Dirección Central de Policía de Turismo
Departamento de Compras

Santo Domingo; Distrito Nacional

FICHA TECNICA
Y/O TERMINOS DE REFERENCIA

SOLICITUD DE ADQUISICIÓN DE LICENCIA DE ANTIVIRUS.

POLITUR-DAF-CM-2022-0027

DESCRIPCIÓN DE LAS NECESIDADES DEL PROCESO:

Solución de Protección de Endpoint y servers con funcionalidad EDR			
LOTE ÚNICO			
Solución de Protección			
Partida	**Cantidad**	**Solicitud**	**Especificaciones Técnicas**
1	**300**	**Agentes de Antivirus con XDR usuarios**	La consola de administración deberá ser una sola consola, basada en web y en nube, que deberá soportar e incluir todos los componentes para la administración, monitoreo y control de la protección en estaciones de trabajo y servidores.
			La consola de administración deberá utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados
			La consola de administración web permitirá definir grupos de usuarios con distintos niveles de acceso a las configuración, políticas y registros.
			La consola de administración web deberá contener un Dashboard con el resumen del estado de protección en estaciones de trabajo, así como de servidores, también tendrá que indicar las alertas de eventos críticos, altos, medios e informativos.
			La consola de administración web debe realizar como mínimo el envío automático de alertas criticas mediante correo electrónico a los administradores.
			La consola de administración web deberá de mostrar información como nombre de la máquina, sistema operativo, dirección IP, versión del antivirus instalado, versión del motor, fecha de la actualización, fecha de la última verificación, evento reciente, estado, grupo, numero de virus detectados, etc.
			La consola de administración web debe permitir la organización en grupos de las estaciones de trabajo, así como de servidores dentro de la estructura de administración.
			La consola de administración web deberá tener la capacidad de aplicar políticas de protección diferentes por grupos de máquinas y equipos individuales.
			La consola de administración web deberá permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
			La consola de administración web tendrá un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.
			Desde la consola de administración web se podrá descargar el o los paquetes de instalación de la solución de antivirus end point, así como las descargas de actualización del producto y de las definiciones de virus y protección contra intrusos.
			La consola de administración web deberá realizar la actualización remota en tiempo real, de la solución y del mecanismo de verificación (Engine) de los clientes.
			La consola de administración web permitirá seleccionar un grupo de dispositivos para aplicar la actualización para controlar el ancho de banda de red.

			La consola de administración web deberá soportar la actualización de la versión de los end point, para que esta se realice de modo transparente para los usuarios finales.
			La comunicación del agente hacia la consola debe permitir controlar el uso de ancho de banda para la descarga de firmas.
			La consola de administración deberá tener la posibilidad de implementar servidores de actualización locales para utilizar de manera eficiente el uso del ancho de banda.
			La consola de administración web deberá tener la posibilidad de instalar un servidor local para reenvío de eventos (message relay) en caso de que el agente no pueda comunicarse con la consola en la nube.
			La consola de administración web deberá permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
			La consola de administración web podrá permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
			Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
			La consola de administración web deberá de permitir la exportación de los informes gerenciales a los formatos csv y pdf.
			La consola de administración deberá tener la capacidad de generar informes, estadísticas o gráficos, detallando la siguiente información: ➢ Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos. ➢ Detalle de los equipos de escritorio y servidores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los equipos. ➢ Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico. ➢ Detalle de las principales aplicaciones bloqueadas y los equipos, usuarios que intentaron acceder a ellas. ➢ Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los equipos, usuarios que las acceden. ➢ Detalle de los equipos y usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder. ➢ Detalle de todas las actividades disparadas por reglas de fuga de información.
			La consola de administración web deberá permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.

