ENMIENDA NÚM. I PLIEGO DE CONDICIONES

ADQUISICIÓN DE HARDWARE Y SERVICIOS DE CIBERSEGURIDAD PARA SER UTILIZADOS EN LA SUPERINTENDENCIA DE PENSIONES

LICITACIÓN PÚBLICA NACIONAL

SIPEN-CCC-LPN-2025-0001

SUPERINTENDENCIA DE PENSIONES
COMITÉ DE COMPRAS Y CONTRATACIONES

Santo Domingo de Guzmán,
Distrito Nacional
República Dominicana
1ro. de agosto de 2025

ENMIENDA NÚM. I AL PLIEGO DE CONDICIONES

VISTO: El Artículo 107 del Reglamento de Aplicación No. 416-23 de la Ley No. 340-06 sobre Compras y Contrataciones Públicas, que establece que: "*La institución contratante podrá realizar adendas o enmiendas a los pliegos de condiciones mediante acto administrativo motivado, cuando sea necesario adicionar, modificar condiciones o especificaciones que no alteren sustancialmente los términos originales y el objeto del contrato se mantenga inalterado. Podrán ser emitidas en un plazo no más allá de la fecha que signifique el setenta y cinco por ciento (75 %) del plazo previsto para la presentación de las ofertas y deberá modificarse el cronograma de actividades para permitir nuevamente la formulación de preguntas y respuestas sobre los aspectos modificados o añadidos. Las adendas o enmiendas deberán ser publicadas en el Sistema Electrónico de Contrataciones Públicas (SECP) y en el portal de la institución contratante.*"

VISTAS: Las consultas recibidas por los interesados dentro del plazo establecido en el procedimiento de selección, conforme al cronograma publicado en el Sistema Electrónico de Contrataciones Públicas (SECP).

VISTAS: Las recomendaciones dadas por Monitoreo Preventivo de la Dirección General de Contrataciones Públicas (DGCP).

CONSIDERANDO: Que el Pliego de Condiciones original contemplaba el suministro del ítem 3 bajo un modelo de licenciamiento perpetuo, lo cual generaba un costo significativamente elevado en comparación con los precios referenciales del mercado establecidos para un período de suscripción anual. En atención a las consultas recibidas, y con el fin de garantizar la razonabilidad económica, la igualdad de condiciones para los oferentes y la comparabilidad objetiva de las ofertas se considera procedente modificar las especificaciones técnicas del ítem referido, ajustándolo a un modelo de licenciamiento por suscripción anual.

El **Comité de Compras y Contrataciones** de la **Superintendencia de Pensiones**, tiene a bien informar a todos los interesados en participar en el procedimiento de Licitación Pública Nacional de Ref. No. **SIPEN-CCC-LPN-2025-0001**, para la **Adquisición de hardware y servicios de ciberseguridad para ser utilizados en la Superintendencia de Pensiones** que mediante la presente Enmienda se **MODIFICA** el "***Pliego de Condiciones***", el cual se leerá de la forma que se encuentra anexa.

El **numeral 3: Descripción del bien – Ítem 3** de la **Sección I: Informaciones particulares del procedimiento** el cual se leerá de la siguiente manera:

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1

Especificaciones Técnicas:

Para 200 computadoras y 20 servidores **suscripción anual** - 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.

Que automatice las 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.

Que administre los dispositivos móviles para desplegar perfiles y políticas, configurar dispositivos para Wifi, VPN, cuentas de email, etc., aplicar restricciones para el uso de la cámara, explorador, etc., y asegurar sus dispositivos para habilitar contraseñas, lock/wipe remoto, etc. Administrar todos los smartphones y tabletas iOS, Android y Windows.

Esta solución / herramienta debe ofrecer seguridad y administración integral 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.

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1

Especificaciones Técnicas:

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.

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, que 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.

Que permita oscurecer la pantalla del usuario durante la resolución de problemas de forma remota.

Que 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 de imágenes en línea y fuera de línea. Que almacene las imágenes en un repositorio centralizado (recurso de red) e implemente el sistema operativo desde cualquier lugar.

