FORTHCOMING 65U35-05-24-01

ARQUITECTURA PROPIA PARA PREVENIR LA FUGA DE INFORMACIÓN EN EL PUNTO FINAL.

Medaimy Rivera Valiente y Yannier Durades Fernández, Esp.
Instituto de Criptografía [1]

ABSTRACT
The topic of information security holds great importance for any organization. How can one know if the information is secure? Issues like these are a concern for many companies. The technology of Data Leak Prevention has come to solve these situations in large part. Cuba has not been exempt from technological development, as well as the risks derived from this new landscape. In this sense, applications have been deployed in isolation, which have not been sufficient. This article defends the hypothesis given that information leakage can occur at the end point, through a storage device, email, among others; in the network channel, through different services, and in resting data through the human factor, accidentally or maliciously, applying a proprietary technology that establishes control measures over processing, storage, and transmission; focused on devices, the network, and content, it will be possible to prevent digital information leakage at the end point and achieve levels of security and protection.

KEYWORDS: sensitive data, loss information

MSC: 68U35

RESUMEN
El tema de la seguridad de la información posee gran importancia para cualquier organización. ¿Cómo saber si la información se encuentra segura? Cuestiones como estas constituyen la preocupación de muchas empresas. La tecnología de Prevención de Fuga de Datos, ha venido a solucionar en gran parte estas situaciones. Cuba no ha estado exenta del desarrollo tecnológico, así como a los riesgos derivados de este nuevo panorama. En tal sentido, se han desplegado de forma aislada aplicaciones, las cuales no han sido suficientes. El presente artículo defiende la hipótesis dado que la fuga de información puede ocurrir en el punto final, a través de un dispositivo de almacenamiento, correo electrónico, entre otros; en el canal de red, a través de diferentes servicios, y en los datos en reposo mediante del factor humano, de manera accidental o mal intencionada, aplicando una tecnología propia que establece medidas de control sobre el procesamiento, almacenamiento y trasmisión; enfocado a los dispositivos, la red y el contenido, será posible prevenir la fuga de información digital en el punto final y alcanzar niveles de seguridad y protección.

PALABRAS CLAVES: datos sensibles, fuga de información

1. INTRODUCCIÓN

"Las empresas hoy en día enfrentan graves consecuencias, debido a las malas prácticas de sus empleados frente a los datos corporativos, lo que pone en riesgo la información confidencial y propietaria de las organizaciones. Los dispositivos de almacenamiento extraíbles, representan una seria amenaza, convirtiéndose en elementos claves a tener en cuenta en el panorama de la seguridad actual. La información se mueve más allá del perímetro empresarial y la capacidad de almacenamiento crece mientras que el tamaño de los dispositivos es cada vez menor. Cualquier persona con un dispositivo removible, puede descargar datos sensibles y exponer información de alto valor para una empresa." (Daniel Martín Santos, 2013)
Por otra parte *"los atacantes intentan apoderarse o vulnerar los dispositivos de los puntos finales con regularidad. Pueden tener un determinado número de objetivos en mente para hacerlo: infectar el dispositivo con malware, rastrear la actividad del usuario en el dispositivo, pedir un rescate por el dispositivo, utilizar el dispositivo como punto de partida para moverse lateralmente y poner en riesgo otros dispositivos de la red, entre otros. En un contexto empresarial, los atacantes suelen tener como objetivo los puntos finales, porque un punto final en riesgo puede ser un punto de entrada a una red de la empresa que, de otro modo, sería segura. Puede que un atacante no pueda atravesar el firewall de la empresa, pero el portátil de un empleado podría ser un objetivo más fácil."* (CLODFLARE, 2020).
Intel define como *"puntos finales aquellos dispositivos que los trabajadores utilizan cada vez más para ser productivos, desde equipos de sobremesa hasta portátiles, tabletas y Smartphone."*

[1] medaimy@gmail.com

El presente trabajo, se centra en los equipos de sobremesa y portátiles que se conectan a la organización, trazando como estrategia de seguridad el desarrollo de una tecnología que ayude a proteger los puntos finales que se conectan a la red.
El nuevo escenario que se presenta ante los administradores de TI (Tecnología de la Información) introduce una mayor complejidad que requiere de ellos asumir este desafío con el apoyo de soluciones innovadoras que faciliten la protección de la información a través de una gestión y control eficaces. Esta tecnología, conocida como Prevención de Fuga de Datos o DLP (Data Leak Prevention), se está convirtiendo en un componente crucial dentro de las organizaciones. La definición común de DLP es una estrategia diseñada para prevenir que los usuarios finales puedan enviar o extraer información sensible fuera de la red corporativa. La tendencia global está orientada hacia el desarrollo y diseño de estas soluciones, impulsada principalmente por el avance tecnológico. Cuba, con el objetivo de garantizar la independencia y soberanía tecnológica, se esfuerza en diseñar una tecnología DLP propia.

