El servicio deberá informar mediante Alertas Oportunas sobre amenazas identificadas que puedan considerarse relevantes de acuerdo con la Definición de Contexto
- El servicio deberá informar mediante Alertas de Protección de marca la detección de incidentes potenciales.
- Monitoreo y Análisis de Amenazas. La solución debe realizar una vigilancia continua de fuentes de inteligencia de amenazas globales para identificar patrones, técnicas y tácticas utilizadas por actores maliciosos, lo que nos permite anticiparnos a posibles ataques dirigidos contra la infraestructura de la institución.
- El servicio debe proveer indicadores de compromiso específicos, como direcciones IP, hashes de archivos y dominios maliciosos, que pueden utilizar para reforzar sus defensas y prevenir infiltraciones.
- El servicio debe realizar informes Personalizados de Amenazas. Generar informes detallados sobre las amenazas más relevantes, incluyendo recomendaciones de mitigación y estrategias de defensa proactiva.
- El servicio debe de realizar un análisis profundo del contexto detrás de las amenazas, evaluando el riesgo específico para cada cliente en función de su industria, geografía y perfil de seguridad.
- El servicio debe emitir alertas en tiempo real sobre nuevas amenazas emergentes, permitiendo a la institución responder rápidamente a cualquier riesgo antes de que pueda causar daño.
- El servicio o solución debe proporcionar una orientación estratégica para que la institución ajuste sus políticas de seguridad y fortalezca sus controles en respuesta a las amenazas identificadas.
- El servicio debe de proporcionar 2 ejercicios de Breach Attack Simulation al año como también dos pruebas de penetración
- El servicio debe de proporcionar informes ejecutivos y presentados con el comportamiento del servicio.
- El servicio debe de proporcionar boletines semanales.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- El servicio debe de proporcionar informes forenses en caso de incidentes
- Gestión de incidentes cibernéticos.
- Apoyo técnico remoto y/o presencial ante incidencias de seguridad que lo ameriten.
- Reportes de incidencias y postura de seguridad de los servicios críticos con periodicidad mensual y en demanda. También se deben generar reportes posteriores a una falla o incidente crítico de ciberseguridad.
- Suscripción del servicio de Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad 24/7 por un (1) año.
- Se debe contemplar la capacitación necesaria para el personal técnico de la Superintendencia de Pensiones (SIPEN)
- Monitoreo Continuo 24/7/365
- Vigilancia ininterrumpida de los eventos de seguridad generados por dispositivos y sistemas críticos: servidores, firewalls, endpoints, bases de datos, aplicaciones, dispositivos móviles, redes y servicios en la nube.
- Revisión y análisis continuo de logs y alertas
- Correlación y Análisis de Eventos
- Uso de motores de correlación que combinan múltiples fuentes de datos (logs, flujos de red, comportamiento de usuarios) para identificar patrones anómalos o actividades maliciosas.
- Integración con bases de datos de inteligencia de amenazas (Threat Intelligence) para enriquecer el análisis.
- Informes y Reportes Ejecutivos
- Gestión y Respuesta a Incidentes de Seguridad, Procedimientos de respuesta ante incidentes
- Contención, análisis forense inicial, mitigación y recomendaciones de recuperación.
- Notificación inmediata de incidentes críticos y coordinación con el equipo interno de TI.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Documentación técnica
  - Evidencia de Experiencias en al menos tres (3) proyectos de naturaleza similar de igual complejidad y/o dimensiones con en los últimos tres (3) años. Deberá suministrar contratos notarizados, órdenes de compras o facturas de clientes para avalar dichas experiencias.
  - Evidencia que demuestre que cuentan con al menos 5 años de experiencia ofreciendo servicio de SOC a proyecto similares en la Republica Dominicana.
  - La empresa debe de contar con al menos 3 servicios redundantes en el territorio Latinoamericano.
  - Proveedor debe asignar un Project Manager y entregar cronograma y plan de implementación.
  - La institución llevara a cabo una visita de inspección obligatoria al Centro de Operaciones de Seguridad local de los proveedores a los fines de verificar la autenticidad de la información proporcionada.
  - El oferente debe de contar con las certificaciones ISO27001, ISO9001, SOC2 tipo 2
  - Certificaciones internacionales del personal requerido:
    - CISSP Certified Information Systems Security Professional
    - CISA (Certified Information Systems Auditor)
    - CISM (Certified Information Security Manager)
    - CEH (Certified Ethical Hacker)
    - ITIL v4
    - ISO/IEC 27001 Lead Auditor
    - PMP

