



IMPUESTOS
INTERNOS

Especificaciones Técnicas - DGII-CCC-LPN-2022-0016
Lote 7

“Adquisición Solución Endpoint Privilege Manager (EPM)”.

- Departamento de Seguridad de la Información y Monitoreo



DIRECCIÓN GENERAL DE
IMPUESTOS INTERNOS

1 Especificaciones Técnicas

1.1 Descripción de los Bienes.

Herramientas que administra y guarda trazabilidad de los usuarios con accesos privilegiados en los servidores, equipos de telecomunicaciones y estaciones de trabajo. Esto permitirá proteger la infraestructura y aplicaciones críticas y a la vez mantener la confidencialidad de los datos sensibles.

Ítems	Descripción	Cantidad
1	Licencia para proveer la Administración de permisos de forma granular, control de aplicaciones para equipos de usuarios finales con sistemas operativos tipos Windows y Mac, licencia por equipo, con vigencia de 12 meses.	3,000
2	Licencias para administrador de privilegios de punto final para servidores - SaaS, con vigencia de 12 meses.	900
3	Inicio rápido de administrador de privilegios de punto final	1

1.2 Requisitos

1.2.1 Requerimientos Técnico de la Solución

No.	Descripción
RT01	La solución deberá poder gestionar los privilegios del EndPoint en estaciones de trabajo y servidores Windows y Mac.
RT02	La solución deberá poder integrarse con diferentes fuentes de orígenes confiables de aplicaciones estándar de la organización como: - Distribuidor de Software por ejemplo Microsoft SCCM and McAfee ePolicy Orchestrator (ePO). - Herramienta de actualización y parches - URL qué exactamente? - Ubicación de Red - Paquete de Instalación - A través de Firma Digital de Compañía creadora de Software
RT03	La solución deberá guardar el historial de instalación de aplicaciones y su fuente de origen. Además de mantener un historial de quién, cuando y de dónde llegaron las aplicaciones y archivos para su análisis forense
RT04	La solución deberá poder aplicar políticas para permitir o bloquear dispositivos de almacenamiento portátiles
RT05	La solución deberá proveer servicios propios de análisis de reputación de aplicaciones y la integración con terceros
RT06	La solución no debe requerir el reinicio de los EndPoints para poder iniciar con la gestión de los privilegios y control de aplicaciones
RT07	La solución deberá permitir la personalización de mensajes de notificaciones, incluyendo, logos, texto, URLs, plantillas de correo electrónico y soporte a múltiples idiomas.
RT08	La solución deberá poder aplicar la gestión de privilegios y control de aplicaciones a equipos no conectados al Dominio
RT09	La solución debe permitir habilitar un flujo de aprobación al momento en el cual un usuario quiere ejecutar una aplicación, realizar alguna modificación en el Sistema Operativo que requiera altos privilegios con la intención de ser aprobado por algún administrador de la solución de gestión de accesos.
RT10	La aprobación de las solicitudes de elevación de privilegios deberá poderse aplicar en escenarios donde los equipos EndPoint se encuentren fuera de línea.

No.	Descripción
RT11	La solución deber permitir la activación / desactivación de políticas de restricción de privilegios, basadas en condiciones del ambiente como si el equipo se encuentra dentro o fuera de la red corporativa, horarios y días de la semana.
RT12	La solución deberá permitir la gestión, elevación / bloqueo de DLLs, Scripts y objetos COM
RT13	La solución deberá permitir aplicar restricciones a aplicaciones nuevas y/o desconocidas como por ejemplo restringir su interacción con Internet, a URLs específicas, repositorios compartidos internos, archivos y llaves de registro en el Sistema.
RT14	<p>La solución deberá permitir detectar, alertar y bloquear ataques de robo de credenciales del Endpoint del siguiente tipo:</p> <ul style="list-style-type: none"> - Robo de credenciales de LSASS - Robo de credenciales de SAM - Robo de credenciales de Dominio desde la memoria cache local - Robo de credenciales de desde cuenta de servicio - Robo de credenciales en modo Windows Safe considerando Microsoft's Virtual Secure Module (VSM) deshabilitado - Robo de credenciales en de Windows Credential Manager - Robo de credenciales en base de datos de Active Directory Database (NTDS.DIT) - Robo de secretos en Local Security Authority (LSA) en Windows - Ataque Pass The Hash - Robo de llaves Crypto RSA Machine Keys - Ataque Pass The Ticket - Robo de credenciales en Total Commander - Robo de credenciales de PuTTY - Robo de credenciales de Okta AD Agent Tamper Protection - Robo de credenciales de Git - Robo de credenciales de DbVisualizer - Robo de credenciales en de WinLogon Automation - Robo de credenciales de Composer - Robo de credenciales de Tortoise SVN - Robo de credenciales de VMware Workstation - Robo de credenciales de Open VPN - Robo de credenciales de KeePass - Solicitudes sospechosas de modo de configuración "Always Install Elevated" - Robo de credenciales en Azure CLI
RT15	La solución deberá tener políticas predefinidas para el bloqueo de Ransomware
RT16	La solución deberá permitir la creación de políticas que creen credenciales de usuario falsas y controladas con la intención de monitorearlas de tal forma que los atacantes traten robarlas y utilizarlas como credenciales anzuelo para identificar la traza del ataque.
RT17	La solución deberá permitir la rotación de la contraseña de credenciales privilegiadas en el Endpoint con la intención de que cada cuenta privilegiada en cada EndPoint tenga un valor aleatorio distinto.
RT18	La solución deberá permitir la gestión de privilegios y el control de aplicaciones en equipos Mac considerando aplicar controles de Elevación, Ejecución y Bloqueo de privilegios en: - Configuraciones y Tareas a nivel Sistema Operativo - Control de paquetes de instalación en MacOS - Permitir la ejecución de aplicaciones
RT19	La solución deberá tener la funcionalidad Just in Time (JIT) en Windows y Mac que permita añadir usuarios al grupo de administradores locales del equipo por un periodo limitado de acuerdo con la aprobación del Administrador de la solución de gestión de privilegios o bien de acuerdo con una solicitud del propio usuario final.

No.	Descripción
RT20	La solución debe permitir la integración con soluciones de MFA para hacer una validación MFA cada que el usuario requiera ejecutar alguna aplicación con privilegios elevados.
RT21	El oferente debe tener una matriz de respuesta incidente indicando un esquema de SLA 24x7x365, 2 horas de respuesta máxima para servicios críticos, 4 horas servicios serios, moderados 6 horas en horario de negocio.

1.2.2 Requerimientos al proveedor

Ítem	Descripción
RP01	Tener autorización del fabricante para comercializar la herramienta ofrecida en la República Dominicana.
RP02	Contar con mínimo 2 técnicos certificados por el Fabricante en las tecnologías ofrecidas, con más de 2 años de experiencia.
RP03	Mínimo de 1 cliente en la región que evidencia la comercialización de la solución ofrecida.

1.3 Cronograma de Entrega.

Ítem	Periodo de Entrega
Licencias	Máximo 10 días calendario a partir de firmado el contrato, con vigencia de 1 año, luego de la instalación.
Implementación	Máximo 3 meses luego de la firma del contrato.
Capacitación del Personal	A lo largo de la duración del contrato.


 DIRECCIÓN GENERAL DE
 IMPUESTOS INTERNOS