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1

Especificaciones Técnicas:

Que provea informes de AD: Cuentas de Usuarios, cuentas creadas-modificadas recientemente, cuentas de usuarios en varios grupos, cuentas que no caducan, no utilizadas.

Que provea informes detodos 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 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

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1
Especificaciones Técnicas:	

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

Gestión de correo electrónico

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1

Especificaciones Técnicas:

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.

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

Ítem	3
Descripción	Herramienta de Administración de parches Centralizada
Cantidad	1
Especificaciones Técnicas:	
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 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	

El **numeral 10.1.2: Documentación técnica** de la **Sección I: Informaciones particulares del procedimiento** el cual se leerá de la siguiente manera:

10.1.2 Documentación técnica:

La documentación técnica deberá ser entregada de acuerdo con los requisitos específicos establecidos para cada ítem, de forma organizada y alineada a los ítems en los que participa el oferente. A continuación, se detallan los documentos requeridos para el ítem correspondiente:

- **Documentación Técnica - Servicios Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad:**

a. Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas. **No subsanable**.

b. Cronograma de implementación: El oferente deberá presentar el cronograma detallado de actividades, con su respectiva duración y secuencia, que permita evaluar la viabilidad temporal del servicio. **No subsanable**.

c. Formulario de Experiencia como Contratista (SNCC.D.049): El formulario debe contener evidencia de lo siguiente:

- Acreditación de trayectoria mínima de cinco (5) años en provisión de servicios TIC: Evidencia documental (registro mercantil, RPE, contratos previos, etc.) que valide dicha experiencia.
- Evidencia de experiencia en al menos tres (3) proyectos de magnitud y complejidad similar a servicios de SOC, Se deberá presentar orden de compra, contrato o carta de referencia

emitida por el cliente, que incluya específicamente implementaciones de servicios de SOC en la República Dominicana. **Subsanable.**

d. Compromiso firmado de permitir una visita de inspección al Centro de Operaciones de Seguridad (SOC) local de los proveedores, a los fines de verificar la autenticidad de la información proporcionada. **Subsanable**.

e. Declaración de disponibilidad de un SOC local, El oferente debe presentar una declaración formal sobre la existencia de un Centro de Operaciones de Seguridad (SOC) local, indicando dirección, capacidad operativa y contacto. **Subsanable.**

f. Carta del fabricante o del representante autorizado, Debe presentarse carta o certificación que valide que el oferente es canal autorizado para la provisión e implementación de los bienes y servicios ofertados. **Subsanable.**

g. Currículum del personal profesional propuesto (Formulario SNCC.D.045): Debe incluir evidencia que sustente las acreditaciones del personal clave asignado, incluyendo copias de títulos universitarios, certificaciones técnicas y constancias de experiencia, conforme a los siguientes perfiles

- Debe acreditar que es miembro de un organismo internacional orientado a centros de incidentes de seguridad, como lo es el FIRST (Global Forum of Incident Response and Security Teams).
- Deberá de contar con capacidades de CSIRT, por lo que deberá entregar la relación de eventos de seguridad de la información, detección y análisis y respuesta a incidentes de seguridad, proporcionando reportes e información en tiempo real y con base en datos históricos.
- Certificaciones del oferente
    - ISO/IEC 20000-1:2018, ISO/IEC 27001:2022, ISO/IEC 9001:2015.
- Certificaciones internacionales del personal requerido
    - CISSP Certified Information Systems Security Professional
    - CISA (Certified Information Systems Auditor)
    - CISM (Certified Information Security Manager)
    - CRISC (Certified in Risk and IS Control) con al menos 5 años de antigüedad
    - CEH (Certified Ethical Hacker)
    - CSA (Certified SOC Analyst)
    - ITIL v4
    - ISO/IEC 27001 Lead Auditor
    - PMP
    - CCIE Security de Cisco
    - NSE4, NSE5 y NSE7 de Fortinet **Subsanable.**

Documentación Técnica - Servicios Web Application Firewall (WAF):

a. Oferta Técnica: Debe contener el detalle técnico del servicio propuesto, evidenciando que cumple con todas las especificaciones solicitadas. **No subsanable.**

b. Carta del fabricante: Carta emitida por el fabricante, dirigida a la SIPEN, que certifique al oferente como representante local autorizado, indicando su nivel de asociación con la solución ofertada. **Subsanable.**

c. Certificación como Authorized Service Delivery Partner (ASDP): Certificación oficial emitida por el fabricante que respalde dicha condición. **Subsanable.**

d. Formulario de Experiencia como Contratista (SNCC.D.049): El formulario debe contener evidencia de lo siguiente:

- Mínimo cinco (5) años de experiencia como proveedor del Estado dominicano (RPE).

