



Ficha Técnica
Proceso de Contratación Menor

Contratación de la Continuidad del Derecho de Uso Herramienta de Email Security **TSS-DAF-CM-2026-0062**

Política Sistema Gestión Integrado

Política Sistema Gestión Integrado La Tesorería de la Seguridad Social como entidad a cargo del proceso de recaudo, distribución y pago de las cotizaciones del Sistema Dominicano Seguridad Social (SDSS) y de la administración del Sistema Único de Información y Recaudo (SUIR), ejecuta de forma transparente los fondos y sus procesos mediante el fomento de una cultura de cumplimiento normativo, donde se prohíbe el soborno en todas sus formas y se promueven los valores éticos, reforzada por un ambiente de confianza para las denuncias libre de represalias, aplicando un sistema de consecuencias bajo la Ley de Función Pública y el Código Penal, desarrollando una efectiva gestión de riesgos que asegure la continuidad del negocio, así como la legalidad, confidencialidad, integridad y disponibilidad de los activos de información. Promueve la innovación y mejora continua de los procesos de su Sistema de Gestión Integrado, así como la satisfacción de las partes interesadas, mediante el uso de una plataforma tecnológica eficiente y un capital humano competente, para lo cual designa un equipo independiente, dotado de recursos, autoridad y con acceso a la MAE.

Santo Domingo, Distrito Nacional
República Dominicana
30 de septiembre 2026

1. OBJETIVOS Y ALCANCE

El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras, que deseen participar del procedimiento de Contratación Menor, llevada a cabo por TESORERIA DE LA SEGURIDAD SOCIAL (Referencia: **TSS-DAF-CM-2026-0062**) para “**Contratación de la Continuidad del Derecho de Uso Herramienta de Email Security**”.

Este documento constituye la base para la preparación de las Ofertas. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en el presente documento o presenta una información que no se ajuste sustancialmente en todos sus aspectos al mismo, el riesgo estará a su cargo y el resultado podrá ser el rechazo de su Propuesta.

2. OBJETO DEL PROCEDIMIENTO DE SELECCIÓN

Constituye el objeto de la presente convocatoria recibir ofertas para la adquisición de **Contratación de la Continuidad del Derecho de Uso Herramienta de Email Security**, de referencia No. **TSS-DAF-CM-2026-0062**, de acuerdo con las condiciones fijadas en las presentes bases de contratación.

Esta contratación ha sido clasificada bajo la actividad comercial **81110000** Servicio de alquiler o arrendamiento de licencias de software informático.

3. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

Las especificaciones técnicas describen todos los elementos, condiciones, parámetros, requisitos que deben cubrir los oferentes/proponentes en sus ofertas para ser consideradas a fines de adjudicación.

DETALLE DEL REQUERIMIENTO					
Ítem	Cant.	Rubro	Descripción	Requisitos Mínimos	Medio de verificación
1	1.00	81112501	Adquisición de la Continuidad del Derecho de Uso Herramienta de Email Security	Ver especificaciones debajo.	Especificaciones de la oferta técnica
1	1.00	81112501	Suscripción central email advanced	Ver especificaciones debajo.	Especificaciones de la oferta técnica

Requerimientos Generales y Arquitectura

1.1 La solución debe proteger de Ciber Amenazas para de correo electrónico en la nube Office 365 y/o Google Workspace.

1.2 La solución suministrada debe ser a través un servicio SaaS en nube.

1.3 El servicio SaaS debe contar con al menos alguna de estas certificaciones:

- SOC 2
- ISO 27001

1.4 La solución debe soportar proteger de Ciber Amenazas, en las siguientes aplicaciones SaaS de Colaboración y Almacenamiento de archivos:

- Slack
- Microsoft Teams
- Microsoft OneDrive
- Microsoft SharePoint
- Google Drive
- Box
- Dropbox
- Citrix ShareFiles

1.5 La solución debe ser reconocida como una solución líder en seguridad de correo electrónico por analistas terceros como Forrester o Gartner en los últimos 3 años.

1.6 La solución debe deberá proporcionar un servicio para 400 usuarios de seguridad para correo y herramientas de colaboración en el servicio de Nube.

1.7 La solución debe proveer protección contra los siguientes Ciber ataques:

- Prevención Ataques a Correo electrónico (Phishing, Spoofing, Spam).
- Prevención de Malware (en correo, herramientas de colaboración y almacenamiento).
- Prevención de Malware de día Cero con Sandboxing (en correo, herramientas de colaboración) y Limpieza de Documentos CDR.
- Anomalías de usuarios e inicios de sesión anómalos (Indicios de robo de cuenta).
- Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT.
- Prevención de Fuga de Datos (DLP) en correo y herramientas de colaboración.

1.8 La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado.

1.9 La solución debe ser fácil y rápida de usar, con configuraciones de políticas listas para usar.

1.10 El servicio debe ofrecer una disponibilidad de al menos 99.9%

1.11 La solución debe utilizar protocolos de cifrados modernos para salvaguardar la organización.

1.12 La solución debe ser escalable y nativa de nube para soportar crecimiento a cientos de miles de usuarios.

1.13 La plataforma deberá poder ser administrada vía HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge.

2. Prevención Ataques a Correo Electrónico BEC, Phishing, Spam

2.1 La solución debe bloquear sofisticados ataques de ingeniería social, como la suplantación de identidad, spam, phishing de día cero y Business Email Compromise (BEC) usando motores de machine learning (ML), Deep Learning e Inteligencia Artificial (IA).

2.2 La solución debe proteger los correos electrónicos de entrada, salientes y proteger la comunicación interna en tiempo real para ataques laterales y amenazas internas.

2.3 La solución debe proveer prevención en línea (no solo detección y/o remediación), es decir intercepción de correo antes que lleguen al usuario final.

2.4 La solución debe permitir el despliegue automático por integración nativa de API sin requerir cambios en los registros MX de DNS para prevenir ataques por correo.

2.5 La integración por API debe ser automática y sencilla de gestionar, debe permitir reglas granulares por usuarios y/o grupos que pueden estar en prevención y/o remediación y no requerir de configuraciones manuales del lado del servicio de correos (Microsoft 365 o Google).

2.6 La solución debe ser invisible para los atacantes, y debe aplicar seguridad en profundidad siendo una capa de seguridad como última línea de defensa y no desactivar la seguridad nativa de las soluciones de Correo de Nube de office 365 y/o Google Workplace.

2.7 La solución debe contar con un periodo de aprendizaje que realice un escaneo de 13 meses de metadatos de correo electrónico (remitente, destinatario, asunto, hora) en los buzones de correo de los usuarios para determinar los patrones de comunicación y ajustar los motores de IA.

2.8 La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico utilizando Inteligencia Artificial, incluyendo al menos 100 idiomas que incluyan el español.

2.9 La solución debe inspeccionar los metadatos, archivos adjuntos, enlaces e idioma de la comunicación, dominios, OCR, QR codes, así como todas comunicaciones históricas, para determinar relaciones de confianza previas entre el emisor y el receptor del correo para de identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.