2. MARCO TEÓRICO CONCEPTUAL

Antecedentes

En enero de 2004 fue construida la primera plataforma para la detección de fuga de información confidencial, llamada Vontu, perteneciente a la empresa estadounidense Vontu fundada en el año 2001. Dicha empresa fue adquirida posteriormente por Symantec, con lo cual se produjo un nivel de maduración cada vez más importante. Este *"fue el primer producto que cambió la percepción acerca de la protección de la información, ya que no se centraba en los patrones tradicionales considerados hasta el momento, que consistían en identificar los servicios que se podían publicar y los que se restringían (firewalls) o en patrones de comportamiento correlacionados para detectar incidentes que atentaran contra la seguridad de la información (IDS e IPS). El concepto se centraba en el contenido de la información sensible con el fin de prevenir que dicha información pudiera salir de la infraestructura de la organización."* (Martínez, 2015)

"Posteriormente surgieron otros productos relacionados con la prevención de fugas de información, como Provilla, la cual fue adquirida por la empresa Trend Micro y redefinida como DLP "TrenMicro LeakProof" y Onigma de quien actualmente es propietario McAfee llamada actualmente "McAfee Data Loss Prevention". (Martínez, 2015)

En resumen, los productos DLP han ido evolucionando progresivamente convirtiéndose en un pilar importante en la industria de la seguridad informática, debido a que contribuyen sustancialmente a disminuir o a prevenir las fugas de datos a través de diferentes vectores o salidas (Correo, USB, unidades de red, móviles, almacenamiento en la nube, internet, impresión, capturas de imagen de pantalla o "Print Screen", mensajería instantánea, entre otros)

Definición

Prevención de Fuga de Datos o DLP: es el término más estandarizado para hablar de esta tecnología, pero en ocasiones lleva a confusión, porque también se emplean los siguientes en inglés para referirse, esencialmente, a lo mismo o a una parte de esta tecnología: Data Leak Prevention, Data Leak Protection, Data Loss Protection, Information Leak Detection and Prevention (ILDP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC), Extrusion Prevention System, Data Exfiltration, Data Leakage Protection, Enterprise DLP, EDLP y IDLP integrados.

(Martínez, 2015) lo define como: *"conjunto de herramientas destinadas a evitar el envío de información sensible, confidencial o crítica, fuera del entorno de la organización, adicionalmente describe las soluciones tecnológicas que detectan, monitorean y evitan que la información clasificada como confidencial sea transmitida y usada de forma indebida hacia el exterior de las organizaciones.*

Esto se logra a través de la inspección de contenidos, el análisis del contexto de seguridad de los flujos de información, es decir propietarios, destinatarios, custodios, contexto de la información, propósitos de transmisión, medios y tiempos de comunicación."

Pero de una forma más simple el autor de la presente investigación lo define como tecnología o conjunto de tecnologías que identifica, monitoriza y protege los datos sensibles en uso, movimiento y en reposo de una organización. En el presente trabajo se considera datos sensibles: aquella información que, al ser revelada, expuesta puede causar de alguna manera algún daño o perjuicio para una organización, empresa o entidad.

Funcionamiento

"La tecnología DLP ofrece un conjunto soluciones unificadas para detectar, supervisar y proteger la información confidencial sin importar donde se almacene o como se utilice:

- *Detecta información sensible localizándola en su medio de almacenamiento, creando un inventario de datos, y sus propietarios con el fin de administrar y simplificar el tratamiento de la información asociada.*
- *Supervisa el modo en que se utiliza la información confidencial por parte de los usuarios, los procesos organizacionales involucrados y su visibilidad.*
- *Protege la información por medio de la aplicación automatizada de políticas de seguridad con el fin de proteger los datos de manera anticipada y evitar las posibles fugas de información.*
- *Administra políticas globales de fuga de datos en toda la organización, identifica incidentes de seguridad y elabora informes de forma centralizada por medio de una plataforma unificada y centralizada."* (Martínez, 2015)

En otras palabras, el autor de la presente investigación describe el funcionamiento de la tecnología DLP como un conjunto de soluciones informáticas o software que detectan y supervisan información confidencial ya sea en descanso, en tránsito o en uso para garantizar su protección sin importar donde se almacene o como se utilice. Detección-Supervisión-Protección.
En la Figura 1, se puede observar el funcionamiento básico de una solución DLP.

Figura. 1: Funcionamiento de un DLP tomado de: https://revista.seguridad.unam.mx/numero25/dlp-tecnolog-para-la-prevenci-n-de-la-fuga-de-informaci-n

Tipos

Existen diferentes tipos de soluciones DLP, cada una orientada a un propósito específico, pero con el mismo objetivo: prevenir la pérdida de datos. De acuerdo con (ostec, 2019) los tipos de DLP son:

"Network DLP: Las soluciones de Prevención de Pérdida de Datos de Red, se encuentran disponibles en las plataformas de software o hardware, integradas a los puntos de salida de datos de la red corporativa. Una vez instalada, la solución monitorea, rastrea y genera informes de todos los datos de tráfico en la red.

Este es el tipo de DLP ideal para explorar todo el contenido que pasa por los puertos y protocolos de la organización, pues proporciona informes importantes que ayudan a garantizar la seguridad de la información, tales como: qué datos están siendo utilizados, por quién están siendo accedidos y hacia dónde van. La información recopilada se guarda en una base de datos que se puede administrar fácilmente.