- 1 Servicios Web Aplication Firewall WAF
  - Licencia para Sistema para Firewall de Aplicaciones Web Empresarial Gestionado.
    - Solución Avanzada de protección de Dominios y Aplicativos Web (DDoS/WAF/SSL) y Aceleración (CDN)
    - DNS queries 30(MM)

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- CDN 30(MM) Request
- WAF - Enterprise 0.5 TB
- Advanced DDoS
- 2 Primary Domains – sipen.gov.do sipen.gob.do
- 2 Advanced Certificate Manager
- Plan Basic Success Offering
- Zero Trust Network: 30 Usuarios
- Soporte Básico /soporte técnico de una persona real 24x7
- 12 meses de Soporte
- Prioridad de tráfico en la red
- Los que pueden ser utilizados para la auditoria ISO 27001
- Integración con SOC Y SIEM

- A continuación, se listan las características que se consideran necesarias para los servicios de protección y aceleración de aplicaciones web.
  - Requerimientos de gestión:
    - Proveer acceso a la consola de administración de la red de entrega de contenidos y medidas de seguridad por medio de Internet.
    - Administración Multi -usuario con roles y diferentes niveles de permisos de administración y usuarios de solo lectura (Read-Only)
    - Contar con una red global inteligente que permita la optimización del Trafico IP, dicha optimización debe enrutarse de forma automática, tomando como base la ubicación del origen de la petición a través de la infraestructura tecnológica del proveedor. Lo anterior, con el objetivo de distribuir el tráfico para reducir la latencia y mejorar el rendimiento de las solicitudes.
    - Contar con al menos 275 Puntos de Presencia (PoPs) globalmente, 50 en Latinoamérica - (al menos uno (1) POP en República Dominicana)

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Limpieza de todo el caché almacenado en la red de entrega de contenidos, o depuración de un archivo específico en menos de 30 segundos por medio de consola GUI o por medio de API.
- Soporte de uso de API para administración de configuraciones.
- Proveer rangos de direccionamiento IP priorizados (enrutamiento y protección) para garantizar la máxima velocidad y disponibilidad.
- Resguardo de datos históricos (logs) de al menos 30 días.
- Capacidad de integración con herramientas de colección de eventos (SIEM).
- Capacidad de enviar los Logs a un storage en la nube (log push) en tiempo real.
- Detección y bloqueo de ataques de denegación de servicio con estas características:
- Entrega de tráfico legítimo, inspeccionado por la red de entrega de contenidos y descartar el tráfico ilegitimo.
- Detección automática y denegación de ataques de capa 3 y capa 4 (TCP SYN, UDP e ICMP) por medio de la infraestructura del proveedor de red de entrega de contenidos.
- Definición y configuración de varios niveles de seguridad con la capacidad de que el cliente pueda incrementar el nivel de seguridad en cualquier momento.
- Permitir la carga de certificado SSL propiedad del cliente para cada dominio.
- Asignación de un certificado wildcard SSL por parte del proveedor de la red de entrega de contenidos. Dicho certificado debe soportar cifrado SSL/TLS 1.2 y 1.3, así como también, compatibilidad con navegadores en las comunicaciones cifradas.
- Generación de reportes en línea que incluyan: análisis de tráfico, solicitudes web y amenazas detectadas hacia los

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

distintos si os web publicados de los dominios del cliente con una periodicidad mínima de recolección de datos de 1 minuto.