2.10 La solución debe etiquetar los correos electrónicos dependiendo del tipo de amenaza identificada, como mínimo:

- Extorsión
- Suplantación
- Estafa Financiera
- Ingeniería Social,
- Facturas falsas
- Robo de credenciales
- Sextorsión

2.11 La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre.

2.12 La solución debe realizar la verificación de más de 200 de indicadores de ataque sobre el correo electrónico como la verificación DMARC, SPF o DKIM para verificar que un correo electrónico se origina en el supuesto dominio de origen, a través de inteligencia artificial evitar ataques evasivos y sofisticados.

2.13 La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación de correo electrónico:

- Sender Policy Framework (SPF),
- Domain Keys Identified Mail (DKIM),
- Domain-based Message Authentication, Reporting & Conformance (DMARC).

2.14 La solución debe contar con la opción de configuración de listas blancas y listas negras

2.15 La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus empleados.

2.16 La solución debe utilizar la integración con el directorio para crear automáticamente listas de usuarios VIP para protegerlos Protección contra la suplantación de identidad.

2.17 La solución debe inspeccionar enlaces cuando el usuario hace clic en la URL, Es decir reescribir el(los) enlace(s) en el correo.

2.18 La solución debe emular (sandboxing) los enlaces URLs reescritos para exponer indicadores de phishing ocultos.

2.19 La solución debe permitir a los administradores detectar a los usuarios que hicieron clic en los enlaces que resultaron maliciosos y que requieren mayor educación y capacitación para evitar hacer clic en enlaces maliciosos.

2.20 La solución debe interactuar con Microsoft a través de la API, no debe generar interferencia cuando Microsoft (MS) ATP o Defender inspecciona la URL antes que se reescriba la URL, por lo tanto, puede usarse con MS ATP o Defender, como una capa adicional de protección.

2.21 La solución debe reescribir enlaces en el cuerpo del correo y también en links dentro de documentos adjuntos en el correo.

2.22 La solución debe permitir a los administradores configurar la lista de excepciones, de correos detectados mediante como maliciosos o sospechosos.

2.23 La solución debe soportar la rescritura de URL's embebidas incluso si son códigos QR.

2.24 La solución debe ser capaz de poner en cuarentena los correos electrónicos, los archivos y los mensajes según las políticas de seguridad y la configuración de los motores de seguridad.

- 2.25 La solución, de acuerdo con la política, debe permitir a los usuarios finales enviar solicitudes de restauración para correos electrónicos en cuarentena, seleccionar administradores autorizados puedan aprobar o no las solicitudes de restauración.
- 2.26 La solución debe admitir correos electrónicos incluidos en la lista de permitidos que también son permitidos por Microsoft/Google.
- 2.27 La solución debe contar con acciones automatizadas, como marcar una alerta al usuario en el correo: mover a la carpeta Spam/Junk, cuarentena el correo, y/o añadir una cabecera en el correo.
- 2.28 La solución debe contar acciones automatizadas diferenciadas para phishing, malware, spam, correo de mercadeo (marketing).
- 2.29 La solución debe permitir al administrador que los usuarios finales confíen en los remitentes para que los correos electrónicos clasificados como spam y entreguen en su buzón, en cambio, si los correos electrónicos se clasifican como phishing o contienen malware, se pondrán en cuarentena.
- 2.30 La solución debe permitir que el administrador personalizar las plantillas que usaría para notificar a los usuarios finales sobre las amenazas.
- 2.31 La solución debe tener un período de retención de correos electrónicos originales cuarentenados por al menos 180 días.
- 2.32 La solución debe tener un período de retención de los metadatos de los correos electrónicos analizados maliciosos por al menos 180 días
- 2.33 La solución debe tener un periodo de retención de todos los correos electrónicos originales analizados por al menos 14 días, aun si son clasificados como limpios.
- 2.34 La solución debe permitir opcionalmente como backup almacenar localmente los correos electrónicos/archivos en cuarentena.
- 2.35 La solución debe tener la capacidad de remediación las amenazas que llegan a las bandejas de entrada de los usuarios, desde la interfaz de gestión debe poder realizar la identificación, el análisis y la corrección. Si llega un correo electrónico o un archivo, y se pueden tomar medidas inmediatas en miles de bandejas de entrada con unos pocos clics, sin PowerShell ni codificación de ningún tipo.
- 2.36 La solución debe permitir a los usuarios y administradores proporcionar comentarios sobre correos electrónicos sospechosos para ayudar en la clasificación de phishing.
- 2.37 La solución debe permitir que los usuarios puedan ayudar a detectar ataques perdidos y permitir que los administradores de seguridad bloqueen los ataques detectados y prevenir ataques similares en el futuro.
- 2.38 La solución debe integrarse con el mecanismo reporte de suplantación de identidad de MS Outlook.
- 2.39 La solución debe permitir la adición de Banners de correo electrónico educativos usando inteligencia artificial para los correos electrónicos entrantes, que permita a la organización concienciación sobre ciberseguridad y recordar a los usuarios que sigan la política. Los banners deben ser totalmente personalizables para el color que represente la gravedad y el texto, e informar al destinatario sobre correos con contenido como:
- Solicitud de pago a través del servicio de pago
 - Correos electrónicos con facturas / órdenes de compra.
 - Correos electrónicos con enlaces a recursos restringidos.
 - Nombre del remitente diferente a la dirección.
 - Dominio de respuesta creado recientemente y su dirección es diferente a la del remitente
 - Error en el SPF del remitente.
 - Dominio del remitente creado recientemente.
 - Correos electrónicos entrantes de remitentes externos.

2.40 La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones:

- Hosts
- Direcciones IP
- Usuarios
- Dominios
- Cabeceras / Headers
- Asunto
- Links
- Adjuntos

2.41 El diagrama de flujo de seguridad del correo electrónico en el tablero principal que muestra cuántos correos electrónicos envió Microsoft a la bandeja de entrada, cuarentena, correo no deseado y detectados y cuarentenados por la solución de seguridad ofertada.

2.42 La solución debe permitir a los administradores desde la misma consola de gestión de seguridad de correo electrónico ver y restaurar todos los correos electrónicos en cuarentena, ya sea que hayan sido puestos en cuarentena por Microsoft o por la solución de seguridad ofertada basada en API.

2.43 La solución debe permitir a los administradores bloquear automáticamente las URL procedentes de las fuentes de indicadores de compromiso (IOC).

2.44 La solución debe permitir a los administradores configurar un comentario automatizado para que se envíe a los usuarios finales cuando informen de correos electrónicos de entrenamiento de phishing.

2.45 La solución debe permitir a los administradores configurar un remitente personalizado para las notificaciones enviadas a los usuarios finales sobre las solicitudes de restauración de cuarentena aprobadas o rechazadas y los informes sobre correos electrónicos de suplantación de identidad (phishing).

2.46 La solución debe permitir a los administradores enviar notificaciones sobre los usuarios que envían solicitudes de restauración a cualquier destinatario de correo.

2.47 La solución debe permitir enviar un reporte diario por correo electrónico a los usuarios finales sobre los correos electrónicos en cuarentena y basura/spam en las últimas 24 horas.

2.48 La solución debe permitir a los usuarios solicitar al administrador la liberación de los correos cuarentenados desde este reporte diario.

