UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

Dependencia solicitante: Oficina de Tecnologías de la Información y las Comunicaciones

ANEXO 1

1. OBJETO	
Adquirir licencias de las herramientas de ciberseguridad de prevención de pérdida de datos DLP Endpoint Protector y de la Herramienta de Cifrado de Datos y de Archivos Mcafee Complete Data Protection	
2. ESPECIFICACIONES TÉCNICAS	
ITEM	**DESCRIPCIÓN**
1.	**Prevención en la pérdida de Datos (DLP) virtual appliance**
1.1	El contratista debe proveer 80 licencias para la herramienta licenciada de Prevención en la Pérdida de Datos (DLP) **Endpoint Protector virtual appliance** a la UBPD. El contratista debe proporcionar 80 licencias de la herramienta **EndPoint Protector** a la UBPD con sus respectivos agentes para cada dispositivo de usuario final o servidor, la cual se debe integrar al licenciamiento ya existente (660 licencias). Las licencias proporcionadas deben mínimo: - Permitir la definición, consulta, modificación y monitoreo de políticas asociadas a los componentes de Data Loss Prevention. - Permitir un esquema de administración de autenticación y autorización que maneje al menos: usuarios, roles y permisos por rol. - Permitir el monitoreo de políticas por usuario, área y roles asociados a los componentes de Data Loss Prevention. - Contar con la funcionalidad para la implementación de etiquetas de clasificación de acuerdo a las categorías de información establecidas por la entidad, las cuales serán suministradas. - Permitir crear configuraciones por grupo, dominio o máquina.

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

	- Detectar huellas digitales de documentos y asimismo soportar la detección del mismo texto o las porciones de texto en diversos formatos de archivo. - Controlar la información usando tecnologías de fingerprint, que permitan revisar el contenido basado en el tipo de archivos y documentos estructurados y no estructurados, incluso si se cambia la extensión o los atributos del mismo. - Realizar analítica de eventos y permitir analizar la metadata de los archivos para facilitar su organización y análisis. - Contar con una lista de reglas de acción, como mínimo: solo lectura, monitoreo, notificaciones, entre otras. - Permitir establecer y administrar políticas de manera centralizada para uso, transferencia, almacenamiento y disposición final de la información. - El agente debe estar equipado con capacidades que prevengan su alteración como: apagado, desinstalado sin utilizar la clave (password) correspondiente, adicionalmente, la carpeta de instalación deberá estar protegida por el mismo agente y no podrá ser modificado por los usuarios (aun y cuando posean privilegios de administrador). - Permitir enviar notificaciones de violaciones a las políticas. - Registrar y monitorear todo el tráfico que haya sido analizado por la misma con mínimo la siguiente información: Número del evento, Número de Incidente (si se ha violentado alguna de las políticas establecidas), Fecha y Hora del evento, canal por donde fue detectado y analizado el tráfico (email, http, https, etc.), componente de la solución que analizó el tráfico (servidor), componente de la solución que detectó el tráfico (servidor), tamaño del tráfico analizado, tiempo de procesamiento, tiempo de latencia, Origen (usuario/dirección IP), Política que ha sido violada, Destino (hacia donde se dirigía la información), URL de destino (en caso de que aplique), Nombre del equipo desde donde se realizó la acción, entre otros. En el caso de que el incidente se presente en el canal correo electrónico la herramienta debe generar un reporte con mínimo la siguiente información: Dirección de correo del usuario remitente y destinatario, Asunto del correo, Archivos Anexos (si contiene), Contenido/texto del mensaje, Área o dependencia donde trabaja el usuario. - Poder generar reportes mensuales de todos los incidentes y eventos, categorizándolos por diferentes criterios. - Permitir la correlación de eventos, el monitoreo y consulta de los eventos correlacionados.

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

- Controlar y generar alertas del envió de información a servidores de correos públicos como yahoo, Hotmail, gmail, etc.

- El agente se debe poder desplegar desde el directorio activo para lo cual debe estar compilado en .exe estándar o .msi.

- Ser compatible con los diferentes sistemas operativos como: Windows 10, Windows server, Mac OS X, Linux (Centos, Redhat, Fedora, entre otros).

- Poder monitorear y bloquear la transferencia de datos confidenciales enviada por canales de comunicación, aplicaciones online y servicios: Skype, Outlook, Dropbox, Google Drive, etc.

- El agente de la herramienta licenciada debe poder detectar, monitorear, prevenir y controlar el uso de los archivos en dispositivos de almacenamiento como dispositivos USB, HDDs externos, CDs, DVDs, etc, en lo siguientes casos: escribiendo a cualquier dispositivo de almacenamiento extraíble, intentando cargar un archivo utilizando un navegador o alguna otra aplicación de acceso web, intentando cargar datos pegandolos del portapapeles hacia un navegador o cualquier aplicación, intentando cargar datos como archivos o pegados del portapapeles hacia un chat o cliente de mensajería instantánea, intentando cargar o pegar hacia una aplicación peer to peer, intentando cargar o pegar hacia una aplicación FTP, intentando cargar o pegar hacia una aplicación SMTP o IMAP.

- El agente debe contener un identificador único para cada usuario con el fin de prevenir IP Spoofing, asimismo deberá registrar el incidente.

- Estar en capacidad de administrar e identificar fugas de datos externas como mínimo por los siguientes canales o vectores:

    - Navegadores Web
    - Correo Electrónico
    - Impresoras de red e impresoras locales (incluido PDF)
    - Mensajería Instantánea
    - Medios de almacenamiento removibles o extraíbles.
    - Aplicaciones para compartir archivos
    - Capturas de pantalla.
    - Redes sociales.