			La consola de administración web deberá tener de forma nativa los recursos de informes y monitoreo.
			La consola de administración web cuando identifique algún problema, deberá permitir corregir por vía remota, las siguientes acciones: ➢ Proteger el dispositivo con la opción de inicio de una exploración ➢ Forzar una actualización en ese momento ➢ Ver los detalles de los eventos ocurridos ➢ Ejecutar la comprobación completa del sistema ➢ Forzar el cumplimiento de una nueva política de seguridad ➢ Mover el dispositivo a otro grupo ➢ Borrar el dispositivo de la lista.
			La consola de administración web deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los equipos que necesitan atención.
			La consola de administra web deberá generar un registro de auditoría seguro que supervise la actividad en dicha consola para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses, etc
			El end point antivirus deberá proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Sistema Operativo Windows, Linux y Mac el agente también deberá detectar PUA, adware y comportamiento sospechoso
			El end point antivirus deberá de contener protección integrada, es decir, en un solo agente tendrá como mínimo: control de amenazas, control de dispositivos, control de aplicaciones, control web, prevención de fuga de información (DLP), gestión del firewall de Windows, protección contra virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).
			El end point antivirus deberá contar con detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
			El end point antivirus deberá poseer la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección. Así como deberá tener algún mecanismo contra la desinstalación del end point como por ejemplo una contraseña.
			El end point antivirus deberá permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.

			El end point antivirus deberá realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
			El end point antivirus deberá realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA);
			El end point antivirus deberá proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
			El end point antivirus deberá permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
			El end point antivirus debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
			El end point antivirus deberá ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
			El end point antivirus deberá permitir el monitoreo y el control de dispositivos extraíbles en los dispositivos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo. Como mínimo de los siguientes dispositivos: ➢ HD (hard disks) externos ➢ Pendrives USB ➢ Almacenables removibles seguras ➢ CD, DVD, Blu-ray, floppy drives. ➢ Interfaces de red inalámbrica ➢ Módems ➢ Bluetooth ➢ Infrarrojo ➢ MTP (Media Transfer Protocol) ➢ PTP (Picture Transfer Protocol) como cámaras digitales.
			El end point antivirus con el control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red
			El end point antivirus deberá tener la capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo
			El end point antivirus deberá actualizar de forma automática la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
			El end point antivirus deberá detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.

			El end point antivirus deberá contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados
			El end point antivirus deberá poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.
			El end point antivirus deberá permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido).
			El end point antivirus deberá permitir el bloqueo o sólo registrar el evento en la consola de administración web, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible.
			El end point antivirus deberá tener listas de CCL pre configuradas con al menos los siguientes identificadores.(DLP) • Números de tarjetas de crédito. • Números de cuentas bancarias. • Números de pasaportes. • Direcciones • Números de teléfono. • Lista de correos electrónicos. • Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.
			El end point antivirus deberá incluir el control web para permitir controlar el acceso a sitios inapropiados, con al menos 12 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
			El end point deberá de contar con la capacidad de monitorear los cambios como creaciones o modificaciones sobre carpetas y archivos críticos del sistema basados en una lista pre definida y poder personalizar dicha lista para sistemas operativos Windows server 2012 o superior debido a la criticidad de la información que manejan.
			El endpoint podrá generar una lista blanca de aplicaciones que se ejecuten en el sistema operativo Windows server 2012 o superior para que esas aplicaciones sean las únicas que se puedan ejecutar
			El end point antivirus deberá contener la funcionalidad de protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
			El end point antivirus deberá contener la funcionalidad de detección de amenazas desconocidas que están en memoria.
			El end point antivirus deberá contener la funcionalidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.

			El end point antivirus deberá contener la funcionalidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
			El end point antivirus no deberá de requerir descarga de firmas de ningún tipo.
			El end point antivirus deberá contener la funcionalidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
			El end point antivirus deberá contener la funcionalidad de análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
			El end point antivirus deberá contener la funcionalidad de bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
			El end point antivirus deberá contener la funcionalidad de poder generar excepciones ante falsos positivos
			El end point antivirus deberá contener la capacidad de protección contra ransomware basada en comportamiento.
			El end point antivirus deberá contener la capacidad de remediación de la acción de encriptación de los ransomware.
			El end point antivirus deberá contener la detección del cifrado malicioso de forma local o remoto.
			El end point antivirus deberá contener la protección antiransomware para el sector de booteo (master boot record).
			El end point antivirus deberá contener la capacidad de restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
			El end point antivirus deberá informar a La consola de administración web todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red.
			El end point antivirus deberá tener la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
			El end point antivirus deberá contar como mínimo con la detección y protección de las siguientes técnicas de explotación: • Enforce Data Execution Prevention; • Mandatory Address Space Layout Randomization; • Bottom-up ASLR; • Null Page (Null Deference Protection); • Heap Spray Allocation; • Dynamic Heap Spray; • Stack Pivot; • Stack Exec (MemProt); • Stack-based ROP Mitigations (Caller); • Branch-based ROP Mitigations (Hardware