- Al menos una (1) carta de recomendación u orden de compra por proyecto similar implementado en el sector público en los últimos treinta y seis (36) meses.
- Al menos cinco (5) cartas de recomendación u órdenes de compra que respalden proyectos de implementación similares. **Subsanable**.

e. Formulario de Currículum del Personal Profesional Propuesto (SNCC.D.045): Debe incluir evidencia de las siguientes certificaciones del personal asignado al proyecto:
- Un (1) ingeniero con certificación en ISO 27001 Lead Implementer, registrado en la TSS.
- Dos (2) ingenieros certificados en la solución ofertada, con certificación oficial del fabricante.
- Personal con certificación ITIL® 4 Managing Professional, registrado en la TSS.
- Un (1) ingeniero adicional certificado por la marca fabricante**.**
- Experiencia profesional como encargado de proyectos similares en los últimos 10 años. **Subsanable.**

- **Documentación Técnica - Herramienta de Administración de parches Centralizada:**

a. Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas. **No subsanable**.

b. Declaración técnica de integración o compatibilidad: El oferente deberá presentar una declaración que evidencie la compatibilidad o integración entre las soluciones ofertadas en los ítems Manage Engine. **Subsanable**.

c. Carta compromiso sobre licencias, suscripciones y garantías: Declaración firmada donde se indique que todas las licencias, suscripciones y garantías serán emitidas a nombre de la Superintendencia de Pensiones (SIPEN), sin costos adicionales por uso en sus dependencias. **Subsanable.**

d. Plan de trabajo de implementación: Debe presentarse un plan detallado de trabajo, indicando claramente las tareas a ejecutar, su secuencia y duración. **No subsanable**.

e. Cronograma de implementación: Debe evidenciar que el plazo de implementación no excederá un (1) mes contado a partir de la firma del contrato. **No subsanable**.

f. Formulario de Experiencia como Contratista (SNCC.D.049):
- Debe evidenciar al menos dos (2) proyectos de magnitud y complejidad similares mediante contratos, órdenes de compra o cartas de referencia.
- Evidencia de experiencia local del oferente: Documentación que acredite presencia operativa en República Dominicana y al menos tres (3) años como proveedor del Estado (RPE). **Subsanable.**

g. Plan de capacitación: El oferente debe presentar el plan de formación a un mínimo de cuatro (4) personas de SIPEN para la administración de las plataformas. **No subsanable**.

h. Compromiso de soporte técnico 24/7: Declaración firmada del oferente que establezca la disponibilidad del soporte técnico vía correo, remoto o presencial por un (1) año. **No subsanable**.

i. Plan de mantenimiento y actualización: Debe incluir la asistencia para la instalación de parches, nuevas versiones y revisiones trimestrales. **No subsanable.**

j. **Formulario de Currículum del Personal Técnico (SNCC.D.045):** Debe contener los siguientes perfiles con sus respectivos respaldos:

- Técnico responsable de la solución CASB:
  - Certificación profesional o experta vigente.
  - Experiencia previa en implementación de la solución.
  - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses.
- Gerente de Proyecto asignado:
  - Certificación PMP vigente, emitida por el PMI.

