

Informe de Estudios Previos
Para la Contratación de la Continuidad del Derecho de Uso Herramienta de Concientización en
Ciberseguridad

A fin de preparar los procedimientos de contrataciones públicas con la información precisa y suficiente que justifique la necesidad de la contratación y la modalidad de selección del proveedor, es necesario que todo procedimiento de contratación se encuentre sustentado en estudios previos, de conformidad con las disposiciones del artículo 87 de la Ley 47-25 de Contrataciones Públicas así como su Reglamento de aplicación aprobado mediante el Decreto 52-26 y las políticas, manuales, guías u orientaciones normativas dictadas por la Dirección General de Contrataciones Públicas o las regulaciones especiales aplicables al objeto contractual, por lo que la Tesorería de la Seguridad Social (TSS), como parte de la etapa precontractual ha realizado el presente informe de estudios previos con la finalidad garantizar la correcta selección de los procedimientos, un mejor aprovechamiento de los recursos y una mayor eficiencia en la ejecución de los contratos.

El objetivo del presente informe es presentar los resultados de los estudios previos, que serán el punto de partida para el diseño del procedimiento a realizar para la Contratación de la Continuidad del Derecho de Uso Herramienta de Concientización en Ciberseguridad, en cumplimiento con lo establecido en la Ley 47-25 y su Reglamento de aplicación aprobado mediante el Decreto No. 52-26.

En este sentido, luego de varias gestiones de levantamiento de información y consultas de las informaciones disponibles, del análisis de procesos históricos y de la validación de las condiciones de disponibilidad de dichos productos en el mercado, así como del análisis de la necesidad que se pretende satisfacer, se establecen a continuación los siguientes resultados.

Identificación de la necesidad y justificación del proceso

La Tesorería de la Seguridad Social (TSS) desempeña un papel fundamental en la gestión eficiente de los procesos de recaudo, distribución y pago de las cotizaciones del Sistema Dominicano de Seguridad Social (SDSS), así como el Sistema Único de Información y Recaudo (SUIR), por lo que, en el Plan Anual de Contrataciones (PAC), ha consignado para el año 2026 la Contratación de la Continuidad del Derecho de Uso Herramienta de Concientización en Ciberseguridad el marco de su Plan Estratégico Institucional (PEI) para el periodo 2025-2028.

Este servicio tiene la finalidad de fortalecer la postura de seguridad de la institución mediante una capacitación avanzada, continua y personalizada. A su vez, permitirá reducir el riesgo humano frente a amenazas digitales a través de simulaciones realistas de ataques, análisis detallados del comportamiento de los usuarios y el fomento de una cultura de seguridad resiliente, en alineación con las mejores prácticas y marcos normativos vigentes.

Especificaciones técnicas

Para la Contratación de la Continuidad del Derecho de Uso Herramienta de Concientización en Ciberseguridad, se requiere que los servicios contengan las siguientes especificaciones técnicas:

Ítem	Rubro	Cantidad	Descripción	Especificaciones
1	81112501	1	Adquisición de la Continuidad del Derecho de Uso Herramienta	*Ver especificaciones debajo.

			de Concientización en Ciberseguridad	
--	--	--	---	--

- 400 usuarios.
- Módulos de capacitación interactivos que incluyan videos, juegos, carteles, boletines informativos y otros materiales de refuerzo.
- Módulos de videos en formato MP4 que puedan visualizarse mediante navegador o descargarse.
- Módulos optimizados para que su visualización e interacción se lleven a cabo desde dispositivos móviles.
- Que permita realizar evaluaciones sobre los puntos de conocimiento fuertes y débiles de su organización. Y que permita utilizar los resultados de esta evaluación para crear un plan de capacitación en concientización sobre seguridad más específico.
- Que permita aprendizaje opcional o recomendado mediante inteligencia artificial, de acuerdo con las necesidades o perfil de riesgo de los usuarios.
- Que cuente con capacidades adaptativas que permitan ajustar la experiencia de aprendizaje en función del riesgo y comportamiento del usuario.
- Que provea juegos u otras actividades interactivas para reforzar las habilidades y conocimientos que los usuarios adquieren durante la capacitación.
- Que incluya boletines informativos y documentos de seguridad en formato PDF, así como imágenes o afiches de alta calidad que puedan imprimirse o compartirse digitalmente con los usuarios y que cubran temas de ciberseguridad para reforzar las habilidades adquiridas durante la capacitación.
- Que incluya plantillas de phishing recomendadas o generadas con apoyo de inteligencia artificial.
- Que permita realizar simulaciones de phishing mediante llamadas o mecanismos de callback phishing.
- Que permita realizar una encuesta de cultura de seguridad, para medir el progreso y los aspectos que impulsan el comportamiento social de los usuarios.
- Que permita realizar una encuesta de cultura de seguridad, para medir el progreso y los aspectos que impulsan el comportamiento social de los usuarios.
- Que incluya agentes de inteligencia artificial o capacidades equivalentes para apoyar al administrador en la gestión de la capacitación, programación y demás tareas administrativas relacionadas con el programa de concientización.
- Que permita ver el puntaje de riesgo general de su organización, así como puntaje de riesgo por grupos y puntaje de riesgo por usuario; basado en los resultados de las actividades realizadas dentro de la plataforma.
- Que permita integraciones de primera parte y con soluciones de terceros.
- Que disponga de conectores iPaaS para integración con otras soluciones.
- Que disponga de integración mediante Graph API.
- Que permita realizar una revisión de las contraseñas de los usuarios en busca de cualquier vulnerabilidad detectada en su Active Directory. Incluyendo comprobación de contraseñas compartidas, débiles o que aparecen con violaciones de seguridad de datos de dominio público para que se pueda establecer una base de referencia de los problemas de contraseñas y gestionar un menor riesgo entre usuarios.
- Que incluya una funcionalidad para la identificación y gestión de riesgos relacionados con las contraseñas de los usuarios, como PasswordIQ o funcionalidad equivalente.