			Assisted); • Structured Exception Handler Overwrite (SEHOP); • Import Address Table Filtering (IAF); • Load Library; • Reflective DLL Injection; • Shellcode; • VBScript God Mode; • Wow64; • Syscall; • Hollow Process; • DLL Hijacking; • Squiblydoo Applocker Bypass; • APC Protection (Double Pulsar / AtomBombing); • Process Privilege Escalation
			El end point antivirus deberá contar con mitigación de inyección de códigos en procesos.
			El end point antivirus deberá contar con protección contra robo de credenciales
			El end point antivirus deberá contar con protección contra malware escondido en aplicaciones legitimas (code cave).
			El end point antivirus deberá evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
			El end point antivirus deberá evitar obtener escalamiento de privilegios.
			El end point antivirus deberá evitar modificación de las claves de registro para la ejecución de código arbitrario
			La solución deberá permitir por lo menos en sistemas operativo Windows, la función de EDR y XDR sin la necesidad de instalar más aplicaciones de la propia solución en estaciones de trabajo, servidores y dispositivos en la red.
			La solución deberá permitir al administrador aislar de forma manual una máquina de la red para su investigación.
			La solución deberá permitir el aislamiento en la red de los equipos de manera automática en caso de presencia de actividad sospechosa.
			La solución deberá permitir que el administrador tenga la capacidad de realizar búsquedas de amenazas en los equipos, al menos por hash, IP o URL.
			La solución deberá permitir la captura de un snapshot forense.
			La solución deberá incluir software de ayuda para la concientización del usuario final en temas de phishing.
			Se debe de tener la capacidad de tomar control remoto de un equipo aislado utilizando una interfaz tipo CMD y de forma segura desde la misma consola de gestión para poder ejecutar

			comandos de sistema operativo y poder llevar a cabo el proceso de remediación.
			La solución deberá permitir que el administrador tenga la capacidad de realizar búsquedas de amenazas en los equipos, al menos por hash, IP o URL.
			La solución deberá de ser capaz de realizar consultas basadas en lenguaje SQL para poder identificar comportamiento malicioso o hacer caza de amenazas (Threat hunting).
			La solución debe de contar con más de 200 consultas predefinidas para facilidad de la institución.
			La solución debe de poder personalizar o crear nuevas consultas para la personalización de esos indicadores de compromiso que le hagan sentido a la institución y poder detectar de forma temprana un posible evento de seguridad informático.
			La solución debe de poder calendarizar las consultas para que se puedan realizar en el horario que más le convenga a la institución y contar con los resultados de las consultas de forma periódica.
			La solución debe de poder almacenar los datos de los Indicadores de Compromiso detectados por la solución de EDR y XDR en la consola de gestión basada en nube por un periodo de 30 días para poder llevar a cabo consultas de forma histórica y sin la necesidad que el equipo y/o servidor se encuentre en línea
			El end point antivirus deberá soportar máquinas con arquitectura de 32 bits y 64 bits.
			El end point antivirus deberá ser compatible para su instalación en estaciones de trabajo con los sistemas operativos: Windows 8 en adelante, Mac OS X 10.11 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS
			El end point antivirus deberá ser compatible para su instalación en servidores con los sistemas operativos: Windows server 2012 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS.
			El soporte de la solución propuesta debe ser por un periodo 12 MESES
Partida	**Cantidad**	**Solicitud**	**Especificaciones Técnicas**
2	**10**	**Agentes de Antivirus con XDR Servers**	La consola de administración deberá ser una sola consola, basada en web y en nube, que deberá soportar e incluir todos los componentes para la administración, monitoreo y control de la protección en estaciones de trabajo y servidores.
			La consola de administración deberá utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados
			La consola de administración web permitirá definir grupos de usuarios con distintos niveles de acceso a las configuración,