3 Prevención de Malware en Correo Electrónico y herramientas de colaboración y almacenamiento SaaS

3.1 Debe escanear malware a través de análisis estático.

3.2 La solución debe tener protección antivirus/malware basado en firmas.

3.3 La solución debe permitir a los administradores configurar la lista de bloqueo cualquier tipo de archivo y marcado como malware y para los tipos de archivos (PDF, EML, HTML) optar por bloquear estos archivos en función de si contienen enlaces o no.

3.4 La solución debe detectar archivos como protegidos con contraseña al menos de las siguientes extensiones:

- Documentos: Word, Excel, PowerPoint y PDF.
- Archivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TB2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, IZH, RPM, WIM, ARJ, CPIO, CRAMFS, QCOW2, UDF, AR e IMG, ISO, AR.

3.5 Si un archivo esta como protegido con contraseña, la solución debe intentar extraer la contraseña mediante varias técnicas, como buscar la contraseña en el cuerpo del correo electrónico y si se encuentra la contraseña, debe usar la contraseña para descifrar el archivo e inspeccionarlo en busca de malware.

3.6 Si no se encuentra la contraseña, el administrador debe poder seleccionar alguna de las siguientes acciones:

- Requerir que el usuario final ingrese una contraseña
- El usuario recibe el correo electrónico con una advertencia.
- Cuarentena.
- Identificar el correo como sospechoso de malware

3.7 Escanea todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados, por lo menos en los siguientes servicios:

- Google Drive
- ShareFile
- OneDrive
- Sharepoint
- Box
- **Dropbox:** de malware, ransomware, ataques laterales

3.8 La solución debe escanear y analizar cada archivo en busca de enlaces maliciosos que luego bloquear en todas sus aplicaciones para compartir archivos.

3.9 La solución debe detectar directamente el comportamiento malicioso y poner en cuarentena los archivos antes de que la amenaza se propague.

3.10 Brindar protección contra enlaces de phishing, código o archivos maliciosos y fuga de datos en plataformas de chat empresarial.

3.11 La solución debe habilitar a los administradores permitir o bloquear direcciones URL exactas y dominios completos en mensajes de Teams y Slack.

3.12 Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Folder (Carpeta bóveda).

4. Prevención de Malware de día Cero (sandboxing) en Correo y herramientas de colaboración y almacenamiento SaaS y Limpieza de Documentos

4.1 La solución debe incluir capacidades de “Sanboxing” resistente a la evasión para bloquear el malware de día cero, con un análisis dinámico en un entorno virtual aislado y escalable basado en la nube.

4.2 La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes. Incluso debe tener la capacidad de ver un vídeo del resultante de la emulación.

4.3 El análisis de sandboxing debe obtener un veredicto respecto de un archivo adjunto o del recurso web asociado a un hipervínculo en un lapso no mayor a 5 minutos.

4.4 La solución debe contar con una página de bloqueo para impedir el acceso de los usuarios a los sitios web maliciosos asociados a los hipervínculos contenidos en los mensajes de correo analizados.

4.5 La solución debe ser capaz de sandboxing al menos los siguientes tipos de archivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, SWF, JAVA (.jar, .js/.jse), VBS, scripts y archivos PowerShell (.ps1).

4.6 La solución debe permitir a los administradores puedan seleccionar los sistemas operativos que utilizará el sandbox del Anti-Malware para emular archivos.

4.7 La Emulación debe soportar hacerlo en Win7, Win8.1, Win10 o inclusive Win11.

4.8 La solución debe admitir capacidades CDR (Content Disarm and Reconstruction) es decir, podrá limpiar los documentos o imágenes adjuntos en los correos electrónicos de contenido malicioso.

4.9 La Solución CDR debe ser capaz de gestionar al menos los siguientes tipos de archivos: PDF, DF, XLSX, XLSB, XLSM, XLTX, XLTM, XLAM, XLSB, XLS, PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM, PPT, PPS, POT, PPA, DOCX, DOCM, DOTX, DOTM, DOC, DOT.

5. Anomalías de usuarios y Detección de Cuentas comprometidas

5.1 La solución debe evitar ataques avanzados de apropiación de cuentas aumentando los procesos de autenticación, evitar usuarios no autorizados y los dispositivos comprometidos accedan a su correo electrónico en la nube o a las aplicaciones SaaS.

5.2 La solución debe contar con un motor analiza el comportamiento utilizando un algoritmo de aprendizaje automático que crea un perfil basado en eventos históricos, que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.

5.3 La solución debe detectar comportamientos y acciones que parecen anormales cuando se observan en el contexto de una organización y la actividad histórica de un usuario.

5.4 Para identificar cuentas potencialmente comprometidas, debe incluir un motor de inteligencia artificial para inspeccionar todos los parámetros de los eventos de inicio de sesión para identificar los realizados por actores malintencionados:

- Borrado de todos los correos electrónicos del buzón.
- Usuarios que envían correos electrónicos maliciosos.
- Mover todos los correos electrónicos a una subcarpeta.
- Detección basada en Inteligencia artificial de inicios de sesión anómalos.
- Iniciar la sesión desde una dirección IP maliciosa.
- Primera vez en un nuevo país.
- Reenvío automático a una dirección de correo electrónico externa.
- Acceso inusual desde un país.
- Acceso desde una geográfica sospechosa (viaje imposible).
- Error de inicio de sesión sospechoso en MFA.
- El cliente es un navegador vulnerable.

5.5 La solución debe un evento de seguridad que brinda el contexto e información necesaria para la investigación, debe clasificar como crítica o sospechosa.

5.6 La solución debe tener la capacidad de tomar las siguientes acciones de respuesta cuando detecte cuentas potencialmente comprometidas o cuentas secuestradas:

- Bloquear la cuenta.
- Restablecer la contraseña.

5.7 Las Anomalías Críticas y de inicio de sesión identificados de los usuarios comprometidos podrán ser bloqueadas automáticamente.

5.8 La solución debe permitir a los administradores configurar un buzón dedicado al que se enviarán alertas sobre cuentas comprometidas.

5.9 Bloqueo de cuentas que inicien se sesión desde direcciones IPs conocidas como maliciosas por una base de inteligencia del fabricante (TIP)

5.10 Entre los eventos que la solución debe analizar para identificar cuentas secuestradas (“account takeover”) deben incluirse:

- El inicio de sesión.
- La ubicación desde donde se hizo el inicio de sesión.
- Anomalías recientes.

- Correos recientes.
- Acciones del usuario recientes.

6. Shadow IT & Application Control

- 6.1 La solución basada en el análisis de correos electrónicos (Office 365 y/o Gmail), debe identificar las aplicaciones en las que se ha estado haciendo uso del correo institucional, para brindar visibilidad de dichas aplicaciones en la nube y que se utilizan en nombre del dominio de la empresa.
- 6.2 La solución detectará y proporcionará informes de aplicaciones de Shadow IT y top de usuarios.
- 6.3 La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.
- 6.4 La solución debe indicar el uso de las aplicaciones a lo largo del tiempo.
- 6.5 La solución debe presentar las aplicaciones usadas según su categoría.
- 6.6 La solución debe permitir a probar una aplicación o crear lista blanca la aplicación.

