SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES

PLIEGO ESTÁNDAR DE CONDICIONES PARA LA COMPRA DE BIENES

ADQUISICIÓN Y RENOVACIÓN DE LICENCIAS INFORMÁTICAS PARA USO DE LA SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES.

SISALRIL-CCC-LPN-2025-0007

Santo Domingo
República Dominicana
Septiembre 2025

CONTENIDO

SECCIÓN I: INFORMACIONES PARTICULARES DEL PROCEDIMIENTO

1. Antecedentes

La Superintendencia de Salud y Riesgos Laborales (SISALRIL) es una entidad estatal, autónoma, con personería jurídica y patrimonio propio, dotada de un personal técnico y administrativo altamente calificado; la cual, a nombre y representación del Estado Dominicano para ejercer funciones, tales como: Velar por el estricto cumplimiento de la ley 87-01 y sus normas complementarias, Proteger los intereses de los afiliados, Vigilar la solvencia financiera del Seguro Nacional de Salud, las Administradoras de Riesgos de Salud (ARS) y la Administradora de Riesgos Laborales (ARL) y Contribuir a fortalecer el Sistema Nacional de Salud.

La Superintendencia de Salud y Riesgos Laborales (SISALRIL) en su Plan Operativo Anual (POA) y en su Plan de Compras y Contrataciones (PACC) ha consignado para este año 2025 la Adquisición y renovación de Licencias Informáticas, con miras a cumplir con los objetivos institucionales y garantizar la operatividad diaria de la institución.

2. Objeto del procedimiento de selección

Constituye el objeto de la presente convocatoria recibir ofertas para la **Adquisición y Renovación de Licencias Informáticas para uso de la Superintendencia de Salud y Riesgos Laborales** de acuerdo con las condiciones fijadas en el presente pliego de condiciones y sus especificaciones técnicas, dicha contratación ha sido clasificada bajo el rubro -clase- **81112500-Servicio de alquiler o arrendamiento de licencias de software informático** por lo que los oferentes deberán tener preferiblemente la actividad comercial **81110000-Servicios informáticos.**

3. Descripción de los bienes

ADQUISICIÓN Y RENOVACIÓN DE LICENCIAS INFORMÁTICAS PARA USO DE LA SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES.

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
1	Renovación de la solución VEEAM Advance de respaldo para 100 instancias, con el módulo de VEAAM DATA CLOUD ADVANCE con 20 TB Numero de contrato 03208836 Licenciamiento por 1 año	1

- La solución debe admitir la copia de seguridad a nivel de imagen sin agentes de las máquinas virtuales Nutanix AHV
- La solución debe admitir copias de seguridad utilizando los snapshots nativos de Nutanix para copias de seguridad frecuentes y rápidas
- La solución debe admitir la recuperación granular de archivos y elementos de aplicaciones desde la copia de seguridad a nivel de imagen sin agentes
- La solución debe permitir la recuperación por snapshot de máquinas desde el respaldo.
- La solución debe tener la capacidad de usar Prism Central Categories como origen de respaldos
- Debe permitir respaldos por snapshots a nivel de Protection Domains con changed blocks tracking

- Debe permitir soporte para clústeres NC2
- Las tareas de respaldo deben permitir agregar o excluir combinaciones de recursos: VM, PD, clústeres
- Debe permitir restaurar discos virtuales a otras VMs ejecutándose en un cluster AHV
- La solución permite respaldo consistente con integración de VSS sin necesidad de agente, así como la posibilidad de integrar scripts durante la tarea de respaldo
- La solución permite el respaldo consistente de PostgreSQL, Oracle, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint y Microsoft Exchange.
- La solución debe poseer mecanismos propios de escaneo de malware durante el respaldo en línea para detectar amenazas a nivel de filesystem y por entropía, como onion links, ransom notes y encriptación.
- La solución debe tener la capacidad de replicar respaldos de VMs a otros sitios o a nube para recuperación ante desastres
- La solución debe permitir flexibilidad de repositorios, incluido repositorios del tipo object Storage, con capacidad de creación de tiers de repositorios
- Debe permitir la integración de Nutanix Guest Tools como opción de consistencia de respaldos.
- La solución debe permitir migrar de Nutanix AHV hacia VMware y Hyper-V, así como hacia AWS EC2, Azure VM y GCP VM. Además, debe permitir realizar migración desde VMware, Hyper-V, Proxmox VE y oVirt KVM hacia Nutanix AHV.
- Debe tener capacidad de recuperación instantánea de VMs en minutos
- La solución debe soportar RBAC y MFA
- La solución debe tener integración con repositorios inmutables y encriptación de respaldos con AES 256bit.
- La solución permite envío de notificaciones del estado de los respaldos por email, incluyendo soporte para OAuth2 (Google, Microsoft)
- La solución cuenta con mecanismos de verificación de respaldos
- La solución debe tener integración con Prism Central para administración centralizada
- Debe tener control granular por job para compresión y tamaño de bloques
- Debe permitir ignorar el archivo swap en VMs Windows para optimizar capacidad de respaldo, así como soporte para Bitlooker
- La solución debe permitir realizar respaldos integrados con otros hipervisores en la misma consola, así como con nubes públicas para movilidad de cargas de trabajo, y respaldo de servidores físicos
- La solución permite exportar los discos de las máquinas virtuales respaldadas desde Nutanix AHV a formatos VMDK, VHD y VHDX
- La solución permite montar los discos de las máquinas virtuales respaldadas desde Nutanix AHV en cualquier servidor y acceder a los datos en modo de solo lectura
- El servicio de implementación debe estar incluido en el costo de la propuesta
- **El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada.**

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
2	**Adquisición de solución de respaldo en la nube de Microsoft Office 365 para 400 cuentas.** **Licenciamiento por 1 año**	1

- Proteger los datos de Exchange Online (buzones de correo, calendarios, contactos).
- Realizar copias de seguridad de SharePoint Online (sitios, bibliotecas de documentos, listas).
- Respaldar los datos de OneDrive for Business (archivos y carpetas de usuarios).
- Proteger la información de Microsoft Teams (chats, archivos, canales, calendarios, etc.).
- Asegurar la capacidad de recuperación granular y a gran escala de los datos respaldados.
- Establecer políticas de retención personalizables y seguras.
- Cifrado de datos en tránsito y en reposo.
- Control de acceso basado en roles (RBAC) con MFA (Multi-Factor Authentication).
- La solución debe ser compatible con la nube para alojar backups.
- Los respaldos deben alojarse en la nube de manera segura.
- El servicio de implementación debe estar incluido en el costo de la propuesta
- **El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada.**
- **La solución ofertada debe ser compatible al 100 % con el ítem 1 de manera nativa, para así tener un manejo centralizado de los respaldos.**

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
3	**Solución de protección de base de datos para dos servidores de 24 núcleos, con un estimado de 2,500 transacciones por segundo.** **Licenciamiento por 1 año**	1

- **Condiciones Generales**

La solución Database Activity Monitoring (DAM) / DBF (Database Firewall) ofertada debe tener la capacidad de capturar todas las acciones de usuario relacionadas con las bases de datos. Estas acciones se deben capturar sin requerir mecanismos propios-nativos de las bases de datos. Los motores que debe soportar la solución deben ser por lo menos los siguientes:

- MariaDB Server
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL
- PostgreSQL On-Prem
- SAP-HANA
- Sybase ASE
- Sybase IQ

- Sybase SQL Anywhere"

La solución ofertada debe contar con el correspondiente respaldo del fabricante, para los servicios de garantía de hardware (si aplica), mantenimiento software y soporte técnico.
El fabricante de la solución deberá contar con un centro de investigación que se encargue de generar mecanismos de detección de ataques hacia las BD y de cumplimiento de estándares de seguridad y auditoría de la industria; estos mecanismos podrán ser firmas, políticas, vulnerabilidades, plantillas, entre otros. Dicho contenido deberá ser descargable de forma periódica por la solución para incrementar su capacidad de detección y mitigación de amenazas y cumplimiento.

- Administración

La solución deberá ser administrada desde una sola consola (centralizada) WEB que permita la gestión de las políticas (auditoría y seguridad), informes, reportes, revisión de auditoría, monitoreo, eventos de seguridad, gestión de los distintos componentes de la solución y el monitoreo de su estado y performance.

La solución debe incluir un servidor central de administración en el cual residan el software de administración y registro de eventos generados por los diferentes componentes de la solución.

La solución deberá permitir realizar backups periódicos en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto utilizando los protocolos SCP y FTP. El backup deberá estar cifrado. La periodicidad de los backups se debe poder establecer desde la consola de administración.

Toda la configuración, administración y monitoreo de la solución se efectuará a través de la consola de administración.

La solución de administración debe permitir asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.

Deberá permitir la definición de roles de usuarios de forma granular, de tal forma que un rol tenga acceso a determinadas vistas o menús de la solución.

Proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.

La solución deberá realizar detección y análisis sobre todo el tráfico en tiempo real, sin necesidad de crear un archivo log primero para su análisis posterior.

La solución de administración permitirá, como mínimo, lo siguiente:

- Agregar, eliminar o modificar la configuración en un entorno gráfico
- Modificar las reglas de los diferentes equipos
- Efectuar la configuración de los componentes de la solución
- Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema.
- Generar reportes ajustables por el usuario"

Permitir la generación de reportes, de toda la actividad registrada en los logs, en los formatos PDF y CSV.

Permitir la elección de información a ser incluida en los reportes de forma granular, con la capacidad de elegir las columnas a mostrar en los reportes y filtrar la información a ser mostrada. Asimismo, podrá diagramas ejecutivos de barra o pie en los reportes PDF.

Capacidad de automatizar la generación de reportes y su posterior remisión por email.

- Análisis de vulnerabilidades

"La solución deberá poder realizar escaneos a las bases de datos en diferentes niveles/capas, según lo siguiente:

- Brindar un puntaje de los riesgos e indicar cómo mitigar esos riesgos
- Escaneo de vulnerabilidades de la base de datos y configuraciones erróneas, como contraseñas predeterminadas.
- Escaneo de cumplimiento de estándares de benchmarks o hardening como CIS y DISA-STIG".

El análisis de vulnerabilidades no debe requerir la instalación de software en el servidor de la base de datos.

La solución deberá contar con un dashboard que permita comparar una tarea de escaneo de vulnerabilidades actual con uno anterior, para verificar si las vulnerabilidades o configuraciones erróneas han sido solucionadas.

- Bloqueo

La funcionalidad de Bloqueo deberá estar activa en el mismo equipo que realiza el monitoreo de actividad de la base de datos (DAM)
La solución deberá realizar bloqueos de ataques y actividades no autorizadas hacia las bases de datos.

La funcionalidad de Bloqueo no deberá depender de la funcionalidad de Auditoría, es decir, se podrá implementar una política de Bloqueo para determinada transacción SQL, independientemente si dicha transacción SQL tiene una política de Auditoría asociada.

- Descubrimiento

La solución deberá realizar descubrimientos automatizados (escaneos) en la red para identificar servidores bases de datos ya sea a nivel de servidor o puertos habilitados

La solución deberá tener la capacidad de descubrir y clasificar información sensible dentro de las tablas de bases de datos de acuerdo con las políticas de negocio. Las definiciones de que se considera información sensible deberán poder crearse de manera flexible y granular. Deberá contar de forma preconfigurada con patrones de detección de datos sensibles acorde a regulaciones como GDPR.

- Despliegue

La solución deberá soportar implementar los appliances en modo “Inline Bridge” para auditar todo tipo de transacción SQL y/o bloquear a nivel de la red antes de que los querys SQL lleguen a los servidores; despliegues en modo Sniffing conectado a un puerto

espejo (port mirror) de un dispositivo de red o utilización de TAPs de red; utilización de agentes en los servidores de bases de datos a nivel de sistema operativo (sin modificar ningún binario de los motores), que también tengan la capacidad de auditar y bloquear transacciones SQL en base a políticas determinadas.

- Integración

La solución debe soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas de terceros. El sistema debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM) a través de syslog.

- Monitoreo

La solución deberá incluir agentes livianos de software para monitoreo de actividad sobre el servidor, sin depender de auditoría nativa de las bases de datos o logs propios de los motores de base de datos. Asimismo, la solución no deberá depender únicamente de dichos agentes para poder protegerlos y/o monitorearlos.

Los agentes deberán poder desactivarse si superan determinado umbral del consumo de CPU del servidor donde se encuentra instalado. Asimismo, para mejorar el performance, el agente podrá contar con políticas que permitan excluir determinados eventos (incluyendo procesos confiables del servidor de BD y/o eventos originados a partir de una IP determinada).

Los agentes deben soportar al menos los siguientes sistemas operativos: Colocar cuales con la versión. Deberá registrar todas las pistas de auditoría de manera detallada de todas las actividades referentes a las bases de datos, que permita conocer por cada transacción "quién, qué, dónde, cuándo y cómo".

"La solución, para efectos de obtener los registros de auditoría de las transacciones de BD no deberá requerir ningún cambio en la configuración o contenido de la base de datos. Esto incluye:

- Creación de usuarios en las bases de datos.
- Modificación de los permisos de los usuarios existentes."

La solución deberá implementar un monitoreo efectivo de usuarios privilegiados (DBA, super usuarios, desarrolladores, etc.).
La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL
La solución deberá monitorear tanto el tráfico local y el remoto de las bases de datos

"La solución deberá ofrecer la posibilidad de auditar las sesiones de base de datos. La auditoría debe incluir los siguientes datos:

- Fecha y hora de la ocurrencia del evento.
- Información de usuario de base de datos.
- Información de los objetos de bases de datos (tablas, vistas, vistas materializadas, store procedures, entre otros) consultados/modificado y los datos consultados (resultados de la consulta).
- Instancia, esquema, base de datos, objeto y operación realizada
- Debe mostrar las variables bind en caso de que éstas sean utilizadas por la aplicación"

"La solución deberá manejar funcionalidades tan amplias o granulares como se requieran, que deberán poder ser construidas manualmente. Los criterios deberán poder usarse varios a la vez y en diferentes combinaciones de ellos:

- Tipo de datos accedido
- Acceso a datos marcados como sensibles
- Base de Datos, Schema, Instancia, Tabla y Columna accedido
- Estado de autenticación de la sesión
- Usuario y/o Grupo de Usuarios de Base de Datos conectado
- Logins, Logouts, Queries
- IPs de origen y destino
- Nombre de Host origen
- Aplicación usada para la conexión a la base de datos
- Tiempo de respuesta/procesamiento del query
- Número de ocurrencias en intervalos de tiempo definidos
- Por operaciones básicas (Select, Insert, Update, Delete)
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Restore)
- Por Stored Procedure o Function utilizada
- Hora del Día.

La solución deberá soportar la importación de certificados en formato PKCS12 y PEM

La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos (local y remoto), esto incluye Oracle ASO y MSSQL con Diffie Helfman.

Por cada política de auditoría se podrá especificar una cuota de espacio en disco para almacenamiento de eventos, de tal forma que las políticas consideradas críticas puedan tener mayor espacio de almacenamiento que otras políticas no críticas. Por cada política de auditoría se podrá determinar si los logs de transacciones SQL serán respaldados en un servidor externo (FTP o SCP), indicando una frecuencia de respaldo automático. Por cada política de auditoría se podrá definir si la solución también tendrá la capacidad de almacenar los logs de respuesta de la BD al hacer una consulta a una tabla (SELECT).

La solución debe poder integrarse a una SAN para poder expandir su capacidad de almacenamiento. La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema, entre otras; hacia otras herramientas de administración por medio de protocolos SNMP y SYSLOG.

- Perfilamiento

La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana. El proceso deberá ser constante y deberá aprender la estructura de las bases de datos, incluyendo bases de datos, tablas, aplicaciones, IP origen, querys, así como el comportamiento de cada usuario; todo esto para el establecimiento de una línea base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.

- Seguridad

La solución deberá proveer detalles sobre alertas generadas y deberá tener la facilidad de modificar las políticas asociadas desde las alertas.

Deberá poder restringir una petición de base dependiendo de:

- Usuarios de bases de datos, Usuarios de Sistema operativo, IP y nombre de host de origen, binario o programa utilizado para conectarse.
- Base de datos, tabla, stored procedure, esquema
- Tablas, esquemas, columnas
- Operaciones realizadas (DELETE, UPDATE, GRANT, ALTER, etc.)
- Horarios de ejecución de operaciones
- Cantidad de registros devueltos en un query y tiempo de respuesta"

La solución deberá detectar anomalías y abusos a los protocolos de red, malformaciones en los protocolos SQL y firmas de ataque conocidas destinadas a los servidores protegidos.

Deberá soportar el modelo negativo de seguridad, el cual define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:

- Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
- Deberá incluir una lista preconfigurada y detallada de las firmas de ataque.
- Deberá permitir la modificación o adición de firmas por el administrador.
- Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
- Deberá detectar o prevenir amenazas conocidas en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.

La solución debe detectar los siguientes eventos de seguridad:

- Acceso de usuario desconocido
- Acceso de aplicación de base de datos desconocida
- Acceso de cliente (origen IP) desconocido
- Intento de ejecución de inyección de comandos SQL
- Ejecución de un Stored Procedure desconocido
- Acceso a una base de datos y o esquema no autorizado
- Acceso a bases de datos, esquemas o tablas previamente definidas
- Ejecución de comandos privilegiados (DDL).
- Ejecución de comandos SQL no autorizados."

La solución deberá examinar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son ataques complejos intentando vulnerar las aplicaciones.

- Requisitos de los oferentes

El oferente debe ser una empresa consolidada en el mercado con más de 5 años experiencia en el área de ciberseguridad, demostrado mediante cartas de empresas a las cuales les haya brindado el servicio.

El oferente debe tener personal técnico mínimo dos (2) con certificación vigente del fabricante que garantice conocimiento para participar en cualquier etapa del ciclo de

vida de la solución ofertada, debe incluirse la documentación correspondiente junto con el currículo del personal asignado de al menos dos (2) personas.

Un (1) gestor de proyecto certificado como PMP Project Management Professional) emitida por el PMI (Project Management Institute) o de otra entidad mundialmente reconocida, con más de 2 años de experiencia. Para lo cual deberá presentar documento donde conste dicha condición y su vigencia.

Uno (1) profesional certificado como ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición.