- Que incluya funcionalidad Second Chance o equivalente.
- Soporte ilimitado de fábrica, en español, con un asesor personalizado
- Reconocimiento: Que la herramienta esté reconocida en al menos dos (2) de los siguientes reportes, plataformas o reconocimientos de la industria: TrustRadius, teissAwards, G2 o Frost & Sullivan.
- Soporte de proveedor con certificaciones mínimas requeridas:
 - 1 certificación en ciberseguridad.
 - 1 certificación relacionada con temas de capacitación o concientización en ciberseguridad.
 - 1 certificación de administrador de la plataforma otorgada por el fabricante.
- Funcionalidad de Políticas Opcionales en Cursos de Capacitación:
 - La plataforma deberá permitir la incorporación y difusión de políticas definidas por la organización dentro de cursos o actividades de capacitación. Dichas políticas podrán presentarse de forma independiente o integradas al contenido del curso.
 - La plataforma deberá permitir que los usuarios reconozcan o confirmen la lectura de las políticas.
 - La plataforma deberá generar reportes que permitan verificar si cada política ha sido reconocida o aceptada por los usuarios.

Objetivos específicos:

1. **Entrenar a los usuarios con contenido premium y actualizado**, adaptado a distintos niveles de conocimiento y roles.
2. **Ejecutar simulaciones avanzadas de phishing, spear phishing**, ataques de ingeniería social y otras amenazas emergentes.
3. **Automatizar campañas de capacitación** basadas en el comportamiento y desempeño del usuario.
4. **Medir y mejorar continuamente** el nivel de riesgo humano a través de reportes avanzados, puntuaciones de riesgo (User Risk Score), y comparaciones con otras organizaciones.
5. **Promover una cultura de seguridad de alto impacto**, alineando comportamientos individuales con las políticas de ciberseguridad de la empresa.

Para la Contratación de la Continuidad del Derecho de Uso Herramienta de Concientización en Ciberseguridad, 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 Concientización en Ciberseguridad 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.

Plazo y Lugar de ejecución del objeto del proceso

El lugar de entrega de ejecución de los servicios será en el domicilio Tesorería de la Seguridad Social (TSS), ubicado en la Avenida Tiradentes No. 33, Torre de la Seguridad Social, Ensanche Naco, Santo Domingo, Distrito Nacional.

Tiempo de ejecución del servicio

El tiempo de ejecución del servicio será por el periodo de **1 año**. A partir del 30 de noviembre de 2026 al 30 de noviembre de 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 de entrega de los servicios objeto del presente contrato será no más de Veinte (20) días hábiles, luego de la recepción de la certificación del contrato por la Contraloría General de la República. En cumplimiento con lo establecido en el Párrafo III del Artículo 134 de la Ley No. 47-25 de Contrataciones Públicas.

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

Modalidad del procedimiento aplicable, tipo de contrato y resultados esperados

Conforme el costo estimado de la contratación se ha determinado, tomando en cuenta la Resolución Núm. PNP-03-2026 que establece los umbrales tope para la determinación de la modalidad de selección de los procedimientos de contratación pública, correspondientes al año dos mil veinticinco (2026) y la naturaleza de lo requerido, que la modalidad de la contratación será a través de un procedimiento de **Contratación Menor** y la adjudicación será a un **único proveedor**.

El Contrato que resulte de este procedimiento de selección será mediante un contrato de **servicios**, para el cual se requiere la presentación de una garantía de seriedad de la oferta y una garantía de fiel cumplimiento de contrato conforme a las disposiciones y porcentajes establecidos a partir del artículo 162 de la Ley 47-25.

Análisis de oferta y demanda y riesgos previsible involucrados en la contratación de los servicios requeridos:

En el proceso de selección de proveedores para la **Adquisición de la Continuidad del Derecho de Uso de la Herramienta de Concientización en Ciberseguridad** se ha identificado un número considerable de proveedores a nivel nacional, considerando los aspectos de oferta y demanda, así como las cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, en tal sentido, es necesario que los oferentes cumplan con los requisitos para garantizar la calidad y el respaldo de los servicios.

