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

INF-0951/26

INFORME SOLICITUD DE ASISTENCIA

FONDO PATRIMONIAL DE LAS EMPRESAS REFORMADAS

FONPER

AGOSTO 31, 2026.-

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 y renovación de licencias y servicios tecnológicos para el fortalecimiento de la seguridad y continuidad operativa institucional del fonper,** 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 pliego de condiciones

A groso modo se solicita:

- **1 Una (1) Licencia de Backup, Recuperación Ante Desastres.**
  - Incluir servicio de Business Continuity & Disaster Recovery (BCDR) a 12 meses, Infraestructura híbrida (Local + Nube) Almacenamiento con 4TB local + 4TB en la nube (Cloud S5).
  - Respaldo automático desde cada 5 minutos, con verificación local (Local Verification) de la integridad y salud del sistema de archivos.
  - Recuperación ante desastres con restauración rápida, incluyendo Bare Metal Restore (BMR) independiente de la marca o modelo del hardware.
  - Virtualización instantánea de servidores físicos y virtuales, laptops y workstations, tanto local como en la nube, sin depender de infraestructura adicional del cliente.
  - Protección integrada contra ransomware.
  - Solución única e integral, gestionada bajo un mismo proveedor y panel de control, sin intervención de terceros aplicativos o plataformas adicionales.
  - Verificación automática de cada copia de respaldo mediante Screenshot Verification.

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

- Administración centralizada, con monitoreo de eventos 24/7 y reportes automáticos de fallos, alertas y advertencias.
- Expansión de almacenamiento en línea sin generar tiempo de inactividad (downtime).
- Escalabilidad, adaptable al crecimiento de la infraestructura de la institución.

- **1 Un (1) Servicio de licenciamiento de SentinelOne – Antivirus para Endpoints.**
  - Incluir servicio de Remote Monitoring & Management (RMM) a un año, modalidad con plataforma en la nube (SaaS), con unidad de medida por dispositivo gestionado y cantidad de 100 licencias para monitoreo y soporte manejado de usuarios finales.
  - Detección basada en firmas, heurística y análisis de comportamiento.
  - Análisis de vulnerabilidades y configuración incorrecta.
  - Escaneo en tiempo real y bajo demanda de archivos, procesos y memoria.
  - Manejo de falsos positivos y capacidad de exclusión.
  - Defensa contra Ransomware y Exploits:
  - Módulos específicos para detectar y bloquear el comportamiento de cifrado malicioso.
  - Capacidad de reversión o restauración de archivos afectados por ransomware.
  - Protección contra exploits que buscan aprovechar vulnerabilidades en el software.
  - Control Avanzado de Amenazas (ATC):
  - Monitoreo continuo del comportamiento de procesos y aplicaciones en ejecución.
  - Análisis de patrones de actividad para identificar acciones sospechosas, incluso de
  - amenazas desconocidas.
  - Correlación de eventos para determinar la intención maliciosa.
  - Análisis en Sandbox (Sandboxing):

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

- Capacidad de ejecutar archivos y procesos sospechosos en un entorno virtual aislado
- (sandbox) para observar su comportamiento sin riesgo para el sistema.
- Generación de informes detallados sobre la actividad del archivo en el sandbox.
- Detección y Respuesta en el Punto Final (EDR - Endpoint Detection and Response):
  - Visibilidad profunda de la actividad en los puntos finales.
  - Recopilación y análisis de telemetría para identificar actividades anómalas.
  - Capacidades de investigación y búsqueda de amenazas (threat hunting).
  - Respuesta automatizada o manual a incidentes (aislamiento de dispositivos, terminación de procesos, eliminación de archivos).

- Firewall Bidireccional:
  - Control granular del tráfico de red entrante y saliente en los puntos finales.
  - Reglas configurables por aplicación, puerto e dirección IP.
  - Detección y prevención de intrusiones a nivel de red en el endpoint.
  - Control de Dispositivos y Aplicaciones:
    - Políticas para controlar el acceso a dispositivos USB, Bluetooth y otros periféricos.
    - Restricción o bloqueo del uso de aplicaciones no autorizadas.
    - Control de acceso a recursos compartidos de red.
- Filtrado Web y Protección Anti-Phishing:
  - Filtrado de contenido web basado en categorías.
  - Bloqueo de acceso a sitios web maliciosos conocidos (phishing, malware).
  - Protección contra descargas de archivos peligrosos.
  - Protección de Servidores (Físicos, Virtuales y en la Nube)
- Optimización para Entornos Virtualizados:

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

- Agentes optimizados para hosts y máquinas virtuales para reducir el consumo de recursos.
- Integración con plataformas de virtualización (VMware vSphere, Microsoft Hyper-V, Citrix XenServer, KVM, etc.).
- Seguridad sin agente para máquinas virtuales (cuando sea aplicable).