- Admisión de conexiones entrantes de direcciones IP de pool IPv4 e IPv6 sin necesitar configuraciones adicionales en la infraestructura tecnológica del cliente mediante el uso de una pasarela IPv6 (IPv6 Gateway)
- Cobertura automática para utilizar los protocolos TLS 1.3, HTTP/2 y Brotli
- Proporcionar un protocolo persistente WebSockets que permita reducir la latencia de comunicación entre el cliente y el servidor.
- Protección contra ataques DDoS: la solución ofrecerá mitigación contra ataques DDoS de cualquier tipo y tamaño sin límites.
- El WAF debe incluir las reglas de seguridad de las 10 principales vulnerabilidades identificadas por el proyecto de seguridad de aplicaciones web abiertas (OWASP).
- Capacidad de integración de aplicaciones de desarrollo ágil por medio de APIs.
- Despliegue de inteligencia para identificar nuevas amenazas, la cual debe extenderse de manera automática (Base de reputación de IP) en la red de entrega de contenidos, así
- Personalización de páginas web para el despliegue de mensajes de advertencia y de error.
- Creación de reglas de seguridad personalizadas para los distintos si os web publicados de los dominios del Cliente. Dichas reglas deben permitir el bloqueo automático o manual con las siguientes opciones:
    - Challenge
    - Reputación de direccionamiento IP.
    - Direccionamiento IP.
    - Número de sistema autónomo (ASN).
    - Código de país. - User Agent

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- SLA:
  - Acuerdo de nivel de servicio del 100%. En caso de tiempo de inactividad, el oferente emitirá un crédito de servicio contra la tarifa mensual, en proporción a la interrupción respectiva y la proporción de clientes afectados.
  - Servicio de soporte técnico con el fabricante para el servicio, que incluya como mínimo lo siguiente:
    - Horario de atención: 24 horas del día, 7 días de la semana, los 365 días del año, sin ninguna excepción.
    - Ningún límite en la cantidad de apertura de casos, incidentes, solicitudes, requerimientos, consultas, soporte técnico, resolución de problemas.
    - Recepción de alertas, mensajes o noticias sobre las actualizaciones del servicio durante el periodo contratado.
  - Soporte telefónico directo con los ingenieros de soporte del servicio.

- 1 Herramienta de Administración de parches Centralizada para 200 computadoras y 20 servidores Perpetua – 1 año de Mantenimiento y Soporte (AMS).
  - Solución de administración unificada de endpoints (UEM) que ayuda a administrar servidores, computadoras portátiles, computadoras de escritorio, smartphones y tabletas desde una ubicación central. Es una versión moderna de la administración de escritorio que se puede escalar según las necesidades de la organización.
  - Automatice sus rutinas regulares de administración de escritorio como la instalación de parches, distribución de software, administración de activos TI, administración de licencias de software, monitoreo de estadísticas de uso de software, administración de uso de dispositivos USB, asumir control de escritorios remotos y más. Es compatible con sistemas operativos Windows, Mac y Linux.
  - Administre sus dispositivos móviles para desplegar perfiles y políticas, configurar dispositivos para Wifi, VPN, cuentas de email,

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

etc., aplicar restricciones para el uso de la cámara, explorador, etc., y asegurar sus dispositivos para habilitar contraseñas, lock/wipe remoto, etc. Administre todos sus smartphones y tabletas iOS, Android y Windows.