Por la naturaleza del proceso, no se requiere presentar muestras, sino que en la propuesta técnica el oferente debe demostrar el cumplimiento de las especificaciones técnicas descritas en este informe de estudios previos.

Los riesgos de esta contratación han sido identificados y establecido en la matriz de riesgos que se anexa al presente informe la cual abarca desde la planificación hasta la adjudicación, liquidación del contrato, vencimiento de garantías de calidad del objeto del contrato.

Supervisor del contrato

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.

Condiciones de pago

- Será realizado **un único pago**, cuya gestión será iniciada 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 hábiles 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 una Póliza de Seguro. Este anticipo le será descontado al monto a pagar por la factura recibida, tras la entrega y aprobación por el señor José Alberto Luna Peña, 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 los servicios 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.

El costo estimado del bien, obra o servicio a contratar, que determine el presupuesto de la contratación e identifique la partida presupuestaria a afectar.

El costo estimado para la **Adquisición de la Continuidad del Derecho de Uso de la Herramienta de Concientización en Ciberseguridad** es de **Ochocientos Cincuenta Mil Pesos Dominicanos con 00/100 (RD\$ 850,000.00), Exento de ITBIS**. El precio puede estar sujeto a cambios debido a:

- **La variación en la tasa del dólar:** Muchos productos se importan o contienen componentes importados que están afectados por la tasa de cambio del dólar estadounidense. Si la tasa de cambio del dólar sube en relación con la moneda local, los productos importados pueden volverse más caros, lo que podría aumentar el precio final para los consumidores.
- **La falta de abastecimiento en el mercado local:** Escasez de un producto en el mercado local debido a factores como problemas de producción, interrupciones en la cadena de suministro o una demanda inesperadamente alta, los precios tienen a subir. La oferta limitada en comparación con la demanda puede conducir a un aumento en los precios.
- **Políticas del fabricante sobre tiempos de renovación o adquisición del producto:** los fabricantes pueden tener políticas que influyen en el precio final de un producto, como establecer precios según la demanda o introducir nuevas versiones o modelos que afectan la percepción del valor anterior. Además, los programas de renovación o adquisición pueden influir en el precio si incluyen descuentos, incentivos u otros términos que afecten el costo para el consumidor.

El costo estimado para la adquisición de los servicios se hace en base a las informaciones disponibles en el SECP, en los catálogos de bienes y servicios y en el Sistema de Información de Precios, administrados por la Dirección General de Contrataciones Públicas. Además, se tomó en cuenta las diferentes variaciones que pueden afectar el precio final.

Los criterios sociales, ambientales y económicos asociados a la contratación, con el propósito de generar los mayores beneficios posibles, con los recursos disponibles.

Por la naturaleza de la contratación, se pudieran considerar criterios sociales que fomenten la inclusión de proveedores identificados como Mipymes o que se demuestre a través de buenas prácticas la inclusión social a través de la contratación de personas con discapacidad certificadas por el CONADIS o el fomento de políticas de responsabilidad ambiental en las empresas. Todo esto será determinado al momento de la elaboración del Pliego de Condiciones pudiéndose utilizar estos criterios como mecanismos de desempate.

Regulaciones aplicables a los bienes, servicios u obras.

El Decreto 71-21 y la Comunicación MINPRE-DMI-2022 del 01/02/2022 establecen la necesidad de que la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) emita informes y peritajes técnicos para los bienes y servicios que se adquieran y/o renuevan para las instituciones públicas en el marco de los procesos de compras y contrataciones relacionadas con Gobierno Digital.

Esto implica que la OGTIC tiene la responsabilidad de evaluar la idoneidad, eficiencia y seguridad de las soluciones tecnológicas que se pretenden adquirir y/o renovar para su uso en las instituciones públicas.



Sus informes y peritajes técnicos ayudarán a garantizar que las adquisiciones y/o renovaciones cumplan con los estándares requeridos en materia de tecnología de la información y comunicación, así como con los objetivos de Gobierno Digital establecidos por el gobierno.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) días del mes de agosto del año dos mil veintiséis (2026).

Jose Alberto Luna Peña
Responsable Técnico

Elisa Cristina Jaquez Diaz
Responsable Legal

Darlin Antonio Martinez Diaz
Responsable Financiero



Tesorería de la Seguridad Social
Jose Alberto Luna Peña - Asesor de Ciberseguridad
Darlin Antonio Martinez Diaz - Analista de Compras y Contrataciones
Elisa Cristina Jaquez Diaz - Analista de Compras y Contrataciones
Documento Firmado digitalmente, para validar por medio electrónico:
<https://buzon.firmagob.gob.do/inbox/app/tss/v/9c51d879-4859-4a1c-9998-e104f8f7693e>