Uno (1) profesional certificado como Certified Information Systems Security Professional (CISSP). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición."

El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada.

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
4	**Solución de análisis y remediación de vulnerabilidades de seguridad.** **Gestión de vulnerabilidades de la seguridad en la red para mínimo 400 dispositivos.** **Gestión de parches para mínimo 400 dispositivos.** **Gestión de activos con superficie de ataque para mínimo 400 dispositivos.** **Gestión de vulnerabilidades en aplicaciones WEB para mínimo 30 aplicaciones.** **Todas las soluciones centralizadas en una sola plataforma.** **Licenciamiento por 1 año**	1

GENERAL PARA TODA LA PLATAFORMA:

- La solución debe ser entregada como un servicio Software-as-a-Service (SaaS) en una nube propietaria del fabricante para todos sus servicios y aplicaciones requeridas en este documento. No se aceptan servicios brindados desde nubes de terceras partes.
- Todos los servicios de la plataforma deben estar disponibles bajo el mismo estándar de calidad de servicio 24x7x365 y garantizar 99% de disponibilidad.
- Las actualizaciones del servicio deben ser transparentes para el administrador de la solución, sin afectar ninguno de los datos almacenados o servicios suministrados.
- Solo se admitirá 1 desconexión al trimestre durante un periodo de tiempo no mayor a 4 horas del servicio ofertado en ventanas de mantenimiento programadas y previamente notificadas.

- La plataforma que brinda los servicios debe contar con la certificación FedRAMP y certificación para procedimientos de seguridad SSAE 18 SOC 2.

FUNCIONES ESPECIFICAS REQUERIDAS:

Descubrimiento y Gestión de Activos

- La solución propuesta deberá:

    - Permitir la detección y crear un inventario de todos los activos conocidos y desconocidos que se conectan al entorno de TI híbrido global de la organización, incluidos los dispositivos y aplicaciones locales, móviles, estaciones de trabajo, servidores, dispositivos de red / telecomunicaciones / seguridad, nubes, contenedores, IoT.
    - Permitir descubrir dispositivos, aunque no sea permitido hacer ping o traceroute.
    - Permitir generar vistas gráficas de los dispositivos descubiertos a través de visualizaciones de mapas de la red.
    - Permitir descubrir activos ofreciendo las siguientes alternativas: Escaneo pasivo de la red, Escaneo activo de la red no autenticado, Escaneo activo de la red autenticado y Agente.

- Ofrecer un inventario de activos que cubra como mínimo los siguientes puntos:

    - Inventario de activos de la red local: Debe detectar todos los dispositivos y aplicaciones conectadas a la red, incluidos servidores, bases de datos, estaciones de trabajo, routers, dispositivos de seguridad y redes, impresoras y dispositivos IoT.
    - Inventario de Certificados: Debe detectar y catalogar todos los certificados TLS/SSL digitales (internos y externos) de cualquier autoridad de certificación.
    - Inventario de Contenedores: Debe permitir descubrir contenedores activos o inactivos brindando información de imágenes, registros, contenedores asociados o creados a partir de la misma imagen y hosts / pods donde se encuentran.
    - Permitir recopilar información detallada del activo gestionado, la misma debe detallar al menos los siguientes datos para cada activo: Servicios en ejecución, Software instalado, Usuarios, Puertos abiertos, Versión de sistema operativo, Hostname, FQDN, IP v4/v6, MAC Address, Procesador, Memoria, Volúmenes de disco y BIOS.
    - Permitir de forma automática clasificar los activos por familias tecnológicas, tipo de dispositivo, tipo de plataforma y fabricante.
    - Automáticamente normalizar los nombres de los fabricantes de HW y SW con sus datos relevantes como nombre de las aplicaciones y versiones, para facilitar su posterior búsqueda en la solución.

- Permitir el etiquetado de activos para facilitar la identificación, debe permitir generar etiquetas al menos utilizando los siguientes parámetros:

    - Estática / manual.
    - Dirección IP y rangos de IPs
    - Segmento de Red

  - Puertos abiertos
  - ID de Vulnerabilidad especifica

- Ofrecer la capacidad de obtener y mostrar información acerca de los ciclos de vida del hardware/software (EOL/EOS).
- Permitir identificar el tipo de licencias asociadas al software instalado, clasificándolas en comerciales, código abierto, y otros tipos de licenciamiento.
- Permitir detectar software no autorizado y permitir su desinstalación en plataformas Microsoft Windows.
- Permitir detectar hardware y software desactualizado, fuera de soporte del fabricante o al final de su vida útil.
- Permitir asignarle criticidad al activo para priorizar el mismo durante el proceso de gestión.
- Permitir integración mediante API con servicios de CMDB

Gestión de Vulnerabilidades

- La solución debe permitir descubrir, evaluar, priorizar y parchear vulnerabilidades / configuraciones en toda la infraestructura de la red, incluyendo estaciones de trabajo, servidores, dispositivos de red, telecomunicaciones y seguridad, hipervisores, máquinas virtuales, orquestadores de contenedores, contenedores y nubes (Azure, GCP, AWS), brindando una única interfaz web de usuario para todos los activos, permitiendo la gestión centralizada de todos los componentes de la solución desde un único punto, sin necesidad de incurrir a consolas adicionales o componentes fuera de la misma para la administración de los servicios ofertados.
- La solución se debe licenciar por IP o HOST y debe proveer capacidades de descubrimiento e inventario ilimitadas con acceso ilimitado a agentes, escáneres, sensores para contenedores, sensores de descubrimiento pasivo sin licenciamientos o costos adicionales.
- La solución debe permitir ejecutar escaneos de vulnerabilidades basados en: Sistemas Operativos, Servicios WEB, Puertos TCP y UDP, Servicios, Aplicaciones, Bases de Datos.

- Detectar y analizar vulnerabilidades de al menos los siguientes sistemas operativos: Microsoft Windows, UNIX, LINUX, MacOsx, Cisco, Vmware.
- Detectar y analizar vulnerabilidades en las principales versiones de Bases de Datos, al menos: Microsoft SQL Server, MySQL, Oracle, Sybase.
- Detectar y analizar vulnerabilidades en plataformas WEB, al menos: IIS y Apache Tomcat.
- Detectar y analizar vulnerabilidades por puertos y servicios como: TCP y UDP.
- Buscar vulnerabilidades en al menos las siguientes aplicaciones y/o plataformas: Adobe, Apple, HP, McAfee, Microsoft (Office, IIS, Exchange), Oracle, Oracle Java, VMware.
- Permitir descubrir vulnerabilidades en la red ofreciendo las siguientes alternativas de escaneo
  - Escaneo activo de la red no autenticado
  - Escaneo activo de la red autenticado
  - Agente
- La base de conocimiento de vulnerabilidades debe ser actualizada semanalmente, asegurando la incorporación de al menos 20 CVEs a la misma y debe contar con al menos una base de conocimiento de más de 120,000 CVEs relacionados incluyendo tecnologías legadas y actuales.

- La solución debe admitir el soporte estándar de la industria para la puntuación de vulnerabilidades Common Vulnerability Scoring System (CVSS).
- La solución debe admitir el soporte estándar de la industria para la adición de detecciones personalizadas utilizando Open Vulnerability Assessment Language (OVAL).
- La solución debe permitir vincular las vulnerabilidades detectadas e indicar su relación con amenazas como Virus, Troyanos y Malware.
- La base datos debe relacionar la mayoría de las vulnerabilidades con CVE y Bugtraq.
- Debe soportar integración para autenticación por con herramientas de bóvedas de contraseña líderes de la industria.
- La solución debe permitir la configuración del tipo de escaneo que se va a realizar, permitiendo como mínimo definir las siguientes configuraciones al definir el mismo: Configuración de puertos, Consumo de ancho de banda, Escaneo a dispositivos que no soportan ping o traceroute, Detección de balanceadores de carga, Configuración de fuerza bruta a utilizar para los passwords, Utilización de un header HTTP personalizado.

Evaluación de Configuración

- La solución debe permitir la evaluación, informar y reportar problemas de configuración, en función de las referencias del estándar de industria Center of Internet Security (CIS).
- La solución debe ofrecer evaluación de configuraciones basado en el estándar de industria CIS Benchmark, dando cobertura de esta funcionalidad en las siguientes categorías, Sistemas operativos, Software de servidor, Proveedores de nube, Dispositivos de red, Software de escritorio.

DETECCIÓN Y PRIORIZACIÓN DE AMENAZAS

La solución propuesta deberá:

- Permitir enviar alertas en tiempo real acerca de las irregularidades en la red, identificar amenazas y supervisar los cambios inesperados que se produzcan en la misma.
- Enviar notificaciones para usuarios específicos y grupos de usuarios para el perfil de monitoreo o múltiples perfiles de monitoreo.
- Permitir la asignación de diferentes destinatarios para cada alerta.
- Enviar de alertas de monitoreo sobre vulnerabilidades, configuraciones incorrectas y otros parámetros definidos por el administrador de la solución, tales como:
    - Activos con sistemas operativos no homologados
    - Certificados expirados o por expirar
    - Puertos abiertos
    - Vulnerabilidades graves
    - Tickets de remediación abiertos, resueltos o cerrados
    - Software no homologado

CALCULO DE RIESGO, AUTOMATIZACIÓN Y PRIORIZACIÓN:

La solución deberá:

- Incorporar un motor de cálculo de riesgo, que automáticamente ayude a priorizar los activos.
- El cálculo de riesgo deberá estar calculado teniendo en cuenta al menos las siguientes variables: Vulnerabilidades asociadas al activo, Criticidad del activo, Ubicación del

activo, Amenazas/Ataques asociados a las vulnerabilidades halladas, Problemas configuración, Controles compensatorios, Certificados asociados al activo y Obsolescencia del software.
- Permitir priorizar acciones de remediación basándose en este cálculo de riesgo.

PROTECCIÓN ANTE AMENAZAS:

La solución propuesta deberá:

- Permitir realizar consultas adhoc con múltiples variables y criterios, como clase de activo, tipo de vulnerabilidad, indicadores de amenazas en tiempo real, etiqueta del activo y sistema operativo, de modo que se pueda, por ejemplo, buscar todas las vulnerabilidades que tienen una clasificación de gravedad alta, son fáciles de explotar y fueron divulgadas en la última semana.
- Hacer una correlación en tiempo real de amenazas activas contra las vulnerabilidades detectadas en los activos corporativos.
- Incluir indicadores de amenazas en tiempo real que ayuden a evaluar y priorizar las vulnerabilidades detectadas, categorizados de la siguiente forma: Día cero, Exploit público, Ataques activos, Movimiento lateral, Fácil explotación, Pérdida de datos, Negación de servicio, Sin Parche, Malware, Kit de explotación

Gestión de Parches

La solución propuesta deberá:

- Correlacionar de forma automática vulnerabilidades y parches para los hosts de la organización.
- Mapear automáticamente los parches con los CVE asociados a las vulnerabilidades detectadas.
- Permitir el despliegue de parches con el mismo agente con el que se hacen resto de los escaneos de seguridad, sin necesidad de agentes de terceros o conectividad a la red VPN.
- Permitir la gestión de parches de sistemas operativos Microsoft Windows / Linux y brindar cobertura a las aplicaciones de uso frecuente oficina para su parcheo y actualización.
- Permitir la notificación al usuario final durante el proceso de despliegue del parche, permitiendo retrasar la tarea o dándole una cuenta regresiva notificándole cuando se va a ejecutar la tarea.
- Reiniciar automáticamente el host para aquellos parches que requieran el reinicio para ser aplicados efectivamente.
- Enviar notificaciones al usuario ante la acción de reinicio, permitiéndole rechazar la acción X cantidad de veces, forzar el reinicio o dar una cuenta regresiva para la tarea.
- Detectar automáticamente cuando se encuentra dentro de la red local y descargar los parches desde un repositorio local, y cuando se encuentra fuera de la red corporativa descargarlos directamente desde internet.
- Permitir limitar la ventana de tiempo en la que se van a ejecutar las tareas de parcheo.

ADMINISTRACIÓN:

La solución propuesta deberá:

- Permitir la administración centralizada vía interfaz gráfica WEB utilizando HTTPS.
- Acceder a la consola de todos los componentes del servicio desde un único punto.
- Permitir definir diferentes perfiles y roles de usuario para su administración.
- Proporcionar controles jerárquicos de acceso de usuarios basados en roles que permitan la delegación de responsabilidades para reflejar la estructura organizacional.

ACCESO:

La solución propuesta deberá:

- Admitir la autenticación de dos factores para los usuarios y el inicio de sesión.
- Admitir la configuración de seguridad de contraseñas y personalizar la política de seguridad para la configuración de administración de contraseñas:
    - Antigüedad y vencimiento de la contraseña.
    - Cuenta de usuario bloqueada después de un número de inicios de sesión fallidos.
    - Longitud mínima de la contraseña.
    - Complejidad de la contraseña, caracteres alfanuméricos y numéricos a utilizar.
    - Forzar el cambio de contraseña en el inicio de sesión inicial
    - Notificación de contraseña caducada antes de varios días.

REPORTES:

La solución propuesta deberá:

- Generar reportes mediante IP, Grupo o Etiquetas
- Permitir generar reportes de cualquier IP o Host escaneado previamente.
- Permitir programar reportes diarios, semanales, mensuales o bajo demanda.
- Permitir el envío de notificaciones por correo electrónico cada vez que un reporte esté disponible al administrador de la solución, usuarios específicos o distintos perfiles creados dentro de la herramienta.
- Permitir al menos los siguientes tipos de reportes: Parches, Vulnerabilidades de alta criticidad, Ejecutivo, Técnico, Autenticación, Cumplimiento, Remediación
- Proporcionar informes de remediación: tendencias de tickets por grupo de activos, usuario y vulnerabilidad.
- Permitir crear reportes basándose en direcciones IPv4, IPv6, Hostname, Grupo de activos y etiquetas personalizadas por el administrador.
- Permitir reportes con cálculo de riesgo de seguridad, permitiendo un cálculo de riesgo global para todos los activos incluidos en el reporte.
- Permitir reportes que incluyan vulnerabilidades en función de su fecha de publicación.
- Permitir incluir o excluir kernels de Linux detectados en el escaneo de vulnerabilidades y que no se ejecutan.
- Permitir exportar informes a formatos HTML, MHT, PDF, DOC, CSV y XML
- Los reportes e informes deben ser mostrados en tablas y en gráficos mostrando los incidentes ocurridos, permitiendo la personalización detallada de cada reporte.

- Contar con un tablero de control por defecto que permita ver las tendencias de vulnerabilidades por severidad, plataforma, antigüedad y estado de remediación las mismas.
- Permitir la personalización de los tableros de control haciendo uso de cualquiera de los datos disponibles asociados a los activos escaneados para seleccionar diferentes tipos de gráficos, tablas o vistas sobre la priorización de vulnerabilidades.

AGENTES Y ESCÁNERES:

La solución propuesta deberá:

- Ofrecer un agente de bajo impacto en los sistemas donde se encuentre instalado y el consumo de ancho de banda que realice en la red.
- Debe instalarse en servidores, estaciones de trabajo, contenedores y máquinas virtuales, soportando su despliegue en una red local, en una red hogareña y en la nube.
- Ofrecer soporte para su despliegue en al menos los siguientes sistemas operativos:
    - Windows 7/Windows Server 2003 SP2 and later (x86, x64)
    - Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64)
    - Ubuntu 14, 16,18,19,20 (x64)
    - Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 through 7.5, Oracle Enterprise Linux (OEL) 6
    - Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03
    - SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11
- Actualizarse automáticamente y gestionarse de forma centralizada.
- Soportar plataformas en la nube AWS, GCP, Azure.
- Debe tener funciones de gestión de vulnerabilidades y cumplimiento de políticas
- Poder recopilar información sobre el inventario de activos.
- En el caso del despliegue de un escáner virtual, el mismo debe ofrecer un sistema operativo cerrado y seguro administrado 100% por el oferente de la solución, sin incurrir en gastos adicionales de licenciamiento y gestión de este.
- El escáner virtual debe poder desplegarse en los siguientes ambientes de virtualización:
    - Localmente: VMware Workstation, Player, Workstation Player, Fusion, Oracle VM VirtualBox, VMware vSphere: vCenter Server, ESXi, Citrix XenServer, Microsoft Windows Server (Microsoft Hyper-V)
    - En la nube Cloud: Amazon EC2-Classic, Amazon EC2-VPC, Microsoft Azure Cloud Platform (ARM), Google Cloud Platform, OpenStack, OCI, OCI-Classic, Alibaba Cloud Compute

Escaneo de vulnerabilidades para aplicaciones web en modalidad de código dinámico

- La solución propuesta debe habilitar escaneos dinámicos profundos para descubrir y catalogar todos los aplicativos de la web y API en la red corporativa externa, redes corporativas internas e instancias de nube.
- Una solución debe permitir escaneos autenticadas, complejas y progresivas.
- La solución debe soportar escaneos programados de servicios SOAP y REST API.
- La solución debe contar con una API e integración con Jenkins para la automatización en un ambiente de CI/CD.
- La solución debe detectar, identificar, evaluar, rastrear los 10 principales riesgos OWASP (Top 10), como inyección de SQL, secuencia de comandos entre sitios (XSS), entidad

externa XML (XXE), autenticación de interrupciones y configuraciones incorrectas, también otras amenazas. de WASC, vulnerabilidades CWE y CVE asociados en aplicaciones web.