Storage DLP: Las soluciones de Prevención de Pérdida de Datos de Almacenamiento, son un sistema que permite ver archivos confidenciales almacenados y compartidos por quienes tienen acceso a la red corporativa, de tal forma que permite la identificación de puntos sensibles y con ello prevenir la filtración de información.

Generalmente, suele emplearse como una buena solución para controlar datos almacenados en la nube, de forma tal que se identifiquen cuáles son los datos que se almacenan y comparten, así como cuanta de esta información se considera sigilosas y pueden estar en riesgo de fugas.

Endpoint DLP: Las soluciones de Prevención de Pérdida de Datos de Estaciones o Puntos Finales son aquellas que se instalan en todas las estaciones de trabajo y dispositivos utilizados por los empleados de la empresa para supervisar e impedir la salida de datos sensibles por dispositivos extraíbles, aplicaciones para compartir o áreas de transferencia.
Con la proliferación de dispositivos de almacenamiento externo como memorias USB o discos duros portátiles, por ejemplo, el riesgo de seguridad por filtración de datos de forma accidental o intencional aumenta, y para evitarlo, este tipo de solución colabora para prevenir la pérdida de datos a través de dispositivos extraíbles."
El autor considera que lo más importante es entender que los tipos de datos requieren estrategias y muchas veces soluciones diferentes para garantizar su protección. Para datos en uso, es necesario prevenir la evasión a través de copia en medios externos y similares. Para datos en tránsito, el DLP debe tener la capacidad de analizar los eventos de red en línea y los datos en reposo, la solución debe ser capaz de supervisar puntos sensibles de datos a los que no se debe tener acceso, copiar o cambiar.

Arquitectura

"Las tecnologías DLP son complejas. Requieren recursos de muchas áreas dispares: WEB, correo electrónico, bases de datos, redes, seguridad, infraestructura, almacenamiento, entre otros. Suelen ser muy difíciles de implementar, configurar y administrar. Requieren de varios dispositivos y software para ejecutar la solución completa. Estos podrían incluir dispositivos (virtuales o reales) y servidores." (GEEKFLARE, 2021)

La arquitectura DLP está formada por varias capas o módulos, lo que se podría llamar una arquitectura N-Capas, facilitando al desarrollador la creación de módulos independientes, que permiten la integración entre los ya desarrollados. Además, esta distribución permite acceder a las capas o módulos inferiores mediante el uso de bibliotecas; de esta forma el desarrollador no tiene que programar a bajo nivel las funcionalidades necesarias para que una aplicación haga uso de los componentes de hardware. Ver Figura 2 Arquitectura DLP.

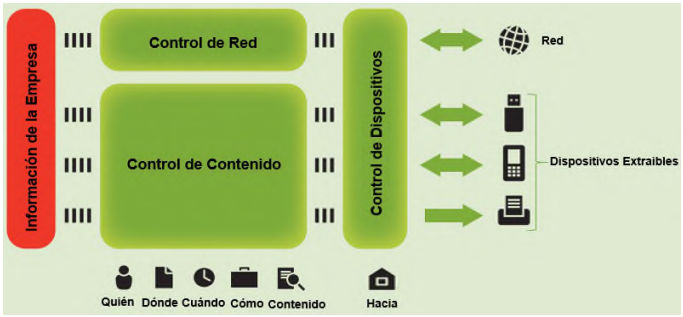

Figura. 2: Arquitectura DLP

En el control de contenido se filtra el contenido de archivos transferidos hacia y desde medios extraíbles y los dispositivos Plug-n-Play, así como de varios objetos de datos de comunicaciones de red que se reconstruyen y pasan por el control de contenido.

En el control de dispositivos se incluye todo un conjunto de controles contextuales junto con el registro de eventos. Estos incluyen los dispositivos periféricos, puertos, Smartphone[2], dispositivos de transferencia de medios (MTP)[3], el portapapeles y la impresión de documentos.

En el control de red se ofrecen funciones de control contextuales sobre las comunicaciones de red como web, correo electrónico, detección de protocolo, control selectivo, mensaje y proporcionar la inspección profunda de paquetes, así como el registro de eventos, alertas y sombreado de datos.

Fabricantes

Un creciente número de grandes empresas están implementando soluciones de seguridad, centradas en el comportamiento del usuario para ofrecer una protección de la propiedad intelectual y visibilidad de datos críticos estén donde estén.

De acuerdo a la información publicada por Gartner, las principales empresas líderes fabricantes de tecnologías DLP en el año 2020 fueron: Symantec, Forcepoint, Digital Guardian e Intel Security. (Gartner Inc, 2021)

[2]Smartphone: Teléfono inteligente
[3]MTP: Media Transfer Protocol por sus siglas en inglés

"El estudio identifica las empresas más importantes, utilizando parámetros de categorización basados en el posicionamiento, la estrategia de mercado y la eficacia en el desempeño de los objetivos." (Gartner Inc, 2021)
La presente investigación realiza un análisis y evaluación de las tecnologías DLP líderes del mercado con el objetivo de crear una base de conocimientos y poder dar solución al problema planteado.

