INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL) COMITÉ DE COMPRAS Y

CONTRATACIONESCIRCULAR

MODIFICATORIA NÚM. 2

QUE ENMIENDA EL PLIEGO DE CONDICIONES ESPECÍFICAS DEL PROCESO DE LICITACIÓN PÚBLICA NACIONAL, ADQUISICIÓN EIMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE INFORMACIÓN Y EVENTOS (SIEM)

El Comité de Compras y Contrataciones del Instituto Dominicano de las Telecomunicaciones (**INDOTEL**) les informa que, en virtud de lo dispuesto en el artículo 81 del Reglamento de aplicación de la Ley Num. 340-06 sobre Compras y Contratacionesde Bienes, Servicios, Obras y Concesiones con modificaciones de Ley No. 449-06, ha decidido realizar una (1) enmienda al Pliego de Condiciones Específicas de la presente contratación, a saber:

2.7 Descripción de los Bienes y/o Especificaciones Técnicas

Adquisición e Implementación de un Gestor de Seguridad de Información y Eventos (SIEM), para las estaciones de trabajo del Instituto Dominicano de las Telecomunicaciones.

ESPECIFICACIONES TÉCNICAS

Objetivo General de la Contratación

Adquisición e implementación de un Gestor de Seguridad de Información y Eventos (SIEM), para la protección de la infraestructura TI y la seguridad de la información del INDOTEL frente a las amenazas presentes en el ciberespacio.

Objetivos Específicos de la Contratación

El Proyecto tiene que cumplir con las siguientes especificaciones, las cuales son:

1. Implementación e integración con la red del INDOTEL.
2. Integración con Sophos Central
3. Solución Cloud, 35 GB de almacenamiento diario
4. Integración Microsoft 365
5. Asesoría para implementación de controles y casos de usos.
6. Soporte 24/7 por el proveedor.
7. Capacitación full de administración para 4 colaboradores. (No se aceptarán transferencia de conocimiento)

Alcance Operativo de la Contratación.

Esta contratación abarca la adquisición de una solución de Gestión de Seguridad de Información y Eventos (SIEM) llave en mano, licenciamiento y soporte 24/7. Las empresas deben presentar

los **SLAs** (Acuerdos Niveles de Servicios) según la prioridad de los incidentes y solicitudes.

NO.	REQUERIMIENTOS
	PLATAFORMA SIEM INTEGRADA
1	Arquitectura de la solución debe ser vendor flexible con capacidad de ingestar fuentes multi-nube, hibrido y local.
2	La solución debe permitir la ingesta de datos sin la necesidad de conectores de clientes o soporte de proveedores.
3	La solución debe tener capacidad de modelos de aprendizajes automáticos usando Machine Learning.
4	La solución debe permitir fácil integración con Sophos Central.
5	La solución debe abordar la gestión de registros y la generación de informes la cual incluya investigaciones de incidentes, análisis forense, capacidad para correlacionar cualquier dato de la máquina, perfil de comportamiento y detección de anomalías, monitoreo de aplicaciones, integración con soluciones de automatización.
6	La solución debe tener la capacidad de integración con soluciones de UBA.
7	La solución debe ser un producto único e integrado para casos de uso de registro y SIEM.
8	La solución debe poseer una arquitectura altamente escalable y que pueda indexar grandes cantidades de datos por día.
9	La solución debe tener la capacidad de indexar todos los datos originales sin modificar y hacer que se puedan buscar sin normalización o reducción de datos.
10	La solución debe ofrecer múltiples opciones para el almacenamiento a largo plazo.
11	La solución debe ser una opción de nube totalmente administrada.
12	El proveedor de la nube de cumplir con certificaciones SOC 2 Type II y ISO 27001.
13	La solución debe incluir búsquedas de correlación predefinidas, informes, paneles y visualizaciones para respaldar los casos de uso de seguridad.
14	La solución debe proporcionar contenido para ayudar en la corrección y educación del panorama de amenazas, y este contenido debe actualizarse regularmente.
15	La solución debe asignar el contenido disponible a mandatos de cumplimiento comunes, marcos de detección o modelos adversarios como CIS20, NIST 800-53, NERC-CIP, PCI, Mitre ATT & CK, Cyber Kill Chain y otros.

