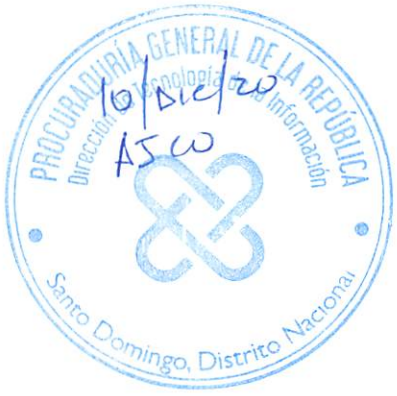
INFORMACIÓN GENERAL (A)	
Bien o Servicio a adquirir	**Antivirus**
Referencia (No. Proceso)	**Req. 020-3466**
Nombre del Proveedor	
Fecha de la Propuesta	

	CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS (B)	CUMPLE (C)
Soporte de plataformas de servidores	La solución deberá soportar los siguientes sistemas operativos de servidores: ➢ Windows Server 2016 RS3, 2016 (incluyendo Server Core mode) ➢ Windows Server 2012, 2012 R2, and 2012 R2 Update 1: Essentials, Standard, Datacenter (incluyendo Server Core mode) ➢ Windows Storage Server 2012 and 2012 R2 ➢ Windows Server 2008 y 2008 R2: Standard, Datacenter, Enterprise, Web (incluyendo Server Core mode) ➢ Windows Storage Server 2008 and 2008 R2 ➢ Windows Small Business Server 2011 ➢ Windows Small Business Server 2008 ➢ Linux CentOS 7.4, 7.3, 7.2, 7.1 (64-bit) ➢ Red Hat Enterprise Linux 7.x, 6.x ➢ SUSE Linux Enterprise Server 12.x, 11.x (64-bit)	
Soporte de plataformas de clientes	La solución deberá soportar los siguientes sistemas operativos de clientes: ➢ Windows 10 Anniversary Update ➢ Windows 10 November Update ➢ Windows 10 ➢ Windows 8.1 Update 1 ➢ Windows 8 (no incluyendo Windows RT edition) ➢ Windows 7 ➢ Windows To Go (All versions) ➢ Windows Vista SP2 ➢ Windows Embedded 8: Pro, Standard, Industry ➢ Windows Embedded Standard 7 ➢ MacOS Big Sur 11..x ➢ MacOS High Sierra 10.13.x ➢ MacOS Sierra 10.12.x ➢ MacOS El Capitan 10.11.x ➢ MacOS Yosemite 10.10.x ➢ MacOS Mavericks 10.9.x ➢ Linux Ubuntu 17.x, 16.10, 16.04, 15.x, 14.04, 12.04 (64-bit) ➢ SUSE Linux Desktop 12, 11 ➢ Amazon Linux AMI 2017.9, 2014 and later ➢ Fedora 26, 25, 24, 23, 22 ➢ Debian 9.0, 8.0	

Administración central	➢ La solución debe ser administrada de forma centralizada. ➢ La solución debe permitir la gestión y manejo de políticas de mecanismos de defensa integrados a Windows 10 (Firewall, Defender) ➢ La solución debe ofrecer distintos modelos de gestión: On-Premises, IaaS o SaaS. ➢ La solución deberá ser administrada en la misma consola que el resto de los componentes de seguridad mencionados en este documento.	
Soporte de Navegadores	➢ Microsoft Internet Explorer (versiones 7, 8, 9, 10, and 11) ➢ Mozilla Firefox (versiones desde 3.0 a 28) ➢ Google Chrome (versiones desde 4.0 a 34)	
Agente	➢ Se debe poder desplegar el agente de la solución desde la consola de administración y este debe ser el componente administrativo de todas las funcionalidades solicitadas en este documento. ➢ La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario. ➢ La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de anti-virus y firewall instalados previamente en la máquina. ➢ Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
AJ
10/DIC/20
Santo Domingo, Distrito Nacional