			políticas y registros.
			La consola de administración web deberá contener un Dashboard con el resumen del estado de protección en estaciones de trabajo, así como de servidores, también tendrá que indicar las alertas de eventos críticos, altos, medios e informativos.
			La consola de administración web debe realizar como mínimo el envío automático de alertas criticas mediante correo electrónico a los administradores.
			La consola de administración web deberá de mostrar información como nombre de la máquina, sistema operativo, dirección IP, versión del antivirus instalado, versión del motor, fecha de la actualización, fecha de la última verificación, evento reciente, estado, grupo, numero de virus detectados, etc.
			La consola de administración web debe permitir la organización en grupos de las estaciones de trabajo, así como de servidores dentro de la estructura de administración.
			La consola de administración web deberá tener la capacidad de aplicar políticas de protección diferentes por grupos de máquinas y equipos individuales.
			La consola de administración web deberá permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
			La consola de administración web tendrá un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.
			Desde la consola de administración web se podrá descargar el o los paquetes de instalación de la solución de antivirus end point, así como las descargas de actualización del producto y de las definiciones de virus y protección contra intrusos.
			La consola de administración web deberá realizar la actualización remota en tiempo real, de la solución y del mecanismo de verificación (Engine) de los clientes.
			La consola de administración web permitirá seleccionar un grupo de dispositivos para aplicar la actualización para controlar el ancho de banda de red.
			La consola de administración web deberá soportar la actualización de la versión de los end point, para que esta se realice de modo transparente para los usuarios finales.
			La comunicación del agente hacia la consola debe permitir controlar el uso de ancho de banda para la descarga de firmas.
			La consola de administración deberá tener la posibilidad de implementar servidores de actualización locales para utilizar de manera eficiente el uso del ancho de banda.
			La consola de administración web deberá tener la posibilidad de instalar un servidor local para reenvío de eventos (message relay) en caso de que el agente no pueda comunicarse con la consola en la nube.
			La consola de administración web deberá permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
			La consola de administración web podrá permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.

			Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
			La consola de administración web deberá de permitir la exportación de los informes gerenciales a los formatos csv y pdf.
			La consola de administración deberá tener la capacidad de generar informes, estadísticas o gráficos, detallando la siguiente información: ➢ Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos. ➢ Detalle de los equipos de escritorio y servidores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los equipos. ➢ Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico. ➢ Detalle de las principales aplicaciones bloqueadas y los equipos, usuarios que intentaron acceder a ellas. ➢ Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los equipos, usuarios que las acceden. ➢ Detalle de los equipos y usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder. Detalle de todas las actividades disparadas por reglas de fuga de información.
			La consola de administración web deberá permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.
			La consola de administración web deberá tener de forma nativa los recursos de informes y monitoreo.
			La consola de administración web cuando identifique algún problema, deberá permitir corregir por vía remota, las siguientes acciones: ➢ Proteger el dispositivo con la opción de inicio de una exploración ➢ Forzar una actualización en ese momento ➢ Ver los detalles de los eventos ocurridos ➢ Ejecutar la comprobación completa del sistema ➢ Forzar el cumplimiento de una nueva política de seguridad ➢ Mover el dispositivo a otro grupo Borrar el dispositivo de la lista.

			La consola de administración web deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los equipos que necesitan atención.
			La consola de administra web deberá generar un registro de auditoría seguro que supervise la actividad en dicha consola para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses, etc
			El end point antivirus deberá proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Sistema Operativo Windows, Linux y Mac el agente también deberá detectar PUA, adware y comportamiento sospechoso
			El end point antivirus deberá de contener protección integrada, es decir, en un solo agente tendrá como mínimo: control de amenazas, control de dispositivos, control de aplicaciones, control web, prevención de fuga de información (DLP), gestión del firewall de Windows, protección contra virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).
			El end point antivirus deberá contar con detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
			El end point antivirus deberá poseer la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección. Así como deberá tener algún mecanismo contra la desinstalación del end point como por ejemplo una contraseña.
			El end point antivirus deberá permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
			El end point antivirus deberá realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
			El end point antivirus deberá realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA);
			El end point antivirus deberá proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
			El end point antivirus deberá permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
			El end point antivirus debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
			El end point antivirus deberá ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
			El end point antivirus deberá permitir el monitoreo y el control de dispositivos extraíbles en los dispositivos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo. Como mínimo de los

			siguientes dispositivos: ➢ HD (hard disks) externos ➢ Pendrives USB ➢ Almacenables removibles seguras ➢ CD, DVD, Blu-ray, floppy drives. ➢ Interfaces de red inalámbrica ➢ Módems ➢ Bluetooth ➢ Infrarrojo ➢ MTP (Media Transfer Protocol) PTP (Picture Transfer Protocol) como cámaras digitales.
			El end point antivirus con el control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red
			El end point antivirus deberá tener la capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo
			El end point antivirus deberá actualizar de forma automática la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
			El end point antivirus deberá detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.
			El end point antivirus deberá contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados
			El end point antivirus deberá poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.
			El end point antivirus deberá permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido).
			El end point antivirus deberá permitir el bloqueo o sólo registrar el evento en la consola de administración web, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible.
			El end point antivirus deberá tener listas de CCL pre configuradas con al menos los siguientes identificadores.(DLP) • Números de tarjetas de crédito. • Números de cuentas bancarias. • Números de pasaportes. • Direcciones