7. Gestión de Eventos, Tableros, Reportes y Auditoria

- 7.1 La solución debe permitir gestionar los eventos de seguridad, ya sea que se detecten/prevenan automáticamente o que los administradores/usuarios finales encuentren después de no haber sido prevenidos.
- 7.2 La solución debe contar con una vista detallada de todos los eventos de seguridad en tiempo real. Mediante la búsqueda y los filtros, puede ver eventos relacionados con cualquier período de tiempo, estado, nivel de gravedad y SaaS.
- 7.3 La solución debe contar comuna vista centrada en las amenazas de correo electrónico con información como:
- Categorías de phishing detectadas.
 - Acción sobre el correo electrónico malicioso, si está en cuarentena, en la bandeja de entrada, o en la carpeta de no deseado.
 - Usuarios involucrados en el evento (destinatarios, remitentes, propietarios de archivos compartidos).
 - Información de quien remedio la amenaza que puede ser el administrador, por la herramienta de seguridad o por el proveedor de correo en nube.
- 7.4 La solución debe proporcionar tableros análisis de eventos maliciosos detallados para cada aplicación SaaS.
- 7.5 Los Tableros (Dashboards) debe detallar los eventos de seguridad por cada aplicación SaaS de almacenamiento y/o colaboración.
- 7.6 Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.
- 7.7 La solución deberá proveer reportes ejecutivos de eventos de seguridad de los última semana, dos semanas y últimos 30 días.
- 7.8 La solución debe permitir a los administradores programar informes de seguridad se envíen con diferentes zonas horarias y a diferentes destinatarios.
- 7.9 Debe proveer capacidades de investigación que apoyen los procesos de cacería de amenazas de la organización, poder realizar consultas a toda la metadata (correos electrónicos, archivos, inicios de sesión de usuario, etc.) capturada y almacenados en el tenant.
- 7.10 La solución debe tener la posibilidad de exportar eventos a archivos CSV, json, xlsx.
- 7.11 La solución deberá proveer reportes de los eventos por hasta 180 días, en formato csv o xlsx.
- 7.12 La solución debe permitir filtrar los correos electrónicos en función de su dirección, entrante, saliente e interno.
- 7.13 La solución debe permitir que los administradores deben tener capacidad de filtrar correos por el campo de Message ID.
- 7.14 La solución debe contar con un tablero con el número de reportes phishing de los usuarios, solicitudes de restauración y socios de riesgo, así como una indicación de si las cuentas comprometidas se bloquean automáticamente o no.

7.15 La solución debe permitir a los administradores tener visibilidad del riesgo de los socios con los que comunican utilizando un motor de IA y recibir alertas sobre los socios que pueden estar comprometidos

7.16 La solución debe permitir a los administradores puedan desencadenar una acción específica cuando el dominio del remitente se parece mucho al dominio de un socio, o evitar ataques de socios comprometidos.

7.17 Solución debe permitir a los administradores puedan ver la justificación de los usuarios finales antes de aprobar / rechazar las solicitudes antes de liberar un correo de cuarentena.

7.18 Los administradores de la solución deben tener visibilidad en tiempo real de como Microsoft 365 clasificó cada correo electrónico y qué acción que tomó son sus soluciones de EOP o Defender, es decir, la solución debe trabajar con seguridad en profundidad y en capas.

7.19 Los eventos y en cada correo electrónico, deben tener la clasificación de (SCL, BCL) y que acción de cumplimiento (cuarentena, mover a junk folder) que tomó sobre el correo electrónico de acuerdo con la clasificación.

7.20 La solución debe permite filtrar correos electrónicos basado en las acciones tomadas por las herramientas o para las decisiones de cumplimiento de Microsoft.

7.21 La solución debe brindar el detalle del análisis de un archivo identificado como malicioso incluyendo los comportamientos riesgosos que fueron identificados y las técnicas identificadas. El resultado de la emulación de un archivo malicioso debe incluir un video indicando el resultado de emulación.

7.22 El panel principal debe proporcionar una descripción general de cómo la solución clasificó los correos electrónicos que Microsoft decidió dejar pasar a los usuarios finales.

7.23 La solución debe permite filtrar correos electrónicos por esta y las decisiones de cumplimiento de Microsoft.

7.24 Los usuarios finales pueden generar un nuevo informe de cuarentena (resumen) para las últimas 24 horas en cualquier momento.

7.25 La solución debe permitir a los administradores personalizar:

- Cuando y cuántas veces al día sus usuarios finales reciben el informe de cuarentena (resumen).
- La dirección de respuesta del informe de cuarentena diario enviado a los usuarios finales.
- Los textos en el cuerpo y el asunto del informe diario de cuarentena del usuario final (resumen).
- El texto del enlace en el que los usuarios hacen clic para generar un reporte.

7.26 La solución debe permitir a los administradores puedan configurar, para cada detección de Microsoft 365, si los usuarios finales pueden solicitar una restauración, restaurar por su cuenta o no pueden restaurar los correos electrónicos en absoluto.

7.27 Todas las solicitudes de restauración enviadas por los usuarios finales estarán disponibles para los administradores en el panel Solicitudes de restauración.

7.28 La solución debe permitir a los administradores puedan cargar un logotipo personalizado para agregarlo a las notificaciones por correo electrónico, las páginas del navegador y los informes.

7.29 La solución debe permitir a los administradores que puedan buscar en la consola de seguridad de correo electrónico ofertado los correos electrónicos detectados debido a una regla de transporte de Microsoft, ya sea que se entreguen al usuario final, en la carpeta de correo no deseado o que la solución de seguridad o Microsoft los pongan en cuarentena.

7.30 La solución debe permitir a los administradores puedan restringir el acceso al portal de la organización a una dirección IP o CIDR específica.

7.31 La solución debe permitir desde portal de gestión que los administradores se mantengan actualizados sobre las actividades de mantenimiento y el estado del servicio.

7.32 La solución debe permitir a los administradores puedan definir buzones dedicados para recibir alertas sobre el estado del servicio.

8. Integraciones a SIEMs y API

8.1 La solución ofertada debe permitir integrarse con soluciones SIEM mediante Syslog vía TCP, o JSON vía HTTP.

8.2 La solución debe soportar API Rest para administrar y actuar sobre los eventos de seguridad detectados.

Para la adquisición de la Continuidad del Derecho de Uso Herramienta de Email Security, los oferentes deben demostrar que poseen las calificaciones profesionales, técnicas y financieras que aseguren su competencia, los recursos financieros y el bien solicitado para cumplir con el objeto contractual.

Resultados o Productos Esperados

Para la Contratación de la Continuidad del Derecho de Uso Herramienta de Email Security se requiere el siguiente resultado: Un (1) año de soporte y actualizaciones.

Análisis de las particularidades del mercado, en cuanto a cómo y en cuáles plazos se ofrece ese bien, se presta el servicio o se ejecuta la obra.