Software Cliente	➢ La solución debe poder desplegar una aplicación cliente stand alone que pueda gestionar cambios localmente en caso de que se necesite. ➢ Se debe poder restringir completamente o parcialmente al acceso a la consola cliente para configurar parámetros individuales sobre el host. ➢ La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador. ➢ Puede existir más de una configuración de idioma para la aplicación cliente.	
Plataforma Colaborativa	➢ La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, control web, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.	
Protección contra amenazas		
Escaneo de sistema	➢ La solución debe de poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente. ➢ Se debe poder configurar acciones sobre infecciones identificadas: Denegar acceso Limpiar Eliminar Ninguna ➢ Debe tener la opción de detectar actividad del usuario, teniendo en cuenta funcionamiento del disco, mouse y teclado para activar escaneos y no afectar la productividad.	



Mecanismos de protección	➢ La solución debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí. ➢ Se deben reportar eventos de amenazas directamente sobre la consola cliente, de forma consolidada (AV, Web e IPS/FW), priorizada y bajo un lenguaje específicamente descriptivo donde de manera natural cada registro explique cuál fue el elemento que causante, cual fue la acción realizada por este, que componentes estuvieron involucrados, que regla de protección fue violada. No se admiten tablas, archivos tabulados en texto plano, listas o cualquier tipo registro que no sea fácilmente entendido por el usuario final. ➢ La solución debe poder habilitar la opción de escaneo de click-derecho sobre carpetas específicas. ➢ Es requerido que la solución en equipos Windows reciba actualizaciones de seguridad bajo un único componente (archivo) consolidado que incluya lo correspondiente a: Antivirus, Protección Web e IPS, con el fin de disminuir la carga administrativa y de red que supondría realizarlos de forma independiente. ➢ Debe contar con mecanismos de protección de exploits Generic Buffer Overflow Protection. ➢ La solución debe contar con características de protección Kevlar para navegadores con Active X. ➢ La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de IE, sean JavaScript o VBScript. ➢ La solución debe poder configurar mediante reglas o políticas de protección de: Entradas y llaves de registro de Windows. Prevención de creación de ejecutables portables (.INI, .PIF). Creación de archivos autorun. Prevención de uso de archivos TFTP (Trivial File Transfer Protocol). Contra lectura de archivos en cache de IE. Creación y modificación remota de archivos o carpetas. Acceso remoto de archivos o carpetas. .EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT. Modificación de procesos Core de Windows. Modificación de configuraciones de exploradores y navegadores web. Proteger procesos con sub reglas personalizadas. Asignar las reglas por nombre de usuario.	
Firewall/IPS		
Reglas de protección	➢ El modulo debe permitir/bloquear tráfico de red para protocolos no soportados. ➢ Permitir o bloquear trafico solo hasta que el modulo y servicios de firewall este arriba. ➢ Habilitar/deshabilitar protección IP Spoof ➢ Habilitar/deshabilitar alertas de intrusión de Firewall ➢ Agregar dominios específicos para bloqueo DNS.	