Diagnóstico de la situación

Gracias al estudio realizado el autor del trabajo sintetiza que, la tecnología DLP ofrece un grupo de soluciones unificadas para detectar, supervisar y proteger la información confidencial dentro de una organización; donde primero hay que identificar cuáles son los datos críticos o sensibles dentro de su organización para así poder detectarlos donde sea que se encuentren almacenados. Sin embargo, surgen interrogantes como:

- ✓ ¿Qué sucede cuando no se identifican correctamente los datos críticos de una entidad?
- ✓ ¿Los datos críticos para una fábrica de cemento serían los mismos para una entidad de seguridad nacional?

De acuerdo con (Dast, 2020) *"para implementar con éxito el software DLP corporativo, se necesita involucrar activamente a personal de todos los niveles de gestión en la creación de las reglas de negocio para las etiquetas. Una vez que las herramientas de software DLP han sido implementadas, un usuario final que intente, de manera accidental o malintencionada, revelar información confidencial que ha sido etiquetada, será repudiado."*

Respondiendo a las interrogantes antes planteadas los datos que para una entidad son valiosos para otra, en un contexto completamente diferente no son considerados igual de valiosos, y que con una errónea clasificación de los datos se puede comprometer el éxito de la tecnología DLP, sin embargo el autor del trabajo considera que existe otra forma de resolver esta problemática, la presente investigación propone una tecnología DLP que a diferencia de las estudiadas aplica una protección desde una perspectiva organizacional que será abordada con mayor profundidad más adelante.
Por otra parte, el autor realiza una comparación entre las tecnologías de prevención de fuga de información líderes del mercado, para ello se establecen los siguientes criterios: ver tabla 1.

Criterios	**Symantec**	**ForcePoint**	**Digital Guardian**	**Intel Security**
Plataforma	Apple Mac OS X, Microsoft Windows (7,8,8.1, Server 2003, 2008), Citrix XenApp y XenDesktop, Microsoft Hyper -V	Mac OS, Microsoft Windows, Linux	Mac OS, Microsoft Windows, Linux	Mac OS, Microsoft Windows (Vista, XP, 7,8,10, Server 2003 y 2008), Linux
Subsistemas	DLP Enforce, IT Analytic, Symantec DLP for Cloud Storage, Cloud Prevent for Microsoft Office 365, Symantec DLP Endpoint Discovery Endpoint Prevent, Symantec DLP Network Discover, Network Protect, Data Insight, Symantec DLP Network Monitor, Network Prevent for Email y Network Prevent for WEB.	ForcePoint DLP-endpoint, ForcePoint DLP- cloud aplications, ForcePoint DLP-discover, ForcePoint DLP-network.	Endpoint DLP, Endpoint Detection and Response, Network DLP, Cloud Data Protection.	McAfee DLP Endpoint, McAfee® ePO DLP Incident Manager, McAfee® Network DLP.
Uso de Licencia	Si	Si	Si	Si
Código abierto	No	No	No	No
Técnicas de control de Contenido	Palabras claves, expresiones regulares, propiedades del archivo, tipos de archivos, reconocimiento de texto en archivos gráficos (OCR).	Palabras claves, expresiones regulares, propiedades del archivo, tipos de archivos, reconocimiento de texto en archivos	Palabras clave, expresiones regulares, tipos de archivos, ubicación de origen o de destino, reconocimiento de texto en archivos	Palabras claves, expresiones regulares, tipos de archivos, ubicación de origen o de destino, reconocimiento de texto en archivos

		gráficos (OCR).	gráficos (OCR).	gráficos (OCR).
Protocolos que controla	HTTP, HTTPS, FTP, SMTP, IM, NNTP, protocolos personalizados de puerto específico y protocolo de internet versión 6 (IPv6).	HTTP, HTTPS, ICAP, FTP	HTTP, HTTPS, FTP, SMTP, SSL	IMAP, POP3, HTTP, LDAP, Telnet, FTP, IRC, SMB
Escenario donde se sitúa el control del red	En un determinado punto de la red.	En un determinado punto de la red.	En un determinado punto de la red.	En un determinado punto de la red.
Dispositivos que controla	Tarjetas USB, MTP, CF e SD, eSATA y FireWire, impresoras.	Dispositivos USB, medios extraíbles, impresoras.	Dispositivos USB, medios extraíbles, impresoras.	Unidades USB, smartphones, dispositivos Bluetooth, impresoras y demás medios extraíbles.
Control de Escritorios Virtuales	Citrix, Microsoft Hyper-V y VMware	No	No	No
Control de Servicios en la Nube	Box, Dropbox, Google Drive y Microsoft OneDrive	Microsoft Office 365 y Box	Microsoft Office 365	-
Protección de Almacenamiento	Cifrado de archivos y carpetas, cifrado de dispositivos enteros e integración con herramientas de cifrado Apple FileVault y Microsoft BitLocker.	Cifrado de archivos y carpetas.	Cifrado de archivos y carpetas.	Cifrado de archivos y carpetas, cifrado de dispositivos enteros e integración con herramientas de cifrado Apple FileVault y Microsoft BitLocker.