			• Números de teléfono. • Lista de correos electrónicos. Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.
			El end point antivirus deberá incluir el control web para permitir controlar el acceso a sitios inapropiados, con al menos 12 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
			El end point deberá de contar con la capacidad de monitorear los cambios como creaciones o modificaciones sobre carpetas y archivos críticos del sistema basados en una lista pre definida y poder personalizar dicha lista para sistemas operativos Windows server 2012 o superior debido a la criticidad de la información que manejan.
			El endpoint podrá generar una lista blanca de aplicaciones que se ejecuten en el sistema operativo Windows server 2012 o superior para que esas aplicaciones sean las únicas que se puedan ejecutar
			El end point antivirus deberá contener la funcionalidad de protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
			El end point antivirus deberá contener la funcionalidad de detección de amenazas desconocidas que están en memoria.
			El end point antivirus deberá contener la funcionalidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
			El end point antivirus deberá contener la funcionalidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
			El end point antivirus no deberá de requerir descarga de firmas de ningún tipo.
			El end point antivirus deberá contener la funcionalidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
			El end point antivirus deberá contener la funcionalidad de análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
			El end point antivirus deberá contener la funcionalidad de bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
			El end point antivirus deberá contener la funcionalidad de poder generar excepciones ante falsos positivos
			El end point antivirus deberá contener la capacidad de protección contra ransomware basada en comportamiento.
			El end point antivirus deberá contener la capacidad de remediación de la acción de encriptación de los ransomware.
			El end point antivirus deberá contener la detección del cifrado malicioso de forma local o remoto.

			El end point antivirus deberá contener la protección antiransomware para el sector de booteo (master boot record).
			El end point antivirus deberá contener la capacidad de restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
			El end point antivirus deberá informar a La consola de administración web todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red.
			El end point antivirus deberá tener la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
			El end point antivirus deberá contar como mínimo con la detección y protección de las siguientes técnicas de explotación: • Enforce Data Execution Prevention; • Mandatory Address Space Layout Randomization; • Bottom-up ASLR; • Null Page (Null Deference Protection); • Heap Spray Allocation; • Dynamic Heap Spray; • Stack Pivot; • Stack Exec (MemProt); • Stack-based ROP Mitigations (Caller); • Branch-based ROP Mitigations (Hardware Assisted); • Structured Exception Handler Overwrite (SEHOP); • Import Address Table Filtering (IAF); • Load Library; • Reflective DLL Injection; • Shellcode; • VBScript God Mode; • Wow64; • Syscall; • Hollow Process; • DLL Hijacking; • Squiblydoo Applocker Bypass; • APC Protection (Double Pulsar / AtomBombing); Process Privilege Escalation
			El end point antivirus deberá contar con mitigación de inyección de códigos en procesos.
			El end point antivirus deberá contar con protección contra robo de credenciales
			El end point antivirus deberá contar con protección contra malware escondido en aplicaciones legitimas (code cave).
			El end point antivirus deberá evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.