- La solución debe permitir la capacidad de volver a probar una vulnerabilidad específica que se detectó anteriormente en la aplicación web.
- La solución debe tener capacidad de encontrar aplicaciones web aprobadas y no aprobadas en su red, generando un proceso continuo de catálogo y descubrimiento de aplicaciones web.
- Generación de etiquetas para facilitar la localización y el uso de activos de aplicaciones web encontradas.
- La solución debe permitir que se hacer escaneos de grandes aplicaciones web usando un mecanismo de escaneo progresivo, también debe permitir escaneos incrementales y evitar cualquier tipo de restricciones que pueden surgir.
- La solución debe definir la hora exacta de inicio y la duración de las verificaciones.
- Esta solución debe permitirle administrar varias herramientas de aplicaciones web, combinando varios escáneres para acelerar el proceso y obtener resultados más rápidamente.
- La solución debe permitir la integración nativa con las siguientes herramientas WAF: F5, Fortinet, Imperva, Citrix NetScaler
- La solución debe consolidar los datos de escaneo automatizado de la solución con datos que permitan una evaluación manual de vulnerabilidades por parte de Burp Suite y Bugcrowd, para una visión unificada de vulnerabilidades de aplicaciones web detectadas automática y manualmente.
- La solución debe ser proporcionar informes resumidos y sobre los escaneos de manera que se puedan exportar con formatos HTML y PDF.
- La solución debe ofrecer soporte para la creación de funciones definidas por el usuario y permitir la creación de permisos con roles y privilegios asociados a perfiles de usuarios.
- La solución debe mostrar los detalles de las vulnerabilidades identificadas junto con el detalle asociado a las mismas: Amenaza, Impacto y Solución a seguir por el desarrollador.
- La solución deberá permitir la entrega de un mapa del sitio (sitemap) derivado de los escaneos con la finalidad de tener perspectiva de elementos que se deseen escanear de manera selectiva.
- Capacidad para detectar malware ya sea por antivirus o por comportamiento en la ejecución de los escaneos dentro de la misma plataforma de gestión.

REQUISITOS DE HABILITACIÓN

- El oferente deberá presentar una carta, dirigida a su nombre por el fabricante, que le autorice como partner oficial de la marca ofertada.
- Cartas de referencias que se demuestre la experiencia comprobable en implementación de al menos 2 proyectos similares de la solución ofertada en países de la región latinoamericana donde cuente con presencia.
- La empresa ofertante deberá contar con más de 5 años de experiencia en el área de ciberseguridad en República Dominicana o en la región latinoamericana. Presentar Cartas de referencias.
- El oferente debe contar con al menos 2 ingenieros certificados por el fabricante en la región latinoamericana donde cuente con presencia para configuración y administración de la solución ofertada, entregar Currículo del personal.

- Para garantizar el soporte y la implementación basado en las mejores prácticas de seguridad el oferente deberá contar con personal, en cualquier país que tenga representación con las siguientes certificaciones:
    - Al menos un (1) gestor de proyecto certificado como PMO con más de 2 años de experiencia
    - Al menos un (1) profesional certificado Certified Network Defense Architect EC Council
    - Al menos un (1) profesional certificado en ISO/IEC 27001.
- Presentar la certificación correspondiente que respalde dichas acreditaciones.

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
5	**Solución de monitoreo basada en inteligencia artificial y machine learning (NDR)** **Licenciamiento por 1 año**	1

- **REQUERIMIENTOS GENERALES**

La solución Propuestas de NDR deberá estar basada en **hardware appliance**, es decir, hardware dentro de la suscripción para propósito específico destinado al alojamiento del sistema de seguridad requerida con las condiciones de endurecimiento propias de un sistema de seguridad. La tecnología ofertada deberá estar reconocida como vendedor líder según el Cuadrante mágico de Gartner para soluciones tipo NDR, publicación reciente del 2025. La solución debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo sobre la red de la Entidad. El motor de IA debe estar nativamente embebido en la arquitectura de la solución, funcionando en tiempo real sin necesidad de enviar datos a motores externos o servicios de nube para su procesamiento principal.

El motor de IA debe poder operar con efectividad aún en entornos sin conexión a Internet, validando que el procesamiento no dependa de análisis o motores de terceros basados en la nube o análisis off-site.

Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente por lo menos:

- El tipo de dispositivo (servidores, PCs, IoT, seguridad Perimetral, entre otros).
- Nombre de host
- Dirección MAC y IP.
- Sistema Operativo
- Red a la que Pertence Tag informativo.
- Credenciales.
- La primera y la última vez que se detectó el dispositivo en la red.

La solución debe basarse en el análisis de comportamiento y correlación inteligente con la capacidad de detectar:

A. Toda conectividad inusual en la red.

B. Todas las actividades anómalas en la red.

C. Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc.

D. Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales.

E. Identificar un volumen de conexiones significativamente inusual.

F. Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo.

La solución debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red.

La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utiliza inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así:

A. La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno.

B. Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y/o firmas.

La solución debe utilizar modelos matemáticos de estimación recursiva bayesiana o similares con el fin de validar los comportamientos anómalos en la red, esto debe ser demostrable en documentación pública.

La solución debe proporcionar visibilidad completa de la red.

La solución debe poder identificar cualquier comportamiento anómalo en el entorno y alertar sobre estos comportamientos en tiempo real.

La solución debe ser capaz de identificar cualquier dispositivo nuevo en la red que está analizando.

Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube.

Capacidad de realizar consultas sobre una MAC, una IP o un evento de seguridad.

Debe basarse en métodos matemáticos probabilísticos, analizando y correlacionando múltiples dimensiones distintas dentro del paquete.

La solución debe poder realizar una detección de anomalías de tráfico, en línea, que permita un análisis exhaustivo del incidente en el momento de su ocurrencia, así como ofrecer la opción de analizar el paquete dentro de su propia interfaz de usuario.

La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red de la entidad.

Ser completamente automatizada, no debe requerir de reglas o intervención humana para instruir a la solución sobre cómo utilizar los logs y flows recolectados para correlacionar y determinar ataques en tiempo real.

La solución debe permitir la integración con LDAP o Directorio Activo.

El sistema podrá permitir integraciones con formatos tales como OPEN API, que admita integraciones con otros elementos de seguridad al menos en los formatos CEF, LEEF, JSON, SYSLOG, entre otros. Explicar la manera en que se hace integración a esos formatos.

La tecnología deberá proporcionar la capacidad de realizar tareas de Threat Hunting para encontrar amenazas, basados en inteligencia artificial con al menos las siguientes capacidades:

A. Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial.

B. Los procesos de Threat Hunting deberán indicar las fases del ciberataque en las que se hayan visto anomalías detectadas en el comportamiento.
C. El proceso de Threat Hunting deberá tener la capacidad de correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que llegan al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia artificial.

D. Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios mediante estándares de interconexión e integraciones disponibles que no requieran licenciamiento, de manera que se puedan generar informes de investigación de amenazas (Threat hunting) de manera automatizada.

E. Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda.

F. El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por analistas humanos.

G. El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial.

H. Se deberán proponer los reportes estadísticos de la solución a nivel ejecutivo.

I. Se deberán acordar los reportes de los Threat Hunting y sus respectivas evidencias con al menos un reporte por cada investigación realizada.

J. Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente, identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técnicas buscadas para cada ejercicio de Threat Hunting propuesto.

La solución debe utilizar algunos algoritmos de inteligencia artificial, como Machine Learning como:

Deep Learning, Machine Learning supervisado o Machine Learning no supervisado.

La plataforma debe detectar amenazas sin depender de archivos maliciosos, muestras previas o firmas de malware conocidas. Se excluirán tecnologías que basan su motor en sandboxing, RNN o aprendizaje supervisado sobre muestras preclasificadas.

No serán consideradas tecnologías cuyo modelo de detección principal se base en aprendizaje supervisado alimentado por muestras estáticas de malware, como es el caso de soluciones que emplean redes neuronales recurrentes (RNN) exclusivamente para análisis de payloads maliciosos.

La solución no debe depender de una conexión hacia Internet para realizar sus operaciones de inteligencia y análisis.

La plataforma debe detectar amenazas emergentes y desconocidas sin requerir creación de reglas manuales, correlaciones predefinidas ni tuning por parte del analista.
No se aceptarán tecnologías que dependan de firmas, indicadores de compromiso (IOCs) o muestras históricas para realizar detecciones, debido a su limitada capacidad para detectar amenazas novedosas o personalizadas.

La plataforma debe observar directamente el tráfico de red (o actividad del entorno digital) en lugar de depender de eventos generados por otros dispositivos (como firewalls, endpoints o SIEMs) para generar inteligencia de amenazas.

No serán consideradas soluciones cuyo enfoque central sea la agregación, normalización y correlación de logs, ni aquellas clasificadas como SIEM o NGSIEM, dado que no cumplen con los requisitos de análisis autónomo y autoaprendizaje en tiempo real.

La solución no debe depender exclusivamente de la ingesta, normalización y correlación de logs para la detección de amenazas. Se priorizarán tecnologías que trabajen directamente sobre el tráfico de red y comportamiento del entorno en tiempo real.

La solución debe poder realizar un aprendizaje autónomo del comportamiento normal de la red sin requerir previo conocimiento del historial de comportamiento anómalo, con la posibilidad de identificar amenazas desde el primer día de instalación.

La solución nunca debe dejar de aprender autónomamente del comportamiento de red de la entidad, no se permiten soluciones con aprendizaje estático que sea configurado por la entidad.

La tecnología debe tener la capacidad de detectar amenazas internas y externas.

La tecnología debe ser auto-configurable, es decir, debe tener la capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.

La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad:

A. Ataques de tipo botnet
B. Propagación de gusanos
C. Ataques de ransomware Infiltración y exfiltración de datos
D. Troyanos bancarios
E. Credenciales comprometidas

F. Minería de bitcoins
G. Malware
H. Insider Threats
I. Ataques de DDoS a través de dispositivos IoT
J. Amenazas avanzadas persistentes (APT).
K. Ataques de fuerza bruta.
L. Detección de consulta masiva al directorio activo desde una misma IP.
M. Instalación o descarga de software no autorizado.
N. Acceso no autorizado a carpetas restringidas.
O. Patrones de virus informáticos o códigos maliciosos.
P. Ejecución de secuencia de operaciones y/o transacciones sobre los sistemas de información que pueden implicar fraudes.
Q. Accesos remotos inusuales
R. Cantidad inusual de conexión a los dispositivos, equipos, servidores y base de datos.

La solución debe ser on premise, no se aceptan soluciones que necesiten de la nube para hacer los análisis de la información, cualquier configuración remota debe ser consultada y autorizada mediante comunicado escrito y formal de parte de la entidad.
La solución contra amenazas deberá funcionar sin necesidad de tener conexión a una nube de inteligencia de amenazas, sandbox o cualquier consola en general que se encuentre en la nube o deba recolectar información desde la nube pública.
La solución debe ser tipo appliance no se aceptarán equipos que involucren la instalación de agentes en los dispositivos a monitorear (agent-less).
La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente.
(Zero Day)

- VISUALIZACIÓN DE RED

La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web, no se requerirá de despliegue de agente o instalador para hacer uso de la gestión.
La solución debe poseer una interfaz de visualización gratis tipo APP para ambientes Android y/o iPhone.
La solución debe contar con una interfaz que represente gráficamente, en un entorno tridimensional, las conexiones de red, dispositivos y flujos de datos, permitiendo una visualización geoespacial en tiempo real de la infraestructura digital.
Se requerirá una vista tipo "3D" que muestre conexiones entre regiones, ubicaciones físicas y dispositivos, con capacidad para rotar, hacer zoom y seleccionar elementos para análisis detallado.
La interfaz de visualización debe permitir tener visibilidad gráfica de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegar a ver gráficamente hasta el nivel del dispositivo y sus conexiones en tiempo real. No deberá necesitar compartir datos con una nube de seguridad global para obtener su inteligencia de seguridad
La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.

NUMERAL A. SOLUCIÓN DE MONITOREO BASADA EN INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

La herramienta debe contar con una funcionalidad tipo “replay” o “time slider” que permita recorrer gráficamente el comportamiento de la red en distintos momentos del pasado, mostrando cómo se desarrollaron eventos de seguridad en la vista 3D.
La solución debe ser capaz de agrupar automáticamente los dispositivos en grupos y/o grupos por su similitud de comportamiento basado en Clustering y tener capacidad de visualizar gráficamente este agrupamiento.
La solución debe tener una barra de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red.
La solución debe permitir a los analistas visualizar de forma retrospectiva la actividad de red, conexiones entre dispositivos y anomalías históricas a través de una interfaz visual tipo reloj o línea de tiempo interactiva, que facilite el análisis forense sin depender de búsquedas manuales o filtros complejos.
La solución debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo:

A. La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria.
B. El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas.
C. El ancho de banda total procesado, el ancho de banda promedio procesado hasta la fecha, el ancho de banda registrado en los últimos periodos de tiempo.
D. Un análisis detallado de todo el tráfico recibido en el dispositivo y la última vez que se identificaron los protocolos principales, entre ellos HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, etc.

La solución debe tener visibilidad en tiempo real de los siguientes datos correspondientes a la red:

A. Cantidad de servidores
B. Cantidad de estaciones cliente
C. Cantidad de credenciales de usuario
D. Tráfico de red

La interfaz de visualización debe poseer una barra de búsqueda que permita identificar de manera
rápida cualquier elemento de la red bajo los siguientes criterios:

A. Dirección IP
B. Tipo de dispositivo
C. Función o protocolo conocido.
D. Nombre del dispositivo

Cuando se haga búsqueda de un dispositivo, la interfaz debe poder mostrar la información de éste en detalle incluyendo: dirección IP, dirección MAC, sistema operativo, logs de eventos, logs de brechas de seguridad identificadas, historial de conexiones, lista de dispositivos similares.

La interfaz debe permitir la visualización de todas las subredes, así como todos los dispositivos que las conforman. Debe permitir la visualización de la subred de manera gráfica en tiempo real, mostrando el esquema de conexiones entre los dispositivos.Las subredes deben poder visualizarse en un mapa global que permita conocer la ubicación real de cada una.

- VISIBILIDAD DE AMENAZAS

La interfaz debe mostrar las amenazas que se van identificando en la red en tiempo real, con el detalle de eventos de cada amenaza generados por la herramienta, así como vistas gráficas que permitan ver el comportamiento de la amenaza en el tiempo.
La solución debe proporcionar filtros simples y rápidos para permitir el análisis de eventos informáticos por parte de Usuarios, Dispositivos y tipo de evento.
La interfaz debe poder mostrar la amenaza de manera gráfica y en tiempo real.
La interfaz debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos.
La solución debe tener una función que permita el análisis retrospectivo de los registros del incidente, devolviendo la conexión en segundos, minutos, horas o días antes de que se haya identificado una anomalía.
La solución debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad.
La interfaz de visualización debe permitir tener visibilidad gráfica en 3D de cualquier elemento de la red con profundidad en el detalle. Debe poder llegar a ver gráficamente hasta el nivel del dispositivo y sus conexiones en tiempo real o en el tiempo.
La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica.
La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.

- ARQUITECTURA DE LA SOLUCIÓN

La solución deberá estar basada en hardware appliance, es decir, hardware dentro de la suscripción para propósito específico destinado al alojamiento del sistema de seguridad requerido con las condiciones de endurecimiento propias de un sistema de seguridad.
Para el dimensionamiento de la solución tomar en cuenta las siguientes consideraciones:

- La solución deberá estar basada en hardware appliance, es decir, hardware específico destinado al alojamiento del sistema de seguridad requerido con las condiciones de endurecimiento propias de un sistema de seguridad.
- La solución a nivel de licenciamiento y hardware debe tener la capacidad de monitorear en su fase inicial un mínimo de 500 dispositivos.
- La arquitectura propuesta debe tener la capacidad de poder monitorizar tráfico este-oeste, norte-sur. Incluyendo el tráfico entre servidores virtuales dentro un mismo host(vmwarehyperv). Incluir protección para una aproximado de 10 nodos Virtuales
- Se requiere que la propuesta incluye la centralización de los posibles incidentes de ciberseguridad, en una consola con el fin de gestionar las alertas y casos.

Cada hardware appliance debe contar con su propia interfaz de administración y visualización, desde la cual cada institución pueda monitorear/visualizar su entorno.
Los equipos que conforma la solución deben ser instalados fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos (port mirroring), de tal manera de no causar retrasos o latencias en el desempeño de la red.

Los hardware appliance deben cumplir con las siguiente es

- Soportar un Throughput promedio de 3 gbps.
- Conexiones por minuto – 300.000 conexiones por minuto
- Eventos por minuto – soportar un mínimo de XXXXX eventos por minuto
- Soportar interfaces de cobre para el análisis de red
  - 1x1000 BASE-T
  - 10G BASE-T

- Soportar interfaces de fibra para el análisis de red
  - 10Gbe
  - 1Gbe SFP+
- El hardware appliance propuesto debe soportar doble fuente de poder.

La solución debe tener al menos tres (3) puertos 10/100/1000 BASE-T de monitoreo y un (1) puerto 10/100/1000 BASE-T para Gestión.
La solución debe ser capaz de recibir y procesar tráfico de red a través de mecanismos estándar de duplicación de tráfico, incluyendo soporte nativo para SPAN (Switched Port Analyzer), RSPAN (Remote SPAN) y ERSPAN (Encapsulated Remote SPAN), permitiendo así una implementación flexible en diferentes topologías de red, tanto locales como remotas.
La arquitectura propuesta debe tener la capacidad de supervisa/monitorear tráfico este-oeste/ norte sur.
Numeral INVESTIGACIONES AVANZADA(AS) y AUTONOMAS
Como parte integral y fundamental de la solución requerida esta deberá incluir un modulo integrado de investigación avanzada, que permitirá a los analistas humanos, buscar y analizar registros de tráfico de red con las siguientes características.

- Almacena registros de conexión de red (eventos "conn") y otros registros específicos de protocolos como HTTP, DNS, etc
- A cada conexión de red se le asigna un identificador único (UID) que se comparte entre los eventos relacionados de esa conexión y que podrá ser usado también, para pivotear con la UI principal y generar una relación de información precisa.
- Los usuarios pueden buscar y filtrar los registros mediante una potente sintaxis de consulta, que permite realizar consultas booleanas complejas en diversos campos como direcciones IP, puertos, protocolos, etc.
- Los resultados de la búsqueda se pueden visualizar en formato tabular, con opciones para

analizar los valores de los campos mediante visualizaciones como gráficos circulares, tendencias, valores máximos, etc.

- Los usuarios pueden ajustar la ventana de tiempo, ampliar el gráfico de tráfico, guardar consultas y exportar los resultados a CSV.
- La Búsqueda Avanzada proporciona datos de tráfico sin procesar antes de cualquier

NUMERAL A. SOLUCIÓN DE MONITOREO BASADA EN INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING análisis de IA/ML, lo que permite una investigación detallada de los eventos de red.

- Este Modulo no deberá tener un licenciamiento adicional.
- El módulo de investigaciones avanzadas debe procesar todas las consultas on premise en cloud privado, sin enviar datos a cloud públicas o dataleak externos.