4 CRONOGRAMA DE ACTIVIDADES

Actividad	Período de Ejecución
Fecha de Publicación del aviso de convocatoria	30 /9/2026
Presentación de aclaraciones	2/10/2026 4:00pm
Plazo máximo para expedir circulares, Enmiendas y/o Adendas	5/10/2026 4:00pm
Presentación de Credenciales/Ofertas Técnicas y Ofertas Económicas	6/10/2026 4:00pm
Apertura de la Credenciales/Ofertas técnicas y Ofertas Económicas	7/10/2026 9:30am
Notificación de errores aritméticos, de solicitud de aclaraciones económicas y de solicitud de subsanación de garantía de seriedad de la oferta	7/10/2026 3:00pm
Aceptación de correcciones de errores aritméticos y de respuesta a subsanación y a las aclaraciones.	9/10/2026 3:00pm
Acto de Adjudicación	20/10/2026
Notificación de Adjudicación	22/10/2026
Suscripción de Orden de Compras / Orden de Servicios	23/10/2026
Publicación de Orden de Compras / Orden de Servicios	26/10/2026

5 FORMA DE PRESENTACIÓN D EOFERTAS

De conformidad con el artículo 105 de la Ley núm. 47-25 y el artículo 46, párrafo I, del Decreto núm. 52-26, los oferentes deberán presentar sus propuestas por vía electrónica, a través del Sistema Electrónico de Contrataciones Públicas (SECP) o en soporte físico.

En caso de que un interesado presente oferta, tanto en formato electrónico como soporte papel, será considerada solamente la oferta electrónica. De existir discrepancias entre lo digitado en el SECP y la documentación publicada en este mismo portal, prevalecerá el documento publicado por el/la oferente, siempre que esté firmado por este/a oferente y además sellado cuando se trate de una persona jurídica.

Ninguna oferta presentada en término podrá ser desestimada en el acto de apertura. Las que fueren observadas durante el acto de apertura se agregarán para su análisis por parte de los(las) peritos designados(as)

5.1 Ofertas presentadas en formato electrónico vía el SECP

Para la presentación en línea a través del SECP, el proveedor deberá haber gestionado su usuario y vinculación del mismo a su RPE (membresía), mismos que pueden realizarse en el portal de la Dirección General de Contrataciones Públicas a través del enlace <https://www.dgcp.gob.do/servicios/vinculacion-de-usuario/>

Los (as) oferentes que presenten sus propuestas mediante el SECP, identificarán cada documentación requerida con su nombre.

Las ofertas presentadas en soporte electrónico deberán estar firmadas por el (la) oferente o de ser una persona jurídica la firma del representante legal y el sello social de la compañía.

5.2 Ofertas presentadas en Soporte Papel

Para las ofertas presentadas en formato papel los(las) oferentes, deberán presentar los documentos en un sobre, tanto en original debidamente marcado como "ORIGINAL" en la primera página del ejemplar, junto con una (01) fotocopia simple de los mismos, debidamente marcada en su primera página, como "COPIA" y en ella deberá constar la firma original del (la) oferente y de ser una persona jurídica la firma del representante legal y el sello social de la compañía.

De igual forma, el original deberá firmarse en todas las páginas por el(la) oferente y estar foliadas, y cuando se trate de una persona jurídica deberá estar firmada por el (la) representante legal y llevar el sello social de la compañía.

El sobre con la propuesta deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL(LA) OFERENTE/PROPONENTE (Sello Social)
Firma del (la) Representante Legal
DIRECCIÓN ADMINISTRATIVA
TESORERÍA DE LA SEGURIDAD SOCIAL
REFERENCIA: TSS-DAF-CM-2026-0062

6 RECEPCIÓN DE OFERTAS

Las ofertas serán recibidas a más tardar el día **6 de octubre del año 2026, hasta las cuatro de la tarde (4:00 p.m.)**. Pasada esta hora no se recibirán más ofertas.

7 DOCUMENTOS A PRESENTAR

La documentación solicitada vinculada al objeto de la contratación será analizada y evaluada por los peritos designados para constatar la elegibilidad, capacidad técnica, financiera y la idoneidad del oferente para ejecutar el contrato.

El (la) oferente/proponente es responsable de la exactitud y veracidad del contenido de los documentos que forman su oferta. Todos los documentos entregados en formato electrónico cargado en el SECP **deben llevar la rúbrica/ firma del(la) oferente o de su representante legal**, apoderado(a) o mandatario(a) designado(a) para dicho fin.

Los oferentes/proponentes extranjeros deben presentar la información homóloga de conformidad con la legislación propia del país de origen, avalados con la firma de quien tenga la competencia para hacerlo y con las traducciones al español y legalizaciones correspondientes para ser acreditados en la República Dominicana.

Un (1) Sobre A contentivo de la oferta técnica y un (1) Sobre B contentivo de la oferta económica

7.1 Credenciales

A. Documentación Legal – Subsancionable

- Formulario de Información sobre el/la Oferente (SNCC.F.042).
- Formulario de Presentación de Oferta (SNCC.F.034).
- Estar al día con sus obligaciones fiscales en la Dirección General de Impuestos Internos (DGII), **no tiene que ser depositado, será verificado en línea por la institución.**
- Estar al día con el pago de sus obligaciones de la Seguridad Social en la Tesorería de la Seguridad Social (TSS), **no tiene que ser depositado, será verificado en línea por la institución.**
- Registro de Proveedores del Estado (RPE), emitido por la Dirección General de Contrataciones Públicas **no tiene que ser depositado, será verificado en línea por la institución**
- ADM-FO-031 Formulario debida diligencia externa simplificada TSS
- Compromiso Ético Proveedores.

- Documento “Recepción y Lectura del Código de Ética” debidamente firmado y sellado. Documento que publicado en nuestro portal www.tss.gob.do sección Transparencia – Compras y Contrataciones- el Código de Ética de la institución, **Esto solo aplica para aquellas empresas que no lo hayan depositado en los registros de la TSS. Subsanable.**
- Formulario Declaración simple sobre Beneficiarios Finales suministrada a DGCP, **no tiene que ser depositado, será verificado en línea por la institución**
- Registro Mercantil vigente, **no tiene que ser depositado, será verificado en línea por la institución**

B. Documentación Técnica – No subsanable

- Oferta Técnica (conforme a las especificaciones técnicas suministradas de acuerdo con el numeral (3. Descripción del Servicio). Indicando todo el detalle técnico incluyendo descripción números de parte y requisitos mínimos imprescindibles. El oferente deberá presentar una propuesta técnica elaborada por este, con los detalles de las especificaciones técnicas del bien o servicio solicitado para este proceso. No será aceptado como oferta técnica una copia o imagen de las especificaciones de este documento en parte o su totalidad

7.2 Oferta Económica – No subsanable

- Formulario SNCC.F.033 Oferta Económica o cotización. En caso de existir discrepancias entre lo digitado en el (SECP) y la documentación publicada en este mismo portal, prevalecerá el documento publicado, siempre que esté sellado y firmado por el oferente. Debe mantenerse la unidad de medida establecida por la TSS.
- **Moneda de la Oferta:** El precio de la oferta deberá estar expresado en moneda nacional, (pesos dominicanos, RD).
- Declaración jurada de oferta libre de colusión. **Subsanable**

8 METODOLOGÍA DE EVALUACION OFERTA TÉCNICA

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar los siguientes aspectos que serán verificados bajo la modalidad “Cumple/No cumple”.