			El end point antivirus deberá evitar obtener escalamiento de privilegios.
			El end point antivirus deberá evitar modificación de las claves de registro para la ejecución de código arbitrario
			La solución deberá permitir por lo menos en sistemas operativo Windows, la función de EDR y XDR sin la necesidad de instalar más aplicaciones de la propia solución en estaciones de trabajo, servidores y dispositivos en la red.
			La solución deberá permitir al administrador aislar de forma manual una máquina de la red para su investigación.
			La solución deberá permitir el aislamiento en la red de los equipos de manera automática en caso de presencia de actividad sospechosa.
			La solución deberá permitir que el administrador tenga la capacidad de realizar búsquedas de amenazas en los equipos, al menos por hash, IP o URL.
			La solución deberá permitir la captura de un snapshot forense.
			La solución deberá incluir software de ayuda para la concientización del usuario final en temas de phishing.
			Se debe de tener la capacidad de tomar control remoto de un equipo aislado utilizando una interfaz tipo CMD y de forma segura desde la misma consola de gestión para poder ejecutar comandos de sistema operativo y poder llevar a cabo el proceso de remediación.
			La solución deberá permitir que el administrador tenga la capacidad de realizar búsquedas de amenazas en los equipos, al menos por hash, IP o URL.
			La solución deberá de ser capaz de realizar consultas basadas en lenguaje SQL para poder identificar comportamiento malicioso o hacer caza de amenazas (Threat hunting).
			La solución debe de contar con más de 200 consultas predefinidas para facilidad de la institución.
			La solución debe de poder personalizar o crear nuevas consultas para la personalización de esos indicadores de compromiso que le hagan sentido a la institución y poder detectar de forma temprana un posible evento de seguridad informático.
			La solución debe de poder calendarizar las consultas para que se puedan realizar en el horario que más le convenga a la institución y contar con los resultados de las consultas de forma periódica.
			La solución debe de poder almacenar los datos de los Indicadores de Compromiso detectados por la solución de EDR y XDR en la consola de gestión basada en nube por un periodo de 30 días para poder llevar a cabo consultas de forma histórica y sin la necesidad que el equipo y/o servidor se encuentre en línea
			El end point antivirus deberá soportar máquinas con arquitectura de 32 bits y 64 bits.
			El end point antivirus deberá ser compatible para su instalación en estaciones de trabajo con los sistemas operativos: Windows

			8 en adelante, Mac OS X 10.11 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS
			El end point antivirus deberá ser compatible para su instalación en servidores con los sistemas operativos: Windows server 2012 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 6, 7 y 8, Debian 9 y 10, Oracle Linux 6, 7 y 8, Suse 12 y 15, Ubunto 16 y 18 LTS.
			El soporte de la solución propuesta debe ser por un periodo 12 MESES
Partida	**Cantidad**	**Solicitud**	**Especificaciones Técnicas**
3	**8**	**Entrenamientos**	El oferente debe proporcionar entrenamientos oficiales del fabricante de manera online para 8 personas de esta institución.
Partida	**Cantidad**	**Solicitud**	**Especificaciones Técnicas**
4	**1**	**Servicios profesionales**	Este proyecto requiere servicios de implementación en sitio a ser ejecutados por el oferente o el fabricante de la solución ofertada.
			El oferente debe ser canal autorizado para la venta de la marca del software ofertado.
			El oferente debe presentar la carta de canal autorizado de la solución ofertada.
			El oferente debe contar con un mínimo de una (1) persona con certificación de Arquitecto que se encuentre local en el país. Dicho personal debe ser empleado del oferente y se debe incluir la TSS para demostrarlo
			El oferente debe contar con un mínimo de una (1) persona con certificación profesional o superior de virtualización para la implementación de las licencias de servidores. Dicho personal debe ser empleado del oferente y se debe incluir la TSS para demostrarlo
			El oferente debe ser canal autorizado de la solución de virtualización y debe presentar carta de fabricante.

Documentación para presentar adjunto con la **COTIZACIÓN**:

1) **Registro de Proveedores del Estado (RPE)** con documentos legales-administrativos actualizados, emitido por la Dirección General de Contrataciones Públicas.

2) **Certificación (DGII),** emitida por la Dirección General de Impuestos Internos donde se manifieste que el oferente se encuentra al día en el pago de sus obligaciones fiscales.

3) **Certificación (TSS),** emitida por la Tesorería de la Seguridad Social, donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social.

4) **Certificación MIPYMES o MIPYMES Mujer.** Según sea la orientación del Proceso. **NO ES SUBSANABLE**

5) **Formulario de Información sobre el Oferente (SNCC.F.042)** debidamente completado y llenado con las informaciones correctas del Proceso y la Dirección, Teléfonos y Correos Electrónicos actualizados, junto a una prueba (factura de servicio de teléfono, luz o basura que así lo certifique). Este formulario **NO ES SUBSANABLE**.