- Esta solución / herramienta debe ofrece seguridad y administración integrales de puntos finales para la institución que se compone de lo siguiente:
  - Gestión de Parches
  - Despliegue de software y Gestión de Aplicaciones
  - Gestión de activos
  - Administración remota del Sistema
  - Administración de dispositivos móviles
  - Administración de aplicaciones móviles
  - Gestión Moderna
  - Imágenes e implementación del sistema operativo
  - Gestión de configuraciones
- A continuación, se detallan los requerimientos para cada bien y servicio requerido:
  - Automatizar el despliegue de parches relacionados con el sistema operativo y otras aplicaciones externas, en ambiente Linux, Mac y Windows.
  - Facilitar la distribución de software para instalar y desinstalar software con plantillas integradas para creación de paquetes.
  - Facilitar el uso de escritorio remoto con colaboración multi-usuario, transferencia de archivos, grabación de video y audio, chat.
  - Inventariar activos TI, medición de software, administrar licencias de software, software prohibido.
  - Creación de configuraciones predefinidas que incluyan administración de energía, administración de dispositivos USB, políticas de seguridad, carpetas compartidas, configuración de pantalla, etc.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Despliegue de paquetes de servicios faltantes de SO y aplicaciones.
- Facilitar la creación de Reportes con visión rápida y completa de la infraestructura de Active Directory.
- Administración de roles con privilegios selectivos y delegación de roles a usuarios para una administración efectiva
- Implementación de sistemas operativos en modo fuera de línea y en línea.
- Restringir y controlar la utilización de los dispositivos USB en la red tanto a nivel de usuario como de computadora.
- Facilitar la administración de energía efectiva mediante la aplicación de esquemas de energía, apagar computadoras inactivas y obtener informe de tiempo de actividad del sistema.
- Administración de dispositivos desktop y servidores, mediante una aplicación móvil.
- Crear Service Portal que permite publicar software en los usuarios/equipos de destino de forma que el usuario pueda autoabastecerse
- Permita administrar escritorios que están distribuidos geográficamente desde un punto central. Esto incluye computadoras que se encuentran en una LAN, WAN y usuarios móviles también.
- Provea Autenticación de Doble Factor para Administradores en base a RBAC
- Permita oscurecer la pantalla del usuario durante la resolución de problemas de forma remota.
- Haga uso de protocolos de codificación del estándar de cifrado avanzado (AES) de 128 bits durante las operaciones de acceso remoto.
- Capturar automáticamente la imagen de un equipo, encendido o apagado, utilizando técnicas inteligentes de creación imágenes en línea y fuera de línea. Almacene las imágenes en un repositorio

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

centralizado (recurso de red) e implemente el sistema operativo desde cualquier lugar.

- Provea informes de AD: Cuentas de Usuarios, cuentas creadas- modificadas recientemente, cuentas de usuarios en varios grupos, cuentas que no caducan, no utilizadas.
- Provea informes de: Todos los equipos (servidores y estaciones de trabajo) descubiertos en la infraestructura, agregados - modificadas – deshabilitadas recientemente.
- Sistemas operativos compatibles
  - Windows, Mac, Linux, Chrome OS, tvOS, Android, iOS, Windows Phone
- Gestión de Parches
  - Soporte para parches de Microsoft, Mac y Linux, Soporte de parche extendido para aplicaciones de terceros, despliegue de parches automatizado, reinicio y acciones personalizables, compatibilidad con actualizaciones de definiciones de antivirus capacidad para probar y aprobar parches antes de la implementación viabilidad para definir y configurar la política de salud del sistema, capacidad de deshabilitar las actualizaciones automáticas, rechazar parches, actualizaciones del sistema operativo para dispositivos móviles
- Despliegue de Software y Aplicaciones
  - Instalar software basado en MSI/EXE/ISS/Script, admite la creación de paquetes basados en plantillas, actualización automática de las plantillas cuando esté disponible la última versión, ejecutar actividades previas y posteriores a la implementación, despliegue programado, portal de autoservicio para Windows Portal de autoservicio para Mac, instalación de aplicaciones de forma silenciosa o desatendida, desinstalar aplicaciones, administre aplicaciones móviles internas/empresariales desde: VPP de Apple (ABM), Google Play para el trabajo, tienda virtual de

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Chrome, tienda Windows para empresas, desinstalar aplicaciones silenciosamente

- Bloqueo de aplicaciones
- Quiosco multiplicación
- Seguimiento de inventario y gestión de activos
  - Información completa sobre el inventario de hardware y software, prohibición de software con política de desinstalación automática, medición de software, gestión de licencias de software historial de auditoría de software prohibido, bloquear ejecutables para Windows, activar alertas en caso de cualquier cambio de hardware/software, seguimiento de ubicación geográfica, adquisición de historial de ubicación, geocercas, Soporte de modo perdido y bloqueo remoto, borrado de datos corporativos y borrado completo de datos, detectar y eliminar dispositivos con jailbreak y rooteados, compatibilidad con el contenedor Samsung Knox, contenedorización para dispositivos que no son de Samsung, filtrado de contenido web, protocolo simple de inscripción de certificados (SCEP) para validar colectivamente el acceso al dispositivo
- Imágenes e implementación del sistema operativo
  - imágenes en línea, imágenes fuera de línea, creación de medios de arranque, personalización de la implementación de imágenes mediante la creación de plantillas, gestión de Drivers, Configuración del repositorio de controladores
- Gestión moderna
  - Administración moderna para dispositivos con Windows 10, Gestión moderna para Mac
- Control remoto
  - Control remoto compatible con HIPAA y PCI, Grabación de pantalla, Transferir archivos durante la sesión remota, Llamada de voz y video integrada, Chat, © 2022 Zoho Corp.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