	➢ La solución debe poder recopilar log en eventos lanzados directamente sobre el cliente y reportar incidentes en la consola de administración central. ➢ Debe proteger ataques tipo "Generic Buffer Overflow" en aplicaciones de 32bits ➢ Debe soportar reglas de protección de acceso para registro, procesos y servicios ➢ Debe tener la funcionalidad "Data Execution Prevention" ➢ Debe soportar la funcionalidad "Generic Privilegie Escalation Protection"
Reglas de trafico de red	➢ Cada una de las reglas debe ser aplicables para tráfico entrante como para tráfico saliente del cliente. ➢ Las reglas de trafico deben ser soportadas para protocolos IP: Ipv4 Ipv6 ➢ La solución debe aplicar reglas de tráfico para conexiones: Alámbricas Inalámbricas Virtuales ➢ Las reglas de tráfico deben poder extenderse a ejecutables por medio de la especificación de ruta (se pueden utilizar wildcards). ➢ El modulo debe poder incluir reglas en base a los protocolos y puertos más conocidos del mundo. ➢ Se debe poder administrar redes y ejecutables de confianza desde la interfaz de usuario de los endpoints.
Reputación global	➢ La herramienta debe contar con un mecanismo de conocimiento global de amenazas que permita
Método de bloqueo de ataques web	➢ La solución debe poder bloquear de forma automática sitios con clasificación de riesgo alto que puedan afectar los equipos y/o la red. ➢ La solución debe tener la capacidad de bloquear y/o dejara al usuario decidir qué acción tomar en caso que el sitio que se esté visitando por alguna razón no cuente con una clasificación en ese momento. ➢ La solución debe contar con un elemento visual que permita identificar el riesgo del sitio visitado en los navegadores soportados. ➢ La solución incluso debe tener la capacidad de ayudar al instituto permitiéndole definir reglas de filtrado de URL por categorías. ➢ La solución debe tener la capacidad de evitar el acceso a sitios de phishing. ➢ La solución deberá poder evitar descargar malware, ayudando así a tener que la protección sea proactiva ➢ La solución deberá de contar con alrededor de 100 categorías de sitios web.

	➢ La solución debe poder especificar que navegadores sean los únicos autorizados para navegar a internet. ➢ La solución debe tener la capacidad de definir rangos de IP privadas (intranet) que no sean analizadas por la herramienta para bloqueo de sitios web. ➢ La solución debe tener la capacidad de forzar búsquedas seguras con los buscadores al menos cuatro de los motores de búsqueda más usados (Google, MSN, Yahoo). ➢ La solución debe poder bloquear iFrames de HTML o advertir de sitios que contengan.	
Soporte de inteligencia de amenazas	➢ La solución debe tener categorías sincronizadas con una base de datos de reputación global de amenazas. ➢ La clasificación deberá ser en tiempo real y contra una base de datos de reputación que al menos correlacione archivos, URL´s	
Personalización de mensajes de bloqueo	➢ La solución debe tener la capacidad de personalizar los mensajes que le aparezcan al usuario cuando una política sea violada.	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
AJCO
30/DIC/20
Santo Domingo, Distrito Nacional

Reportes	➢ Se deben poder ver reportes de amenazas web detectadas y políticas violadas.	
Logs	➢ La solución debe captar logs o registros para eventuales temas de compliance y troubleshooting.	
Aspectos Generales	➢ La solución permitirá proteger estaciones de trabajo mediante el control de la ejecución de aplicaciones, software y código ejecutable, realizado a través de listas blancas dinámicas y por medio de la prevención de modificaciones hacia los archivos de la máquina. ➢ La solución debe emplear un modelo dinámico de confianza para bloquear las aplicaciones no autorizada ➢ La generación de listas blancas dinámicas debe ser un proceso automático sin necesidad de intervención manual ➢ La solución debe tener en cuenta ejecutables, activeX, Java, Pearl Scripts, archivos .bat, archivos VBS, dll y archivos .SYS ➢ Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas. ➢ Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca ➢ No debe permitir que las aplicaciones denegadas se ejecuten desde el disco o desde memoria ➢ La solución debe soportar el control mediante: listas blancas, listas negras, inventario y modo híbrido (combinación entre las anteriores) ➢ Debe soportar flujos de auto aprobación (usuario final) cuando se presente el bloqueo de una aplicación ➢ La solución debe estar en capacidad de hacer un inventario de todas las aplicaciones incluyendo sus códigos asociados y dll de forma centralizada para su catalogación ➢ La solución debe estar en capacidad de investigar un inventario de aplicaciones y clasificarlas basado en su reputación de manera que se puedan aislar las buenas de las malas ➢ La solución no debe requerir una actualización de políticas para aprobar la ejecución de una aplicación ➢ La solución debe soportar estaciones de trabajo, servidores y equipos de propósito específico. ➢ La solución debe estar diseñada para funcionar en modo desconectado (offline mode) ➢ La solución debe soportar un modo de observación luego de la creación de la lista blanca, donde las aplicaciones, software y código no permitido	