- Permitir efectuar control de manera que los administradores puedan permitir/negar funcionalidades tales como copiar, pegar, imprimir pantallas, imprimir, acceso a los archivos y acceso a información confidencial.

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

	- Permitir crear políticas para clasificar el contenido sensible por medio de categorización de aplicaciones como; editores, exploradores, confiables y archivadores. - Permitir crear filtros según el tipo de archivo y bloquear los tipos de archivos especificados. Crear filtros también a base de contenido predefinido, personalizado, de expresiones regulares, palabras claves completamente adaptables, las funciones hash, y la coincidencia de patrones. - Permitir guardar los registros de actividad de todos los dispositivos conectados y las transferencias de archivos, proporcionando un historial completo para auditorías y análisis. - El agente debe incluir la habilidad o funcionalidad de descubrir, monitorear y proteger información confidencial sin importar que los usuarios estén o no conectados a una red de datos. - Permitir la integración con el Directorio Activo. - El agente debe permitir parametrizar el intervalo de revisión de conectividad con la consola central. - Reportar el estado de los agentes, con el fin de tomar acciones sobre aquellos agentes que reporten alguna falla o anomalía, el reporte debe incluir mínimo la siguiente información: fecha y hora de inicio del último escaneo ejecutado, fecha y hora de finalización del último escaneo ejecutado, Archivos escaneados, estado de la tarea de descubrimiento de datos, detalles el equipo donde está instalado el agente, dirección IP , usuario autenticado en el equipo, versión del agente, política y perfil que se encuentran aplicados en el agente, resultado de la última sincronización, estado del agente, fecha/hora de la última actualización del perfil, fecha y Hora de la última actualización de la política, versión de la política aplicada. - El agente deben co-existir con otros agentes de endpoint comerciales tales como antivirus, antispyware, firewalls, EDR, entre otros, para Windows 10, Windows server, Mac OS X, Linux. - Contar con consola de administración centralizada (tablero de control), el cual deberá reportar el estado de salud de los diferentes componentes de la solución. - Registrar todos los eventos asociados con la transferencia, modificación, eliminación y guardado de archivos en el computador, en los eventos en los que la información está siendo exfiltrada y hay una política que lo restringe. - Ejercer control y gestionar por el tipo de archivos, ejemplo: .doc,.xls, zip,pdf etc.

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

	- Poder gestionar el control de archivos por su contenido, utilizando tipos de información y combinación de palabras claves a criterio de la entidad. - Permitir o bloquear de forma automática las transferencias de archivos confidenciales entre las estaciones de trabajo. - Contar con un tablero de control gráfico con reporte detallado sobre las diferentes transacciones realizadas por los diferentes perfiles. - Registrar a través de logs de auditoría las acciones ejecutadas por los administradores o usuarios delegados que accedan la consola de administración, se debe registrar mínimo la siguiente información: Número de identificación del evento, Fecha y hora, Usuario, Rol del Usuario, Acción realizada.

Nota: El proveedor deberá incluir con su cotización las fichas técnicas del fabricante de la/s herramienta/s ofertada/s en español o en inglés con traducción simple (la cual deberá ser técnica).

3. OTRAS ESPECIFICACIONES

- La vigencia de las licencias y soporte es de 11 meses.
- El proveedor debe garantizar la instalación e integración de las nuevas licencias con la consola existente.
- El proveedor debe realizar la instalación en la consola actual, para lo cual la UBPD proporcionará los accesos requeridos.
- El periodo de soporte debe ser igual al tiempo de licenciamiento de las nuevas licencias.

INSTALACIÓN

- Acompañar a la UBPD en la instalación y configuración de las nuevas licencias en las consolas existentes, garantizando la integralidad y el correcto funcionamiento y operación. Al presentarse errores en la instalación, configuración o funcionamiento de las herramientas licenciadas, el contratista debe prestar apoyo hasta que queden funcionando correctamente.
- El apoyo que se requiere del proveedor debe ser presencial para la sede central o según lo acordado con el supervisor del contrato.

FUNCIONAMIENTO

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

FICHA TÉCNICA PARA COTIZAR BIENES Y/O SERVICIOS

- El contratista debe prestar soporte sobre las licencias suministradas a la Entidad, para lo cual se debe adelantar mínimo una (1) revisión durante la vigencia de las licencias, según cronograma que se establecerá al inicio del contrato con el supervisor del mismo. En esta visita se llevarán a cabo todas las labores pertenecientes a revisión preventiva (diagnósticos, revisiones técnicas y ajustes necesarios para el correcto funcionamiento de las herramientas licenciadas adquiridas). Este servicio no deberá significar costo alguno para la entidad, para lo cual deberá entregar un informe de la labor realizada.

SOPORTE TÉCNICO

a. El contratista debe atender los requerimientos de Soporte Técnico presencial y/o remoto, en la modalidad 5*12 (cinco días a la semana, doce horas al día), con dos (2) horas máximo de respuesta.

b. El contratista debe incluir en la oferta el soporte directo con el fabricante. Este debe ofrecer canales telefónicos, correo y/o web, y presencial (cuando el incidente así lo requiera).

c. El contratista garantizará tanto el servicio de soporte técnico como las actualizaciones por el término de vigencia de las licencias. El tiempo será contado a partir de la instalación y recibo a satisfacción de las licencias.

d. El contratista debe informar a la entidad los datos de contacto para el soporte e informar los cambios en los mismos.

e. En caso de que se requiera soporte con el fabricante, el contratista garantizará el escalamiento al fabricante, en modalidad 7x24.

f. El contratista debe estar en capacidad técnica de configurar, mantener y brindar el soporte sobre las herramientas licenciadas.