All rights reserved, Compatibilidad con varios monitores, Configuración de sesión inactiva, Bloquear el teclado y el mouse de los usuarios finales, Controlar el rendimiento ajustando la calidad del color y FPS, Oscurecer la pantalla de los usuarios finales para garantizar la confidencialidad, Colaboración multiusuario, Uso de protocolos de cifrado de estándares de cifrado, avanzado (AES) de 128 bits, Control Remoto para dispositivos móviles

- Herramientas e informes
  - Wake on LAN, Apagado/reinicio remoto, Administrador del sistema, Herramientas de administración de Windows como limpieza de disco y desfragmentador de disco, Publicación de anuncios, Informes de inicio de sesión de usuario con historial de inicio de sesión, Informes de directorio activo, Informes de administración de energía, Informes de configuración, Informes de parches, Informes USB Informes de activos, Informes MDM, informes personalizados.
- Configuraciones y gestión de perfiles
  - Gestión del ciclo de vida de la configuración, Plantillas de configuración predefinidas, Gestión de la configuración, Ejecución de script personalizado, Gestión de seguridad de dispositivos USB, Gestión local de usuarios y grupos, Agrupar equipos en función de un rango de IP, Agrupación dinámica de equipos en función de un criterio predefinido, Gestión de conexión WiFi, Gestión de Firewall, Mapeo de unidades, Gestión de permisos, Gestión de impresoras, Distribución de certificados, Administración de energía, Gestión de políticas de seguridad, Gestión de MS Office, Gestión de Linux, Gestión de pantalla, Gestión de seguridad de Endpoint, Restricciones para dispositivos móviles (Cámara, Bluetooth, Safari, etc.), Restringir instalaciones de aplicaciones, Gestión de iCloud, sincronización de

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

documentos, copia de seguridad, etc. Aplicación de contraseña para iTunes, Configuración VPN, VPN por aplicación, Servidor de Failover

- Gestión de correo electrónico
  - Configurar cuentas de correo electrónico empresariales, Microsoft Exchange ActiveSync, configuración de Office 365, Acceso condicional a Exchange.
- Gestión de contenido
  - Configurar cuentas de correo electrónico empresariales, Visor de documentos, Copiar/pegar restricciones de Workspace a aplicaciones personales.
- Inscripción de dispositivos
  - Auto inscripción, Inscripción a través de Active Directory, Inscripción por SMS, Inscripción por correo electrónico, Inscripción masiva, Apple (ABM), Apple Configurator, Inscripción NFC, Inscripción de token, EMM (QR), Inscripción de Samsung Knox, Inscripción de Android Zero Touch, Inscripción de Windows ICD, Inscripción de Windows Azure AD y AutoPilot, Herramienta de activación por cable de BlackBerry, Autenticación de dispositivos multifactor.

- General
  - Acceso basado en la web a la interfaz de usuario, Gestión de oficinas remotas, Servidor de distribución para optimización de ancho de banda, Gestión de dispositivos de usuarios itinerantes, Servidor de Failover, Base de datos incorporada, Servidor de puerta de enlace segura, Administrar Sistemas en LAN y WAN, Copia de seguridad y recuperación de la base de datos, Autenticación de directorio activo, Administración basada en roles y soporte multitécnico, Instalación de agente remoto, Actualización automática de agentes, Reintentar la instalación del agente, Personalización de marca del agente, Autenticación multifactor, Administrador de Credenciales, Soporte de VMware, Alertas por correo electrónico, Soporte multilenguaje.