16	La solución debe respaldar la capacidad de los equipos de seguridad para investigar de manera colaborativa incidentes, problemas y brechas de seguridad.
17	La solución debe cumplir con los requisitos reglamentarios en torno a la administración, retención, revisión y monitoreo continuo de registros.
18	La solución debe admitir la creación de cuadros de mando e informes para medir el cumplimiento de algún control técnico rastreable en los datos de la máquina.
19	La solución debe poder generar hashes criptográficos para los datos ingeridos para demostrar que no se ha producido ninguna manipulación después de la ingesta.
20	La solución debe proporcionar cifrado de datos de eventos antes de la ingesta.
21	La solución debe admitir diversas fuentes de datos de forma inmediata.
22	La solución debe admitir de forma nativa la recopilación de todos los tipos de fuentes de datos multi-nube. Proveedores de nube comunes, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).
23	La solución debe tener la capacidad de indexar todos los datos originales no modificados y hacerlos disponibles tanto para búsquedas como para informes.
24	La solución debe ofrecer una tecnología de agente ligera y segura para recopilar datos de hosts * NIX, MacOS o Windows.
25	La solución debe poder configurarse para capturar datos detallados de terminales para detectar ejecuciones de procesos comunes y poco comunes.
26	La solución debe admitir tipos comunes de ingestión de datos por cable, como Netflow, IPFIX, Bro y Cisco NVM, ya sea de forma nativa desde fuentes o desde taps como Gigamon.
27	La solución debe tener la capacidad de conectarse directamente a cualquier tabla (s) de base de datos SQL y extraer el contenido para indexarlo.
28	La solución debe tener la capacidad de consultar cualquier base de datos SQL y traer los resultados para verlos ad-hoc.
29	La solución debe tener la capacidad de realizar búsquedas de texto completo en cualquier campo de los datos indexados basándose en palabras clave, rangos de tiempo, lógica booleana, expresiones regulares, sintaxis de comodines y análisis estadístico.
30	La solución debe tener la capacidad de realizar líneas de base y luego aplicar la lógica de búsqueda para encontrar valores atípicos / anomalías desde la línea de base que pueden ser amenazas avanzadas no basadas en firmas.
31	La solución debe tener la capacidad de ejecutar múltiples búsquedas simultáneas.

32	La solución debe poder extraer nuevos campos de cualquier fuente de datos sobre la marcha, sin tener que volver a ingerir los datos.
33	La solución debe permitir crear comandos personalizados para buscar en sus datos de nuevas formas.
34	La solución debe utilizar varias técnicas para acelerar la devolución de datos a los analistas.
35	La solución debe permitir crear fácilmente visualizaciones personalizadas y actualizar esas visualizaciones en tiempo real.
36	La solución debe incluir una interfaz de usuario de arrastrar y soltar para permitir a los usuarios no técnicos crear informes complejos sin tener que usar comandos de búsqueda o comprender el formato de los datos sin procesar subyacentes.
37	La solución debe proporcionar una interfaz compatible con dispositivos móviles.
38	La solución debe ser compatible con el control de acceso basado en roles (RBAC) flexible para el acceso controlado de usuarios y API. Debe poder restringir el acceso a fuentes de datos, tipos de datos, períodos de tiempo, vistas específicas, informes o paneles de control específicos.
39	La solución debe admitir la integración de autenticación y autorización con Active Directory, eDirectory y otras implementaciones compatibles con LDAP.
40	La solución debe integrarse con las soluciones empresariales de inicio de sesión único para permitir la autenticación de paso a través de credenciales de terceros.
41	La solución debe permitir la indexación remota de datos en tiempo real para minimizar la oportunidad de alteración de pistas de auditoría en hosts comprometidos.
42	La solución debe proporcionar acceso seguro al flujo de datos y funcionalidad distribuida a través de SSL / TCP.
43	La solución debe admitir eventos de signos de bloqueo con una firma digital para demostrar la integridad de los datos indexados.
44	La solución debe monitorear sus propias configuraciones y uso para mantener una pista de auditoría completa y firmada digitalmente de quién está accediendo al sistema, qué búsquedas están ejecutando, qué informes están viendo y qué cambios de configuración están haciendo.
45	La solución debe ofrecer una API REST para exponer todos los datos indexados, los comandos de búsqueda y la funcionalidad a sistemas, aplicaciones y paneles externos.
46	La solución debe tener varios SDK escritos en la parte superior de la API. De ser así, se deben especificar los nombres de los SDK.