	puedan ser monitoreados sin afectar su ejecución, con el fin de identificar posibles nuevos ítems que sean agregados a la política ➢ Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración ➢ La solución deberá soportar los siguientes sistemas operativos: Microsoft Windows: XP, Vista, 7, 8, 8.1 y 10 Linux: CentOS, SUSE, OEL, Ubuntu. Microsoft Windows Embedded XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8 Industry, 8.1. ➢ La solución deberá soportar los siguientes Sistemas Operativos de Microsoft los cuales ya no cuentan con soporte del fabricante: Windows Server NT, 2000, 2003, 2003 R2, Windows XP. ➢ La autorización de aplicaciones permitidas se debe poder realizar a través de: Checksum, certificados, editor, nombre, adición manual a través de inventario ➢ La solución deberá soportar la administración mediante línea de comandos en caso de ser necesario ➢ Esta funcionalidad debe consumir menos de 10Mb de RAM	
Control de dispositivos		
Capacidad de gestión	➢ La solución debe ser soportada en sistemas operativos Windows y MacOS ➢ La solución debe permitir el monitoreo o bloqueo total de los dispositivos conectados ➢ En los casos que aplique, la solución debe permitir la creación de políticas unificadas para sistemas operativos Windows y MacOS. ➢ La gestión de control de dispositivos debe estar unificada en la misma consola utilizada para la gestión de anti-malware. ➢ La solución debe permitir la extensión de sus funcionalidades hacia Prevención de Fuga de Datos, con el propósito de evitar despliegues adicionales ➢ Cada regla debe permitir la configuración basada en localización del usuario, de tal forma que permita tomar distintas acciones cuando el usuario está dentro o fuera de la organización. ➢ La solución debe permitir la desactivación de una regla o un conjunto de reglas.	
Control de dispositivos	➢ La solución debe permitir el control de los siguientes tipos de dispositivos: - Almacenamiento Removible; - Bluetooth; - Dispositivo Multimedia; - Smartphones; - Dispositivos Plug and Play; - CDs/DVDs; ➢ La solución debe permitir el bloqueo de ejecución de aplicaciones desde dispositivos removibles, permitiendo también configurar excepciones. ➢ La solución debe permitir el control de dispositivos bajo los siguientes criterios:	

- Clase de Dispositivo;
- Medio de conexión;
- Fabricante y/o modelo;
- Número de serie;

- La solución debe permitir crear políticas de bloqueo, monitoreo o solo lectura para dispositivos de almacenamiento removible.
- La solución debe permitir la configuración de definiciones de dispositivos bajo las siguientes categorías:
  - Gestionado;
  - No gestionado;
  - Lista Blanca;
- La solución debe permitir el agrupamiento de dispositivos por medio de propiedades comunes, como: Vendor ID, Product ID o Device Class.
- La solución debe ser capaz de identificar los dispositivos Plug and Play bajo las siguientes propiedades:
  - Tipo de Bus;
  - Clase de Dispositivo (Device Class)
  - ID de fabricante (Vendor ID)
  - ID de producto (Product ID)
- La solución debe ser capaz de identificar los dispositivos removibles bajo las siguientes propiedades:
  - Tipo de Bus;
  - Sistema de Archivo;
  - Número de Serie;
  - Permisos de lectura/escritura;
- La solución debe poseer las siguientes clases de dispositivos de manera nativa:
  - Batería;
  - Lectores de huella y dispositivos biométricos;
  - Bluetooth;
  - Drives de CD/DVD;
  - Impresoras y scanners;
  - Adaptadores de video;
  - Disco Duro;
  - Controladoras y drives de diskette;
  - GPS;
  - Infrarrojo;
  - IEEE 1394;
  - Mouse;
  - Modem;
  - Fax;
  - Adaptadores de Red;
  - PCMCIA;
- Debe ser posible habilitar o deshabilitar una determinada regla de protección de acuerdo a la localización del equipo (ej. Dentro o fuera de la red organizacional)
- La solución debe poseer los siguientes tipos de dispositivos de manera nativa:
  - Dispositivos Apple;
  - Dispositivos Bluetooth;