ogtic
Oficina Gubernamental de Tecnologías de la Información y Comunicación

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Seguridad (Endpoint security add-on)
  - Escaneo y evaluación de vulnerabilidades de SO, vulnerabilidades de terceros y de día cero, Detección de errores de configuración del sistema, Detección de software de alto riesgo, Fortalecimiento de servidores web, Auditoria de antivirus, Auditoria de puertos
- Gestión de Dispositivos
  - Restricción de dispositivos de almacenamiento extraíbles, USB, CD-ROM, Impresoras, Adaptadores de red, etc.) para Windows y MAC, Permitir dispositivos de confianza, Acceso temporal de dispositivos, Control de transferencia de archivos.
- Control de Aplicaciones
  - Control mediante listas blancas, Bloqueo mediante listas negras, Gestión de privilegios de aplicaciones en Endpoints, Detección y eliminación de privilegios de Administrador, Acceso temporal o programado a aplicaciones con acceso privilegiado.
- Gestión de Navegadores
  - Restricción de uso del navegador, Centralizar las configuraciones de seguridad en los navegadores (Edge, Chrome y Firefox), Gestión de complementos o extensiones, Gestión de cumplimiento de seguridad de los navegadores, Gestión de Java de aplicaciones Web, Filtrado Web, Restricción de descargas de sitios no autorizados, Redirección de sitios web a navegadores determinados.
- BitLocker
  - Gestión centralizada de BitLocker, Despliegue de políticas granulares, Monitoreo de estado de cifrado Compatibilidad con TPM y métodos de cifrado tradicionales, Autenticación multifactor, Configuración de la clave de recuperación
- Integración
  - Integración con Directorio Activo, Integración con Azure AD, Integración con el servicio de asistencia de TI para ayudarlo a realizar operaciones completas basadas en el marco ITIL, Integración con la plataforma de análisis

ogtic
Oficina Gubernamental de Tecnologías de la Información y Comunicación

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Soporte e Implementación
  - Soporte de chat en vivo, soporte de correo, Asistencia telefónica 24 horas al día, 5 días a la semana Formación sobre el producto en sitio por un formador autorizado, Recursos de formación en línea Comunidades de usuarios en línea y foros de discusión, Actualizaciones periódicas de productos a través de boletines.

- 1 Firewall de última generación con Bundle de 3 Años (NGFW).
  - Interfaces de Red
  - 22 puertos GE RJ45
  - 2 puertos RJ45 WAN
  - 1 puerto DMZ
  - 1 puerto de administración
  - 2 puertos HA
  - 16 puertos de conmutación
  - 4 puertos SFP
  - 2 puertos 10 GE SFP+
  - Capacidades de Seguridad
    - Throughput de Firewall (64/512/1518 byte, UDP): Hasta 10/18/20 Gbps.
    - Throughput de IPS: Hasta 2.6 Gbps.
    - Throughput de NGFW (Firewall de Próxima Generación): Hasta 1.6 Gbps.
    - Throughput de Protección contra Amenazas: Hasta 1 Gbps.
  - Capacidades de VPN:
    - Throughput de SSL-VPN: Hasta 1 Gbps.
    - Throughput de IPSec VPN: Hasta 11.5 Gbps.
    - Máximo de usuarios concurrentes SSL-VPN: 500.
  - Conectividad y Administración:
    - Compatibilidad con IPv4 e IPv6.
    - Administración mediante GUI web y CLI vía SSH/Telnet.
  - Almacenamiento:
    - Almacenamiento a bordo de 1X480 GB SSD
  - Características del hardware:

SUPERINTENDENCIA DE PENSIONES

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Doble fuente de alimentación
- La redundancia de la fuente de alimentación es esencial para el funcionamiento de redes de misión crítica.