47	La solución debe incluir aplicaciones públicas y gratuitas para productos puntuales o casos de uso para crear más valor.
48	La solución debe permitir que las configuraciones del sistema se configuren a través de la interfaz de usuario, la CLI o los archivos del sistema de archivos para permitir cambios granulares y personalización.
49	La solución debe permitir que los informes y paneles se editen a través de la interfaz de usuario o archivos XML subyacentes.
50	La solución debe permitir que los datos se reenvíen fácilmente a sistemas externos o herramientas de registro.
51	La solución debe admitir algún método seguro basado en estándares (p. Ej., HTTPS) de ingesta de datos de aplicaciones personalizadas.
52	La solución debe proporcionar actualizaciones públicas periódicas sobre nuevas técnicas de seguridad que se deben lograr con su sistema.
53	La solución debe tener la capacidad de minimizar o consolidar la cantidad de conexiones hacia la nube entorno a controlar el tráfico en el ancho de banda.
54	El proveedor debe ser un partner autorizado de la solución a ofertada.
55	El proveedor deberá tener la capacidad de realizar la implementación de la solución.
56	El proveedor debe realizar la integración con nuestras diferentes fuentes de datos.
57	El proveedor debe realizar la integración de los componentes necesarios para la colección eventos de nuestros fuentes con la nube.
58	El proveedor deberá implementar paneles de Postura de Seguridad, los cuales indiquen: • Alertas de intrusión por gravedad clasificada • Alertas de intrusión por gravedad • Alertas de intrusión • Alertas con vistas de 24 horas de Las 10 principales alertas de intrusión de gravedad indicando su nivel de gravedad.

59	El proveedor deberá implementar paneles de monitoreo continuo de: • Cambios de Windows para ver eventos en Windows. • Tablero de todas las autenticaciones para ver todas las acciones de autenticación. • Panel de malware para ver soluciones antivirus • Panel de control de detección de intrusos (IDS/IPS) para ver los sistemas de prevención y detección de intrusos. • Tablero de firewalls para ver eventos de firewall. • Tablero de tráfico de red para ver los datos del firewall en su red. • Tablero de acceso VPN para ver los datos de la sesión VPN. • Cuentas bloqueadas • Escaladas de privilegios • Cambiar métricas • Métricas de autenticación
60	El proveedor deberá implementar paneles para amenazas avanzadas que incluyan los siguientes parámetros: • Panel de Anomalías para identificar riesgos de seguridad • Paneles de anomalías de red para identificar anomalías de red • Panales de casos de uso personalizado para incorporar búsquedas y tableros personalizados
61	El proveedor deberá implementar paneles Investigar las actividades de comportamiento del usuario tales como: • Información del usuario. • Acceso de usuarios por fuente. • Acceso en el tiempo por acción. • Acceso por fuente. • Mapa de autenticación que muestra hasta 250. Destinos de autenticación. • Los 100 eventos más recientes. Comportamiento para investigar la actividad del host utilizando la siguiente información: • Comunicaciones de red • Mapa de comunicaciones de la red • Autenticaciones y cambios • Malware e intrusión
62	El proveedor deberá implementar paneles e informes. Ejemplos • Administración activamente el ciclo de vida de las cuentas de aplicaciones y sistemas, incluida su creación, uso, inactividad y eliminación, para minimizar las oportunidades para los atacantes. • Detección, prevención y corrección de flujo de información de seguridad en redes de diferentes niveles de confianza • Controle la instalación, propagación e implementación de código malicioso en varios puntos de la plataforma. • Optimización y automatización de actualizaciones de contra medidas y las acciones correctivas