Con el análisis de la tabla anterior se pudo arribar a las siguientes conclusiones:

✓ La arquitectura inicial de la tecnología DLP ha evolucionado. Como resultado han desarrollado un gran cúmulo de soluciones, subsistemas, o componentes que cubren el punto final, la red y el contenido. Por ejemplo, Symantec tiene más de 10 subsistemas, mientras Digital Guardian solo posee 4 componentes en función de los mismos objetivos.

✓ La evolución de la tecnología DLP demuestra que el control va mucho más allá del perímetro de red, siendo necesario un control de los servicios en la nube.

✓ Todas requieren de licencia para su uso y son de empresas norteamericanas lo cual constituye un problema para la adquisición del producto debido al bloqueo financiero de EEUU contra Cuba, lo que conlleva al desarrollo de una tecnología propia.

✓ Al ser de código propietario y tomando en cuenta que las propuestas comerciales cuyos diseños se basan en los estándares establecidos, generalmente disponen de puertas traseras, que son explotadas por los servicios especiales, el autor de la investigación considera que es necesario desarrollar una tecnología DLP propia.

✓ Las tecnologías analizadas sitúan el componente para el control de red en puntos estratégicos con el objetivo de evitar la fuga de información de la red interna hacia la red externa, el autor del presente trabajo considera que esta funcionalidad no permite evitar la propagación de virus, fuga de información desde el punto final y una degradación del rendimiento en el tráfico de la red interna, considerando que debe ser evaluada la ubicación del componente control de red.

✓ Realizan el cifrado de dispositivos enteros e integración con herramientas de cifrado como Apple FileVault y Microsoft BitLocker, donde el usuario establece la contraseña o certificado para el cifrado del medio, el autor del presente trabajo considera que esta funcionalidad no permite evitar la fuga de información a través de los empleados mal intencionados, debido a que los mismos poseen los mecanismos para acceder a la información en cualquier lugar fuera del entorno, identificándose este último como la debilidad principal de las tecnologías estudiadas que dan paso a un nuevo enfoque.

3. RESULTADOS Y DISCUSIÓN

Como se ha podido observar, existen antecedentes que dan solución al problema de la fuga de información digital, particularmente tecnologías consolidadas y probadas con tiempo de explotación que proporcionan visibilidad y un control completo de todos los canales en los que puede producirse la fuga de datos: aplicaciones en la nube, en el punto final, repositorios de datos, correos electrónicos y comunicaciones por Internet.

El criterio y enfoque seguido anteriormente son resultados de la investigación y experiencias de las empresas líderes de Ciberseguridad, aun así, hay elementos claves que cuestionan su empleo, que deben ser tomados en cuenta:

- Son de código propietario, lo que se traduce como una caja negra que puede contener puertas traseras y no deben ser empleadas tecnologías de seguridad de terceros.
- Son capaces de detectar, monitorear y proteger información sensible. Sin embargo, también se puede observar que se ha identificado que el éxito de éstas depende en gran medida la forma de su implementación práctica, donde juega un rol esencial las medidas técnicas organizativas de su despliegue y puesta en marcha.
- Realizan el cifrado del volumen completo y se integran con herramientas, como Apple FileVault y Microsoft BitLocker, donde el usuario establece la contraseña o certificado para el cifrado de manera aislada, considerándose que esta funcionalidad no permite evitar la fuga de información a través de los empleados internos mal intencionado.

Los elementos antes mencionados y los problemas identificados al inicio de la investigación evidencian la necesidad e importancia de la conceptualización y diseño de una tecnología DLP propia, capaz de prevenir la fuga de información. Capaz de detectar las transmisiones de datos sensibles y prevenir su fuga a través del monitoreo, detección y bloqueo mientras está en uso (acciones de extremos/Control de Dispositivos), en movimiento (tráfico de red/ Control de Red), y en reposo (almacenamiento de datos/Control de Contenido). La fuga de información puede ocurrir en el punto final a través de un dispositivo de almacenamiento, correo electrónico, entre otros o en el canal de red, a través de diferentes protocolos de red. Para el caso de los datos en reposo, la fuga de información puede estar dada, a través del factor humano, por el acceso, accidental o mal intencionado, a los puntos finales, incluyendo el Servidor. Ver Figura 3. Puntos claves de fuga de información.