- Experiencia previa en gestión de proyectos tecnológicos.
- Registro laboral en la TSS con una antigüedad mínima de seis (6) meses.
- Dedicación exclusiva al proyecto. **Subsanable.**

- **Documentación Técnica – Firewall de Última Generación (NGFW) con Bundle de 3 Años:**

a. Oferta Técnica: Debe incluir marca, modelo, ficha técnica y fotografías del equipo ofertado, con indicación expresa de las licencias y funcionalidades requeridas. **No subsanable.**

b. Garantía de autenticidad y origen del equipo. Declaración formal emitida por el oferente que garantice el origen legítimo y autenticidad del equipo ofertado. **No subsanable.**

c. Licencias necesarias para funcionamiento completo por 3 años: Listado detallado de las licencias incluidas, indicando el período de cobertura y condiciones de uso. **No subsanable.**

d. Especificaciones técnicas del equipo ofertado: Ficha técnica del fabricante que acredite que el equipo incluye:

- Prevención de intrusiones (IPS)
- Antivirus
- Filtrado web
- Control de aplicaciones
- Protección contra amenazas avanzadas (ATP) **No subsanable.**

e. Condiciones de soporte técnico 24/7 y por 3 años: Declaración del oferente que establezca la disponibilidad de soporte técnico remoto o presencial, 24/7 durante los tres (3) años del contrato. **No subsanable.**

f. Pase de conocimiento: Compromiso firmado por el oferente indicando que brindará transferencia de conocimiento documentada sobre la configuración implementada. **Subsanable.**

g. Disponibilidad para trabajar fines de semana: Declaración formal indicando disponibilidad para ejecución de tareas técnicas los fines de semana. **Subsanable**.

h. Documentación final del trabajo realizado: Compromiso escrito de entrega de informe técnico final que incluya configuración, resultados, recomendaciones y validación de funcionamiento. **Subsanable.**

i. Formulario de Currículum del Personal Técnico (SNCC.D.045): Debe contener los siguientes perfiles con sus respectivos respaldos:

- Al menos dos (2) ingenieros certificados FCP (Fortinet Certified Professional).
- Al menos un (1) ingeniero certificado FCSS (Fortinet Certified Solution Specialist). **Subsanable.**

j. Formulario de Experiencia como Contratista (SNCC.D.049), Experiencia previa en proyectos similares: Evidencia de al menos tres (3) implementaciones similares en los últimos cinco (5) años, mediante contratos, órdenes de compra o cartas de referencia. **Subsanable.**

- **Documentación Técnica – Herramienta de monitoreo y auditoria:**

a. Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas. **No subsanable**.

b. Declaración técnica de integración o compatibilidad: El oferente deberá presentar una declaración que evidencie la compatibilidad o integración entre las soluciones ofertadas con ManageEngine. **No subsanable**.

c. Carta compromiso sobre licencias, suscripciones y garantías: Declaración firmada donde se indique que todas las licencias, suscripciones y garantías serán emitidas a nombre de la Superintendencia de Pensiones (SIPEN), sin costos adicionales por uso en sus dependencias. **Subsanable.**

d. Plan de trabajo de implementación: Debe presentarse un plan detallado de trabajo, indicando claramente las tareas a ejecutar, su secuencia y duración. **No subsanable**.

e. Cronograma de implementación: Debe evidenciar que el plazo de implementación no excederá un (1) mes contado a partir de la firma del contrato. **No subsanable**.

f. Formulario de Experiencia como Contratista (SNCC.D.049):

- Debe evidenciar al menos dos (2) proyectos de magnitud y complejidad similares mediante contratos, órdenes de compra o cartas de referencia.
- Evidencia de experiencia local del oferente: Documentación que acredite presencia operativa en República Dominicana y al menos tres (3) años como proveedor del Estado (RPE). **Subsanable.**

g. Plan de capacitación: El oferente debe presentar el plan de formación a un mínimo de cuatro (4) personas de SIPEN para la administración de las plataformas. **No subsanable.**

h. Compromiso de soporte técnico 24/7: Declaración firmada del oferente que establezca la disponibilidad del soporte técnico vía correo, remoto o presencial por un (1) año. **No subsanable.**

i. Plan de mantenimiento y actualización: Debe incluir la asistencia para la instalación de parches, nuevas versiones y revisiones trimestrales. **No subsanable.**

j. Formulario de Currículum del Personal Técnico (SNCC.D.045): Debe contener los siguientes perfiles con sus respectivos respaldos:

- Técnico responsable de la solución CASB:
  - Certificación profesional o experta vigente.
  - Experiencia previa en implementación de la solución.
  - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses.
- Gerente de Proyecto asignado:
  - Certificación PMP vigente, emitida por el PMI.
  - Experiencia previa en gestión de proyectos tecnológicos.
  - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses.
  - Dedicación exclusiva al proyecto. **Subsanable.**