DOCUMENTACIÓN LEGAL	CUMPLE	NO CUMPLE
Formulario de Información sobre el/la Oferente (SNCC.F.042).		
Formulario de Presentación de Oferta (SNCC.F.034).		
Estar al día con sus obligaciones fiscales en la Dirección General de Impuestos Internos (DGII), no tiene que ser depositado, será verificado en línea por la institución.		
Estar al día con el pago de sus obligaciones de la Seguridad Social en la Tesorería de la Seguridad Social (TSS), no tiene que ser depositado, será verificado en línea por la institución.		
Registro de Proveedores del Estado (RPE), emitido por la Dirección General de Contrataciones Públicas no tiene que ser depositado, será verificado en línea por la institución		
ADM-FO-031 Formulario debida diligencia externa simplificada TSS		
Compromiso Ético Proveedores.		
Documento “Recepción y Lectura del Código de Ética” debidamente firmado y sellado. Documento que publicado en nuestro portal www.tss.gob.do sección Transparencia – Compras y Contrataciones- el Código de Ética de la institución, Esto solo aplica para aquellas empresas que no lo hayan depositado en los registros de la TSS.. Subsanable.		
Formulario Declaración simple sobre Beneficiarios Finales suministrada a DGCP, no tiene que ser depositado, será verificado en línea por la institución		
Declaración jurada de No Colusión		
Registro Mercantil vigente, no tiene que ser depositado, será verificado en línea por la institución		
Documento donde se haga constar que el proveedor es distribuidor autorizado de la Marca, emitido por el fabricante, con fecha de expedición en período no mayor a noventa (90) días.		

DOCUMENTACIÓN TÉCNICA	CUMPLE	NO CUMPLE
Oferta Técnica (conforme a las especificaciones técnicas suministradas de acuerdo con el numeral (3. Descripción del Servicio). Indicando por escrito todo el detalle técnico incluyendo descripción y requisitos mínimos imprescindibles. El oferente deberá presentar una propuesta técnica elaborada por este, con los detalles de las especificaciones técnicas del bien o servicio solicitado para este proceso.		

No será aceptado como oferta técnica una copia o imagen de las especificaciones de este documento en parte o su totalidad		
---	--	--

9 METODOLOGÍA DE EVALUACION OFERTA ECONÓMICA

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar los siguientes aspectos que serán verificados bajo la modalidad "Cumple/No cumple".

OFERTA ECONÓMICA	CUMPLE	NO CUMPLE
Formulario SNCC.F.033 Oferta Económica o cotización. (No subsanable). En caso de existir discrepancias entre lo digitado en el (SECP) y la documentación publicada en este mismo portal, prevalecerá el documento publicado, siempre que esté sellado y firmado por el oferente. Debe mantenerse la unidad de medida establecida por la TSS		
Moneda de la Oferta: El precio de la oferta deberá estar expresado en moneda nacional, (pesos dominicanos, RD)		
Declaración Jurada de Oferta Libre de Colusión, subsanable		

10 CRITERIOS DE ADJUDICACIÓN

Se evaluará las Ofertas dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás, que regulan la actividad contractual, y comunicará por escrito al Oferente/Proponente que resulte favorecido. Al efecto, se tendrán en cuenta los factores económicos y técnicos más favorables.

El criterio de adjudicación para determinar la oferta más conveniente en este procedimiento de contratación es **adjudicación basada en menor precio**.

11 DEBIDA DILIGENCIA

TESORERÍA DE LA SEGURIDAD SOCIAL, para reducir la exposición de este procedimiento de contratación a riesgos legales, operativos, financieros, tecnológicos, antrópicos, económicos, de corrupción, de integridad, reputacionales, de lavado de activos, de conflictos de interés, de colusión, entre otros, se llevará a cabo la debida diligencia a los oferentes participantes como medida de mitigación para los diversos riesgos asociados con el procedimiento, garantizando la integridad, transparencia y legalidad de este.

En ese sentido, la TESORERÍA DE LA SEGURIDAD SOCIAL se reserva la facultad de realizar el proceso de debida diligencia dentro del marco de la presente contratación a fin de:

- Comprobar y verificar la identidad del proveedor sobre la base de documentos, datos o informaciones obtenidas de fuentes fiables e independientes;
- Identificar al Beneficiario Final de la empresa proveedora;
- La existencia o no de procesos judiciales actuales o pasados vinculados a delitos contra la administración pública, lavado de activos y otros;
- Constatar errores o escrituras similares en los documentos presentados por diferentes empresas en el procedimiento de contratación;
- Identificar coincidencias en algunos de los datos suministrados por distintos proveedores tales como: domicilio accionistas, teléfonos, entre otros;
- Validar los permisos, licencias o autorizaciones de entidades competentes como Dirección General de Impuestos Internos o las Cámaras de Comercio y Producción, que administran el Registro Mercantil, entre otros;
- Prevenir vulneraciones al régimen de inhabilidades para contratar con el Estado, establecido en el artículo 14 de la Ley Núm. 340-06 y sus modificaciones;
- Determinar posibles vinculaciones entre oferentes y funcionarios públicos de la organización para gestionar posibles conflictos de interés;
- Identificar propuestas idénticas en el procedimiento de contratación;
- Detectar si una Persona Expuesta Políticamente (PEP) es accionista o socia de una persona jurídica, la cual, a su vez se encuentra participando en el procedimiento.
- Determinar la presencia de empresas recién constituidas en un procedimiento de contratación, que no presentan la

capacidad financiera para ser adjudicadas, a la vez que se asocian a un mismo proponente.

Si durante la realización de la debida diligencia, se determina que el oferente está sujeto a inhabilidades, ha proporcionado información falsa, o ha manipulado o falsificado documentos, así como participado en prácticas de colusión, coerción u obstrucción, la entidad contratante deberá comunicar al oferente por escrito la existencia de tales indicios. Además, le otorgará un plazo de cinco (05) días hábiles para que el oferente presente, también por escrito, sus argumentos y evidencias que demuestren que no existe lo alegado.

Si el oferente no presenta sus argumentos dentro del plazo estipulado, no se refiere a lo solicitado o no logra demostrar la inexactitud de los indicios identificados, quedará descalificado. En consecuencia, su oferta será desestimada, lo cual será documentado y motivado en el correspondiente informe de evaluación técnica, sin perjuicio de las demás acciones civiles, administrativas y penales que pudieran corresponder.

12 ADJUDICACIÓN

La Adjudicación será **a un único oferente**, decidida a favor del Oferente/Proponente cuya propuesta cumpla con los requisitos exigidos y sea calificada como la más razonable para los intereses institucionales tomando en cuenta la recomendación de los peritos técnicos mediante el informe pericial y considerando calidad y precio en las evaluaciones además las condiciones que se establecen en el presente Pliego de Condiciones Específicas.

Si se presentase una sola Oferta, ella deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en las Especificaciones Técnicas, se le considera conveniente a los intereses de la Institución.