6) Formulario de Entrega de Muestra **(SNCC.F.056) MUESTRA OBLIGATORIA**

7) **Formulario de Presentación de Oferta (SNCC.F.034),** debidamente completado y llenado con las informaciones correctas del Proceso, en el cual el Oferente indicará lo que está ofertando, detallando correctamente cantidades y especificaciones (conforme a las especificaciones técnicas suministradas y acorde a los bienes ofertados con el nombre de la Marca que nos oferta y con Disponibilidad para entrega Inmediata). Este formulario **NO ES SUBSANABLE**.

8) Anexar la **Oferta Técnica** que describan las características, bondades y garantías de la marca de los Ítems que nos ofertan. **NO ES SUBSANABLE**.

9) Copia del **Registro Mercantil**/Documento que avale el Objeto Social de la Empresa.

10) **Credenciales** (Copia de la Cedula de Identidad y Electoral del Representante Legal de la Empresa).

El oferente puede presentar ofertas parciales en cada ITEM si así lo decide, esto debe estar indicado en el formulario de presentación de oferta (SNCC.F.034), el cual no es subsanable.

LA ENTIDAD CONTRATANTE NO RECIBIRÁ PROPUESTAS ECONOMICAS, YA PASADO EL PLAZO DE PRESENTACION DE OFERTAS.

A) Condiciones Del Proceso

La Oferta deberá presentarse en Pesos Dominicanos (RD$) Los precios deberán expresarse en **dos decimales (XX.XX)** que tendrán que incluir todas las tasas (divisas) impuestos y gastos que correspondan, transparentados e implícitos según corresponda.

El Oferente que resulte favorecido con la Adjudicación del presente proceso, debe mantener durante todo el plazo de ejecución del Contrato el precio que proponga en el momento de presentación de la Oferta.

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 y servicios conexos a ser suministrados.

El Oferente/Proponente que cotice en cualquier moneda distinta al Peso Dominicano (RD$) **se auto descalifica para ser objeto de Adjudicación**.

Los precios no deberán presentar alteraciones ni correcciones y **deberán ser dados por la unidad de medida establecida en el Formulario de Oferta Económica, el cual no puede ser modificado por el proponente.** Cualquier diferencia o error numérico dentro de este formulario, descalifica automáticamente al Oferente que lo haya presentado.

En adición a las disposiciones del **Artículo 14 de la Ley No. 340-06** con sus modificaciones **NO** podrán

contratar con el Estado Dominicano los proveedores que no hayan actualizado sus datos en el Registro de Proveedores del Estado.

B) Criterios De Evaluación

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar la pertinencia de su oferta bajo la modalidad **"CUMPLE/ NO CUMPLE".**

La presentación de las muestras es imprescindible para la evaluación de las mismas.

El cumplimiento de este criterio será evaluado conforme a la documentación requerida.

C) EVALUACIÓN OFERTA ECONÓMICA

El Comité de Compras y Contrataciones evaluará únicamente las Ofertas que se ajustan sustancialmente al presente Términos de Referencia, tomando en cuenta la calidad y el precio ofertado.

D) CRITERIOS DE ADJUDICACIÓN

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

La adjudicación será decidida a favor del oferente/proponente cuya propuesta cumpla con los requisitos exigidos y sea calificada como la más conveniente para los intereses institucionales, teniendo en cuenta el precio, la calidad, y las demás condiciones que se establecen en el presente término de referencia.

E) INICIO DEL SUMINISTRO

Una vez formalizado el correspondiente Contrato de Suministro entre la Entidad Contratante y el Proveedor, éste último iniciará el Suministro de los Bienes que se requieran mediante el correspondiente pedido, sustentado en el Cronograma de Entrega de Cantidades Adjudicadas, que forma parte constitutiva, obligatoria y vinculante del presente Pliego de Condiciones Específicas.

F) REQUISITOS DE ENTREGA

Los Proveedores tendrán desde el 22/11/2022, hasta el día 24/11/2022, a las 8:00 a.m., único día para recibir las muestras por los interesados en participar en dicho proceso.

Todos los bienes adjudicados deben ser entregados conforme a las Especificaciones Técnicas solicitadas, en el **Departamento de Administración de Servicios TIC** de la Dirección Central de Policía de Turismo, (POLITUR), Ubicado en Ave. Gustavo Mejía Ricart No. 121 esq. Theodore Chasseriau (antigua Privada), del Sector El Millón, Santo Domingo Distrito Nacional, siempre con previa coordinación con el Sub-Director de Compras a los fines de dar entrada a los bienes adquiridos.