- Seguridad para Cargas de Trabajo en la Nube:
  - Soporte para plataformas de nube pública (AWS, Azure, GCP) y privada.
  - Protección para instancias de máquinas virtuales y contenedores en la nube.
  - Protección de Servidores de Archivos y Bases de Datos:
  - Análisis en tiempo real de archivos y bases de datos para detectar malware.
  - Prevención de intrusiones y control de acceso a datos sensibles.
  - Protección de Buzones de Correo Electrónico
- Antispam y Antiphishing:
  - Detección avanzada de spam, phishing, spear-phishing y ataques de compromiso de correo electrónico (BEC).
  - Análisis de URL y adjuntos sospechosos
- Detección de Malware en el Correo:
  - Escaneo de adjuntos y enlaces en tiempo real para detectar malware antes de que lleguen al usuario final.
  - Integración con análisis en sandbox para adjuntos desconocidos.
- Protección de Dispositivos Móviles
  - Seguridad Móvil Integral:
    - Protección antivirus y antimalware para dispositivos Android e iOS
    - Anti-phishing y filtrado web para navegación segura.
    - Funcionalidades antirrobo (localización, bloqueo, borrado remoto).
    - Integración con soluciones de gestión de dispositivos móviles (MDM) existentes.
- Consola de Administración Centralizada:

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

  - Gestión Unificada: Una única consola para administrar la seguridad de todos los componentes (endpoints, servidores, móviles, correo).
  - Despliegue Flexible:
    - Disponible como servicio en la nube (SaaS) o como implementación local (on-premise).
  - Interfaz Intuitiva:
    - Interfaz de usuario gráfica, fácil de usar, con paneles de control personalizables y vista de estado general de la seguridad.
- Gestión Basada en Roles:
  - Asignación de permisos y roles a diferentes administradores.
- Creación y Gestión de Políticas:
  - Flexibilidad para crear y aplicar políticas de seguridad a diferentes grupos de usuarios o tipos de dispositivos.
- Herencia de Políticas:
  - Capacidad de heredar políticas para simplificar la configuración.
- Generación de Informes Detallados:
  - Informes sobre amenazas detectadas, estado de la seguridad, cumplimiento de políticas, etc.
- Paneles de Control (Dashboards):
  - Vistas en tiempo real del estado de la seguridad, incidentes y tendencias.
- Registro de Auditoría:
  - Historial de eventos y acciones realizadas en la consola de administración.
- Evaluación de Vulnerabilidades:
  - Identificación de vulnerabilidades en sistemas operativos y aplicaciones de terceros.
- Gestión y Despliegue de Parches:
  - Automatización del proceso de distribución e instalación de parches críticos para reducir la superficie de ataque.
- Cifrado de Disco Completo (FDE):

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

  - Capacidad de cifrar discos duros completos en estaciones de trabajo y portátiles para proteger los datos en caso de pérdida o robo del dispositivo.
- Gestión Centralizada del Cifrado:
  - Administración de claves de cifrado y recuperación.
- Automatización de Tareas:
  - Posibilidad de automatizar escaneos, actualizaciones, respuestas a incidentes y generación de informes.
- Integración con Directorio Activo:
  - Sincronización con Microsoft Active Directory para una gestión de usuarios y grupos simplificada.
- APIs (Application Programming Interfaces):
  - Disponibilidad de APIs para integrar la plataforma con otros sistemas de seguridad o gestión de TI (SIEM, SOAR, etc.).
- Rendimiento Optimizado:
  - La solución debe tener un impacto mínimo en el rendimiento de los puntos finales y servidores.
- Escalabilidad:
  - Capacidad de escalar para proteger un número creciente de dispositivos y usuarios sin degradar el rendimiento.
- Compatibilidad:
  - Soporte para una amplia gama de sistemas operativos (Windows, macOS,Linux, Android, iOS) y entornos de servidor.
- Estabilidad:
  - Solución probada y estable con alta disponibilidad.
- Actualizaciones Continuas:
  - La solución debe proporcionar monitoreo y alertas automatizadas para la gestión de equipos de tecnología reduciendo riesgos internos de seguridad.
  - Debe permitir la integración de scripts para detección temprana de problemas en la infraestructura de TI y minimizar interrupciones o vulnerabilidades.