Para los consorcios: En adición a los requisitos anteriormente expuestos, los consorcios deberán presentar un Acuerdo o Promesa de consorcio, el cual debe incluir: Las generales actualizadas de los(as) consorciados(as): El objeto del consorcio, las partes que lo integran; Las obligaciones de las partes; La capacidad de ejercicio de cada miembro del consorcio, así como la solvencia económica y financiera y la idoneidad técnica y profesional; Designación del(la) representante o gerente único(a) del consorcio; Reconocer la responsabilidad solidaria de los(as) integrantes por los actos practicados en el consorcio, tanto en la fase de selección, como en la de ejecución del contrato; Hacer constar que las personas físicas y/ o jurídicas que lo componen no presentarán ofertas en forma individual o como integrantes de otro consorcio, siempre que se tratare del mismo objeto de la contratación.

El **numeral 11.1.3 Metodología y criterios de evaluación para la documentación técnica** de la **Sección I: Informaciones particulares del procedimiento** el cual se leerá de la siguiente manera:

11.1.3 Metodología y criterios de evaluación para la documentación técnica

Las ofertas deberán contener la documentación técnica solicitada en la "Documentación técnica" para demostrar los requerimientos exigidos en las especificaciones técnicas y/o fichas descritas en este pliego (con sus anexos), la cual será evaluada bajo la metodología Cumple/No cumple, de acuerdo al artículo 81 del Reglamento de aplicación núm. 416-23. En esta, todos los documentos referidos se convierten en habilitantes y obligatorios de la oferta y deberán ser cumplidos totalmente para que los oferentes puedan resultar habilitados para la segunda etapa, es decir, para la apertura y evaluación de las ofertas económicas.

La forma de evaluación será la siguiente:

Evaluación Técnica Servicios Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad				
#	**Requisito Técnico**	**Documento Soporte**	**Subsanable**	**(Cumple / No cumple)**
1	Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas.	Oferta técnica	No	
2	Cronograma de implementación: El oferente deberá presentar el cronograma detallado de actividades, con su respectiva duración y secuencia, que permita evaluar la viabilidad temporal del servicio	Cronograma de implementación	No	
3	Formulario de Experiencia como Contratista (SNCC.D.049): El formulario debe contener evidencia de lo siguiente: - Acreditación de trayectoria mínima de cinco (5) años en provisión de servicios TIC: Evidencia documental (registro mercantil, RPE, contratos previos, etc.) que valide dicha experiencia. - Evidencia de experiencia en al menos tres (3) proyectos de magnitud y complejidad similar a servicios de SOC, Se deberá presentar orden de compra, contrato o carta de referencia emitida por el cliente, que incluya	Formulario SNCC.D.049 y sus anexos	Sí	

Evaluación Técnica Servicios Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	específicamente implementaciones de servicios de SOC en la República Dominicana.			
4	Compromiso firmado de permitir una visita de inspección al Centro de Operaciones de Seguridad (SOC) local de los proveedores, a los fines de verificar la autenticidad de la información proporcionada.	Carta permiso de visita de inspección / Visita técnica	Sí	
5	Declaración de disponibilidad de un SOC local, El oferente debe presentar una declaración formal sobre la existencia de un Centro de Operaciones de Seguridad (SOC) local, indicando dirección, capacidad operativa y contacto.	Declaración de disponibilidad de un SOC local	Sí	
6	Carta del fabricante o representante autorizado que certifique al oferente como canal autorizado.	Carta oficial del fabricante	Sí	
7	Currículum del personal profesional propuesto (Formulario SNCC.D.045): Debe incluir evidencia que sustente las acreditaciones del personal clave asignado, incluyendo copias de títulos universitarios, certificaciones técnicas y constancias de experiencia, conforme a los siguientes perfiles - Debe acreditar que es miembro de un organismo internacional orientado a centros de incidentes de seguridad, como lo es el FIRST (Global Forum of Incident Response and Security Teams). - Deberá de contar con capacidades de CSIRT, por lo que deberá entregar la relación de eventos de seguridad de la información, detección y análisis y respuesta a incidentes de seguridad, proporcionando reportes e información en tiempo real y con base en datos históricos. ❖ Certificaciones del oferente	Currículum del personal profesional propuesto (Formulario SNCC.D.045) con sus anexos	Sí	