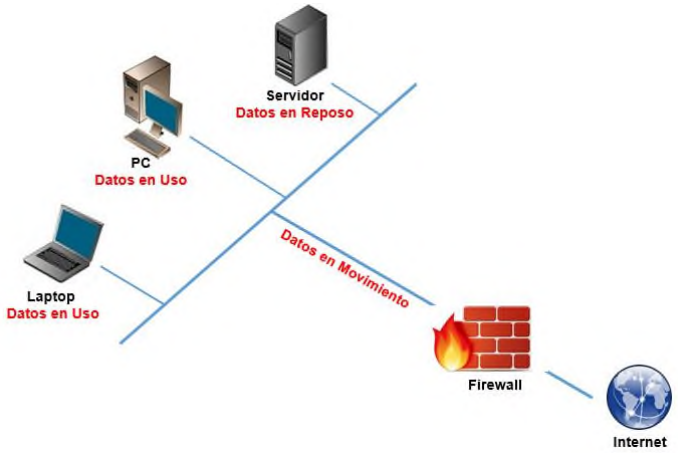

Figura 3: Puntos claves de fuga de información.

Basado en los diseños estudiados, una vez identificado los puntos claves donde puede ocurrir la fuga de información, se propone un diseño modular, que consta de tres componentes: Control de Contenido, Control de Red y Control de Dispositivos. Ver Figura 4. Componentes DLP.

Figura 4: Componentes DLP.

Control de Contenido:

- ✓ Descubrir: Filtrar y clasificar el contenido de los archivos, en uso, en movimiento y en reposo.
- ✓ Proteger: Aplicar protección a los archivos de acuerdo al contenido.

Control de Red:

- ✓ Detectar: Transmisión de datos confidenciales enviados a través de un rango de protocolos. Se propone monitorizar el tráfico desde el punto final y en cualquier punto de la red.
- ✓ Proteger (Correo): Bloquear o redirigir el correo a puertas de enlace de cifrado para un envío seguro.
- ✓ Proteger (Web): Bloquear o remover los datos de los mensajes web.

Control de Dispositivos:

- ✓ Controlar: Permitir o denegar el acceso de dispositivos a la PC, y controlar las operaciones de lectura y escritura desde (y hacia) los dispositivos de almacenamiento extraíbles.
- ✓ Proteger: Aplicar protección de almacenamiento a los dispositivos de almacenamiento USB.

En los sistemas de almacenamiento, los principales problemas, relacionados con robo o pérdida de dispositivos y que propician fuga de información por su portabilidad y movilidad, se presentan con los dispositivos USB. Por lo tanto, los dispositivos de almacenamientos USB, son el principal destino hacia el cual se orienta la protección. En este sentido el presente trabajo propone un **nuevo enfoque: Cifrado propio donde el usuario desconoce la contraseña empleada para el cifrado de los dispositivos, lo cual constituye la principal novedad científica de la investigación**. Ver figura 5: Protección USB desde un nuevo enfoque.

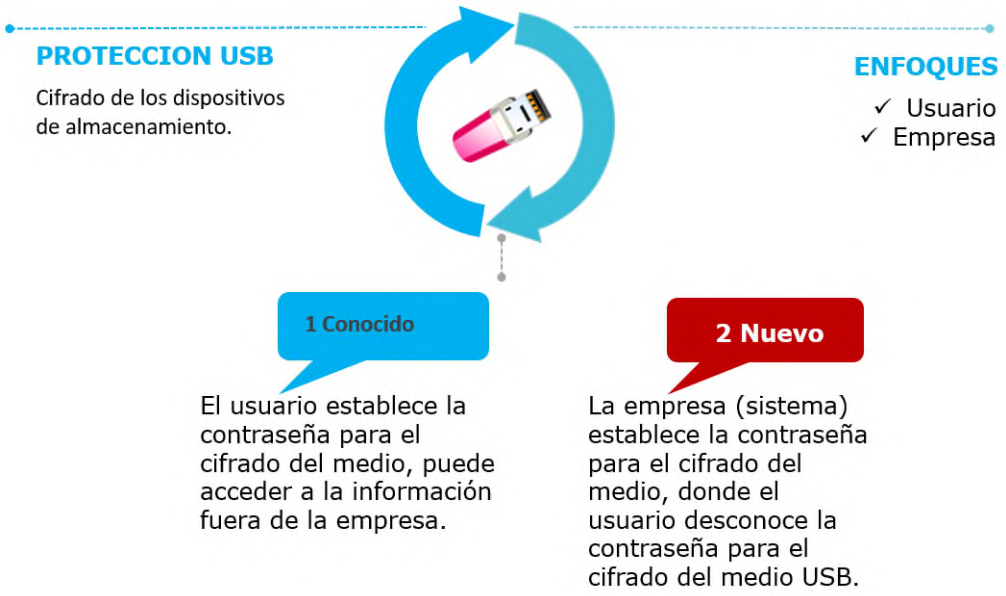

Figura 5: Protección USB desde un nuevo enfoque.

Se propone transformar un dispositivo de almacenamiento USB en un volumen cifrado, aplicando un formato lógico al dispositivo, que consiste en crear un contenedor cifrado en el dispositivo.
Modelos de Comportamiento – Procesamiento de Datos: Muestran cómo los datos son procesados. Para prevenir la fuga de datos en uso, movimiento y en reposo se propone el siguiente modelo:
Modelo DLP para datos en uso y datos en movimiento:
Si los DATOS fluyen de FUENTE a DESTINO a través del CANAL, el sistema toma ACCIONES, ver Figura 6.