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

- La solución debe ofrecer compatibilidad con servicios en la nube como Microsoft 365®, para administración de usuarios.
- Debe contar con herramientas de auditoría y reportes que faciliten la verificación del cumplimiento de los requisitos regulatorios.
- Debe incluir a través de scripts automatizados con calendarios monitoreo continuo para detectar y mitigar amenazas antes de que comprometan la infraestructura de TI.
- Debe garantizar la trazabilidad y responsabilidad en la gestión de incidentes de seguridad, asegurando que todas las acciones sean auditables.
- La solución debe proporcionar una visibilidad integral de todos los dispositivos dentro del entorno de TI, incluyendo dispositivos BYOD (Bring Your Own Device) y IoT.
- Debe permitir la detección y el mapeo automático de todos los activos conectados a la red.
- La solución debe contar con capacidades de monitoreo continuo para mantener un inventario actualizado de dispositivos en la organización.
- Debe ofrecer reportes detallados sobre el estado y actividad de los dispositivos para mejorar la gestión de activos y la seguridad de la red.
- La solución debe incluir monitoreo continuo para la detección temprana de vulnerabilidades en el entorno de TI.
- Debe contar con mecanismos automatizados para identificar, priorizar y alertar sobre posibles riesgos de seguridad en tiempo real.
- La solución debe generar alertas críticas cuando se detecten amenazas o incidentes de seguridad que requieran acción inmediata.
- Debe proporcionar herramientas para la remediación eficiente de vulnerabilidades, asegurando una respuesta ágil ante cualquier riesgo identificado.
- La solución debe proporcionar monitoreo continuo para detectar vulnerabilidades de seguridad críticas en tiempo real.

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

- Debe contar con análisis automatizados que identifiquen posibles amenazas antes de que sean explotadas.
- La solución debe permitir la ejecución de acciones correctivas inmediatas para mitigar riesgos y prevenir la explotación de vulnerabilidades.
- Debe ofrecer integración con herramientas de seguridad para aplicar parches, bloquear amenazas y reforzar las medidas de protección automáticamente.
- La solución debe permitir la aplicación automática de actualizaciones y parches de seguridad en tiempo real, evitando retrasos que puedan aumentar la exposición a vulnerabilidades.
- Debe contar con capacidades de programación y despliegue inmediato de parches críticos para minimizar riesgos.
- La solución debe garantizar que las actualizaciones de seguridad sean implementadas sin demoras para reducir la necesidad de remediaciones costosas.
- Debe ofrecer reportes detallados sobre el estado de los parches aplicados y pendientes, asegurando el cumplimiento de las mejores prácticas de ciberseguridad.
- La solución debe proporcionar monitoreo en tiempo real de dispositivos, y sistemas para detectar y abordar posibles problemas antes de que impacten la red.
- Debe contar con capacidades de remediación automatizada para solucionar problemas comunes de manera proactiva, minimizando interrupciones en la operación.
- La solución debe permitir la automatización del parcheo de software en dispositivos y aplicaciones, garantizando que todos los sistemas estén actualizados con las últimas medidas de seguridad.
- La solución debe ofrecer monitoreo y soporte continuo (24/7/365) para mantener en funcionamiento servidores, estaciones de trabajo críticas y otros dispositivos esenciales.

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

- La solución debe permitir la identificación y resolución rápida de problemas en cuanto surjan, minimizando el impacto en las operaciones del negocio.
- Debe garantizar que los incidentes críticos reciban atención prioritaria para reducir tiempos de inactividad y mejorar la continuidad del servicio.
- La solución debe permitir el acceso remoto inmediato a cualquier dispositivo (dentro de la matriz de soporte) desde cualquier ubicación, sin necesidad de intervención in situ.
- Debe incluir funcionalidades avanzadas como ejecución remota de scripts y automatización de tareas, con capacidad para operar fuera del horario laboral si es necesario para evitar interrupciones.
- La solución debe contar con capacidades de remediación automatizada para solucionar problemas recurrentes sin intervención manual.
- Debe permitir la configuración de respuestas automáticas a incidentes específicos, garantizando una resolución eficiente sin afectar la operatividad del negocio.
- Debe permitir la recopilación y análisis de datos para optimizar las inversiones tecnológicas basándose en información precisa.
- Debe capturar información clave sobre hardware, software y licencias, además de rastrear cualquier cambio en los sistemas diariamente.
- La solución debe generar informes claros y personalizados que faciliten la toma de decisiones estratégicas basadas en datos.
- Los informes deben identificar dispositivos con problemas recurrentes, falta de actualizaciones de seguridad o próximos a vencer su garantía, permitiendo la planificación proactiva de mantenimiento y renovación.
- La solución debe contar con medidas de seguridad integradas en todos los niveles para proteger la infraestructura de TI y los dispositivos empresariales.