Evaluación Técnica Servicios Sistema de fortalecimiento y capacidades a respuesta antes incidente de ciberseguridad				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	· ISO/IEC 20000-1:2018, ISO/IEC 27001:2022, ISO/IEC 9001:2015. ❖ Certificaciones internacionales del personal requerido · CISSP Certified Information Systems Security Professional · CISA (Certified Information Systems Auditor) · CISM (Certified Information Security Manager) · CRISC (Certified in Risk and IS Control) con al menos 5 años de antiguedad · CEH (Certified Ethical Hacker) · CSA (Certified SOC Analyst) · ITIL v4 · ISO/IEC 27001 Lead Auditor · PMP · CCIE Security de Cisco · NSE4, NSE5 y NSE7 de Fortinet			

Evaluación Técnica – Servicios Web Application Firewall (WAF)				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
1	Oferta Técnica: Debe contener el detalle técnico del servicio propuesto, evidenciando que cumple con todas las especificaciones solicitadas.	Oferta técnica	No	
2	Carta del fabricante: Carta emitida por el fabricante, dirigida a la SIPEN, que certifique al oferente como representante local autorizado, indicando su nivel de asociación con la solución ofertada.	Carta de la fabricante dirigida a SIPEN	Sí	
3	Certificación como Authorized Service Delivery Partner (ASDP) del fabricante.	Certificación ASDP oficial del fabricante	Sí	
4	Formulario de Experiencia como Contratista (SNCC.D.049): El formulario debe contener evidencia de lo siguiente:	Formulario SNCC.D.049 y sus anexos	Sí	

Evaluación Técnica – Servicios Web Application Firewall (WAF)				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	- Mínimo cinco (5) años de experiencia como proveedor del Estado dominicano (RPE). - Al menos una (1) carta de recomendación u orden de compra por proyecto similar implementado en el sector público en los últimos treinta y seis (36) meses. - Al menos cinco (5) cartas de recomendación u órdenes de compra que respalden proyectos de implementación similares			
5	Formulario de Currículum del Personal Profesional Propuesto (SNCC.D.045): Debe incluir evidencia de las siguientes certificaciones del personal asignado al proyecto: - Un (1) ingeniero con certificación en ISO 27001 Lead Implementer, registrado en la TSS. - Dos (2) ingenieros certificados en la solución ofertada, con certificación oficial del fabricante. - Personal con certificación ITIL® 4 Managing Professional, registrado en la TSS. - Un (1) ingeniero adicional certificado por la marca fabricante. - Experiencia profesional como encargado de proyectos similares en los últimos 10 años.	Formulario SNCC.D.045 y sus anexos	Sí	

Evaluación Técnica – Herramienta de Administración de parches Centralizada				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
1	Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas.	Oferta técnica	No	
2	Integración o compatibilidad entre las soluciones ofertadas con ManageEngine.	Declaración técnica / ficha técnica	Si	
3	Carta compromiso sobre licencias, suscripciones y garantías:	Carta compromiso	Si	

Evaluación Técnica – Herramienta de Administración de parches Centralizada				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	Declaración firmada donde se indique que todas las licencias, suscripciones y garantías serán emitidas a nombre de la Superintendencia de Pensiones (SIPEN), sin costos adicionales por uso en sus dependencias.	sobre licencias, suscripciones y garantías		
4	Plan de trabajo de implementación: Debe presentarse un plan detallado de trabajo, indicando claramente las tareas a ejecutar, su secuencia y duración.	Plan de trabajo de implementación:	No	
5	Cronograma de implementación: Debe evidenciar que el plazo de implementación no excederá un (1) mes contado a partir de la firma del contrato	Cronograma de implementación	No	
6	Formulario de Experiencia como Contratista (SNCC.D.049), - Debe evidenciar al menos dos (2) proyectos de magnitud y complejidad similares mediante contratos, órdenes de compra o cartas de referencia. - Evidencia de experiencia local del oferente: Documentación que acredite presencia operativa en República Dominicana y al menos tres (3) años como proveedor del Estado.	Formulario SNCC.D.049 y anexos	Sí	
7	Plan de capacitación: El oferente debe presentar el plan de formación a un mínimo de cuatro (4) personas de SIPEN para la administración de las plataformas.	Plan de capacitación	No	
8	Compromiso de soporte técnico 24/7: Declaración firmada del oferente que establezca la disponibilidad del soporte técnico vía correo, remoto o presencial por un (1) año.	Compromiso de soporte técnico 24/7	No	
9	Plan de mantenimiento y actualización: Debe incluir la asistencia para la instalación de	Plan de mantenimiento	No	

