



PERÚ

Ministerio
de la Producción

| OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACION

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 006-2023

“Software para protección contra pérdida de datos”

1. NOMBRE DEL ÁREA

Oficina General de Tecnologías de la Información (OGTI).

2. RESPONSABLES DE LA EVALUACIÓN – CARGO

Giusseppe Jose Contreras Montalvo – Técnico en Infraestructura Tecnológica

3. FECHA

Febrero - 2023

4. JUSTIFICACIÓN

La Oficina General de Tecnologías de la Información, en calidad de órgano responsable de la seguridad informática del Ministerio de la Producción, permite reducir el riesgo de que la información sea atacada o sujeto de filtración, el número de amenazas existentes, tales como extracción no autorizada o espionaje, se incrementa cada día. Adicionalmente, la sofisticación de las técnicas utilizadas por los posibles atacantes incrementa el número y los tipos de riesgos a los que la información está expuesta, especialmente en aquellas estaciones de trabajo que, por sus funciones, se encuentran al acceso del público o a usuarios externos a la Institución.

Esta problemática hace necesaria la adquisición las licencias para protección contra pérdida de datos que permita minimizar los riesgos de extracción no autorizada de la información institucional, independientemente de la tecnología utilizada para ello o del formato o del medio electrónico en el que se encuentre almacenado. Dicha herramienta deberá contar con parámetros de evaluación y monitoreo de la solución, incluyendo la verificación del correcto acceso a los sistemas de información, así como permitir mejoras y cambios futuros en su diseño. Los resultados de estas actividades permiten, incluso, implementar planes de educación dirigidos a los usuarios finales, relacionados a reforzar la cultura de seguridad de la información existente en la institución.

En este contexto, la Oficina General de Tecnologías de la Información manifiesta la necesidad de adquirir e implementar una software de prevención de fuga de información (Data Leak Prevention – DLP), que permita asegurar la información con carácter sensible y confidencial de la Superintendencia.

5. ALTERNATIVAS

Actualmente en el mercado existen diferentes tipos de software correspondiente para protección contra pérdida de datos.

Teniendo en cuenta la calidad y las facilidades que se desea brindar, a continuación, se detallarán las características y atributos técnicos necesarios para la evaluación del software requerido para la institución, con la aplicación de las respectivas métricas.

Se considera conveniente evaluar los siguientes productos a fin de definir una solución:

- RSA Data Loss Prevention Suite



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

- Forcepoint DLP Endpoint

5.1 Consideraciones previas:

Para la determinación del software seleccionado, así como la evaluación técnica, se ha tomado como referencia lo siguiente:

- Información disponible en la página web de cada uno de los fabricantes
- Información disponible en internet
- Evaluaciones similares en otras instituciones del Estado Peruano

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado según los lineamientos establecidos en la "Guía técnica sobre evaluación de software para la administración pública" aprobado por R.M. N° 139-2004-PCM tal como exige el reglamento de la ley N° 28612 -"Ley que norma el uso, adquisición y adecuación del software en la administración pública":

6.1. Propósito de la Evaluación:

Determinar los atributos o características mínimas para el producto final más adecuado para la necesidad de esta Oficina General de Tecnologías de la Información (OGTI), materia de este informe.

6.2. Identificar el tipo de producto

Programa o aplicación que permite la prevención de fuga de información.

6.3. Especificación del Modelo de Calidad.

La evaluación se ha realizado bajo los parámetros establecidos en la RM N° 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

6.4. Selección de métricas

Las métricas fueron identificadas de acuerdo a las funcionalidades que ofrecen los productos señalados en el punto "5. Alternativas" del presente informe. Asimismo, las métricas fueron seleccionadas en base a los requerimientos mínimos necesario para el tipo de programa evaluado.