- Drives CD/DVD;
- Dispositivos de almacenamiento removible;
- Lectores de tarjetas SD;
- Dispositivos Windows Portable;
- Dispositivos Plug and Play;

- La solución debe permitir la creación de clases y tipos de dispositivos personalizados, utilizando, como mínimo, los siguientes criterios:
  - Clase de Dispositivo;
  - Tipo de Bus;
  - Número de Serie;
  - ID de fabricante;
  - ID de producto;
  - Sistema de Archivo;
- Al identificar un nuevo dispositivo conectado a las estaciones de trabajo, cuyo hardware es desconocido, la solución debe tener la capacidad de emitir una alerta a la consola centralizada indicando una nueva clase de dispositivo encontrada.
  La solución debe permitir el control de dispositivos mediante su GUID.
- La solución debe permitir la creación de los siguientes tipos de controles:
  - Regla para control de dispositivo en Citrix XenApp;
  - Regla para control de discos duros;
  - Regla para dispositivos Plug and Play;
  - Regla para dispositivos de almacenamiento removible;
  - Regla de acceso de archivos a dispositivos de almacenamiento removible;
  - Regla de dispositivo TrueCrypt;
- Cada regla debe tener la capacidad de ser aplicada a:
  - Cualquier usuario (All);
  - Usuario que pertenece a un grupo específico (OR);
  - Usuario que pertenezca a todos los grupos (AND);
  - Usuario local o usuario fuera del dominio;
- Durante la definición de las reglas, la solución debe permitir la creación de objetos LDAP en base a:
  - SID de Objeto;
  - Nombre de Objeto;
  - Dominio de Objeto;
- Cada regla debe permitir crear exclusiones para, como mínimo:
  - Usuarios;
  - Dispositivos;
- Cada regla debe permitir la asignación de los siguientes niveles de severidad:
  - Información;
  - Warning;
  - Minor;
  - Major;
  - Crítico;

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
AJC
16/Dic/20
Santo Domingo, Distrito Nacional

Inspección avanzada mediante inteligencia artificial (Machine Learning)	➢ La solución tener una funcionalidad específica diseñada para inspeccionar archivos y actividad sospechosa con el fin de detectar patrones maliciosos mediante el uso de técnicas de "Machine Learning". ➢ Debe tener dos modos de análisis: en la nube y en el cliente, dependiendo de la conectividad de los equipos ➢ Debe recolectar información de los atributos de los archivos y su comportamiento para realizar el análisis ➢ La solución debe tener la capacidad de detectar y tomar acción sobre amenazas "file-less" ➢ La solución debe tener la capacidad de realizar acciones de remediación y rollback ante ataques ➢ Esta funcionalidad debe ser opcional y deberá poder ser desactivada tanto en la consola cliente como mediante política centralizada a través de la consola central de administración ➢ Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración	
Contención dinámica de Aplicaciones	➢ Debe permitir seleccionar que aplicaciones con una reputación específica deben ser ejecutadas en modo "contenido", es decir que esta funcionalidad no le permitirá realizar ciertas acciones que hayan sido consideradas como maliciosas dentro del sistema operativo ➢ La solución deberá poder tomar acciones o de bloqueo o registro según su configuración ➢ Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración ➢ Este módulo debe permitir la ejecución de las aplicaciones potencialmente maliciosas permitiéndoles la ejecución dentro del ambiente (punto final), mientras que limita los cambios en el sistema operativo que esta puede realizar ➢ Debe estar basado en reglas de comportamiento configurables tanto desde la consola cliente como la consola central ➢ La funcionalidad debe poder liberar una aplicación contenida mediante: Cambio en la reputación dentro del sistema de inteligencia contra amenazas Exclusión en la política	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
Santo Domingo, Distrito Nacional
30/12/20