La solución propuesta deberá tener la capacidad de integrar sin licenciamiento adicional, un módulo de Analista Virtual, con las siguientes consideraciones.

- El proceso de ejecución de investigaciones autónomas, sin intervención humana, deberá realizarse desde la solución implementada en las instalaciones del cliente (on-premise), sin requerir envío de datos a servicios externos o nubes públicas (tipo dataleak o cloud analytics) .
- El sistema debe generar automáticamente narrativas en lenguaje Natural que describan el incidente de seguridad, incluyendo cronología de eventos, activos comprometidos, posibles vectores de ataque y acciones recomendadas, sin necesidad de configuración previa ni reglas manuales.
- Debe contar con una interfaz de usuario que permita ver los informes del analista virtual con visualizaciones explicativas, incluyendo mapas de relación entre eventos, dispositivos y usuarios implicados.

- La solución debe demostrar el uso de Graph Neural Networks (GNN) para modelar relaciones topológicas en tiempo real entre entidades (dispositivos, usuarios, flujos) y Recurrent Neural Networks (RNN) para análisis de secuencias temporales (logs, tráfico)
- El proveedor deberá demostrar cómo el módulo del analista mejorar en:

- Reducción del *tiempo medio de detección (MTTD)*
- Eficiencia del SOC (ej. horas ahorradas en investigaciones manuales).

La solución debe ejecutar acciones de mitigación (ej. aislamiento de endpoints, bloqueo de tráfico) sin requerir aprobación manual, basándose en un modelo de confianza cuantificable. Debe poder realizar investigaciones autónomas basadas en inteligencia artificial, a través de la interfaz gráfica, esta investigación debe incluso poder realizarse sin intervención humana y generar un reporte donde se evidencia al menos un resumen ejecutivo del incidente, las alertas que fueron investigadas que hacen parte de incidente e información técnica de cada uno de los eventos identificados, asociándose al framework ATT&CK Mitre.

La Investigación basada en Inteligencia Artificial debe generar un reporte como resultado del proceso investigativo que contenga como mínimo:

A. Una reconstrucción cronológica de los eventos que hacen parte del Incidente.

NUMERAL A. SOLUCIÓN DE MONITOREO BASADA EN INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

B. Un resumen del incidente con una narrativa basada en procesamiento de lenguaje natural que describa a alto nivel los comportamientos evidenciados durante el incidente.

Detalles técnicos relevantes a la investigación realizada como direcciones Ips, Hostnames, cuentas de usuario involucradas, saltos de conexión, cantidad de transferencia de datos, destinos externos, rareza de los destinos, rareza de las conexiones y resúmenes de conexiones. Se excluirán soluciones ofertadas que requieran intervención humana constante para realizar investigaciones, análisis manual o correlaciones de datos sin contexto visual ni comportamiento auto-modelado.

- NOTIFICACIONES Y REPORTES

La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos. Explicar la capacidad de envío haciendo uso de formato planos y en formatos enriquecidos (HTML).

- Se debe manejar el envío de notificaciones de tipo (.txt y .csv).
- Adicionalmente se utilizará el lenguaje HTML enriquecido para el envío de las notificaciones más detalladas, para dar formato al texto, permitiendo la inclusión de imágenes, enlaces, tablas y otros elementos visuales.

Contar con una interfaz móvil disponible para Android y iOS, activa 7x24 que acelere las tareas de mitigación de riesgos mediante el envío de notificaciones push para dar aviso de amenazas en proceso y la posibilidad de confirmar acciones de respuesta autónoma.
La solución deberá generar Reportes en enfocados en Maximiza el ROI de la inversión en NDR, encontrando información de Horas ahorradas por investigaciones generadas por la plataforma.

- ADMINISTRACIÓN

La herramienta debe ser capaz de realizar backup y restore de la configuración, permitiendo al administrador programar la realización de los backup's en el momento deseado.

Los backups deben poder ser transferidos a un repositorio vía SFTP o alguna tecnología de transferencia equivalente, es decir, que considere las medidas de seguridad bajo protocolos aceptados por la industria.

- RESPUESTA AUTONOMA

Para la contención y bloqueos de ataques, se debe utilizar el mismo equipo ofertado en la solución de detección de amenazas, no se permite equipos adicionales (físicos o virtualizados) o licenciamiento adicional.

La solución debe estar en la capacidad de responder frente a incidentes de forma autónoma, esto es a partir del aprendizaje obtenido de la inteligencia artificial debe decidir qué debe bloquear y cómo debe hacerlo, no debe utilizar configuraciones ni políticas predefinidas para realizar el bloqueo y debe bloquear únicamente el tráfico asociado a la amenaza mientras permite que el tráfico restante (no anómalo) siga fluyendo.

Las acciones de bloqueo deben ser generadas con la precisión necesaria para interrumpir exclusivamente el tráfico que corresponde a las acciones maliciosas detectadas, de manera que no se afecte al tráfico de las actividades normales de los dispositivos involucrados.

Capacidad para bloquear tráfico Norte-Sur y Este-Oeste de forma automática sin la instalación de dispositivos de control adicionales.

Capacidad de determinar automáticamente como bloquear el tráfico sin causar mayor impacto a la organización utilizando inteligencia artificial, bloqueando conexiones específicas a través del envío de TCP-RST sin necesidad de integraciones con la infraestructura de la entidad.

El bloqueo de conexiones a través de TCP-RST no debe necesitar más appliance físicos para su ejecución, se debe usar el mismo appliance de detección.

Deberá ser gestionable desde la misma interfaz gráfica (GUI) de detección de la solución.
Se requiere que las capacidades de respuesta estén disponibles de forma nativa en entornos híbridos y multinube, incluyendo redes on-premise, AWS, Azure y GCP.

La solución debe ofrecer acciones de respuesta automáticas sin depender de XDR SIEM, SOAR u otros sistemas de orquestación externos.

Debe ofrecer la opción de operar en modo pasivo, para validar la efectividad de las respuestas antes de su despliegue automático en producción.

La plataforma debe contar con un motor de respuesta capaz de actuar en función de su propia observación del entorno, y no limitado a playbooks, flujos SOAR o correlaciones preprogramadas.

- SOPORTE DEL FABRICANTE

El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia del contrato.
En caso de falla del equipo, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o en su defecto un equipo nuevo para el reemplazo sin costo adicional.
Modalidad RMA.

El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada.

- **CAPACITACIÓN**

El fabricante debe tener un portal de capacitaciones sin costo adicional, donde se encuentren capacitaciones técnicas sobre la solución ofertada, estás capacitaciones deben ser en español, las personas de la entidad deben poder inscribirse a estos cursos y tomarlos en vivo y en directo con un capacitador del fabricante.

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
6	Renovación SOPHOS Central Managed Detection and Response para 450 usuarios y 50 servidores ID de licencia L0011171947 y L0011171948 El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada. Licenciamiento por 1 año.	1

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
7	Renovación SOPHOS Xtream protección y Webserver protection ID LICENCIA LN1000932496 para XGS 3300 número de serial X330046G2D882B2. El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada. Licenciamiento por 1 año.	1

ÍTEM	ELEMENTO/DESCRIPCIÓN	CANTIDAD
8	Figma Profesional puesto full 1 año	4

Todas las licencias deberán ser implementadas por el adjudicatario. El costo correspondiente a la implementación deberá estar contemplado dentro de su propuesta como un único ítem todo incluido.

4. Valor referencial

El valor referencial para esta compra asciende a **DIECISÉIS MILLONES CUATROCIENTOS TREINTA MIL PESOS DOMINICANOS CON 00/100 (RD$16,430,000.00)**, incluidos cualquier otro concepto que incida en el costo total del bien a adquirir, valor que ha sido obtenido en el marco de los estudios previos[1] realizados y que sustentan el expediente de la presente contratación. **Observaciones: Las Licencias NO GRAVAN ITBIS.**

[1] Ver definición numeral 6 del artículo 4 del Decreto Núm. 416-23.

ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO TOTAL RD$
1	Renovación de la VEEAM Advance, Licenciamiento por 1 año.	1	RD$1,800,000.00
2	Adquisición de solución de respaldo en la nube de Microsoft Office 365	1	RD$2,050,000.00
3	Adquisición Solución de protección de base de datos.	1	RD$3,000,000.00
4	Adquisición Solución de análisis y remediación de vulnerabilidades de seguridad	1	RD$4,000,000.00
5	Adquisición solución de monitoreo basada en Inteligencia Artificial	1	RD$2,500,000.00
6	Renovación SOPHOS Central Managed Detection and Response	1	RD$2,500,000.00
7	Renovación SOPHOS Xtream protección y Webserver protection para XGS 3300	1	RD$500,000.00
8	Adquisición Figma Profesional puesto full 1 año	4	RD$80,000.00

5. Lugar de entrega de los bienes

El lugar de entrega de los bienes a adquirir es en la Sede Central de la **Superintendencia de Salud y Riesgos Laborales (SISALRIL),** ubicada en la Avenida 27 de febrero Núm. 261, Edificio SISALRIL, Ensanche Piantini, Distrito Nacional.

6. Tiempo para la entrega de los bienes

Los bienes deberán entregarse dentro de los plazos secuenciales y finales establecidos en este pliego (y sus anexos) así como en los cronogramas de trabajo presentados por el (la) proveedor (a) aprobados por la institución contratante.

El plazo mencionado supone que el oferente debe realizar el cálculo de los tiempos estimados de las prestaciones accesorias, según aplique, y ser expresados en su oferta, para que la institución contratante realice los controles que le competen. Los aumentos de tiempo que disponga el (la) proveedor (a), luego de adjudicado, para garantizar la entrega del o los bienes, no originarán mayores erogaciones para la institución contratante y serán asumidas exclusivamente por éste.

El plazo para la entrega de los bienes propuesto por el proveedor adjudicatario se convertirá en el plazo contractual, siempre y cuando se ajuste al estimado propuesto por la institución contratante en el presente Pliego de Condiciones Específicas.

7. Entregables/ cronograma

Los bienes y sus prestaciones accesorias (si aplica) que debe entregar el oferente/proponente que resulte Adjudicatario son los siguientes:

ITEMS	PRODUCTO	CANTIDAD	FECHA DE ENTREGA
1	Renovación de la VEEAM Advance, Licenciamiento por 1 año.	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
2	Adquisición de solución de respaldo en la nube de Microsoft Office 365	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
3	Adquisición Solución de protección de base de datos.	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
4	Adquisición Solución de análisis y remediación de vulnerabilidades de seguridad	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
5	Adquisición solución de monitoreo basada en Inteligencia Artificial	1	**No mayor a cuarenta y cinco (45) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
6	Renovación SOPHOS Central Managed Detection and Response	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
7	Renovación SOPHOS Xtream protección y Webserver protection para XGS 3300	1	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.
8	Adquisición Figma Profesional puesto full 1 año	4	**No mayor a quince (15) días calendarios** a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República.

8. Cronograma de Actividades

Fecha de publicación del aviso de convocatoria	1/9/2025 09:00 *
Presentación de aclaraciones	22/9/2025 14:00 *
Reunión aclaratoria	
Acto de asignación de riesgo	
Plazo máximo para expedir Emisión de Circulares, Enmiendas y/o Adendas	3/10/2025 11:30 *
Presentación de Ofertas Técnicas y Económicas	15/10/2025 09:00 * Sugerir restantes fechas
Apertura de la Oferta Técnica	15/10/2025 10:00 *
Verificación, Validación y Evaluación de Ofertas Técnicas	20/10/2025 14:00 *
Informe Preliminar de Evaluación de Oferta Técnica	21/10/2025 15:00 *
Notificación de Errores u Omisiones de Naturaleza Subsanable	23/10/2025 15:00 *
Ponderación y Evaluación de Subsanaciones	28/10/2025 15:00 *
Notificación de Informe Definitivo y Habilitación para apertura Oferta Económica	29/10/2025 15:00 *
Apertura Oferta Económica	30/10/2025 11:00 *
Evaluación de Ofertas Económicas	4/11/2025 14:00 *
Notificación de errores aritméticos, de solicitud de aclaraciones económicas y de solicitud de subsanación de garantía de seriedad de la oferta	5/11/2025 15:00 *
Aceptación de correcciones de errores aritméticos y de respuesta a las aclaraciones	7/11/2025 15:00 *
Periodo para subsanar la garantía de seriedad de la oferta	11/11/2025 15:00 *
Acto de Adjudicación	14/11/2025 15:00 *
Notificación de Adjudicación	17/11/2025 15:00 *
Constitución de garantia de Fiel Cumplimiento	20/11/2025 14:00 *
Suscripción del Contrato	4/12/2025 14:00 *
Publicación del Contrato	9/12/2025 14:00 *
Plazo de validez de las ofertas	60 * Días *

9. Forma de presentación de ofertas técnicas y económicas “Sobre A” y “Sobre B”

De conformidad con el artículo 109 del Reglamento núm. 416-23 los(as) oferentes deberán presentar sus propuestas por vía electrónica, a través del SECP, o en formato papel ante la institución contratante en el **Edificio Sede Central de la Superintendencia de Salud y Riesgos Laborales ubicada en la Av. 27 de febrero Núm. 261** en la fecha y hora fijadas en el cronograma de actividades de este Pliego de Condiciones.

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.

9.1 Ofertas presentadas en formato papel

Para las ofertas presentadas en formato papel los(las) oferentes presentarán dos sobres, uno contentivo de la oferta técnica que se denominará “Sobre A” y otro contentivo de la oferta económica que se denominará “Sobre B”.

Los documentos contenidos en el "Sobre A" y en el "Sobre B", deberán ser presentados tanto en original debidamente marcado como "ORIGINAL" en la primera página del ejemplar, junto con **una (1)** fotocopia simple de los mismos, debidamente marcada en su primera página, como "COPIA" y en ella deberá constar en la primera página 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 p**or 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.

Tanto el "Sobre A" como el "Sobre B" deberán contener en su cubierta la siguiente identificación:

NOMBRE DEL(LA) OFERENTE/PROPONENTE (Sello Social)
Firma del (la) Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Superintendencia de Salud y Riesgos Laborales (SISALRIL)
IDENTIFICACIÓN DEL TIPO DE SOBRE (Sobre A o Sobre B)
REFERENCIA: SISALRIL-CCC-LPN-2025-0007

No se recibirán sobres que no estuviesen debidamente cerrados e identificados según lo dispuesto anteriormente.

9.1 .1 Ofertas presentadas en formato electrónico vía el SECP

Los oferentes que presenten sus propuestas mediante el SECP clasificarán la documentación requerida marcando cual pertenece al contenido de la oferta técnica que aparecerá denominado como **"Sobre 1"** y otro contentivo de la oferta económica "**Sobre 2**".

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

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 cargada en este mismo portal, prevalecerá el documento cargado por el oferente, siempre que esté firmado por el oferente y además sellada cuando se trate de una persona jurídica.

10. Documentación a presentar[2]

La documentación solicitada vinculada al objeto de la contratación[3] 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 oferente/proponente es responsable de la exactitud y veracidad del contenido de los documentos que forman su oferta. Todos los documentos entregados en papel mediante Sobres

[2] No podrá exigirse a los oferentes presentar documentos que no hayan sido indicados en esta sección.
[3] Se debe indicar cuales documentos solicitados no serán subsanables. Conforme al artículo 8 párrafo III y artículo 21 sobre *principio de competencia*, establecido en la Ley núm. 340-06, así como también artículo 120 del Reglamento núm. 416-23, todo documento relativo a credenciales de los oferentes (ejemplo, documentación legal, financiera, experiencia) será subsanable, siempre y cuando cumpla con el requisito al momento de presentación de la oferta o sea inherente a su capacidad, para no afectar el principio de igualdad de trato entre los oferentes.

cerrados y sellados o 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.

11. Contenido de la Oferta Técnica

Con base en el criterio de descentralización de la gestión operativa, las instituciones contratantes son responsables de diseñar sus pliegos de condiciones, términos de referencia, especificaciones técnicas y son autónomas para requerir la documentación con la que verificarán el cumplimiento del requerimiento, sin perjuicio de lo anterior, no podrá solicitarse documento alguno que no tenga como objetivo acreditar una condición o el cumplimiento de un requerimiento establecido en este pliego y en sus fichas/ especificaciones técnicas.

11.1 Documentación de la oferta técnica "Sobre A"

11.1.1 Credenciales:

a) **Documentación Legal: (Subsanable)**

a) DOCUMENTACIÓN LEGAL	SUBSANABLE / NO SUBSANABLE
1) Formulario de Presentación de Oferta (SNCC.F.034)	(Subsanable)
2) Formulario de Información sobre el(la) Oferente (SNCC.F.042)	(Subsanable)
3) 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. Puede incluirla para mayor rapidez.	(Subsanable)
4) 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. Puede incluirla para mayor rapidez.	(Subsanable)
5) Registro de Proveedores del Estado (RPE), emitido por la Dirección General de Contrataciones Públicas, debe tener inscrita, conforme a la codificación UNSPSC la actividad comercial **81110000-Servicios informáticos**, referida en el numeral 2 sobre "objeto del procedimiento de selección" de este pliego, no tiene que ser depositado, será verificado en línea por la institución. Puede incluirla para mayor rapidez. **(No Subsanable, después de la fecha establecida en cronograma)**	(Subsanable)
6) Copia del Registro Mercantil expedido por la Cámara de Comercio y	(Subsanable)

Producción correspondiente (vigente).	
7) Copia de los Estatutos sociales vigentes debidamente registrado en la Cámara de Comercio y Producción correspondiente.	**(Subsanable)**
8) Copia de la nómina de accionistas y acta de la última asamblea realizada debidamente registrada por ante la Cámara de Comercio y Producción correspondiente.	**(Subsanable)**
9) Copia de la nómina de accionistas y acta de asamblea realizada mediante la cual se designe expresamente el actual gerente o consejo de administración, según aplique, que tiene potestad para firmar contratos a nombre de la empresa participante, debidamente registrada en la Cámara de Comercio y Producción correspondiente.	**(Subsanable)**
10) Formulario de Compromiso ético de proveedores (as) del Estado[4] debidamente firmado y sellado.	**(Subsanable)**
11) Declaración jurada simple (no requiere firma de notario público) del oferente manifestando que no se encuentra dentro de las prohibiciones en el artículo 8 numeral 3 y artículo 14 de la Ley núm. 340-06 y sus modificaciones.	**(Subsanable)**
12) Formulario de Debida Diligencia	**(Subsanable)**
13) Copia de la cédula de identidad y electoral del representante legal.	**(Subsanable)**

b) Documentación financiera[5]:

DOCUMENTACIÓN FINANCIERA	
DOCUMENTOS A EVALUAR	SUBSANABLE / NO SUBSANABLE
Se solicita a los participantes de este proceso de contratación Certificados e instrumentos financieros que acrediten la disponibilidad de recursos, incluyendo constancia de líneas de créditos activas dirigida a la Institución Contratante, cuyo monto sea equivalente, como mínimo **al diez por ciento (10%) del valor de la contratación**.	**SUBSANABLE** **(Nota:** La entrega de este documento es de carácter subsanable. En cuanto a la validación realizada al documento, en caso de no tener veracidad, se considera de carácter **NO SUBSANABLE).**

[4] Para participar en este procedimiento, es un requisito indispensable que los(as) oferentes suscriban y entreguen junto a su oferta, el documento "compromiso ético de proveedores(as) del Estado", que consta como anexo en el presente pliego de condiciones. De no ser presentado junto a su oferta, podrá ser incluido en la fase de subsanación prevista en el cronograma de actividades; vencido este plazo sin haberlo acreditado, su oferta será descalificada haciéndose constar en el informe de evaluación que deberá ser emitido en el marco del procedimiento.