63	El proveedor deberá implementar vistas ejecutivas que incluya paneles, que muestre la siguiente información para informar sobre el estado del entorno a: • Ataques detenidos • Malware bloqueado • Usuarios protegidos • Dispositivos protegidos • Tendencias de usuario • Orígenes del ataque
64	Proveedor deberá entregar la arquitectura propuesta para la solución.
65	El proveedor deberá entregar un cronograma de la implementación

- Se modifica el numeral 2.7, Descripción de los Bienes y/o Especificaciones Técnicas para que en lo adelante indique lo siguiente:

2.7 Descripción de los Bienes y/o Especificaciones Técnicas

Adquisición e Implementación de un Gestor de Seguridad de Información y Eventos (SIEM),para las estaciones de trabajo del Instituto Dominicano de las Telecomunicaciones.

ESPECIFICACIONES TÉCNICAS

Objetivo General de la Contratación

Adquisición e implementación de un Gestor de Seguridad de Información y Eventos (SIEM), para la protección de la infraestructura TI y la seguridad de la información del INDOTEL frente a las amenazas presentes en el ciberespacio.

Objetivos Específicos de la Contratación

El Proyecto tiene que cumplir con las siguientes especificaciones, las cuales son:

1. Implementación, alta disponibilidad e integración con la red del INDOTEL.
2. Integración con Sophos Central
3. Solución Cloud, 35 GB mínimo de almacenamiento diario
4. Integración Microsoft 365 Standard y E3.
5. Asesoría para implementación de controles y casos de usos.
6. Soporte 24/7 por el proveedor.
7. Capacitación full de administración para 04 colaboradores. (No se aceptarán transferencia de conocimiento)

Alcance Operativo de la Contratación.

Esta contratación abarca la adquisición de una solución de Gestión de Seguridad de Información y Eventos (SIEM) llave en mano, licenciamiento y soporte 24/7 por un año a partir de la entrega de la

plataforma web. Las empresas deben presentar los **SLAs** (Acuerdos Niveles de Servicios) según la prioridad de los incidentes y solicitudes.

NO.	REQUERIMIENTOS
	PLATAFORMA SIEM INTEGRADA
1	Arquitectura de la solución debe ser vendor flexible con capacidad de ingestar fuentes multi-nube, hibrido y local, tomando en cuenta que no contamos con un gestor de SIEM.
2	La solución debe permitir la ingesta de datos sin la necesidad de conectores de clientes o soporte de proveedores.
3	La solución debe tener capacidad de modelos de aprendizajes automáticos usando Machine Learning.
4	La solución debe permitir fácil integración con Sophos Central XG430 SFOS 19.5.3 MR-3-Build652
5	La solución debe abordar la gestión de registros y la generación de informes la cual incluya investigaciones de incidentes, análisis forense, capacidad para correlacionar cualquier dato de la máquina, perfil de comportamiento y detección de anomalías, monitoreo de aplicaciones, integración con soluciones de automatización.
6	La solución debe tener la capacidad de integración con soluciones de Análisis del comportamiento del usuario (UBA, user behavior analytics).
7	La solución debe ser un producto único e integrado para casos de uso de registro y SIEM, actualmente, No disponemos de un gestor SIEM.
8	La solución debe poseer una arquitectura altamente escalable y que pueda indexar grandes cantidades de datos por día, conun máximo de 11,084 (Eventos Por Segundos, EPS).
9	La solución debe tener la capacidad de indexar todos los datos originales sin modificar y hacer que se puedan buscar sin normalización o reducción de datos.
10	La solución debe ofrecer múltiples opciones para el almacenamiento a largo plazo, como máximo de retención por día de 89 GB.
11	La solución debe ser una opción de nube totalmente administrada.
12	El proveedor de la nube de cumplir con certificaciones SOC 2 Tipo II y ISO 27001.
13	La solución debe incluir búsquedas de correlación predefinidas, informes, paneles y visualizaciones para respaldar los casos de uso de seguridad.
14	La solución debe proporcionar contenido para ayudar en la corrección y educación del panorama de amenazas, y este contenido debe actualizarse regularmente.