Evaluación Técnica – Herramienta de Administración de parches Centralizada				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	parches, nuevas versiones y revisiones trimestrales			
10	Formulario de Currículum del Personal Técnico (SNCC.D.045): Debe contener los siguientes perfiles con sus respectivos respaldos: ❖ Técnico responsable de la solución CASB: - Certificación profesional o experta vigente. - Experiencia previa en implementación de la solución. - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses. Subsanable. ❖ Gerente de Proyecto asignado: - Certificación PMP vigente, emitida por el PMI. - Experiencia previa en gestión de proyectos tecnológicos. - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses. - Dedicación exclusiva al proyecto. Subsanable.	Formulario SNCC.D.045 y anexos	Si	

Evaluación Técnica - Firewall de Última Generación (NGFW) con Bundle de 3 Años				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
1	Oferta Técnica: Debe incluir marca, modelo, ficha técnica y fotografías del equipo ofertado, con indicación expresa de las licencias y funcionalidades requeridas.	Oferta técnica	No	
2	Garantía de autenticidad y origen del equipo.	Declaración del oferente	No	
3	Licencias necesarias para funcionamiento completo por 3 años: Listado detallado de las licencias incluidas, indicando el período de cobertura y condiciones de uso.	Listado de licencias	No	
4	Especificaciones técnicas del equipo ofertado: Ficha técnica del fabricante que acredite que el	Ficha técnica del fabricante	No	

Evaluación Técnica - Firewall de Última Generación (NGFW) con Bundle de 3 Años				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	equipo incluye: - Prevención de intrusiones (IPS) - Antivirus - Filtrado web - Control de aplicaciones Protección contra amenazas avanzadas (ATP)			
5	Condiciones de soporte técnico 24/7 y por 3 años: Declaración del oferente que establezca la disponibilidad de soporte técnico remoto o presencial, 24/7 durante los tres (3) años del contrato.	Declaración del oferente	No	
6	Pase de conocimiento: Compromiso firmado por el oferente indicando que brindará transferencia de conocimiento documentada sobre la configuración implementada.	Carta compromiso del oferente	Sí	
7	Disponibilidad para trabajar fines de semana: Declaración formal indicando disponibilidad para ejecución de tareas técnicas los fines de semana. Subsanable.	Declaración firmada del oferente	Sí	
8	Documentación final del trabajo realizado: Compromiso escrito de entrega de informe técnico final que incluya configuración, resultados, recomendaciones y validación de funcionamiento.	Carta compromiso del oferente	Sí	
9	Formulario de Currículum del Personal Técnico (SNCC.D.045): Debe contener los siguientes perfiles con sus respectivos respaldos: - Al menos dos (2) ingenieros certificados FCP (Fortinet Certified Professional). - Al menos un (1) ingeniero certificado FCSS (Fortinet Certified Solution Specialist).	Formulario SNCC.D.045 y anexos	Sí	
10	Formulario de Experiencia como Contratista (SNCC.D.049), Experiencia previa en proyectos similares: Evidencia de al menos tres	Formulario SNCC.D.049 y anexos	Sí	

Evaluación Técnica - Firewall de Última Generación (NGFW) con Bundle de 3 Años				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	(3) implementaciones similares en los últimos cinco (5) años, mediante contratos, órdenes de compra o cartas de referencia			