Cuadro N° 01: Cuadro de atributos

ITEM	ATRIBUTO	DESCRIPCIÓN
1	DLP Endpoint	<ul style="list-style-type: none"> • El software está basado en un agente que se instala en cada una de las estaciones de trabajo que son parte del alcance del software. Mínimamente soporta: Windows 8.1, 10, 11 Windows Server 2012, 2016, 2019 • Detecta y protege la información de datos estructurados, por ejemplo, de Bases de Datos.



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		<ul style="list-style-type: none">• Puede detectar y proteger la información de datos estructurados sin necesidad de contar con una conexión al servidor remoto• Monitorea y bloquea transferencias de archivos en dispositivos móviles, como tabletas y teléfonos inteligentes Android, utilizando el protocolo MTP (también conocido como Windows Portable Devices)• Soporta el monitoreo y el bloqueo de cargas de datos confidenciales (uploads) así como actividades de sincronización de archivos a soluciones de almacenamiento personal o corporativo en la nube, tales como DropBox y Google Drive• Incluye conocimiento sobre la aplicación y control de manera que los administradores puedan permitir/negar funcionalidades tales como copiar, pegar, imprimir pantallas, imprimir, y acceso a los archivos en base a la aplicación y si está accediendo a información confidencial.• Incluye una lista de aplicaciones predefinidas y de categorías de aplicaciones las cuales el administrador podrá reconfigurar para adicionar aplicaciones customizadas tales como P2P, IM, Procesadores de texto, clientes de correo, etc.• Coexiste con otros agentes de endpoint tales como antivirus, antispyware y firewalls.• Solamente los administradores utilizando una clave (password) única generado en el servidor mediante su llave privada, podrá cambiar manualmente la configuración del agente de punto final.• El agente endpoint tiene la capacidad de encriptar los datos en medios removibles tales como dispositivos de USB de medios masivos. Podrá de forma automática permitir el traslado de información específica de forma encriptada.
2	Consola central, logs y Manejo de Incidentes de la Solución	<ul style="list-style-type: none">• La consola web de administración centralizada, reporta el estado de salud de los diferentes componentes de la solución, dentro de los componentes reportados incluye:<ul style="list-style-type: none">a. Reporte del Sistema: Sistema operativo, versión de sistema operativo, zona horaria, numero de procesadores disponibles y espacio en disco disponible.b. Porcentaje de utilización de CPUc. Porcentaje de utilización de memoria RAM



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		<ul style="list-style-type: none">d. Servidor de Administrador de Punto final: Carga del servidor de punto final, numero de requerimientos generados por los agentes de punto final.e. Políticas: Número de incidentes de políticas relacionadas con la utilización de información, Numero de incidentes generados por las políticas de descubrimiento de información.f. Escaneo/Huella Digital de datos: Numero de archivos sobre los cuales se ha realizado escaneo o toma de huella digital de datos, Numero de celdas (en bases de datos) archivos sobre los cuales se ha realizado escaneo o toma de huella digital de datos. <ul style="list-style-type: none">• Cuenta con un log conteniendo información de todo el tráfico que haya sido analizado por la solución bien sea que este haya o no generados incidentes de seguridad, esto con el fin de tener trazabilidad del tráfico siendo monitoreado por el software.• Cuenta con un log de auditoría donde se registren las acciones ejecutas por los administradores o usuarios delegados que accedan la consola de administración.• Los incidentes relacionados con violaciones a las políticas de seguridad deberán ser reportados en la consola web de administración centralizada, dichos incidentes deberán tener campos que faciliten la interpretación de los mismos con el fin de ejecutar las acciones requeridas, dentro de los campos requeridos y presentes en la herramienta deberán estar:<ul style="list-style-type: none">1. Número de registro del incidente (ID)2. Fecha y hora del incidente3. Origen (usuario/dirección IP)4. Política que ha sido violada.5. Canal donde se ha genera el incidente (email, http, https, etc)6. Destino (hacia donde se dirigía la información)7. Severidad8. Acción tomada9. Tamaño de la información10. Estado del incidente (nuevo, en investigación, cerrado)11. Servidor que analizo la información-trafico12. Servidor que detecto la información-trafico13. Usuario que tiene asignado el incidente (para investigación o sustentación)
--	--	---