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

- Debe estar alojada en una plataforma en la nube de clase mundial, como Amazon Cloud, con una infraestructura fortalecida y sometida a pruebas de seguridad continuas para prevenir amenazas externas.
- La solución debe ofrecer autenticación multifactor (MFA) para proteger el acceso a cada cuenta de usuario y prevenir accesos no autorizados.
- Debe incluir controles de seguridad avanzados, como el modo de privacidad, que requiera la aprobación del usuario antes de permitir el acceso remoto a sus dispositivos por parte de un técnico.
- La solución debe proporcionar visibilidad y control centralizados sobre la gestión de TI, abarcando inventario de hardware y software, licenciamiento, monitoreo de eventos y tiempos de respuesta.
- Debe permitir la supervisión del uso de recursos, la gestión del ciclo de vida de los activos para minimizar interrupciones operativas.
- La solución debe permitir la administración centralizada de la infraestructura tecnológica del cliente, servidores, estaciones de trabajo y dispositivos conectados.
- La solución debe ofrecer capacidades de monitoreo remoto en tiempo real para identificar y solucionar problemas antes de que impacten las operaciones del negocio.
- La solución debe proporcionar herramientas avanzadas de supervisión para garantizar la estabilidad de plataforma y las aplicaciones empresariales.
- Debe minimizar el tiempo de inactividad y mejorar la continuidad del negocio mediante la detección automática de fallos y la aplicación de medidas correctivas de manera inmediata.
- La solución debe permitir que los usuarios finales operen sin interrupciones al garantizar la disponibilidad y eficiencia de la infraestructura de TI.
- Debe facilitar a la organización la gestión tecnológica en conjunto con un proveedor de servicios gestionados confiable.

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

- Debe generar alertas inmediatas en cuanto se detecte actividad sospechosa, como el cifrado masivo de archivos por parte de un atacante.
- Debe permitir el aislamiento automático del dispositivo infectado para evitar la propagación del ataque dentro de la red.
- La solución debe ofrecer monitoreo 24/7, servidores, PCs y dispositivos conectados para identificar y corregir problemas antes de que afecten las operaciones.
- La solución debe permitir el monitoreo en tiempo real de dispositivos, aplicaciones y sistemas de la empresa para detectar y abordar problemas antes de que impacten la operación.
- Debe contar con capacidades de remediación proactiva para solucionar fallos comunes antes de que afecten equipos o la productividad de los empleados.
- La solución debe automatizar la aplicación de parches de seguridad en dispositivos y aplicaciones para reducir vulnerabilidades explotadas por ciberdelincuentes.
- Debe garantizar que todos los dispositivos estén actualizados y correctamente configurados para cumplir con los estándares de seguridad.
- La solución debe ofrecer monitoreo y soporte ininterrumpido (24/7/365) para mantener el funcionamiento óptimo de computadoras, servidores, y dispositivos.
- Debe proporcionar alertas y reportes en tiempo real sobre el estado de los activos tecnológicos, asegurando su correcta operación y mantenimiento.
- La solución debe permitir la asistencia remota para cualquier dispositivo desde cualquier ubicación en cuestión de minutos, sin necesidad de intervención en sitio.
- Debe contar con la capacidad de ejecutar scripts y realizar tareas de mantenimiento de manera remota, incluso fuera del horario laboral, para minimizar interrupciones en la operación del negocio.