Inteligencia de Amenazas	➢ La solución deberá permitir generar una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido, virtual o en los equipos de usuario final puedan intercambiar información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito. ➢ La solución deberá permitir reputar archivos localmente (de forma manual o a través de reglas de comportamiento) y mediante distintas fuentes de reputación dentro de la infraestructura de seguridad como: Sandbox y Proxys Web) ➢ La solución debe permitir asignar diferentes niveles de reputación a aplicaciones y certificados que se ejecutan en un ambiente con un punto de análisis a nivel local, la difusión de esta asignación debe realizarse en tiempo real mediante un protocolo diseñado para este propósito sin requerir que los agentes realicen un proceso de actualización firmas o configuraciones. ➢ En caso de generarse un evento, la comunicación de este debe ser en tiempo real mediante el protocolo de comunicación diseñado para este fin, no debe depender de los ciclos de actualización de eventos a la consola central ni del "llamado/despertar de agentes" ➢ La solución no deberá ser un sistema de antivirus, control de aplicativos y/o control de cambios, pero debe poder integrarse con estos dispositivos en caso de que se encuentren presentes ➢ La solución al determinar la reputación de un archivo ejecutable, deberá comunicarla al resto de los equipos de usuarios finales con el objetivo de crear una inteligencia de seguridad en la red.	
Protección de dispositivos móviles		
Gestión	➢ La solución debe permitir la protección de dispositivos móviles sin necesidad de desplegar componentes on-premises ➢ La solución debe entregar la siguiente información sobre los dispositivos móviles: - Vulnerabilidades - Riesgo de aplicaciones - Usuario asociado al dispositivo - Sistema Operativo - Estado de configuración - Estado de Sistema Operativo (actualizable y/o vulnerable) ➢ La solución debe colectar la siguiente información en sus eventos: - Vector (Dispositivo, Red, Aplicación) - Usuario - Ubicación en donde ocurrió el evento - Detalle de amenaza de red (Wifi conectado, direcciones IP asociadas, redes Wifi cercanas) - Detalle de amenaza de aplicación (riesgos de privacidad y seguridad) ➢ La solución debe soportar dispositivos iOS y Android ➢ La solución debe permitir la integración con las soluciones de gestión de dispositivos móviles (MDM/EMM) líderes en el mercado ➢ La solución debe permitir la integración con soluciones de SIEM vía Syslog ➢ La solución debe permitir controlar la información colectada sobre los eventos de amenazas, con el propósito de gestionar el nivel de privacidad de los usuarios finales de acuerdo a las políticas BYOD que tenga la organización ➢ La solución debe permitir la gestión centralizada desde una misma consola	