<table>
<tr><td>15</td><td>La solución debe asignar el contenido disponible a mandatos de cumplimiento comunes, marcos de detección o modelos adversarios como CIS20, NIST 800-53, NERC-CIP, PCI, Mitre ATT & CK, Cyber Kill Chain y otros.</td></tr>
<tr><td>16</td><td>La solución debe respaldar la capacidad de los equipos de seguridad para investigar de manera colaborativa incidentes, problemas y brechas de seguridad.</td></tr>
<tr><td>17</td><td>La solución debe cumplir con los requisitos reglamentarios en torno a la administración, retención por día de 89 GB como máximo, revisión y monitoreo continuo de registros.</td></tr>
<tr><td>18</td><td>La solución debe admitir la creación de cuadros de mando e informes para medir el cumplimiento de algún control técnico rastreable en los datos de la máquina.</td></tr>
<tr><td>19</td><td>La solución debe poder generar hashes criptográficos para los datos ingeridos para demostrar que no se ha producido ninguna manipulación después de la ingesta.</td></tr>
<tr><td>20</td><td>La solución debe proporcionar cifrado de datos de eventos antes de la ingesta.</td></tr>
<tr><td>21</td><td>La solución debe admitir diversas fuentes de datos de forma inmediata.</td></tr>
<tr><td>22</td><td>La solución debe admitir de forma nativa la recopilación de todos los tipos de fuentes de datos multi-nube y Proveedores de nube comunes. El Indotel Cuenta con la suscripción de Microsoft azure.</td></tr>
<tr><td>23</td><td>La solución debe tener la capacidad de indexar todos los datos originales no modificados y hacerlos disponibles tanto para búsquedas como para informes.</td></tr>
<tr><td>24</td><td>La solución debe ofrecer una tecnología de agente ligera y segura para recopilar datos de hosts NIX, MacOS o Windows para un total de 626 dispositivos incluyendo los siguientes servicios:
<table>
<tr><th>Cant.</th><th>Equipo</th><th>Marca</th><th>Modelo</th><th>Firmware / Sistema Operativo</th></tr>
<tr><td>16</td><td>SERVIDORES</td><td>VM</td><td>On Premise</td><td>WINDOWS SERVER 2019</td></tr>
<tr><td>12</td><td>SERVIDORES</td><td>VM</td><td>On Premise</td><td>LINUX UBUNTU SEVER 22.04</td></tr>
<tr><td>2</td><td>SERVIDORES</td><td>VM</td><td>AZURE</td><td>WINDOWS SERVER 2019</td></tr>
<tr><td>5</td><td>SERVIDORES</td><td>VM</td><td>AZURE</td><td>LINUX UBUNTU SEVER 22.04</td></tr>
<tr><td>1</td><td>FIREWALL</td><td>FORTINET</td><td>FORTIGATE 400F</td><td>v7.0.7 build4701</td></tr>
<tr><td>1</td><td>FIREWALL</td><td>FORTINET</td><td>FORTIGATE 100F</td><td>v6.4.14 build2093 (GA)</td></tr>
</table>
</td></tr>
</table>

	1	FIREWALL	FORTINET	FORTIGATE 60F	v6.4.6 build6083 (GA)
	1	FIREWALL	FORTINET	FORTIGATE 100E	v6.4.14 build2093 (GA)
	2	FIREWALL	SOPHOS	XG430	SFOS 19.5.3 MR-3-Build652
	2	FIREWALL	FORTINET	FORTIGATE 60D	v5.4.1,build5447 (GA)
	1	FIREWALL	FORTINET	FORTIGATE 30E	v5.4.1,build5447 (GA)
	8	FIREWALL	FORTINET	FORTIGATE 30D	v5.2.3,build670
	12	SWITCH	CISCO	C9200L-24P-4X	versión 17.03.05
	8	SWITCH	CISCO	C9200L-48P-4X	versión 17.06.03
	4	SWITCH	CISCO	WS-C2960X-48FPD-L	V3 15.2(4)E /V4 15.2(2)E7
	6	SWITCH	CISCO	WS-C3560-48PS	V7 12.2(50) SE1