El Contrato que resulte de este procedimiento de selección será mediante un contrato de servicio, este Contrato con independencia de su firma tendrá una duración de doce (12) meses

13 ENTREGA Y RECEPCIÓN

El servicio deberá ser entregado no más de Veinte (20) días hábiles, luego de la recepción de la certificación del contrato. de acuerdo con lo establecido en el presente documento.

Agotado este proceso y presentada la factura por parte del proveedor se procederá a tramitar el pago correspondiente a esta etapa.

No se entenderán suministrados, ni entregados los servicios que no hayan sido objeto de recepción definitiva.

Si se estimase que los citados servicios no son aptos para la finalidad para la cual se adquirieron, se rechazarán los mismos y se dejarán a cuenta del Proveedor, quedando la Entidad Contratante exenta de la obligación de pago y de cualquier otra obligación.

El oferente interesado en participar en el referido proceso debe estar en la disposición de prestar el servicio luego que se le emita la orden de servicios de acuerdo con requerimiento y coordinación del área requirente de esta entidad.

Por ningún motivo la empresa adjudicada podrá cambiar o modificar las características de lo cotizado.

El lugar de entrega del bien será en el domicilio: Torre de la Tesorería de la Seguridad, Num.33, ubicado en la Avenida Tiradentes, Ensanche Naco, Santo Domingo, Distrito Nacional.

14 Tiempo de ejecución del servicio

Se requiere la continuidad de la suscripción de derecho de uso durante 12 meses, período establecido en las especificaciones técnicas, abarcando desde el 22 de octubre 2026 hasta el 22 de octubre del 2027.

El plazo mencionado supone un ritmo de labor con jornadas y horarios que el oferente deberá expresar en su propuesta, para que la institución contratante realice los controles que le competen. Los aumentos de horario que disponga el proveedor no originarán mayores erogaciones para la institución contratante y serán asumidas exclusivamente por éste.

El plazo para la ejecución del servicio propuesto por el proveedor adjudicatario se convertirá en el plazo contractual, siempre y cuanto se ajuste al estimado propuesto por la institución contratante.

SUPERVISOR DE LA CONTRATACIÓN

La Tesorería de la Seguridad Social ha designado como supervisor o responsable del contrato a la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad, bajo la responsabilidad de José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad

15 PERITO TÉCNICO

Se designa al Sr. José Alberto Luna Peña o quien este designe como perito técnico a los fines de que evalúen las ofertas de los proponentes que participarán, y rinda los informes según corresponda.

16 TIEMPO PARA ENTREGA DE LOS BIENES/SERVICIOS

Los servicios deberán entregarse no más de Veinte (20) días hábiles, luego de la recepción de la orden de compras y/o certificación de contrato en los casos que aplique.

17 PRESUPUESTO REFERENCIAL

El presupuesto base para la adquisición de **Continuidad del Derecho de Uso de la Herramienta de Email Security** asciende a **RD\$ 1,930,800.00 exento de ITBIS**, valor que ha sido obtenido en el marco de los estudios previos realizados y que sustentan el expediente de la presente contratación.

18 CONDICIONES DE PAGO

- Será realizado un único pago cuya gestión de pago se iniciará una vez recibidos conforme por José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad, o quien este designe en su representación. El proveedor que resulte adjudicado deberá emitir una factura con Número de Comprobante Gubernamental.
- El pago se realizará dentro de los treinta (30) días laborales siguientes a la fecha de recepción de la factura.
- Si una MIPYME resulta adjudicada, se hará un anticipo del 30% del valor del contrato en un plazo no mayor a treinta (30) días hábiles desde la certificación del contrato, contra presentación de la Garantía de Buen Uso del anticipo. El 70% restante se pagará en un único pago tras la entrega y aprobación por la Dirección de Tecnología de la Información y Comunicación, en un plazo no mayor a treinta (30) días hábiles.
- Conforme establece el artículo 225 del reglamento de aplicación de la ley 47-25 aprobado con el decreto 52-26, el desembolso del pago realizado a una MIPYME por concepto de anticipo debe ser registrado obligatoriamente en el Sistema Electrónico de Contrataciones Públicas, así como la constancia de su aplicación en la ejecución contractual.
- En cada factura podrán ser solicitadas certificaciones de la DGII y TSS a los fines de gestionar el pago, según corresponda.
- El proveedor adjudicatario deberá mantenerse en todo momento al día con sus obligaciones fiscales y de seguridad social, según corresponda, para poder recibir el pago correspondiente. En ese sentido, si por el no cumplimiento de estas obligaciones por parte del adjudicatario la Tesorería se ve imposibilitada de recibir el servicio objeto de la presente contratación, el contrato podrá ser rescindido dando pie a la adjudicación del proveedor que haya quedado en segundo lugar o a un nuevo proceso según corresponda.
- Los pagos se harán por transferencia bancaria a la cuenta que el proveedor tenga registrada en la DGCP, por lo que para recibir los pagos el suplidor debe encontrarse registrado como beneficiario en la Dirección General de Contrataciones Públicas y tener cuenta registrada. Esta cuenta debe ser en pesos dominicanos.
- La Tesorería de la Seguridad Social realiza retención del Impuesto Sobre la Renta de acuerdo con las Normas Legales Vigentes de la Dirección General de Impuestos Internos.

19 GARANTÍAS

Garantía de Fiel Cumplimiento de Contrato.

La garantía de fiel cumplimiento debe ser obligatoriamente integrada por los adjudicatarios cuyos contratos u órdenes de compra o de servicio excedan el equivalente en pesos dominicanos de US\$10.000,00, en el plazo de cinco (5) días hábiles, contados a partir de la notificación de la adjudicación.

En esos casos, corresponderá al adjudicatario(a) presentar en un plazo no mayor de (cinco (5) días hábiles una garantía de tipo Póliza de Fianza equivalente al cuatro por ciento (4 %) del monto de la adjudicación.

Si se trata de un adjudicatario certificado como MIPYME, el equivalente será uno por ciento (1 %) del monto de la adjudicación y solo le será exigida la fianza de seguro, con la condición de ser **incondicional, irrevocable y renovable**. Si se trata de un adjudicatario extranjero, el plazo para presentar la garantía es de diez (10) días hábiles.

La vigencia de la garantía será de mínimo de un (1) año contado a partir de la constitución de esta y hasta el fiel cumplimiento y la liquidación del contrato.

Si el (la) o los (las) adjudicatarios (as) no presenta la garantía de fiel cumplimiento de contrato en el plazo señalado, se considerará una renuncia a la adjudicación que dará paso a que la institución proceda a realizar una adjudicación posterior al oferente que haya quedado en segundo lugar, conforme al reporte de lugares ocupados.

La garantía de fiel cumplimiento será devuelta luego de la recepción conforme del servicio incluidas las obligaciones de seguridad social y tras ser constituida y presentada la garantía de vicios ocultos a favor de la institución contratante.

Garantía de Buen Uso del Anticipo

El proveedor que por su condición de MIPYME requiera el treinta por ciento (30%) como anticipo, deberá entregar una fianza de seguro, con la condición de ser **incondicional, irrevocable y renovable**, por el valor total del anticipo, en un plazo no mayor a cinco (05) días hábiles.