Detección de amenazas	➢ La solución debe analizar las amenazas en el dispositivo, garantizando que el mismo esté protegido aun estando offline o en modo avión ➢ La solución debe utilizar mecanismos de Inteligencia Artificial para la detección de amenazas ➢ La solución debe tomar acción en cuanto a amenazas basadas en: - Dispositivo - Red - Aplicación ➢ La integración con MDMs/EMMs debe permitir extender la toma de acción de las políticas a partir de acciones que puede tomar un MDM, por ejemplo, hacer un wipe del dispositivo móvil. ➢ La solución debe tener la capacidad de crear políticas de aplicaciones, desde la cual permita perfilar las aplicaciones de acuerdo a los permisos y accesos que tienen en el dispositivo móvil, para luego marcarlas fuera de cumplimiento o definir una lista blanca/lista negra. ➢ La solución debe tener la capacidad de detectar la navegación a sitios web maliciosos y phishing. ➢ La solución debe entregar funcionalidades de sandboxing en la nube, la cual entrega resultados sobre los riesgos de privacidad y seguridad que pueden tener las aplicaciones móviles. ➢ Las funcionalidades de sandboxing deben permitir que el usuario administrador pueda someter aplicaciones de manera manual, y entregar reportes ejecutivos y técnicos con los hallazgos. ➢ La solución debe permitir tomar las siguientes acciones en torno a las amenazas detectadas: - Bloqueo y desconexión de Bluetooth o Wifi - Bloqueo de conexiones de red (sinkhole) - Terminar un proceso ➢ Debe estar basado en reglas de comportamiento configurables desde la consola central	
Soporte	Soporte de 12 meses incluido en la solución	
Especialistas	➢ Certificacion del fabricante de distribución autorizada ➢ Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos. ➢ Empresa con técnicos certificados en: CEH, ECIH, ECSA, ENCA	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
Santo Domingo, Distrito Nacional
10/DIC/20

Firma del Vendedor	**Sello de la Empresa**

INSTRUCCIONES

En la sección (A) aparece la información general del proceso el tipo de bien o servicio a adquirir y el número de referencia del proceso. En esta sección el oferente deberá registrar, en los campos correspondientes, el nombre de la empresa y la fecha en la que se presenta la propuesta

En la sección (b) se muestra las características o requisitos mínimos solicitados para el bien o servicio

En la sección (c) el oferente deberá marcar con una x las características con las que cuenta el bien o servicio ofertado

Finalmente, el representante firmara las páginas con las que cuenta este formulario y colocara el sello de la empresa en la última página.

Nota: para que pueda ser evaluada su propuesta deberá presentar este formulario debidamente completado y anexarle la cotización correspondiente.

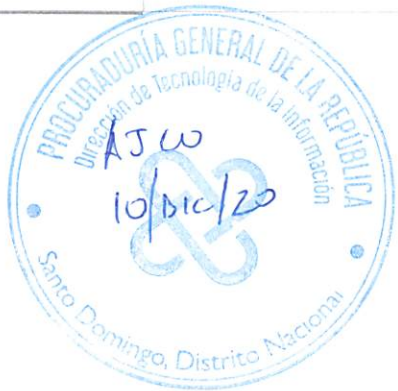
INFORMACIÓN GENERAL (A)	
Bien o Servicio a adquirir	**EDR antivirus**
Referencia (No. Proceso)	**REQ. 020-3466**
Nombre del Proveedor	
Fecha de la Propuesta	

	CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS (B)	CUMPLE (C)
Arquitectura y funcionamiento	○ La solución ofertada debe ser basada en cloud, es decir, todo el procesamiento de datos se debe realizar en la nube. ○ La herramienta debe permitir la búsqueda de información en tiempo real de distintos elementos dentro del endpoint ○ La solución ofertada debe permitir la creación de procesos de investigación, carga de información y análisis directamente desde la consola de monitoreo. ○ La solución debe permitir aplicar mecanismos de contención directamente de la consola y sin la necesidad de contar con herramientas de terceros para estos efectos ○ La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información de terceros para detectar posibles incidentes dentro del ecosistema ○ La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización. ○ En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente. ○ La solución debe permitir poner en cuarentena al host comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos ○ La solución debe permitir detener y/o eliminar un proceso en ejecución o persistente en las estaciones de trabajo. ○ La solución ofertada debe permitir la segmentación de políticas para la operación de la plataforma, es decir, la herramienta debe permitir aplicar distintos tipos de políticas para un mismo ecosistema cliente. ○ La solución debe permitir mecanismo de contención remotos en el endpoint ○ La solución debe permitir mecanismos de remediación remotos en el endpoint. ○ La solución debe estar en capacidad de colectar información de procesos en ejecución ○ La solución debe ser capaz de recolectar información de servicios que se ejecutan en el endpoint ○ La solución debe ser capaz de recolectar información de las tareas programadas en el endpoint.	