[5] Para requerir apropiadamente la referencia de crédito comercial deberá observarse los lineamientos establecidos por la Dirección General de Contrataciones Públicas.

DOCUMENTACIÓN FINANCIERA	
DOCUMENTOS A EVALUAR	SUBSANABLE / NO SUBSANABLE
Declaraciones juradas anuales del Impuesto sobre la Renta de sociedades y personas físicas. Copia de las declaraciones juradas anuales del impuesto sobre la renta y sociedades y personas físicas presentadas ante la Dirección de General de Impuestos Internos **(Formularios IR—1 e IR-2).**	SUBSANABLE

11.1.2 Documentación técnica:

DESCRIPCIÓN	SUBSANABLE / NO SUBSANABLE
Oferta Técnica (conforme a los Términos de Referencias y cantidades suministradas en el punto 3. **APLICA PARA TODOS LOS ITEMS**.	NO SUBSANABLE
Carta de aceptación de condición de pagos y tiempo de entrega, en que el proveedor se comprometa a realizar la entrega en plazo establecido en el presente pliego de condiciones. **APLICA PARA TODOS LOS ITEMS**.	SUBSANABLE
Certificación donde el oferente se compromete a entregar la solución tal como es solicitada en las especificaciones detalladas en el TDR anexo a este Pliego de Condiciones. **APLICA PARA TODOS LOS ITEMS**.	SUBSANABLE
El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada. **APLICA PARA LOS ITEMS DEL 1-7.**	SUBSANABLE
El oferente debe ser una empresa consolidada en el mercado con más de 5 años experiencia en el área de ciberseguridad, demostrado mediante cartas de empresas a las cuales les haya brindado el servicio. **APLICA PARA EL ÍTEM 3.**	SUBSANABLE
El oferente debe tener personal técnico mínimo dos (2) con certificación vigente del fabricante que garantice conocimiento para participar en cualquier etapa del ciclo de vida de la solución ofertada, debe incluirse la documentación correspondiente junto con el currículo del personal asignado de al menos dos (2) personas. **APLICA PARA EL ÍTEM 3.**	SUBSANABLE
Un (1) gestor de proyecto certificado como PMP Project Management Professional) emitida por el PMI (Project Management Institute) o de otra entidad mundialmente reconocida, con más de 2 años de experiencia. Para lo cual deberá presentar documento donde conste dicha condición y su vigencia. **APLICA PARA EL ÍTEM 3.**	SUBSANABLE
Un (1) profesional certificado como ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición. **APLICA PARA EL ÍTEM 3.**	SUBSANABLE

Un (1) profesional certificado como Certified Information Systems Security Professional (CISSP). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición. APLICA PARA EL ÍTEM 3.	SUBSANABLE
Cartas de referencias que se demuestre la experiencia comprobable en implementación de al menos 2 proyectos similares de la solución ofertada en países de la región latinoamericana donde cuente con presencia. APLICA PARA EL ITEM 4.	SUBSANABLE
La empresa ofertante deberá contar con más de 5 años de experiencia en el área de ciberseguridad en República Dominicana o región Latinoamericana. Presentar cartas de referencias. APLICA PARA EL ITEM 4.	SUBSANABLE
El oferente debe contar con al menos 2 ingenieros certificados por el fabricante en la región latinoamericana donde cuente con presencia para configuración y administración de la solución ofertada, entregar Currículo del personal. APLICA PARA EL ITEM 4.	SUBSANABLE
Para garantizar el soporte y la implementación basado en las mejores prácticas de seguridad el oferente deberá contar con personal, en cualquier país que tenga representación con las siguientes certificaciones: o Al menos un (1) gestor de proyecto certificado como PMO con más de 2 años de experiencia o Al menos un (1) profesional certificado Certified Network Defense Architect EC Council o Al menos un (1) profesional certificado en ISO/IEC 27001. Presentar la certificación correspondiente que respalde dichas acreditaciones. APLICA PARA EL ITEM 4.	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.

11.2 Contenido de la Oferta Económica

a) Precio de la oferta

Los precios cotizados por el oferente en el Formulario de Presentación de Oferta Económica deberán ajustarse a los requerimientos que se indican a continuación. No deberán presentar alteraciones ni correcciones, ni tachaduras.

NOTA IMPORTANTE:
Para la confección de sus ofertas económicas los oferentes deberán considerar, la cláusula dictaminada en el Reglamento aprobado por el Decreto Núm. 293-11, para la Aplicación del Título III, del Código Tributario de la República Dominicana, del Impuesto sobre Transferencias de Bienes Industrializados y Servicios (ITBIS), que establece en su Artículo 4, literales c y d, lo siguiente: **OPERACIONES NO SUJETAS AL IMPUESTO (ITBIS)** No están sujetas al impuesto las siguientes transferencias de bienes y derechos: c) La transferencia de derechos de autor, propiedad intelectual, permisos, licencias y otros derechos que no impliquen la transmisión de un bien mueble corporal. d) El arrendamiento de derechos o de bienes intangibles**. Por lo que, deberán presentar la oferta sin ITBIS.**

El oferente/proponente cotizará el precio del bien o producto, de manera individual y global, según corresponda. Este precio deberá expresarse en dos decimales (XX.XX), inclusión de todos los gastos, tasas, divisas según corresponda. El oferente será responsable y pagará todos los impuestos, derechos de aduana, o gravámenes que hubiesen sido fijados por autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los bienes a ser suministrados.

b) Moneda de la oferta

El precio en la oferta deberá estar expresado en moneda nacional, (PESOS DOMINICANOS, RD$).

c) Plazo mantenimiento de oferta

Las ofertas presentadas por los oferentes deben estar vigentes desde el día **quince (15) de octubre del año 2025 hasta el cuatro (04) de diciembre del año 2025.**

Se podrá solicitar a los oferentes/proponentes una prórroga, antes del vencimiento del período de validez de sus ofertas, con indicación del plazo. Los oferentes/proponentes podrán rechazar dicha solicitud, considerándose por tanto que han retirado sus ofertas. Aquellos(as) que la consientan no podrán modificar sus ofertas y deberán ampliar el plazo de la garantía de seriedad de oferta oportunamente constituida.

d) Garantía de seriedad de la oferta

Con la finalidad de garantizar que los oferentes y eventuales adjudicatarios no retiren sin causa justificada las ofertas presentadas en el procedimiento de selección y para proteger a la **Superintendencia de Salud y Riesgos Laborales (SISALRIL)** ante dicho incumplimiento, los oferentes/proponentes deberán constituir una garantía de seriedad de su oferta, que esté vigente hasta veinte (20) días después de la fecha prevista en el cronograma para la suscripción del contrato y que cumpla con las siguientes características:

1) **Póliza o Garantía Bancaria** por un monto equivalente a uno por ciento (1%) del monto de la oferta a presentar. Si se trata de un oferente certificado como MIPYME solo será exigida la fianza de seguro.
2) En la misma moneda de la oferta, dígase en PESOS DOMINICANOS, RD$.
3) En beneficio de la **SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES (SISALRIL).**
4) Tener la condición de: **INCONDICIONAL, IRREVOCABLE Y RENOVABLE;**
5) Con una vigencia desde el **quince (15) de octubre del año 2025 hasta el cuatro (04) de diciembre del año 2025.**

Nota: Conforme las disposiciones del párrafo II del artículo 30 de la Ley Núm. 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras y Sus Modificaciones, así como las del párrafo I del artículo 192 del Reglamento de Aplicación Núm. 416-23, las modalidades de garantía permitidas son la garantía bancaria y la póliza de seguro, las mismas deben contener las condiciones de **INCONDICIONALES, IRREVOCABLES Y RENOVABLES.** Para el caso de MIPYMES, solo será exigida la fianza de seguro.

Las condiciones de irrevocables e incondicionales deben estar explícitamente en el contenido de las garantías que son exigidas en los procedimientos de contratación pública, esto con la finalidad de evitar ambigüedades y proteger a la Administración ante un incumplimiento del oferente o adjudicatario. Por lo tanto, la omisión o el incumplimiento de las referidas características dispuestas en el párrafo II del artículo 30 de la Ley Núm. 340-06 sobre Compras Y Contrataciones de Bienes, Servicios y Obras y Sus Modificaciones, **PODRÍA AFECTAR SU ACEPTACIÓN EN EL PROCEDIMIENTO DE CONTRATACIÓN DE QUE SE TRATE. ES DECIR, QUE ESTE ASPECTO NO ES CONSIDERADO UN ERROR MATERIAL Y POR ENDE NO ES SUSCEPTIBLE DE SUBSANACIÓN**. Para más información, consultar Circular de Aclaraciones sobre las garantías en el Sistema Nacional de Compras y Contrataciones Públicas (SNCCP).

e) **Devolución y ejecución de Garantía de Seriedad de la Oferta**

Las garantías de seriedad de las ofertas presentadas por los oferentes serán devueltas en plazo no mayor de diez (10) días hábiles contados de la manera siguiente:

1) A los oferentes descalificados en la etapa de evaluación técnica, a partir de la notificación del acto administrativo de descalificación;
2) A los oferentes que no fueron adjudicados, a partir de la notificación del acto administrativo de adjudicación;
3) Al adjudicatario, a partir de la recepción de su garantía de fiel cumplimiento.

11.2.1 Documentos de la oferta económica "Sobre B"

Los oferentes deberán presentar en su oferta económica "Sobre B", los siguientes documentos:

DESCRIPCIÓN	CONDICIÓN SUBSANABLE / NO SUBSANABLE
1) **Formulario de Presentación de Oferta Económica** (SNCC.F.033), presentado en Un (1) original debidamente marcado como "ORIGINAL" en la primera página de la Oferta, junto con **una (1)** fotocopia simple de la misma. El original deberá estar firmado en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía. Las copias deben ser	**NO SUBSANABLE**

fiel al original y solo deben estar firmadas y selladas en la primera página. **(No subsanable) Presentar la oferta sin ITBIS.** Salvo lo establecido en el artículo 129, del decreto No. 416-23.	
2) **Garantía bancaria o póliza de seriedad de la Oferta,** equivalente al 1% del monto ofertado a nombre de la Superintendencia de Salud y Riesgos Laborales (SISALRIL). **La misma debe contener la condición de: *INCONDICIONAL, IRREVOCABLE y RENOVABLE.*** Si se trata de un oferente certificado como MIPYME solo será exigida la fianza de seguro.	**NO SUBSANABLE**

Nota: Conforme el artículo 198 del Reglamento núm. 416-23, cuando la garantía de seriedad de la oferta resulte en un monto insuficiente, producto de una corrección aritmética realizada a la oferta económica y cuando contenga errores materiales o el tipo de moneda sea distinta a la solicitada, podrá requerirse subsanación.

12. Metodología de evaluación

Para evaluar la documentación solicitada a los oferentes y verificar si las ofertas cumplen sustancialmente con lo solicitado en el pliego de condiciones y sus especificaciones técnicas, los peritos designados aplicarán la metodología y criterios de evaluación establecidos en esta sección y así determinar la oferta más conveniente para fines de adjudicación, suscripción y ejecución del contrato.

12.1 Metodología y criterios de evaluación de la oferta técnica "Sobre A"[6]

Las ofertas técnicas deberán contener toda la documentación requerida en el numeral 11.1 sobre **"Documentos de la oferta técnica "Sobre A"** de este pliego, de manera que los(as) peritos designados al momento de evaluar puedan examinar detenidamente la documentación presentada y asegurarse de la veracidad de la información proporcionada por los oferentes/proponentes y determinar si una oferta cumple o no con lo requerido, Serán evaluadas con la siguiente metodología, y bajo los criterios que se desglosan en los siguientes subapartados:

OFERTA TÉCNICA "SOBRE A"	METODOLOGÍA[7]
Documentación legal	Cumple/No cumple
Documentación financiera	Cumple/ No cumple
Documentación técnica	Cumple/ No cumple

De no cumplirse con uno cualquiera de los requerimientos, el oferente/proponente quedará descalificado y en consecuencia su oferta será desestimada, lo cual será documentado y motivado en el correspondiente informe de evaluación técnica emitido por los peritos

[6] De conformidad con el artículo 72 del Reglamento núm. 416-23 no podrán establecerse reservas de derecho para ampliar o reducir los criterios de evaluación y adjudicación, así como tampoco evaluar con base a criterios no establecidos en esta sección.

[7] La documentación legal y la documentación financiera solo pueden ser evaluada bajo el criterio Cumple/No cumple, por ser credenciales habilitantes para poder ser oferente y ejecutar satisfactoriamente el contrato (artículo 82 Reglamento núm. 416-23).

evaluadores designados. La institución agotará el proceso de debida diligencia conjuntamente con las fases de evaluación.

12.1.1 Metodología y criterios de evaluación para la documentación legal

La **documentación legal** debe permitir validar la elegibilidad del oferente/proponente, es decir, que las personas física o jurídica está legalmente autorizado y habilitado para realizar las actividades comerciales solicitadas en el país, y su vez, para presentar ofertas. Esta documentación solo podrá ser evaluada bajo la metodología **CUMPLE / NO CUMPLE**. Tendrá carácter subsanable conforme a lo establecido en la sección 11.1.1 sobre **"a) Documentación legal"** siempre y cuando cumpla con el requisito al momento de presentación de la oferta. El esquema de evaluación será el siguiente:

CRITERIO A EVALUAR: ELEGIBILIDAD	
DOCUMENTO A EVALUAR	CUMPLE/ NO CUMPLE
Formulario de Presentación de Oferta (SNCC.F.034)	CUMPLE/NO CUMPLE
Formulario de Información sobre el(la) Oferente (SNCC.F.042)	CUMPLE/NO CUMPLE
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. Puede incluirla para mayor rapidez.	CUMPLE/NO CUMPLE
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. Puede incluirla para mayor rapidez.	CUMPLE/NO CUMPLE
Registro de Proveedores del Estado (RPE), emitido por la Dirección General de Contrataciones Públicas, debe tener inscrita, conforme a la codificación UNSPSC la actividad comercial - **81110000-Servicios informáticos**, referida en el numeral 2 sobre "objeto del procedimiento de selección" de este pliego, no tiene que ser depositado, será verificado en línea por la institución. Puede incluirla para mayor rapidez. **(No Subsanable, después de la fecha establecida en cronograma)**	CUMPLE/NO CUMPLE
Copia del Registro Mercantil expedido por la Cámara de Comercio y Producción correspondiente (vigente).	CUMPLE/NO CUMPLE
Copia de los Estatutos sociales vigentes debidamente registrado en la Cámara de Comercio y Producción correspondiente.	CUMPLE/NO CUMPLE
Copia de la nómina de accionistas y acta de la última asamblea realizada debidamente registrada por ante la Cámara de Comercio y Producción correspondiente	CUMPLE/NO CUMPLE
Copia de la nómina de accionistas y acta de asamblea realizada mediante la cual se designe expresamente el actual gerente o consejo de administración, según aplique, que tiene potestad para firmar contratos a nombre de la empresa participante, debidamente registrada en la Cámara de Comercio y Producción correspondiente.	CUMPLE/NO CUMPLE

CRITERIO A EVALUAR: ELEGIBILIDAD	
DOCUMENTO A EVALUAR	CUMPLE/ NO CUMPLE
Formulario de Compromiso ético de proveedores (as) del Estado[8] debidamente firmado y sellado.	CUMPLE/NO CUMPLE
Declaración jurada simple (no requiere firma de notario público) del oferente manifestando que no se encuentra dentro de las prohibiciones en el artículo 8 numeral 3 y artículo 14 de la Ley núm. 340-06 y sus modificaciones.	CUMPLE/NO CUMPLE
Formulario de Debida Diligencia.	CUMPLE/NO CUMPLE
Copia de la cédula de identidad y electoral del representante legal.	CUMPLE/NO CUMPLE

12.1.2 Metodología y criterios de evaluación para la documentación financiera

La **documentación financiera** debe permitir validar que el oferente/proponente cuenta con estabilidad financiera para ejecutar satisfactoriamente el eventual contrato. En tal sentido, el Oferente/Proponente debe acreditar su capacidad financiera con los documentos requeridos en el 11.1.1 sobre **"documentación financiera"** de este pliego, que solo podrá ser evaluada bajo la metodología **CUMPLE/NO CUMPLE.**

DOCUMENTACIÓN FINANCIERA	
DOCUMENTOS A EVALUAR	CUMPLE/NO CUMPLE
Se solicita a los participantes de este proceso de contratación Certificados e instrumentos financieros que acrediten la disponibilidad de recursos, incluyendo constancia de líneas de créditos activas dirigida a la Institución Contratante, cuyo monto sea equivalente, como mínimo **al diez por ciento (10%) del valor de la contratación**.	CUMPLE/NO CUMPLE
Declaraciones juradas anuales del Impuesto sobre la Renta de sociedades y personas físicas. Copia de las declaraciones juradas anuales del impuesto sobre la renta y sociedades y personas físicas presentadas ante la Dirección de General de Impuestos Internos **(Formularios IR—1 e IR-2).**	CUMPLE/NO CUMPLE

12.1.3 Metodología y criterios de evaluación para la documentación técnica

a) Las ofertas deberán contener la documentación técnica solicitada en 11.1.2 "**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

[8] Para participar en este procedimiento, es un requisito indispensable que los(as) oferentes suscriban y entreguen junto a su oferta, el documento "compromiso ético de proveedores(as) del Estado", que consta como anexo en el presente pliego de condiciones. De no ser presentado junto a su oferta, podrá ser incluido en la fase de subsanación prevista en el cronograma de actividades; vencido este plazo sin haberlo acreditado, su oferta será descalificada haciéndose constar en el informe de evaluación que deberá ser emitido en el marco del procedimiento.