- 1 Herramienta de monitoreo y auditoria
  - Herramienta de monitoreo y auditoria edición profesional para 2 dominios (Domain Controllers) 20 servidores (Windows server) y 200 PC (Workstation) suscripción anual y soporte por un año
  - Herramienta de monitoreo y auditoria que suministra una imagen clara de todos los cambios hechos a sus recursos de AD, incluidos objetos de AD y sus atributos, políticas de grupos y más.
  - Las auditorías de AD ayudan a detectar y responder a amenazas internas, abusos de privilegios y otros indicadores de compromisos y en pocas palabras, fortalece la postura de seguridad de su organización.
  - Le permitirá obtener información sobre quién ha cambiado qué archivo o carpeta, cuándo y desde dónde, en sus sistemas de archivos de Windows, NetApp, EMC, Synology, Huawei e Hitachi.
  - Podrá monitorear los servidores Windows con informes y alertas en tiempo real para vigilar de cerca la actividad en su red de Windows. Utilice gráficos e informes intuitivos para saber quién hizo qué, cuándo y dónde.
  - Auditoría de Active Directory
    - Debe tener auditoría de inicio de sesión, obteniendo información sobre toda la actividad de inicio de sesión, desde errores de inicio de sesión hasta el historial de inicio de sesión, en controladores de dominio, servidores Windows y estaciones de trabajo.
    - Debe realizar análisis de bloqueo de cuentas, mostrando notificaciones de bloqueo y enviando información sobre el origen del error de autenticación componentes de Windows, como servicios de Windows, tareas programadas, asignaciones de unidades de red, etc.
    - Debe realizar auditoría de cambios de objetos obteniendo información sobre los cambios en objetos de AD, como usuarios,

SUPERINTENDENCIA DE PENSIONES
Contraloría

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

equipos, grupos, unidades organizativas (OU), DNS, esquema, sitios, objetos PSO, etc.

- Debe realizar auditoría en los cambios de directiva de grupo, obteniendo información sobre los cambios en objetos de directiva de grupo (GPO) y su configuración, como la directiva de contraseñas, la directiva de bloqueo de cuentas, etc.
- Debe realizar auditoría de cambios de permisos, obteniendo información sobre los cambios en los permisos de AD en unidades organizativas, grupos, usuarios, equipos, esquema, configuración, DNS y mucho más.
- Debe realizar supervisión de usuarios privilegiados, obteniendo información sobre todas las actividades realizadas por los usuarios con privilegios en el dominio.

- Auditoría de Azure AD
  - Debe realizar auditoría de inicio de sesión, obteniendo información sobre todos los inicios de sesión correctos y fallidos.
  - Debe realizar auditoría de cambios de usuarios, grupos, equipos, GPO y dispositivos, obteniendo información sobre de todas las acciones de administración de usuarios y dispositivos.
  - Debe obtener información sobre los cambios de pertenencia a grupos, y grupos dinámicos, y la asignación y eliminación de roles a los usuarios.
  - Debe obtener información sobre las aplicaciones que se han agregado, actualizado y eliminado, y el consentimiento otorgado a las API.
  - Debe realizar auditoría de cambio de licencia, obteniendo información sobre los cambios en las licencias de usuarios y grupos.
  - Debe tener una vista correlacionada de información contextual como el nombre distintivo, el SID y el GUID locales de un usuario.
  - Debe auditar los accesos a archivos y los cambios de permisos en los dispositivos Huawei OceanStor Dorado All-Flash Storage y OceanStor Hybrid Flash Storage.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Debe contar con informes de detección de riesgos que brindan información sobre los intentos de inicio de sesión riesgosos en Azure AD.