INFORMACIÓN GENERAL (A)

Bien o Servicio a adquirir	**EDR antivirus**
Referencia (No. Proceso)	**REQ. 020-3466**
Nombre del Proveedor	
Fecha de la Propuesta	

	○ La solución debe ser capaz de colectar información histórica de navegación web y descargas ○ La solución debe colectar información del filesystem ○ La solución debe colectar logs de eventos. ○ La solución debe tener la capacidad de eliminar/modificar llaves de registro ○ La solución debe permitir eliminar archivos remotamente ○ La solución debe permitir ejecutar script de manera arbitraria ○ la solución debe tener la capacidad de desinstalar programas de manera remota. ○ La solución debe ser capaz de alertar un incidente en un tiempo muy cercano al tiempo real ○ La solución debe llevar el proceso de investigación a minutos. ○ La solución debe tener la capacidad de recolectar una imagen full de la memoria ○ La solución debe colectar información de Bash/Shell históricamente ○ La solución debe tener cobertura sobre TTPs descritos en Mitre Att&ck Framework. ○ La solución debe permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y en proceso de hunting ○ La solución debe permitir la creación de reacciones de manera personalizada para contener y aplicar remediaciones que se ajusten a las necesidades de la organización. ○ La solución debe permitir soportar la creación de script de ejecución en Pyhton, Vbscritp y/o la ejecución de comandos de sistemas operativos de manera remota.	



INFORMACIÓN GENERAL (A)

Bien o Servicio a adquirir	**EDR antivirus**
Referencia (No. Proceso)	**REQ. 020-3466**
Nombre del Proveedor	
Fecha de la Propuesta	

Reporteria y Administracion	○ La solución debe contar con un panel de visualización de métricas de uso de la plataforma ○ La solución debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios. ○ La herramienta debe permitir la vinculación de procesos mediante mecanismos de trace ○ La solución ofertada debe permitir la visualización de información en distintos modelos, desde vistas graficas de los hallazgos hasta el detalle de la información recolectada ○ La herramienta debe permitir la visualización de los hallazgos mediante vistas graficas ○ La herramienta debe permitir visualizar eventos históricos	
Integracion	○ La solución debe poseer integración con una herramienta para la gestión de políticas y despliegue ya sea en la nube o desplegada on-premises ○ La solución ofertada debe poder integrarse con diferentes soluciones de correlación	
Soporte	○ Soporte de 12 meses incluido en la solución	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
Santo Domingo, Distrito Nacional

INFORMACIÓN GENERAL (A)

Bien o Servicio a adquirir	**EDR antivirus**
Referencia (No. Proceso)	**REQ. 020-3466**
Nombre del Proveedor	
Fecha de la Propuesta	

Especialistas	○ Certificacion del fabricante de distribución autorizada ○ Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos. ○ Empresa con técnicos certificados en: CEH, ECIH, ECSA, ENCA	

Firma del Vendedor	Sello de la Empresa

INSTRUCCIONES

En la sección (A) aparece la información general del proceso el tipo de bien o servicio a adquirir y el número de referencia del proceso. En esta sección el oferente deberá registrar, en los campos correspondientes, el nombre de la empresa y la fecha en la que se presenta la propuesta

En la sección (b) se muestra las características o requisitos mínimos solicitados para el bien o servicio

En la sección (c) el oferente deberá marcar con una x las características con las que cuenta el bien o servicio ofertado

Finalmente, el representante firmara las páginas con las que cuenta este formulario y colocara el sello de la empresa en la última página.

Nota: para que pueda ser evaluada su propuesta deberá presentar este formulario debidamente completado y anexarle la cotización correspondiente.

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
AJ 00
10/DIC/20
Santo Domingo, Distrito Nacional