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:

DESCRIPCIÓN	CUMPLE/NO CUMPLE
Oferta Técnica (conforme a los Términos de Referencias y cantidades suministradas en el punto 3.) **APLICA PARA TODOS LOS ITEMS**.	**CUMPLE/NO CUMPLE**
Carta de aceptación de condición de pagos y tiempo de entrega, en que el proveedor se comprometa a realizar la entrega en plazo establecido en el presente pliego de condiciones. **APLICA PARA TODOS LOS ITEMS**.	**CUMPLE/NO CUMPLE**
Certificación donde el oferente se compromete a entregar la solución tal como es solicitada en las especificaciones detalladas en el TDR anexo a este Pliego de Condiciones. **APLICA PARA TODOS LOS ITEMS**.	**CUMPLE/NO CUMPLE**
El oferente deberá presentar una carta elaborada por el fabricante, mediante la cual se acredite al oferente como Partner Oficial de la marca ofertada. **APLICA PARA LOS ITEMS DEL 1-7.**	**CUMPLE/NO CUMPLE**
El oferente debe ser una empresa consolidada en el mercado con más de 5 años experiencia en el área de ciberseguridad, demostrado mediante cartas de empresas a las cuales les haya brindado el servicio. **APLICA PARA EL ÍTEM 3.**	**CUMPLE/NO CUMPLE**
El oferente debe tener personal técnico mínimo dos (2) con certificación vigente del fabricante que garantice conocimiento para participar en cualquier etapa del ciclo de vida de la solución ofertada, debe incluirse la documentación correspondiente junto con el currículo del personal asignado de al menos dos (2) personas. **APLICA PARA EL ÍTEM 3.**	**CUMPLE/NO CUMPLE**
Un (1) gestor de proyecto certificado como PMP Project Management Professional) emitida por el PMI (Project Management Institute) o de otra entidad mundialmente reconocida, con más de 2 años de experiencia. Para lo cual deberá presentar documento donde conste dicha condición y su vigencia. **APLICA PARA EL ÍTEM 3.**	**CUMPLE/NO CUMPLE**
Un (1) profesional certificado como ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición. **APLICA PARA EL ÍTEM 3.**	**CUMPLE/NO CUMPLE**

Un (1) profesional certificado como Certified Information Systems Security Professional (CISSP). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición. APLICA PARA EL ÍTEM 3.	CUMPLE/NO CUMPLE
Cartas de referencias que se demuestre la experiencia comprobable en implementación de al menos 2 proyectos similares de la solución ofertada en países de la región latinoamericana donde cuente con presencia. APLICA PARA EL ITEM 4	CUMPLE/NO CUMPLE
La empresa ofertante deberá contar con más de 5 años de experiencia en el área de ciberseguridad en República Dominicana o en la región latinoamericana. Presentar Cartas de referencias. APLICA PARA EL ITEM 4.	CUMPLE/NO CUMPLE
El oferente debe contar con al menos 2 ingenieros certificados por el fabricante en la región latinoamericana donde cuente con presencia para configuración y administración de la solución ofertada, entregar Currículo del personal. APLICA PARA EL ITEM 4	CUMPLE/NO CUMPLE
Para garantizar el soporte y la implementación basado en las mejores prácticas de seguridad el oferente deberá contar con personal, en cualquier país que tenga representación con las siguientes certificaciones: ○ Al menos un (1) gestor de proyecto certificado como PMO con más de 2 años de experiencia ○ Al menos un (1) profesional certificado Certified Network Defense Architect EC Council ○ Al menos un (1) profesional certificado en ISO/IEC 27001. Presentar la certificación correspondiente que respalde dichas acreditaciones. APLICA PARA EL ITEM 4	CUMPLE/NO CUMPLE

12.2 Metodología y criterios de evaluación de oferta económica

La evaluación de las ofertas económicas será bajo la metodología **Cumple/ no cumple.**

PROPUESTA ECONÓMICA	
CRITERIO A EVALUAR	CUMPLE/ NO CUMPLE
Oferta económica presentada en PESOS DOMINICANOS (RD$). Los precios deberán expresarse en dos decimales (XX.XX) que tendrán que incluir todas las	CUMPLE/NO CUMPLE

PROPUESTA ECONÓMICA	
CRITERIO A EVALUAR	CUMPLE/ NO CUMPLE
tasas, impuestos (si aplican) y gastos que correspondan, transparentados e implícitos según corresponda y en la unidad de medida establecida en el Formulario de **Oferta Económica SNCC.F.033** sin alteraciones ni correcciones. NO SUBSANABLE.	
Garantía bancaria o póliza de seriedad de la Oferta, equivalente al 1% del monto ofertado a nombre de la Superintendencia de Salud y Riesgos Laborales (SISALRIL). **La misma debe contener la condición de: *INCONDICIONAL, IRREVOCABLE Y RENOVABLE*** Si se trata de un oferente certificado como MIPYME solo será exigida la fianza de seguro. NO SUBSANABLE.	**CUMPLE/NO CUMPLE**

La omisión en la presentación de la Oferta de la Garantía de Seriedad de Oferta conllevará la desestimación de la Oferta sin más trámite. La vigencia de la garantía deberá ser igual al plazo de validez de la oferta.

12.3 Criterio de adjudicación.

La Superintendencia de Salud y Riesgos Laborales evaluará las ofertas dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás, que regulan la actividad contractual, y comunicará por escrito a todos los participantes el oferente que resulte favorecido.

El criterio de adjudicación para determinar la oferta más conveniente para este procedimiento de contratación es: La adjudicación será favor del oferente que oferte el menor precio y cumpla con lo establecido en los TDR anexo como parte integral y vinculante de este Pliegos de Condiciones y con cada requisito que demuestre la experiencia buscada, siempre que su oferta sea calificada como la más conveniente para los intereses de la institución, teniendo en cuenta la idoneidad del oferente. Si se presentase una sola Oferta, ella deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en este documento, se le considera conveniente a los intereses de la Institución.

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

La adjudicación será por **ITEMS** a favor del oferente que presente el **menor precio,** de entre de entre aquellas ofertas técnicas que hayan cumplido previamente con todo lo solicitado en el pliego de condiciones.

Serán rechazadas las ofertas cuyas cantidades o características sean diferentes a lo solicitado, necesario para la realización de la propuesta, será descalificado sin más transmite; solo se tomarán en cuenta la oferta que cumpla con todo lo establecido en las especificaciones técnicas.

En caso de empate entre dos o más oferentes/proponentes, el Comité de Compras y Contrataciones (CCC), de esta institución procederá a llamar a las empresas que resultaron empatadas a mejorar las ofertas adjudicando de ese modo a la empresa que menor precio

presente y haya cumplido con todo lo solicitado en el sobre A, de lo contrario el CCC realizara una elección al azar, utilizando para tales fines el procedimiento de sorteo en presencia de un notario público y los oferentes empatados.

SECCIÓN II: RECEPCIÓN, APERTURA, EVALUACIÓN Y ADJUDICACIÓN

1. Recepción de ofertas técnicas "Sobre A" y ofertas económicas "Sobre B"

De conformidad con el artículo 114 del Reglamento 416-23 este procedimiento de Licitación Pública Nacional para la **ADQUISICIÓN Y RENOVACIÓN DE LICENCIAS INFORMÁTICAS PARA USO DE LA SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES** con el número de Referencia **SISALRIL-CCC-LPN-2025-0007**, la recepción, apertura y evaluación de las ofertas se llevará a cabo en dos etapas:

Primera etapa. Para la presentación y recepción de las ofertas técnicas y las ofertas económicas y la apertura y evaluación de las ofertas técnicas y;

Segunda etapa. La apertura y evaluación de las ofertas económicas.

Las ofertas podrán ser recibidas desde el día de publicada la convocatoria en el SECP hasta **miércoles quince (15) de octubre del año dos mil veinticinco (2025) hasta las nueve (9:00 a.m.) de la mañana.**

Cuando se trate de ofertas electrónicas recibidas por el SECP, el sistema de forma automática se registra la fecha y hora de la recepción de las ofertas, manteniéndolas encriptadas, sin posibilidad de que se conozca su contenido hasta que la institución contratante realice la apertura, en la fecha y hora fijadas en el cronograma de actividades previsto en el presente pliego de condiciones.

Cuando se trate de ofertas en formato o soporte papel, la Unidad Operativa de Compras y Contrataciones (UOCC) será responsable de recibirlas, custodiarlas y de elaborar y llevar registro de oferentes con nombre, fecha y hora. Cada oferente tendrá derecho a recibir un conduce de recepción de oferta entregada.

Una vez pasada la hora establecida para la recepción de los sobres de los(as) oferentes/proponentes, no se aceptará la presentación de nuevas propuestas, aunque el acto de apertura no se inicie en la fecha y/o en la hora señalada en el pliego de condiciones.

2. Apertura de ofertas técnicas "Sobre A"

La apertura de las ofertas técnicas recibidas ya sea en formato papel o electrónico se realizará en acto público en presencia del CCC y del(la) Notario Público actuante y de los(las) oferentes que deseen participar para quienes la asistencia será voluntaria y nunca obligatoria, en la fecha, lugar y hora establecidos en el cronograma de actividades y a través de **Microsoft Teams mediante la cual será transmitido de manera simultánea (en vivo) el acto de apertura y el acceso a participar.**

Los interesados deberán remitir al correo electrónico: gerencia_compras@sisalril.gob.do y an.gonzalez@sisalril.gob.do de manera que podamos compartirle el link de acceso a dicho acto con la siguiente información.

REFERENCIA DEL PROCESO:
NOMBRE DEL OFERENTE/PROPONENTE.
NOMBRE DEL REPRESENTANTE:
CORREO ELECTRÓNICO:
NÚMERO DE CONTACTO:

Concluido el acto de apertura, el(la) Notario Público actuante dará por cerrado el mismo, indicando la hora de cierre. Las actas notariales deberán ser publicadas en el SECP a los fines de que estén disponibles para consulta de todos los interesados.

3. Evaluación de ofertas técnicas "Sobre A", aclaraciones y subsanación

Los peritos designados para la evaluación procederán a la validación y verificación de los documentos de la oferta técnica o "Sobre A" evaluando conforme a la metodología y criterios establecidos en el pliego 12.1.3 Metodología y criterios de evaluación para la documentación técnica "Sobre A"

Ante duda sobre la información presentada, los(as) peritos podrán solicitar hasta antes de emitir el informe definitivo, mediante acto administrativo emitido por el CCC, según corresponda y notificado por la UOCC al (la) oferente, las aclaraciones en los términos del artículo 123 del Reglamento núm. 416-23 que considere necesarias y comprobar la veracidad de la información recibida, cursándole del mismo modo.

Los peritos emitirán un ***informe preliminar de evaluación técnica*** en el cual se indicará si las ofertas cumplen con los criterios establecidos en este pliego o si existen desviaciones, reservas, omisiones o errores de naturaleza o de tipo subsanables de conformidad con la normativa.

En los casos en que se presenten desviaciones, reservas, omisiones o errores de naturaleza o tipo subsanables, los(as) peritos procederán de conformidad con lo establecido en el párrafo III del artículo 8 de la Ley núm. 340-06 y sus modificaciones y artículos 120, 121 y 122 del Reglamento núm. 416-23 para solicitar, mediante acto administrativo emitido por el CCC o la DAF, según corresponda y notificado por la UOCC al (la) oferente, las subsanaciones en el plazo previsto en el cronograma de actividades.

Este informe también será publicado en el SECP y notificado a todos(as) los(as) oferentes participantes y contendrá los elementos a subsanar y el resultado de la ponderación preliminar.

Concluido el plazo para las subsanaciones, los peritos emitirán un ***informe definitivo de evaluación técnica*** que describirá de manera pormenorizada la evaluación realizada a todas las ofertas recibidas, su ponderación, nivel de cumplimiento, si agotó fase de subsanación y la recomendación, con base en los criterios establecidos, de los(as) oferentes que deben ser habilitados para la evaluación de sus ofertas económicas. El CCC aprobará si procede el informe definitivo de evaluación de ofertas técnicas, mediante un acto administrativo debidamente motivado. El acta indicará los oferentes habilitados y no habilitados para la apertura y evaluación de sus ofertas económicas.

A los oferentes cuyas ofertas técnicas no hayan superado los mínimos establecidos en el pliego de condiciones, les serán devueltas sus ofertas económicas sin abrir si fueron recibidas en soporte papel, y si fueron recibidas a través de SECP permanecerán sin abrir encriptadas y sin ser ponderadas.

Todos los informes de evaluación y el acto de aprobación del CCC, así como las notificaciones de subsanación y las subsanaciones realizadas en plazo, se harán constar en el SECP aun hayan sido recibidas en formato papel o físico.

4. Debida diligencia

La **Superintendencia de Salud y Riesgos Laborales,** 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, durante la fase de evaluación técnica 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, **Superintendencia de Salud y Riesgos Laborales** se reserva la facultad de realizar el proceso de debida diligencia dentro del marco de la presente contratación a fin de:

1) Comprobar y verificar la identidad del proveedor sobre la base de documentos, datos o informaciones obtenidas de fuentes fiables e independientes;
2) Identificar al Beneficiario Final de la empresa proveedora;
3) La existencia o no de procesos judiciales actuales o pasados vinculados a delitos contra la administración pública, lavado de activos y otros;
4) Constatar errores o escrituras similares en los documentos presentados por diferentes empresas en el procedimiento de contratación;
5) Identificar coincidencias en algunos de los datos suministrados por distintos proveedores tales como: domicilio accionistas, teléfonos, entre otros:
6) 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;
7) 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;
8) Determinar posibles vinculaciones entre oferentes y funcionarios públicos de la organización para gestionar posibles conflictos de interés;
9) Identificar propuestas idénticas en el procedimiento de contratación;
10) 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.
11) 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 tres (3) 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.

5. Apertura y evaluación de las ofertas económicas "Sobre B"

Posterior a la evaluación técnica y al conocer los oferentes habilitados para el examen de la propuesta económica se convocará nueva vez en la fecha establecida en el cronograma de actividades del presente pliego de condiciones, a un acto público con el CCC y oferentes habilitados y el (la) Notario Público para abrir las ofertas económicas recibidas en formato o soporte papel y para desencriptar las ofertas enviadas electrónicamente vía la plataforma SECP.

Se entregará a los (as) peritos las ofertas económicas para que las evalúen y recomienden la adjudicación conforme a la metodología y criterios establecidos en este pliego de condiciones junto a la garantía de seriedad de la oferta.

En la fase de evaluación de las ofertas económicas los peritos también podrán solicitar aclaraciones en los términos del artículo 123 del Reglamento núm. 416-23 vinculadas a éstas, siempre que se realicen en el plazo establecido en el cronograma de actividades de este pliego condiciones.

Del mismo modo, los peritos podrán aplicar correcciones de errores aritméticos, en los términos y condiciones del artículo 129 del citado Reglamento. Dichas correcciones luego de realizadas deberán ser expresamente aceptadas por lo oferentes en los plazos establecidos en el cronograma de actividades del presente pliego de condiciones. Si el oferente no acepta las correcciones su oferta será rechazada lo cual será documentado y motivado en el correspondiente informe de evaluación emitida por los peritos evaluadores designados.

Los resultados de la evaluación se presentarán mediante ***informe de evaluación de ofertas económicas*** informe pericial debidamente motivado y con los detalles de la evaluación de cada oferta de forma individualizada, en el que se incluirá un reporte de lugares ocupados que indiquen el orden de preferencia, para fines de adjudicación y suplencia, ante un eventual incumplimiento del(la) adjudicatario(a), o en su defecto, se recomiende la declaratoria de desierto o cancelación del procedimiento.

6. Subsanación de la Garantía de Seriedad de la Oferta

La garantía de seriedad de la oferta podrá ser subsanada en estos casos dos casos:

1) Cuando contiene errores materiales o en la moneda solicitada y;
2) Cuando resulte en un monto insuficiente, producto de una corrección aritmética realizada a la oferta económica.

Verificada una de estas situaciones, los(as) peritos deberán solicitar antes de emitir el *informe de evaluación de ofertas económicas*, mediante acto administrativo emitido por el CCC y notificado por la UOCC, que el (la) oferente subsane la garantía de seriedad de la oferta, quien deberá presentarla en el plazo señalado en el cronograma de actividades del pliego de condiciones, en caso contrario, su oferta será desestimada, lo cual será documentado y motivado en el correspondiente informe.

7. Confidencialidad de la evaluación

La información relativa al contenido de las ofertas, las subsanaciones, solicitudes de aclaraciones y las evaluaciones realizadas por los peritos no serán reveladas a los oferentes ni a otra persona que no participe oficialmente en el procedimiento, hasta tanto el CCC haya aprobado los informes de evaluación de ofertas emitidos, los cuales deberán ser publicados en el SECP y notificarse directamente a todos los oferentes participantes, de conformidad con los artículos 125 y 133 del Reglamento núm. 416-23.

8. Desempate de ofertas

En caso de empate entre dos o más Oferentes/Proponentes, se procederá a elegir la oferta de la empresa que haya presentado un plan empresarial de responsabilidad para protección del medio ambiente en su cadena de producción, para confirmar el cumplimiento con el criterio deberá existir constancia inequívoca en la oferta evaluada.

Si ninguna de las ofertas cumple con algunos de los criterios de preferencia para el desempate, 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 CCC y en presencia de Notario Público, quien certificará el acto.