20 TERMINOS Y CONDICIONES

- En caso de empate entre oferentes, se dará preferencia a aquellos oferentes que hayan demostrado la contratación de personas con discapacidad como una buena práctica de inclusión, lo cual se debe evidenciar con la certificación del CONADIS. Si ninguno de los oferentes cumple con este requerimiento, se hará por sorteo entre los oferentes.
- En caso de que el oferente no cumpla en los requisitos técnicos no será necesario solicitar subsanación de credenciales.
- No se acepta variación en los precios ofertados ni las unidades requeridas, la remisión de la propuesta indica la aceptación de lo establecido en los presentes Términos de Presentación de Propuestas.
- Si por el no cumplimiento de estas obligaciones por parte del adjudicatario la Tesorería de la Seguridad Social se ve imposibilitada de recibir los servicios objeto de la presente contratación, el contrato podrá ser rescindido dando pie a la adjudicación de la empresa que haya quedado en segundo lugar o a un nuevo proceso.
- La remisión de la oferta indica la aceptación de los términos establecidos
- Tener en su registro mercantil, registro en la administración tributaria y registro de proveedor, la actividad comercial relacionada al objeto del proceso de contratación que se esté celebrando. **De no contar con la actividad comercial no será tomado en cuenta para evaluación.**

21 DERECHO A PARTICIPAR

Toda persona natural o jurídica, nacional o extranjera, de manera individual o en consorcio, que tenga conocimiento de este procedimiento tendrá derecho a participar, siempre y cuando reúna las condiciones siguientes:

- 1) Demuestre su plena capacidad conforme a los requisitos exigidos en el artículo 35 de la Ley Núm. 47-25;
- 2) No se encuentre afectado por el régimen de prohibiciones o inhabilidades indicado en el artículo 38 de la Ley Núm. 47-25;
- 3) Cumple con las condiciones de participación establecidas en este pliego de condiciones, adendas/enmiendas, circulares y en sus anexos (formularios, modelos de contratos, planos, presupuestos, estudios, etc., según aplique).

No se permite la múltiple participación, esto es, una persona física no podrá participar como persona física si la empresa en la que es socio también participa y viceversa. En ese sentido, los participantes que posean esta condición deben elegir inscribirse únicamente en una de sus calidades: persona física o jurídica en el procedimiento convocado. De igual manera, no podrán

participar simultáneamente empresas que: 1) posean la misma identidad de socios o accionistas, o 2) coincidan en alguno de los socios. En ese sentido, deberán participar por una sola de las empresas

En cuanto a los consorcios, de conformidad con el párrafo I del artículo 36 de la Ley núm. 47-25 y sus modificaciones, las personas físicas o jurídicas que formasen parte de un consorcio o unión temporal de oferentes, no podrán presentar otras ofertas en forma individual o como integrante de otro consorcio, en el presente procedimiento de contratación.

22 PRACTICAS PROHIBIDAS

En el curso del procedimiento de selección la institución contratante puede advertir que alguno de los oferentes incumple alguna de las condiciones previstas en el numeral 21 sobre “Derecho a participar”, así como las prácticas corruptas o fraudulentas, comprendidas en la Ley 47-25 y su reglamento de aplicación, el Código Penal o dentro de la Convención Interamericana contra la Corrupción, o cualquier acuerdo entre proponentes o con terceros, que establecieren prácticas restrictivas de la libre competencia como los acuerdos colusorios o carteles. También intentos de un Oferente/Proponente para influir en la evaluación de las ofertas o decisión de la adjudicación.

Lo anterior, serán causales determinantes del rechazo de la propuesta en cualquier estado del procedimiento de selección o de la rescisión del contrato, si éste ya se hubiere celebrado sin perjuicio de las demás acciones administrativas, civiles o penales que establezcan las normas; lo cual será documentado y motivado en el correspondiente informe de evaluación emitido por los peritos designados, según la fase en la que se encuentren. En ese tenor, la institución contratante deberá agotar el debido proceso y dejar constancia documental de la decisión de descalificación en el expediente de contratación.

23 ERRORES NO SUBSANABLES

Los errores NO subsanables en este proceso son:

- Omitir cualquiera de los documentos No Subsanales o que los mismos no incluyan las informaciones solicitadas.
- Omitir la Presentación de Oferta Económica o que en la misma no estén los datos requeridos.
- El no estar evidenciado en la oferta técnica el cumplimiento de los requisitos de acuerdo con lo establecido por la TSS
- Presentar la oferta en moneda diferente a pesos dominicanos.
- Presentar la propuesta técnica diferente a lo solicitado en el pliego de condiciones
- Entregar una imagen del pliego de condiciones como oferta técnica o parte de ella, conforme a las especificaciones técnicas suministradas en el numeral correspondiente a las Especificaciones técnicas del servicio.
- Omitir uno o varios de los documentos enviados a subsanar o no subsanar en el tiempo establecido en el cronograma del procedimiento o en la comunicación de notificación
- Las subsanaciones deben hacerse dentro del período de subsanación establecido en el cronograma, de lo contrario la propuesta será rechazada sin más trámite.

24 NOTA IMPORTANTE:

El incumplimiento del Contrato y/o Orden de Compra por parte del adjudicatario determinará la finalización de la Orden de Compras o Contrato, en ese caso, esta Tesorería de la Seguridad Social aplicará las sanciones previstas en la Ley 47-25, reservándose el derecho de solicitar a la Dirección General de Contrataciones Públicas, en su calidad de Órgano Rector del Sistema las sanciones establecidas en la Ley 47-25 dependiendo de la gravedad de la falta.

25 PENALIDADES:

En caso de retraso en el cumplimiento de las obligaciones de EL PROVEEDOR por causas imputables a éste, se deberá resarcir a la parte afectada por los daños y perjuicios ocasionados, a través de la ejecución de la garantía y/o la indemnización correspondiente, conforme establecen los artículos 134, 144 y 145 de la ley 47-25.

26 ANEXOS:

- Formulario de Oferta Económica (SNCC.F.033)
- Presentación de Oferta (SNCC.F.034)
- Formulario de Información sobre el oferente (SNCC.F.042)
- Formulario de recepción y lectura de Código de Ética
- Compromiso Ético de Proveedores
- Formulario Declaración simple sobre Beneficiarios Finales suministrada a DGCP
- ADM-FO-031 Formulario debida diligencia externa simplificada TSS
- Declaración jurada de oferta libre de colusión **subsanable**

27 CONTACTO

Para consultas sobre el proceso puede comunicarse por mensaje en el SECP o a por las siguientes vías:

Departamento de Compras y Contrataciones de la TSS

Correo electrónico: cotizaciones@tss.gob.do

Dirección: Avenida Tiradentes, No.33, Ensanche Naco

Teléfono: 809-567-5049 ext. 3051



Tesorería de la Seguridad Social

Rosa Elizabeth Nuñez Fernández - Enc. Dpto. de Compras y Contrataciones

Documento Firmado digitalmente, para validar por medio electrónico:

<https://buzon.firmagob.gob.do/inbox/app/tss/v/98dd1715-cc13-4cd3-a963-4889132349a9>