- DATOS especifica información sensible.
- FUENTE puede ser un usuario, un punto final, dirección de un correo electrónico, o un grupo de ellos.
- DESTINO puede ser un punto final, una dirección de correo electrónico, o un grupo de ellos, o simplemente el mundo externo
- CANAL indica el canal de fuga de datos, como USB, correo electrónico, protocolos de red, entre otros.
- ACCIÓN es la acción que debe tomar DLP cuando ocurre un incidente

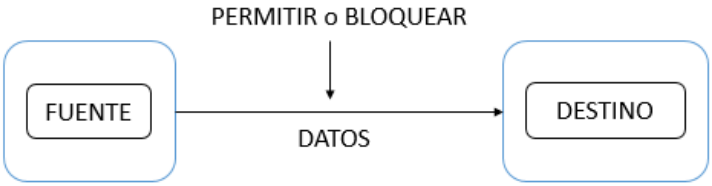

Figura 6: DLP para datos en uso y datos en movimientos.

Desde el punto de vista funcional de cada uno de los componentes identificados en el diseño (control de red y control de dispositivos) para describir el modelo DLP para datos en uso y datos en movimiento se puede observar la Figura 7.

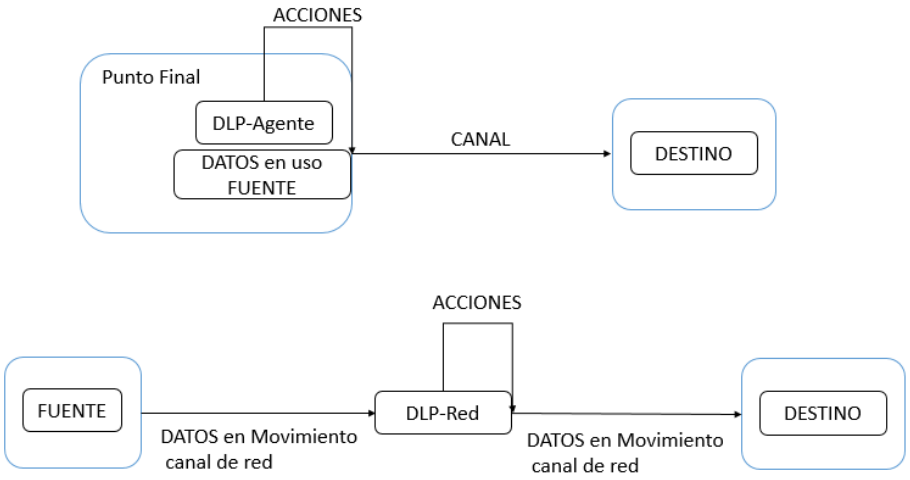

Figura 7: DLP- Punto final para datos en uso y DLP-Red para datos en movimientos.

Modelo DLP para datos en reposo:

Si los DATOS residen en FUENTE, el sistema toma ACCIONES, ver Figura 8.

- DATOS especifica información sensible (que tienen potencial de fuga)
- FUENTE puede ser un punto final, un servidor de almacenamiento o un grupo de ellos
- ACCIÓN es la acción que debe tomar el DLP cuando se identifican datos confidenciales en reposo.

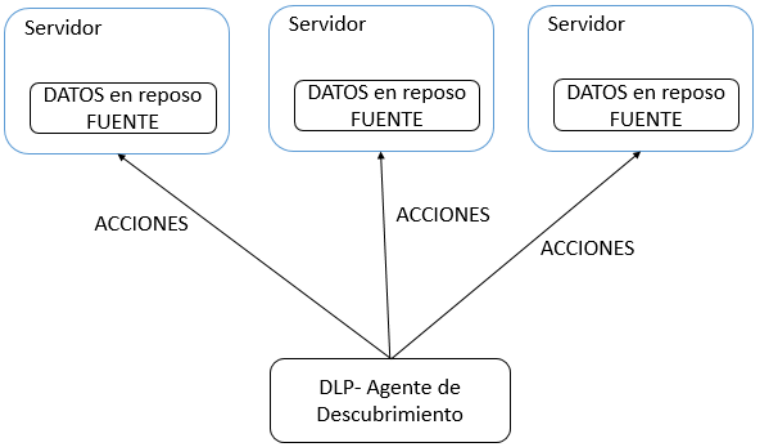

Figura 8: DLP para datos en reposo

Las tecnologías DLP estudiadas, contienen un grupo de soluciones o sistemas que responden a cada uno de los componentes antes definidos en la fase de diseño de la solución Control de Contenido, Control de Red y Control de Dispositivos, partiendo de ese principio se propone en primera instancia los siguientes módulos o soluciones:

- ✓ DLP- Administración
- ✓ DLP- Agente de Punto Final
- ✓ DLP- Agente de Red
- ✓ DLP- Agente de Descubrimiento de Datos Sensibles

Los mismos pueden ser desarrollados como productos independientes en la medida de su desarrollo e integración, ver Figura 9. Arquitectura General Tecnología DLP.