9. Adjudicación[9]

El Comité de Compras y Contrataciones, luego del proceso de verificación y validación del informe de evaluación y recomendación de adjudicación emitido por los peritos y, tras verificar que la evaluación se haya realizado con base en los criterios y condiciones establecidos en el pliego de condiciones, aprueban el informe y emiten el acto contentivo de la adjudicación. Tanto el informe de los peritos como el acta del Comité de Compras y Contrataciones deberá publicarse inmediatamente en el SECP.

La UOCC deberá notificar el acto de adjudicación y sus anexos, si tuviese, incluido el informe de evaluación de los peritos a todos(as) los(as) oferentes participantes, conforme al procedimiento y plazo establecido en el Cronograma de Actividades de este pliego.

En el evento de que el adjudicatario se negase de forma injustificada a presentar la garantía de fiel cumplimiento y a suscribir el contrato, el Comité de Compras y Contrataciones ejecutará la garantía de seriedad de la oferta siguiendo el procedimiento previsto en el artículo 210 del Reglamento núm. 416-23.

10. Garantías del fiel cumplimiento de contrato

Para poder suscribir el contrato el(la) o los(las) adjudicatarios(as) deberán constituir previamente una garantía de fiel cumplimiento de contrato en favor de la **Superintendencia de Salud y Riesgos Laborales** para asegurar que cumplirá con las condiciones y cláusulas establecidas en el pliego de condiciones y en el contrato y que los bienes sean entregados de acuerdo con las condiciones y requisitos previstos en pliego de condiciones, las especificaciones técnicas, la oferta adjudicada y el propio contrato.

[9] Ver definición numeral 1 del artículo 4 del Decreto Núm. 416-23.

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 o Garantía Bancaria por el 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. Si se trata de un adjudicatario extranjero, el plazo para presentar la garantía es de diez (10) días hábiles.

Nota: Conforme las disposiciones del párrafo II del artículo 30 de la Ley Núm. 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras y Sus Modificaciones, así como las del párrafo I del artículo 192 del Reglamento de Aplicación Núm. 416-23, las modalidades de garantía permitidas son la garantía bancaria y la póliza de seguro, las mismas deben contener las condiciones de INCONDICIONALES, IRREVOCABLES Y RENOVABLES. Para el caso de MIPYMES, solo será exigida la fianza de seguro.

Las condiciones de irrevocables e incondicionales deben estar explícitamente en el contenido de las garantías que son exigidas en los procedimientos de contratación pública, esto con la finalidad de evitar ambigüedades y proteger a la Administración ante un incumplimiento del oferente o adjudicatario. Por lo tanto, la omisión o el incumplimiento de las referidas características dispuestas en el párrafo II del artículo 30 de la Ley Núm. 340-06 sobre Compras Y Contrataciones de Bienes, Servicios y Obras y Sus Modificaciones, PODRÍA AFECTAR SU ACEPTACIÓN EN EL PROCEDIMIENTO DE CONTRATACIÓN DE QUE SE TRATE. ES DECIR, QUE ESTE ASPECTO NO ES CONSIDERADO UN ERROR MATERIAL Y POR ENDE NO ES SUSCEPTIBLE DE SUBSANACIÓN. Para más información, consultar Circular de Aclaraciones sobre las garantías en el Sistema Nacional de Compras y Contrataciones Públicas (SNCCP).

La vigencia de la garantía será de mínimo de **doce (12) meses** contados a partir de la constitución de la misma y hasta el fiel cumplimiento y hasta la liquidación del contrato.

Si el o los adjudicatarios 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 contratante ejecute su garantía de seriedad de la oferta y 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 de los bienes contratados.

11. Adjudicaciones posteriores

En caso de incumplimiento del(la) oferente adjudicatario, de no presentar la garantía de fiel cumplimento o de rechazar suscribir el contrato, se procederá a solicitar, mediante ***"Carta de Solicitud de Disponibilidad"***, al oferente en segundo lugar, de conformidad con el reporte de lugares ocupados, que certifique si está en capacidad de suministrar los bienes ofertados. Dicho Oferente/Proponente contará con un plazo de **48 horas** para responder la referida solicitud. En caso de respuesta afirmativa, el(la) Oferente/Proponente deberá presentar la Garantía de Fiel cumplimiento de contrato, como se requiere en el numeral 10 para suscribir el contrato.

En caso de que el oferente en segundo lugar no acepte ejecutar el contrato, así como sucesivamente ninguno de los demás oferentes del reporte de lugares, el CCC declarará el procedimiento desierto mediante acto administrativo debidamente motivado e iniciará la convocatoria a un nuevo procedimiento de selección.

SECCIÓN III: DISPOSCIONES GENERALES PARA EL CONTRATO

1. Plazo para la suscripción del contrato[10]

El contrato entre la **Superintendencia de Salud y Riesgos Laborales** y el adjudicatario deberá ser suscrito en la fecha que establece el cronograma de actividades del presente pliego de condiciones, el cual no deberá ser mayor a veinte (20) días hábiles, contados desde la fecha de notificación de la adjudicación, de conformidad con el artículo 164 del Reglamento 416-23.

2. Validez y perfeccionamiento del contrato

El contrato será válido cuando para su suscripción se haya cumplido con ordenamiento jurídico y cuando el acto definitivo de adjudicación y la constitución de la Garantía de Fiel Cumplimiento de contrato hayan sido satisfechas.

El contrato se considerará perfeccionado una vez se publique por el SECP y en el portal institucional de la **Superintendencia de Salud y Riesgos Laborales,** en un plazo no mayor de cinco (5) días hábiles luego de su suscripción y, además, en el caso de las instituciones sujetas a la Ley núm. 10-07 del Sistema Nacional de Control Interno, se haya registrado en la Contraloría General de la República.

3. Gastos legales del contrato:

En este procedimiento de contratación los gastos de la legalización de firmas del contrato resultante por parte del notario serán asumidos por la institución contratante en este proceso de Licitación Pública Nacional.

4. Vigencia del contrato

La vigencia del Contrato será de **doce (12) meses**, contados a partir de la fecha de la suscripción del mismo y hasta su fiel cumplimiento y liquidación, de conformidad con el Cronograma de entrega, el cual formará parte integral y vinculante del mismo.

5. Supervisor o responsable del contrato

La **Superintendencia de Salud y Riesgos Laborales** ha designado como supervisor o responsable del contrato a la Dirección de Tecnología.

6. Entregas a requerimiento

La **Superintendencia de Salud y Riesgos Laborales** solicitará que los bienes se entreguen en su totalidad dentro de un periodo no mayor a **quince (15) días calendarios** contados a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República para los **ítems 1,2,3,4,6,7,8** y no mayor cuarenta y cinco (45) días calendarios, contados a partir de que sea emitida la certificación del contrato por parte de la Contraloría General de la República, para el **ítem 5**.

[10] Ver definición en el artículo 4 de la Ley Núm. 340-06 y sus modificaciones.

7. Anticipo y Garantía de buen uso de anticipo

El anticipo que le será otorgado al adjudicatario, si se trata de un oferente certificado como MIPYME, el valor será de un 20% al valor del contrato, el mismo, se efectuará en un plazo no mayor de **treinta (30)** días a partir de la Certificación del contrato y contra presentación de una garantía de buen uso de anticipo de tipo póliza de seguro o Garantía Bancaria que cubra la totalidad del Avance Inicial.

La garantía de buen uso de anticipo será devuelta cuando el(la) contratista demuestre que cumplió con todas las obligaciones del contrato. El monto máximo que será devuelto debe ser igual al monto dado como anticipo.

8. Suspensión del contrato

La **Superintendencia de Salud y Riesgos Laborales** podrá ordenar la suspensión temporal del contrato mediante acto administrativo motivado suscrito por la máxima autoridad y notificado al(la) contratista, por las causas que establece el artículo 31 numeral 5) de la Ley núm. 340-06 y sus modificaciones y el artículo 182 del Reglamento 416-23.

La Dirección General de Contrataciones Públicas, también podrá ordenar la suspensión del contrato como resultado de una medida cautelar impuesta en el marco del conocimiento de un recurso, investigación o inhabilitación.

9. Modificación de los contratos

Toda modificación del contrato sea unilateral o prevista en el pliego de condiciones, se formalizará a través de una enmienda con el contenido previsto en el artículo 164 del Reglamento de Aplicación de la Ley 340-06 emitido mediante Decreto Núm. 416-23 y previo a realizarse cualquier prestación sustentada en la modificación deberá ser publicada en el SECP.

10. Equilibrio económico y financiero del contrato

La **Superintendencia de Salud y Riesgos Laborales** adoptará todas las medidas necesarias para mantener las condiciones técnicas, económicas y financieras del contrato durante su ejecución. En el evento de que estas condiciones no se mantengan, puede dar paso a una ruptura del equilibrio económico y financiero del contrato, que afecte al contratista o a la institución, siempre que se origine por razones no imputables a la parte que reclama la afectación y que no tenía la obligación de soportar.

La afectación puede dar paso al derecho tanto al contratista como a la **Superintendencia de Salud y Riesgos Laborales** a procurar el restablecimiento del equilibro económico y financiero del contrato con sus correspondientes ajustes. No obstante, el hecho de que una de las causas que provocan la ruptura del equilibrio económico se materialice, no significa que, automáticamente, se ha podido comprobar el daño económico para quien lo invoque.

En ese sentido, para el restablecimiento del equilibro económico y financiero del contrato, quien lo invoque deberá demostrarlo y solicitarlo, conforme a los criterios y el procedimiento previsto en el artículo 32 numeral 1) de la Ley núm. 340-06 y sus modificaciones y los artículos 176, 177 y 178 del Reglamento núm. 416-23.

11. Condiciones de pago y retenciones

Los pagos serán realizados en un período **no mayor a sesenta (60) días hábiles** contados a partir de que sea emitida la Certificación del Contrato por parte de la Contraloría General de la República, así como el recibido conforme por parte del área solicitante y luego de que el proveedor remita al área correspondiente, las facturas de los bienes ofrecidos. las cuales deberán ser remitidas detallando los bienes entregados.

Dicha factura deberá cumplir con las siguientes especificaciones: 1. Número de Comprobante Fiscal Gubernamental (B15). 2. Estar expedida a nombre de la Superintendencia de Salud y Riesgos Laborales. 3. Los precios incluidos en la misma deberán estar en pesos dominicanos RD$.

En caso de que el adjudicatario del contrato sea una Micro, Pequeña y Mediana empresa (MIPYME), a solicitud de la parte interesada, les será entregado un avance inicial correspondiente al veinte por ciento (20%) del valor del contrato, para fortalecer su capacidad económica y este pago se hará en un plazo no mayor de **treinta días (30) días** a partir de la certificación del Contrato y contra la presentación de la Garantía de Buen Uso del Anticipo, de acuerdo con la normativa vigente.

La suma restante será pagada al proveedor, en la totalidad a partir de la recepción conforme del bien contratado. Estos pagos se harán en un período no mayor de **sesenta (60) días hábiles** contados a partir de que el proveedor remita al área correspondiente las facturas de los bienes ofrecidos. No está permitido que el proveedor reciba el pago total de los bienes sin que el objeto del contrato se haya cumplido. Las facturas deberán ser remitidas detallando los bienes o servicios entregados.

12. Recepción de los bienes

Concluida la entrega de los bienes, el personal designado por la institución como responsable del contrato procederá a completar un acta de recepción provisional donde determine, a partir de las especificaciones técnicas, si los bienes adquiridos cumplieron o no con lo pactado.

Si el suministro de bienes fue acorde con las especificaciones técnicas, la institución deberá formalizarla mediante la recepción conforme en un plazo de siete (07) días hábiles, a partir del día siguiente de notificada entrega de los bienes. El proveedor tiene derecho de intimar a la institución contratante la emisión de la recepción conforme, sino lo realiza en el referido plazo.

De existir cualquier anomalía con la entrega o posibles desperfectos o diferencias en los bienes ofertados y los recibidos por la entidad contratante, y se tenga tiempo suficiente para que el proveedor corrija las faltas antes de que se cumpla el período en que se necesita, la institución deberá notificar en un plazo de cinco (5) días hábiles[11], al proveedor para que subsane los defectos y proceda, en un plazo[12] no superior a **quince (15) días hábiles**, a la corrección de los errores detectados.

En los casos donde el proveedor no haya cumplido con la corrección en los bienes o en la entrega de los mismos, antes del período en que la institución lo requería, esta deberá notificar en un plazo de cinco (5) días hábiles, el acta de no conformidad con la recepción de los bienes y,

[11] Plazo fijado por el párrafo II del artículo 185 del Reglamento núm. 416-23.
[12] El plazo debe ser proporcional y congruente al tipo de correcciones y servicio.

conforme con el debido proceso, puede iniciar las medidas administrativas correspondientes por la falta del proveedor.

13. Finalización del contrato

El contrato finalizará por una de las siguientes condiciones que acontezca en el tiempo: **a)** Cumplimiento del objeto; **b)** por mutuo acuerdo entre las partes o; **c)** por las causas de resolución previstas en el artículo 190 del Reglamento núm. 416-23.

14. Incumplimiento de contrato y sus consecuencias.

Se considerará incumplimiento del contrato las siguientes situaciones, sin perjuicio de aquellas contempladas en la normativa:

a) La mora del proveedor en la entrega de los bienes por causas imputables a éste por más de **diez (10) días calendarios.**
b) El incumplimiento de la calidad de los bienes exigidas en las especificaciones técnicas, prevista en el presente pliego de condiciones;
c) El suministro, prestación o entregas incompletas de las solicitadas y/o adjudicadas.

El incumplimiento del contrato por parte del(la) proveedor podrá suponer una causa de resolución del mismo de conformidad con el artículo 190 del Reglamento de Aplicación, y además el(la) contratista ser pasible de las siguientes sanciones previstas en el artículo 66 de la Ley núm. 340-06 y sus modificaciones, sin perjuicio de las acciones penales o civiles que correspondan.

15. Penalidades por retraso

a) Advertencia por escrito.
b) Ejecución de garantía.
c) Penalidades establecidas en el pliego de condiciones o en el contrato.
d) Rescisión unilateral sin responsabilidad para la entidad contratante.

16. Causas de inhabilitación del Registro de Proveedores del Estado.

La institución contratante podrá solicitar a la Dirección General de Contrataciones Públicas el inicio de un procedimiento administrativo sancionador, contra el(la) oferente o contratista que ha cometido alguna de las infracciones regladas en el artículo 66 de la Ley núm. 340-06 y sus modificaciones.

El procedimiento administrativo sancionador por las infracciones administrativas referidas en los numerales 7) al 10) del indicado artículo, podrá ser iniciado de oficio por la DGCP, si en el cumplimiento de su función de verificar que se cumplan con las normas del SNCPP, identifica indicios de que han sido cometidas.

SECCIÓN IV: GENERALIDADES

1. Siglas y acrónimos

CAP	Certificado de Apropiación Presupuestaria
CCPC	Certificado de disponibilidad de cuota para comprometer
CCC	Comité de Compras y Contrataciones

DAF	Dirección Administrativa Financiera
DGCP	Dirección General de Contrataciones Pública
PACC	Plan Anual de Compras y Contrataciones
MAE	Máxima Autoridad Ejecutiva
SECP	Sistema Electrónico de Contrataciones Públicas.
SNCP	Sistema Nacional de Compras y Contrataciones Públicas
SIGEF	Sistema de Información de la Gestión Financiera
UOCC	Unidad Operativa de Compras y Contrataciones

2. Definiciones

Para la implementación e interpretación del presente pliego de condiciones estándar, las palabras y expresiones que se citan tienen el siguiente significado:

1) Bienes[13]: Los objetos de cualquier índole, incluyendo las materias primas, los productos, los equipos otros objetos en estado sólido, liquido o gaseoso, así como los servicios accesorios al suministro de esos bienes, siempre que el valor de los servicios no exceda del de los propios bienes.

2) Bienes Comunes[14]: Son aquellos que pueden ser objetivamente definidos por el mercado, de forma sencilla y corriente debido a que son regularmente comprados y utilizados por el sector privado, o que tienen especificaciones técnicas y patrones de desempeño y calidad objetivamente definidos.

3) Bienes no comunes[15]: Son aquellos que por sus características y especificaciones especiales no pueden ser considerados como comunes, debido a su alto nivel de complejidad.

4) Ciclo de vida del producto[16]: Se refiera a todas las fases consecutivas o interrelacionadas que sucedan durante su existencia de un producto, obra o servicio, desde la investigación y desarrollo, diseño, materiales utilizados, fabricación, comercialización, incluido el transporte, utilización y mantenimiento del producto o servicio, hasta que se produzca la eliminación, el desmantelamiento o el final de la vida útil.

5) Conflictos de Interés[17]: Es aquella situación en la que el juicio del individuo (concerniente a su interés primario) y la integridad de una acción, tienden a estar indebidamente influidos por un interés secundario, de tipo generalmente económico o personal.

6) Debida Diligencia[18]: Conjunto de procedimientos, políticas y gestiones mediante el cual los sujetos obligados establecen un adecuado conocimiento sobre el comité de compras y contrataciones, personal de las unidades operativas de compras y contrataciones.

7) Desglose de Precios Unitarios: La lista detallada de tarifas y precios que muestren la composición de cada uno de los precios de las partidas que intervienen en el Presupuesto Detallado.

---

[13] Artículo 4 de la Ley 340-06 y sus modificaciones
[14] Numeral 2, artículo 4 del Reglamento de Aplicación 416-23
[15] Numeral 3, artículo 4 del Reglamento de Aplicación 416-23
[16] Numeral 6.10 del Artículo 6 de la Política de Compras Públicas Verdes, emitida por la DGCP y MIMARENA.
[17] Definición extraída de la *Guía de Gestión Integral de Riesgos en los procesos de contratación pública* de la DGCP.
[18] Definición extraída de la *Guía de Gestión Integral de Riesgos en los procesos de contratación pública* de la DGCP.

8) Empresa vinculada: Empresa subsidiaria, afiliada y/o controlante. Se considera que una empresa es subsidiaria a otra cuando esta última controla a aquella, y es afiliada con respecto a otra u otras, cuando todas se encuentran bajo un control común.

9) Gestión de Riesgos[19]: Es un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance de los objetivos de la organización.

10) Informe pericial: Documento elaborado por una persona o grupo de personas en su calidad de peritos que contiene los resultados de sus indagaciones, evaluaciones, sus conclusiones y recomendaciones que servirá de sustento para deliberación y posterior decisión del órgano responsable de un proceso de contratación.