Evaluación Técnica – Herramienta de monitoreo y auditoria				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
1	Oferta Técnica: Debe contener el detalle técnico de la solución propuesta, evidenciando que cumple con todas las especificaciones solicitadas.	Oferta técnica	No	
2	Declaración técnica de integración o compatibilidad: El oferente deberá presentar una declaración que evidencie la compatibilidad o integración entre las soluciones ofertadas con ManageEngine.	Declaración técnica de integración	No	
3	Carta compromiso sobre licencias, suscripciones y garantías: Declaración firmada donde se indique que todas las licencias, suscripciones y garantías serán emitidas a nombre de la Superintendencia de Pensiones (SIPEN), sin costos adicionales por uso en sus dependencias	Carta compromiso sobre licencias, suscripciones y garantías	Sí	
4	Plan de trabajo de implementación: Debe presentarse un plan detallado de trabajo, indicando claramente las tareas a ejecutar, su secuencia y duración.	Plan de trabajo de implementación	No	
5	Cronograma de implementación: Debe evidenciar que el plazo de implementación no excederá un (1) mes contado a partir de la firma del contrato.	Cronograma de implementación	No	
6	Formulario de Experiencia como Contratista (SNCC.D.049): - Debe evidenciar al menos dos (2) proyectos de magnitud y complejidad similares mediante	Formulario SNCC.D.049 y anexos	Sí	

Evaluación Técnica – Herramienta de monitoreo y auditoria				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	contratos, órdenes de compra o cartas de referencia. - Evidencia de experiencia local del oferente: Documentación que acredite presencia operativa en República Dominicana y al menos tres (3) años como proveedor del Estado (RPE).			
7	Plan de capacitación: El oferente debe presentar el plan de formación a un mínimo de cuatro (4) personas de SIPEN para la administración de las plataformas.	Plan de capacitación	No	
8	Compromiso de soporte técnico 24/7: Declaración firmada del oferente que establezca la disponibilidad del soporte técnico vía correo, remoto o presencial por un (1) año.	Declaración del oferente	No	
9	Plan de mantenimiento y actualización: Debe incluir la asistencia para la instalación de parches, nuevas versiones y revisiones trimestrales.	Plan de mantenimiento y actualización	No	
10	Formulario de Currículum del Personal Técnico (SNCC.D.045): Debe contener los siguientes perfiles con sus respectivos respaldos: ❖ Técnico responsable de la solución CASB: - Certificación profesional o experta vigente. - Experiencia previa en implementación de la solución. - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses. ❖ Gerente de Proyecto asignado: - Certificación PMP vigente, emitida por el PMI.	Formulario SNCC.D.045 y anexos	Sí	

Evaluación Técnica – Herramienta de monitoreo y auditoria				
#	Requisito Técnico	Documento Soporte	Subsanable	(Cumple / No cumple)
	- Experiencia previa en gestión de proyectos tecnológicos. - Registro laboral en la TSS con una antigüedad mínima de seis (6) meses. - Dedicación exclusiva al proyecto.			

El **numeral 8: Desempate de ofertas de la Sección II: Recepción, Apertura, Evaluación Y Adjudicación** el cual se leerá de la siguiente manera:

8. Desempate de ofertas

En caso de empate entre dos o más Oferentes/Proponentes, se aplicará como criterio de desempate el establecido en el artículo 131 del Reglamento de Aplicación núm. 416-23, correspondiente a:

Preferencia al oferente que tenga mayor participación de mujeres en su plantilla de personal.

Para confirmar el cumplimiento de este criterio, deberá presentarse certificación vigente emitida por la Tesorería de la Seguridad Social (TSS), con un corte no mayor a treinta (30) días a la fecha de presentación de la oferta.

Si ninguna de las ofertas empatadas cumple con este criterio, se procederá con la adjudicación mediante una selección al azar, tipo sorteo, el cual se llevará a cabo de manera pública, con los oferentes empatados, el Comité de Compras y Contrataciones (CCC) y en presencia de un Notario Público, quien certificará el acto.

Esta enmienda forma parte integral del Pliego de Condiciones y deberá ser considerada por todos los interesados para la elaboración de sus ofertas.

Dado en Santo Domingo, D.N., a los un (1) días del mes de agosto del año dos mil veinticinco (2025).

SUPERINTENDENCIA DE PENSIONES
COMITÉ DE COMPRAS Y CONTRATACIONES

Comité de Compras y Contrataciones
Superintendencia de Pensiones