25	La solución debe poder configurarse para capturar datos detallados de terminales para detectar ejecuciones de procesos comunes y poco comunes.
26	La solución debe admitir tipos comunes de ingestión de datos por cable, como Netflow, IPFIX, Bro y Cisco NVM, ya sea de forma nativa desde fuentes o desde taps como Gigamon.
27	La solución debe tener la capacidad de conectarse directamente a cualquier tabla (s) de base de datos SQL y extraer el contenido para indexarlo.
28	La solución debe tener la capacidad de consultar cualquier base de datos SQL y traer los resultados para verlos ad-hoc.
29	La solución debe tener la capacidad de realizar búsquedas de texto completo en cualquier campo de los datos indexados basándose en palabras clave, rangos de tiempo, lógica booleana, expresiones regulares, sintaxis de comodines y análisis estadístico.
30	La solución debe tener la capacidad de realizar líneas de base y luego aplicar la lógica de búsqueda para encontrar valores atípicos / anomalías desde la línea de base que pueden ser amenazas avanzadas no basadas en firmas.
31	La solución debe tener la capacidad de ejecutar múltiples búsquedas simultáneas.
32	La solución debe poder extraer nuevos campos de cualquier fuente de datos sobre la marcha, sin tener que volver a ingerir los datos.

33	La solución debe permitir crear comandos personalizados para buscar en sus datos de nuevas formas.
34	La solución debe utilizar varias técnicas para acelerar la devolución de datos a los analistas.
35	La solución debe permitir crear fácilmente visualizaciones personalizadas y actualizar esas visualizaciones en tiempo real.
36	La solución debe incluir una interfaz de usuario de arrastrar y soltar para permitir a los usuarios no técnicos crear informes complejos sin tener que usar comandos de búsqueda o comprender el formato de los datos sin procesar subyacentes.
37	La solución debe proporcionar una interfaz compatible con dispositivos móviles.
38	La solución debe ser compatible con el control de acceso basado en roles (RBAC) flexible para el acceso controlado de usuarios y API. Debe poder restringir el acceso a fuentes de datos, tipos de datos, períodos de tiempo, vistas específicas, informes o paneles de control específicos.
39	La solución debe admitir la integración de autenticación y autorización con Active Directory, eDirectory y otras implementaciones compatibles con LDAP.
40	La solución debe integrarse con las soluciones empresariales de inicio de sesión único para permitir la autenticación de paso a través de credenciales de terceros.
41	La solución debe permitir la indexación remota de datos en tiempo real para minimizar la oportunidad de alteración de pistas de auditoría en hosts comprometidos.
42	La solución debe proporcionar acceso seguro al flujo de datos y funcionalidad distribuida a través de SSL / TCP.
43	La solución debe admitir eventos de signos de bloqueo con una firma digital para demostrar la integridad de los datos indexados.
44	La solución debe monitorear sus propias configuraciones y uso para mantener una pista de auditoría completa y firmada digitalmente de quién está accediendo al sistema, qué búsquedas están ejecutando, qué informes están viendo y qué cambios de configuración están haciendo.
45	La solución debe ofrecer una API REST para exponer todos los datos indexados, los comandos de búsqueda y la funcionalidad a sistemas, aplicaciones y paneles externos.
46	La solución debe tener varios SDK escritos en la parte superior de la API. De ser así, se deben especificar los nombres de los SDK.
47	La solución debe incluir aplicaciones públicas y gratuitas para productos puntuales o casos de uso para crear más valor.