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

3	Reportes DLP y Manejo centralizado de Incidentes	<ul style="list-style-type: none"> • El módulo de reportes es centralizado para todas las coberturas de: Discovery y DLP del Endpoint. • Contiene reportes favoritos y reportes estándares tipo ejecutivo, que contiene como mínimo 30 reportes predefinidos relacionados con las violaciones a las políticas de seguridad y 30 reportes predefinidos relacionados con las políticas de descubrimiento de información. • Tiene un flujo de trabajo y reportes basados en web, en administración por roles y controles, automáticos, basados en reglas, por incidentes y tendencias. • Deja registro, logs y archivos forenses del uso de los archivos protegidos del sistema y que pueda auditar los cambios de eventos, así como cambios en la política. • Los reportes de incidentes incluyen una indicación clara de cómo se llevó a cabo la transmisión o el archivo violaron la política (no solamente que indique que política fue violada) que incluya una clara identificación de que contenido motivó la activación de la regla o política. • Los incidentes son asegurados para prevenir su edición y/o borrado.
---	--	--

En tal sentido, en el Cuadro N° 02 se muestra el comparativo de métricas de las alternativas de software indicados en el numeral 5:

Cuadro N° 02: Cuadro comparativo técnico

ITEM	ATRIBUTO	Puntaje Máximo	RSA Data Loss Prevention Suite	Forcepoint DLP Endpoint
1	DLP Endpoint	30	25	25
2	Consola central, logs y Manejo de Incidentes de la Solución	40	35	40
3	Reportes DLP y Manejo centralizado de Incidentes	30	25	30
TOTAL		100	85	95

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Se comparan las características técnicas de las alternativas evaluadas para los productos de software seleccionados, para lo cual se ha tomado como base la “Parte 3: Proceso de Evaluación de Software” de la Guía de Evaluación de Software, aprobada por Resolución Ministerial N°139-2004-PCM.



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

7.1. Soporte y mantenimiento externo

El fabricante o proveedor de los productos ofertados debe poseer oficina de representación en Perú, así como personal de soporte técnico que garantice la adecuada y oportuna prestación de la garantía y de servicios. Este servicio debe ser 8x5.

7.2. Costo

No se ha realizado un Análisis de Costos Beneficio, por cuanto en el presente Informe Técnico Previo de Evaluación de Software, sólo se desea establecer el software más adecuado técnicamente de acuerdo al puntaje obtenido en la Evaluación Técnica de las Métricas.

La evaluación formal del análisis de costos se realizará durante el proceso de oficial de compras, según la ley de contrataciones y adquisiciones del estado N° 30225.

8. CONCLUSIONES Y RECOMENDACIONES:

Las conclusiones del presente informe son las siguientes:

- La información del Ministerio de la Producción requiere ser protegida contra intentos de extracción no autorizada y ataques de índole informático, independientemente del formato electrónico en el que se encuentre almacenada.
- La implementación de una solución de prevención de fuga de información (Data Leak Prevention – DLP) permitirá implementar políticas flexibles para minimizar el riesgo de extracción no autorizada de la información de la Institución.
- Los nuevos proyectos a desarrollar por la Oficina General de Tecnologías de la Información durante los próximos meses requieren de una plataforma segura, para garantizar la integridad de la información procesada y almacenada en la misma.

Por lo expuesto, se requiere la adquisición de licencia de software para protección contra pérdida de datos (Data Leak Prevention – DLP) para la Institución, con su respectivo servicio de soporte técnico, por un período de doce (12) meses.

9. FIRMA

Giusseppe Jose Contreras Montalvo
Oficina General de Tecnologías de la Información