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

- La solución debe incluir herramientas de remediación automatizada para corregir problemas recurrentes sin intervención manual y sin impacto en las operaciones comerciales.
- Debe permitir la configuración de respuestas automáticas a incidentes específicos, asegurando una resolución eficiente y sin afectar la productividad del negocio.
- La solución debe realizar auditorías exhaustivas de todos los dispositivos y actividades dentro de la red de la organización.
- Debe proporcionar visibilidad completa de los activos de TI, incluyendo hardware, software, información de licencias y cambios en los sistemas en tiempo real.
- La solución debe ofrecer reportes claros y fáciles de entender, alineados con las necesidades del negocio.
- Los informes deben identificar dispositivos con problemas recurrentes, falta de actualizaciones de seguridad o próximos a vencer su garantía, permitiendo una gestión proactiva de los activos tecnológicos.
- La solución debe proporcionar información basada en datos para ayudar a la organización a tomar decisiones estratégicas sobre la adquisición, mantenimiento y renovación de su infraestructura de TI.
- Debe facilitar el análisis del rendimiento de los activos tecnológicos, asegurando su uso eficiente y maximizando su valor para el negocio.
- Debe contar con una infraestructura de nube endurecida y sometida a pruebas de seguridad continuas para garantizar su resistencia a ataques.
- Debe garantizar que solo personal autorizado pueda acceder a dispositivos y datos críticos, minimizando los riesgos de seguridad asociados al acceso remoto.
- Las soluciones que se ofrezcan deben contar con integración nativa, lo que implica que todos los componentes, funciones y módulos de la solución estén diseñados para trabajar de manera conjunta y sin la necesidad de realizar ajustes adicionales o configuraciones complejas.

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

- **1 Una (1) Licencia ScandAll Pro (OCR) Captura de alta calidad y separación de documentos OCR zonal básico**
  - Descripción técnica del ScandAll Pro con el que debe ser compatible la licencia:
    - Página fija
    - Página en blanco
    - Código de barras
    - Código de parche
- **1 Una (1) Licencia de Paper Stream Capture**
  - PRO-APLICACIÓN
    - Compatibilidad con los escáneres institucionales.
    - Compatibilidad con los sistemas operativos utilizados por la institución.
    - Funcionalidades de captura, edición y procesamiento de imágenes.
    - Soporte para OCR, reconocimiento de códigos de barras e indexación de documentos.
    - Compatibilidad con controladores TWAIN, ISIS y Kofax VRS, según versión ofertada.
- **40 Cuarenta (40) Licencias Oracle Database Standard Edition 2 Named User Plus Perpetual.**
  - Descripción:
    - Compatibilidad con la infraestructura tecnológica institucional.
    - Cobertura y alcance del soporte técnico.
    - Acceso a actualizaciones, parches y nuevas versiones durante la vigencia del servicio un (1) año.
    - Soporte y asistencia técnica del fabricante.
- **40 Cuarenta (40) licencias Software Update and License**
  - Support Oracle- Database.
  - 2 Dos (2) Licencia Microsoft Visio 365. Facilitar la elaboración de diagramas de procesos, arquitectura tecnológica y documentación institucional Suscripciones gestionadas bajo la consola administrativa de Microsoft 365, la misma permite trabajar bajo el ecosistema Microsoft. Herramienta destinada a la elaboración de diagramas,

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

flujogramas, mapas de procesos y organigramas, facilitando la documentación, análisis y mejora de los procesos institucionales.

- **1 Una (1) Licencia ALDABA Publicar ofertas de empleo y consultar currículums en forma ilimitada.**
  - Este servicio le permite publicar todas las ofertas de empleo que necesite y hacer consultas abiertas en la base de datos de currículums en forma ilimitada durante el período de tiempo que seleccione. No tiene restricciones en cuanto a la cantidad de ofertas de empleo que puede publicar ni la cantidad de currículums que puede consultar y contactar durante el período de tiempo contratado. Permite el acceso multiusuario de hasta 6 personas e incluye crédito para destacar 1 oferta de empleo por cada mes contratado. Este servicio también incluye reinicios y prórrogas ilimitados durante el período de contratación. Servicio válido para República Dominicana. Suscripción al servicio Aldaba, plataforma digital destinada a la publicación y difusión de vacantes y oportunidades de empleo, facilitando a la institución la divulgación de posiciones disponibles y el acceso de potenciales candidatos a las ofertas laborales.
  - Acceso mediante credenciales individuales para los usuarios autorizados.
  - Compatibilidad con navegadores web actualizados.
  - Disponibilidad del servicio durante el período contratado.
  - Mecanismos adecuados de autenticación y control de acceso.
  - Protección de la información manejada a través de la plataforma.
  - Mantenimiento y actualización de la solución.
  - Atención de incidentes y solicitudes de soporte.
  - Cumplimiento de las condiciones de seguridad y confidencialidad aplicables.
- **2 Dos (2) Licencias Windows Server 2025 Standard – 16 Cores + 2 CALs.**
  - Licencia del sistema operativo servidor de Microsoft diseñada para ambientes físicos o con virtualización ligera.

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

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 noviembre 2026.

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

MF/ma