- Auditoría del servidor de archivos
  - Debe realizar auditoría de acceso a archivos, obteniendo información sobre archivos de lectura, creación, modificación, eliminación, cambio de nombre, movimiento y otras acciones.
  - Debe realizar auditoría de intentos fallidos de archivo, obteniendo información sobre los intentos fallidos de leer, escribir y eliminar archivos.
  - Debe realizar auditoría de cambio de permisos de archivo, obteniendo información sobre los cambios de archivo DACL y SACL.
  - La aplicación debe registrar cambios y eliminaciones de permisos compartidos en la auditoría de NetApp.
  - Debe auditar accesos, modificaciones y eliminaciones de archivos en sus sistemas de archivos de Windows de Amazon FSx.
  - La aplicación debe soportar las siguientes plataformas: Windows File Server 2003 y superior Dell VNX, VNXe, Celerra, Unity e Isilon Synology DSM 5.0 y superior NetApp ONTAP 7.2 y superior para archivadores NetApp ONTAP 8.2.1 y superior para clústeres Hitachi NAS 13.2 y superior Huawei OceanStor V5 series y Sistemas de almacenamiento.
- Auditoría de Windows Server y estación de trabajo
  - Debe realizar auditoría de inicio de sesión remoto, obteniendo
  - información sobre las conexiones de escritorio remoto y los inicios de sesión remotos que se producen a través de servidores de puerta de enlace de Escritorio remoto (RDG) y servidores de directivas de red (NPS) de RADIUS.
  - Debe realizar auditoría del Servicio de federación de AD (AD FS), obteniendo información sobre los inicios de sesión de AD FS correctos y fallidos.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Debe generar seguimiento de horas de trabajo del usuario, obteniendo información sobre el tiempo de inactividad, activo y de inactividad que pasan los empleados en sus estaciones de trabajo.
- Debe realizar auditoría de cambio de objeto local, obteniendo información sobre las acciones de administración de usuarios y grupos locales.
- Debe realizar supervisión de la integridad de los archivos, obteniendo información sobre los cambios en el sistema, el programa y otros archivos locales críticos.
- Debe realizar auditoría de cambio de directiva de seguridad local, obteniendo información sobre los cambios en la política de seguridad local.
- Debe realizar auditoría de impresoras y almacenamiento extraíble, obteniendo información sobre el uso y la actividad de archivos en impresoras y dispositivos de almacenamientos extraíbles, como USB, discos duros externos y más.
- Debe realizar auditoría procesos, obteniendo información sobre las tareas programadas que se han creado, eliminado o modificado, y los procesos que se han iniciado o detenido.
- Debe realizar auditoría LAPS, obteniendo información sobre quién está viendo o modificando las credenciales de administrador DA.
- Debe realizar auditoría de PowerShell Obtener información sobre los procesos de PowerShell que se ejecutan en servidores Windows, junto con los comandos ejecutados en ellos.

- Funcionalidades clave
  - La solución debe realizar análisis del comportamiento del usuario (UBA), aprovechando las capacidades de aprendizaje automático de para establecer patrones de actividad y detectar anomalías, como un volumen inusual de errores de inicio de sesión, inicios de sesión en servidores no consultados anteriormente, entre otros

SUPERINTENDENCIA DE PENSIONES CONTRALORÍA

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- La solución debe generar alertas en tiempo real, enviando notificaciones por correo electrónico y SMS sobre actividades críticas, como cuando un usuario se agrega a grupos privilegiados o confidenciales.
- La solución debe contar con umbrales de alerta, los cuales pueden ser definidos basados en el volumen, el tiempo y otros criterios para detectar actividades sospechosas como el acceso masivo a archivos.
- La solución debe contar con respuesta a incidentes ejecutando scripts para automatizar las acciones de respuesta, como apagar un dispositivo o deshabilitar una cuenta una vez que se activa una alerta.
- La solución debe poder generar informes para auditorías, obteniendo una pista de auditoría completa de quién hizo qué, cuándo y desde dónde, con solo unos pocos clics y cumpla las normativas de SOX, HIPAA, PCI DSS, FISMA, GLBA, GDPR y Requisitos ISO 27001.
- La solución debe permitir la personalización de informes, creando informes para satisfacer necesidades empresariales específicas.
- La solución debe permitir búsqueda rápida en informes, realizando rastreo rápido de la información específica contenida en los informes.
- La solución debe permitir una representación visual de los datos de auditoría.
- La solución debe permitir exportación de informes a múltiples formatos como PDF, XLS, CSV y HTML.
- La solución debe permitir la generación automatizada de informes en intervalos de tiempo definidos por el usuario.
- La solución debe permitir la entrega automatizada por correo electrónico de informes a direcciones de correo electrónico especificadas por el usuario.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- La solución debe permitir la retención de registros a largo plazo, conservando los datos de auditoría de forma segura durante el tiempo que desee.
- La solución debe permitir integración con una solución de SIEM, reenviando los datos de auditoría a los servidores Syslog y otras soluciones SIEM.
- La solución debe permitir reducción de ruido, excluyendo los datos que son irrelevantes para las auditorías basadas en el usuario, el tipo de archivo y otros criterios.
- La solución debe acceder a través de la web.
- La solución debe permitir el acceso basado en roles, concediendo a diferentes usuarios diferentes niveles de acceso al producto.
- La solución debe permitir la recopilación de datos de auditoría sin agente.

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 20 de agosto 2025.

Mario Adames
Encargado Departamento Asistencia Técnica Especializada
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

SUPERINTENDENCIA DE PENSIONES CONTRALORÍA