11) Oferente/proponente habilitado: Aquel que participa en el proceso de selección y resulta habilitado en la fase de Evaluación Técnica del Proceso.

12) Riesgo[20]: Efecto de la incertidumbre sobre los objetivos. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

13) Servicios[21]: La prestación de actividades o serie de actividades cuyo objeto implica el desarrollo de prestaciones identificables para satisfacer necesidades de los entes y órganos relacionados con el normal cumplimiento de su función administrativa vinculada al interés general o como solución de problemas y necesidades de la institución contratante.

14) Especificaciones técnicas: [22]Son aquellas que describen los bienes y las obras a contratar atendiendo estrictamente a lo requerido por la institución contratante para satisfacer una necesidad, con fundamento en estudios previos realizados, sin incluir características que tiendan a favorecer a una marca o a un tipo de oferente en particular, buscando generar la más amplia competencia posible entre oferentes de diversas marcas y productos que puedan satisfacerla.

3. Objetivo y alcance del pliego

El presente pliego establece un conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras, que deseen participar en el procedimiento, de Licitación Pública Nacional, para la ADQUISICIÓN Y RENOVACIÓN DE LICENCIAS INFORMÁTICAS PARA USO DE LA SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES convocado por la Superintendencia de Salud y Riesgos Laborales con el número de Referencia: SISALRIL-CCC-LPN-2025-0007, así como el debido proceso que será llevado a cabo para la recepción, evaluación y determinación de la oferta más conveniente para fines de adjudicación y suscripción del contrato.

El pliego de condiciones se encuentra organizado en función de las instrucciones que debe suministrarse a los(as) oferentes para que puedan elaborar sus ofertas, conozcan cómo serán evaluados y las características y condiciones del contrato a suscribir.

[19] Definición extraída de la *Guía de Gestión Integral de Riesgos en los procesos de contratación pública* de la DGCP.
[20] Definición extraída de la *Guía de Gestión Integral de Riesgos en los procesos de contratación pública* de la DGCP.
[21] Artículo 4, numeral 7 del Decreto Núm. 416-23.
[22] Numeral 5, artículo 4 del Reglamento de Aplicación 416-23

4. Órgano y personas responsables del procedimiento de selección

Para la **ADQUISICIÓN Y RENOVACIÓN DE LICENCIAS INFORMÁTICAS PARA USO DE LA SUPERINTENDENCIA DE SALUD Y RIESGOS LABORALES** marcado con el número de referencia: **SISALRIL-CCC-LPN-2025-0007** el órgano responsable de la organización, conducción y ejecución es el CCC, que debe ser conformado dentro de la institución, de acuerdo con lo previsto en el artículo 9 del Reglamento Aplicación 416-23.

El CCC considerando los criterios de competencia, experiencia en el área y conocimiento del mercado, bajo los lineamientos del instructivo para la selección de peritos emitido por la Dirección General de Contrataciones Públicas[23]. Los peritos designados no podrán tener conflicto de interés potencial ni real con los oferentes ni con el objeto de la contratación.

Los peritos designados deberán suscribir, previo a evaluar las ofertas, una declaración de que no tienen conocimiento de ningún hecho que genere un conflicto de interés real, potencial o aparente conforme al Código de Pautas de Ética e Integridad del SNCCP.

Si se comprueba la existencia de un conflicto de interés la institución **Superintendencia de Salud y Riesgos Laborales** podrá determinar si el conflicto no puede evitarse, neutralizarse, mitigarse o resolverse de otro modo, en cuyo caso el perito designado mediante acto motivado deberá ser sustituido y notificarse a los proponentes mediante circular del CCC mediante el SECP.

Todas las comunicaciones y solicitudes que realicen los (las) oferentes serán dirigidas al Comité de Compras y Contrataciones como órgano deliberativo y decisorio de la compra o contratación de que se trate.

5. Marco normativo aplicable

En este procedimiento de selección, el contrato y su posterior ejecución, para la aplicación de la normativa vigente en contrataciones públicas, su interpretación o resolución de controversias e investigaciones, se aplicará el siguiente orden de prelación:

1) Constitución de la República Dominicana, proclamada el 27 de octubre del 2024.

2) Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana (DR-CAFTA).

3) Ley núm. 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras y sus modificaciones, del 18 de agosto de 2006.

4) Ley núm. 107-13 sobre los derechos de las personas en sus relaciones con la Administración y de Procedimiento Administrativo de fecha 08 de agosto de 2013.

5) Reglamento de Aplicación de la Ley núm. 340-06, aprobado mediante Decreto núm. 416-23 del 14 de septiembre de 2023;

6) Pliego de condiciones específicas, especificaciones técnicas, términos de referencia, fichas técnicas, anexos, enmiendas y circulares;

[23] Consultar instructivo emitido por la Dirección General de Contrataciones Públicas vigente, disponible en el enlace: https://www.dgcp.gob.do, sección "Sobre Nosotros", apartado "Marco Legal", "Instructivos".

7) Las ofertas y las muestras que se hubieren acompañado (Si aplica);

8) La Adjudicación;

9) El contrato (si aplica) y;

10) La orden de compra.

De igual modo, les serán aplicables todas las normas, resoluciones, circulares, instructivos, guías u orientaciones emitidas por esta Dirección General, según corresponda.

6. Interpretaciones

Para la interpretación del presente pliego y sus anexos, se siguen las siguientes reglas:

1) Cuando los términos están definidos en la normativa vigente o en el contrato, se interpretará en su sentido literal.

2) Las palabras o designaciones en singular deben entenderse igualmente al plural y viceversa, cuando la interpretación de los textos escritos lo requiera.

3) El término "por escrito" significa una comunicación escrita con prueba de recepción, acuse de recibido o realizada a través de la plataforma SECP.

4) Toda indicación a capítulo, numeral, inciso, circular, enmienda, formulario o anexo se entiende referida a la expresión correspondiente de este pliego, salvo indicación expresa en contrario. Los títulos de capítulos, formularios y anexos son utilizados exclusivamente a efectos indicativos y no afectarán su interpretación.

5) Las referencias a días se entenderán como días hábiles, excluyéndose del cómputo los sábados, domingos y feriados, de acuerdo con lo establecido en el párrafo I del artículo 20 de la Ley núm. 107-13 sobre los derechos de las personas en sus relaciones con la Administración y de procedimientos administrativos, salvo que expresamente se utilice la expresión de "días calendario", en cuyo caso serán días calendario.

7. Idioma

El idioma oficial del presente procedimiento es el castellano o español, por tanto, toda la correspondencia y documentos generados durante el procedimiento que intercambien el (la) interesado u oferente y el CCC deberán ser presentados en este idioma.

En ese sentido, se aclara para el (la) oferente que los documentos que acompañan sus ofertas deben presentarse en idioma castellano o, en su defecto, acompañados de traducción efectuada por la autoridad competente, ya sea del país de procedencia o de la República Dominicana.

Cuando un(a) oferente no haya presentado la información traducida al idioma castellano, deberá aportarla durante la fase de subsanación.

8. Disponibilidad y acceso al pliego de condiciones

El Pliego de Condiciones, así como los documentos que lo conforman (anexos, formularios, circulares, adendas/enmiendas, cronogramas de entrega, etc.) y el expediente electrónico, estarán disponibles para todas las personas interesadas, tanto en el SECP www.portaltransaccional.gob.do, como en la página web de la www.sisalril.gob.do a partir de la fecha de su convocatoria.

Constituye una obligación del(la) oferente consultar de manera permanente las precitadas direcciones electrónicas, sin perjuicio de acercarse a las instalaciones de la institución. No será admisible como excusa, el desconocimiento o desinformación por no consultar en tiempo oportuno.

9. Conocimiento y aceptación del Pliego de Condiciones

Será responsabilidad del(la) oferente conocer todas y cada una de las implicaciones para el ofrecimiento del objeto del presente proceso de contratación, y realizar todas las evaluaciones que sean necesarias para presentar su propuesta sobre la base de un examen cuidadoso de las características del negocio.

En caso de que los bienes a suministrar requieran de alguna instalación, los oferentes podrán realizar una visita técnica al lugar, de manera que obtengan por sí mismos y bajo su responsabilidad y riesgo, toda la información que pueda ser necesaria para preparar sus Ofertas. El hecho que los oferentes no se familiaricen debidamente con los detalles y condiciones bajo las cuales serán ejecutados los trabajos, no se considerará como argumento válido para posteriores reclamaciones **ni causa de descalificación en caso de que la institución contratante lo prevea en el cronograma de actividades**. El costo de esta visita será de exclusiva cuenta de los oferentes. La institución contratante suministrará, cuando sea necesario, los permisos pertinentes para efectuar las inspecciones correspondientes.

El solo hecho de un(a) oferente participar presentando oferta, implica pleno conocimiento, aceptación y sometimiento por sí mismo(a), por sus miembros, ejecutivos, y su representante legal, a los procedimientos, condiciones, estipulaciones y normativas, establecidos en el presente pliego de condiciones, el cual tiene carácter jurídicamente obligatorio y vinculante entre los(as) oferentes y la institución contratante.

Si el(la) oferente omite suministrar alguna parte de la información requerida 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 su descalificación o la nulidad del contrato si el caso lo amerita.

10. 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 8 de la Ley Núm. 340-06 y sus modificaciones.
2) No se encuentre afectado por el régimen de prohibiciones o inhabilidades indicado en el artículo 14 de la Ley Núm. 340-06 y sus modificaciones y;

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 II del artículo 5 de la Ley núm. 340-06 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.

11. Prácticas 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 11 sobre "Derecho a participar", así como las prácticas corruptas o fraudulentas[24], comprendidas en 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.

12. De los Comportamientos Violatorios, Contrarios y Restrictivos a la Competencia.

Los oferentes deberán respetar las disposiciones contenidas en la Ley núm. 42-08 promulgada en fecha 16 de enero de 2008 relativa a la Defensa a la Competencia, la cual tiene por objeto, con carácter de orden público, promover y defender la competencia efectiva para incrementar la eficiencia económica, así como las establecidas en el artículo 11 de la Ley núm. 340-06 sobre Compras y Contrataciones. Las violaciones a la Ley núm. 42-08 y al artículo 11 de la Ley núm. 340-06, darán lugar a:

A. La descalificación del oferente que lleve a cabo la conducta ya sea en condición de autor o cómplice de la misma.
B. El rechazo de la propuesta presentada por el oferente responsable de la conducta en cuestión ya sea en calidad de autor o cómplice, rechazo que podrá establecerse en cualquier etapa del procedimiento de selección o la contratación en sentido general.

[24] Artículo 11 de la Ley núm. 340-06 y sus modificaciones.

C. La rescisión del contrato por parte de la entidad contratante, más una acción en daños y perjuicios en contra del oferente por ante la jurisdicción competente.
D. La denuncia del ilícito a las autoridades de defensa a la competencia a los fines de lugar.

De manera no limitativa, se entenderán como comportamientos violatorios, contrarios y restrictivos a la competencia los siguientes:

A. Las prácticas concertadas y acuerdos anticompetitivos, conforme se establece en el artículo 5 de la Ley núm. 42-08.
B. Concertación o coordinación de las ofertas o la abstención en este proceso.
C. **La participación de empresas que posean accionistas en común, mismo domicilio en común y la misma unidad productiva, teléfonos, correos electrónicos, propuestas idénticas, errores o escrituras similares presentados por estas, entre otras.**
D. El abuso de posición dominante, conforme se establece en el artículo 6 de la Ley núm. 42-08.
E. La competencia desleal, conforme se establece en los artículos 10 y siguientes de la Ley núm. 42-08.
F. Los precios predatorios ofertados en cualquier procedimiento de selección o en una contratación bajo las excepciones de la Ley núm. 340-06 y su reglamento de aplicación, siendo los precios predatorios, aquellos establecidos de una manera excesivamente baja, más allá de los costos razonables del oferente y que sin lugar a duda tienen por finalidad expulsar a los competidores fuera del mercado, o crear barreras de entrada para los potenciales nuevos competidores.
G. Cualquier tipo de conducta anticompetitiva ejercida por los oferentes o por cualquier tercero, relacionada con el procedimiento de selección o una contratación bajo las excepciones de la Ley núm. 340-06.

En este sentido, la institución contratante se compromete dentro del marco del Programa de Cumplimiento Regulatorio en las Contrataciones Públicas (Si aplica), y, dando cumplimiento a las políticas emitidas por la DGCP, a realizar la Debida Diligencia, los fines de detectar los comportamientos violatorios a Ley núm. 340-06, así como la detección oportuna de los posibles conflictos de interés, y comportamientos contrarios y restrictivos a la libre competencia.

13. Consultas, solicitud de aclaraciones y enmiendas

Las consultas, aclaraciones y observaciones las formularán los(as) interesados(as), sus representantes legales, o agentes autorizados a través del SECP o en físico mediante comunicación escrita presentada en la institución contratante dirigida al CCC dependiendo la modalidad de contratación, dentro del plazo previsto en el cronograma de actividades.

Las respuestas (ya sean a través de una circular, enmienda/adenda) serán publicadas por la institución contratante en el SECP en el plazo previsto en el cronograma. Así como por correo electrónico u otros medios, a todos quienes hayan mostrado interés en participar.

Ninguna aclaración verbal por parte de la institución podrá afectar el alcance y condiciones del pliego y sus anexos. Para estos efectos, sólo se tendrán como válidas las circulares/ adendas/ enmiendas que sean publicadas el SECP dentro del plazo permitido por la Ley y conforme al cronograma de actividades.

14. Contratación Pública Responsable

En el(los) contrato(s) suscrito(s) derivado(s) del presente procedimiento de selección, la **Superintendencia de Salud y Riesgos Laborales** exigirá que el contratista ejecute el contrato público de manera responsable cumpliendo con sus obligaciones fiscales y de seguridad social, con el régimen de seguridad y protección a sus trabajadores establecidas en las normas vigentes, con la participación y la inclusión laboral de las personas con discapacidad en sus nóminas de trabajo en los términos y porcentajes requeridos por la Ley núm. 5-13, sobre discapacidad en la República Dominicana y cualquier otra normativa vinculada a la promoción y protección de los Derechos Humanos. Así como también se exigirá el cumplimiento de las normas prevención, protección y uso sostenible del medio ambiente.

En caso de incumplimiento o violación por parte del contratista de sus obligaciones de contratación responsable la **Superintendencia de Salud y Riesgos Laborales** otorgará un plazo razonable para que el Contratista implemente las medidas correctivas correspondientes. Vencido el plazo sin que se haya regularizado la actuación la Superintendencia de Salud y Riesgos Laborales) podrá declarar la resolución del contrato y el(la) contratista podrá ser pasible de las demás sanciones previstas en el artículo 66 de la Ley núm. 340-06 y sus modificaciones, sin perjuicio de las acciones penales o civiles que correspondan.

15. Firma digital

En consonancia con las disposiciones del artículo 19 de la Ley núm. 340-06, párrafo II del artículo 13 del Reglamento núm. 416-23, la Ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, la Resolución núm. 206-2022, la Circular núm. 012415 del Ministerio de Administración Pública (MAP), la Circular núm. DGCP44-PNP-2022-0006 sobre implementación de la firma digital, y la Resolución núm. IN-CGR-2023-007173 que establece las Directrices sobre los documentos firmados digitalmente a ser admitidos en el proceso de registro de contratos por ante la Contraloría General de la República (CGR), todos los documentos que componen el expediente administrativo de la contratación podrán ser firmados digitalmente, incluidas las ofertas y la suscripción de los contratos.

16. Reclamaciones, impugnaciones, controversias y competencia para decidirlas

Los(as) interesados(as) y oferentes tendrán derecho a presentar recursos administrativos como son los recursos de impugnación ante la institución contratante o recursos jerárquicos y solicitudes de investigación ante la DGCP, según corresponda, y en los términos o condiciones previstos en los artículos 67 y 72 en la Ley núm. 340-06 y sus modificaciones.

A tales fines, los(as) interesados(as) podrán consultar los requisitos, condiciones y plazos para formalizar sus reclamos, así como las acciones disponibles, incluso para cuando la institución hace silencio administrativo y no responde en tiempo oportuno, accediendo a las "*Guías para presentar Recursos, Denuncias y Solicitudes de Inhabilitación"* disponibles en el portal institucional de la DGCP, en el apartado "Marco Legal" en el siguiente enlace *https://www.dgcp.gob.do/sobre-nosotros/marco-legal/guias-del-sistema-nacional-de-compras-y-contrataciones-publicas-snccp/.*

Los recursos administrativos son optativos, por lo que en cualquier caso el interesado u oferente podrá presentar reclamación ante la jurisdicción judicial.

Para los conflictos y controversias que susciten en la fase de ejecución contractual, entre la institución y el (la) contratista, la competencia está reservada para el Tribunal Superior

Administrativo, en virtud del artículo 3 de la Ley 1494 de 1947 y cuando se trate de municipios, con excepción del Distrito Nacional y la provincia de Santo Domingo, se interpondrá un recurso contencioso administrativo municipal por ante el juzgado de primera instancia en atribuciones civiles del municipio.

El plazo para los(as) interesados(as) impugnar el pliego de condiciones es de 10 días hábiles a partir de la convocatoria del procedimiento en el SECP; mientras que para los oferentes presentar las acciones descritas será a partir de las notificaciones de los informes de evaluación de ofertas correspondiente, así como de la adjudicación.

17. Anexos documentos estandarizados

El(la) oferente presentará sus ofertas a través de los formularios y documentos estándar determinados en el presente pliego, los cuales se anexan como parte integral del mismo, a los fines de facilitar la evaluación de las ofertas por parte de los(as) peritos designados(as).

Se aclara que, en el evento de que un(a) oferente no presente su oferta en alguno de estos documentos estandarizados, esto no será motivo de rechazo de su oferta, ni será obstáculo para que los peritos la evalúen. A continuación, se mencionan los documentos de este procedimiento:

1. Formulario de presentación de oferta técnica **(SNCC.F.034)**
2. Formulario de presentación de oferta económica **(SNCC.F.033)**
3. Formulario información del oferente **(SNCC.F.042)**
4. Modelo de Contrato de Suministro de Bienes **(SNCC.C.023)**
5. Compromiso ético para oferentes del Estado.
6. Formulario de debida diligencia. (anexo)