48	La solución debe permitir que las configuraciones del sistema se configuren a través de la interfaz de usuario, la CLI o los archivos del sistema de archivos para permitir cambios granulares y personalización.
49	La solución debe permitir que los informes y paneles se editen a través de la interfaz de usuario o archivos XML subyacentes.
50	La solución debe permitir que los datos se reenvíen fácilmente a sistemas externos o herramientas de registro.
51	La solución debe admitir algún método seguro basado en estándares (p. Ej., HTTPS) de ingesta de datos de aplicaciones personalizadas.
52	La solución debe proporcionar actualizaciones públicas periódicas sobre nuevas técnicas de seguridad que se deben lograr con su sistema.
53	La solución debe tener la capacidad de minimizar o consolidar la cantidad de conexiones hacia la nube entorno a controlar el tráfico en el ancho de banda.
54	El proveedor debe ser un partner autorizado de la solución a ofertada.
55	El proveedor deberá tener la capacidad de realizar la implementación de la solución.
56	El proveedor debe realizar la integración con nuestras diferentes fuentes de datos.
57	El proveedor debe realizar la integración de los componentes necesarios para la colección eventos de nuestros fuentes con la nube.
58	El proveedor deberá implementar paneles de Postura de Seguridad, los cuales indiquen: • Alertas de intrusión por gravedad clasificada • Alertas de intrusión por gravedad • Alertas de intrusión • Alertas con vistas de 24 horas de Las 10 principales alertas de intrusión de gravedad indicando su nivel de gravedad.

59	El proveedor deberá implementar paneles de monitoreo continuo de: • Cambios de Windows para ver eventos en Windows. • Tablero de todas las autenticaciones para ver todas las acciones de autenticación. • Panel de malware para ver soluciones antivirus • Panel de control de detección de intrusos (IDS/IPS) para ver los sistemas de prevención y detección de intrusos. • Tablero de firewalls para ver eventos de firewall. • Tablero de tráfico de red para ver los datos del firewall en su red. • Tablero de acceso VPN para ver los datos de la sesión VPN. • Cuentas bloqueadas • Escaladas de privilegios • Cambiar métricas • Métricas de autenticación
60	El proveedor deberá implementar paneles para amenazas avanzadas que incluyan los siguientes parámetros: • Panel de Anomalías para identificar riesgos de seguridad • Paneles de anomalías de red para identificar anomalías de red • Panales de casos de uso personalizado para incorporar búsquedas y tableros personalizados
61	El proveedor deberá implementar paneles Investigar las actividades de comportamiento del usuario tales como: • Información del usuario. • Acceso de usuarios por fuente. • Acceso en el tiempo por acción. • Acceso por fuente. • Mapa de autenticación que muestra hasta 250. Destinos de autenticación. • Los 100 eventos más recientes. Comportamiento para investigar la actividad del host utilizando la siguiente información: • Comunicaciones de red • Mapa de comunicaciones de la red • Autenticaciones y cambios • Malware e intrusión
62	El proveedor deberá implementar paneles e informes. Ejemplos • Administración activamente el ciclo de vida de las cuentas de aplicaciones y sistemas, incluida su creación, uso, inactividad y eliminación, para minimizar las oportunidades para los atacantes. • Detección, prevención y corrección de flujo de información de seguridad en redes de diferentes niveles de confianza • Controle la instalación, propagación e implementación de código malicioso en varios puntos de la plataforma. • Optimización y automatización de actualizaciones de contra medidas y las acciones correctivas

63	El proveedor deberá implementar vistas ejecutivas que incluya paneles, que muestre la siguiente información para informar sobre el estado del entorno a: • Ataques detenidos • Malware bloqueado • Usuarios protegidos • Dispositivos protegidos • Tendencias de usuario • Orígenes del ataque
64	Proveedor deberá entregar la arquitectura propuesta para la solución.
65	El proveedor deberá entregar un cronograma de la implementación

En virtud de lo anterior, se dispone la publicación de la presente circular en el sub-portalde Transparencia del **INDOTEL**, y el portal de transaccional de la Dirección General de Contrataciones Públicas.

Así ha sido aprobada, adoptada y firmada la presente circular, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, hoy día veintiuno (21) del mes de noviembre del año dos mil veintitrés (2023).

Firmados:

Nelson Arroyo
Presidente del Comité de
Compras y Contrataciones

Juan Feliz Moreta
Miembro del Comité de
Compras y Contrataciones

Yennifer de la Rosa
Miembro del Comité de
Compras y Contrataciones

Annia Pórtela
Miembro del Comité de
Compras y Contrataciones

Yanira Bueno
Miembro del Comité de
Compras y Contrataciones