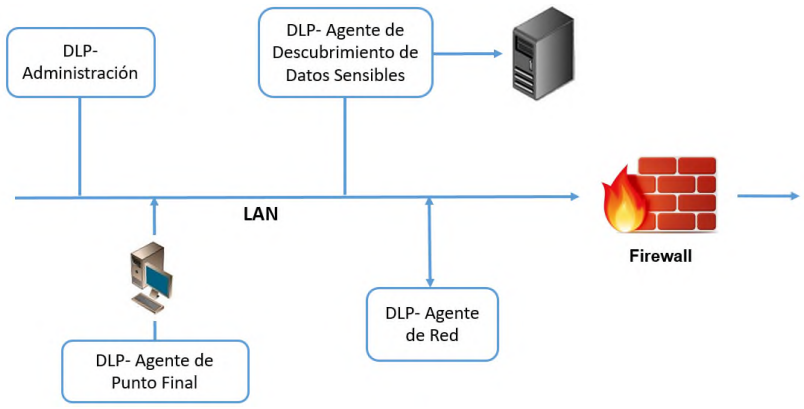

Figura 9: Arquitectura General Tecnología DLP

Modelo de Contexto: Ilustran el contexto operacional de una tecnología, donde se observan las soluciones con las que se interactúa, ver Figura 10.

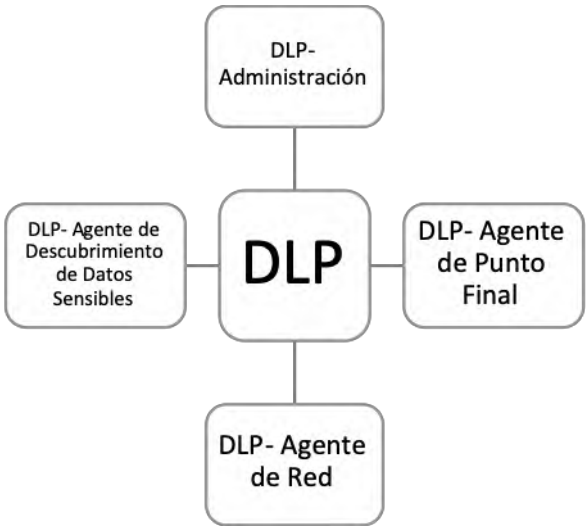

Figura 10: Modelo de Contexto DLP

Arquitectura del sistema

"La arquitectura de software es una planificación basada en modelos, patrones y abstracciones teóricas, a la hora de realizar un software de cierta complejidad y como paso previo a cualquier implementación. Hay diferentes patrones, el desarrollo de una arquitectura puede ser visto como un proceso de selección, adaptación y combinación de patrones." (Huet, 2022)

Para la arquitectura de la tecnología DLP propuesta se eligió un estilo basado en capas. En este estilo *"cada una proporciona servicios a la superior y se sirve de las prestaciones que le brinda la inferior, al dividir un sistema en capas, cada una de ellas puede tratarse de forma independiente, sin tener que conocer los detalles de las demás."* (Huet, 2022)

La división de un sistema en capas facilita el diseño modular, en la que cada capa encapsula un aspecto concreto del sistema y permite además, la construcción de sistemas débilmente acoplados, lo que significa que, si se minimiza las dependencias entre capas, resulta más fácil sustituir la implementación de una capa sin afectar el resto del sistema, por lo que se propone para la realización del DLP crear una arquitectura utilizando una arquitectura de cuatro capas, Presentación, Lógica de Negocio, Acceso a Datos y Modelo de Datos, utilizando interfaces para la comunicación entre dichas capas, para que su posterior desarrollo sea en paralelo e independiente.

Presentación: Esta capa contiene las interfaces necesarias para que el usuario y el sistema intercambien toda la información necesaria. Presenta el sistema al usuario, le comunica y captura la información del usuario en un mínimo de proceso (realiza un filtrado previo para comprobar que no hay errores de formato). También es conocida como interfaz gráfica y debe tener la característica de ser «amigable» (entendible y fácil de usar) para el usuario.
Lógica de Negocio: Esta capa almacena todos los procesos de negocio, todas las transformaciones y procesos del sistema. La capa de presentación y la capa de lógica de negocio van a interactuar con la base de datos a través de servicios, esta capa sirve como intermediario para el intercambio de datos entre la capa de presentación y la capa de acceso a datos.
Acceso a Datos: Esta capa es la encargada de manipular toda la información relacionada con el acceso a la base de datos, a través de los servicios, este último es el encargado de interactuar con la base de datos para realizar todos los procesos de persistencia.
Modelo de Datos: Contiene el modelo de datos de la aplicación, está compuesta por las tablas que almacenan los datos requeridos por la aplicación y las relaciones entre ellas.

4. CONCLUSIONES

La relevancia de una solución DLP radica en su capacidad para abordar necesidades críticas de seguridad, dado que la información es un activo valioso en la era digital, y es crucial evitar fugas de datos almacenados en medios digitales. Una característica distintiva de la tecnología DLP frente a otras herramientas de seguridad es su habilidad para examinar diversos protocolos y formatos de almacenamiento, así como su contenido, para determinar las formas óptimas de uso, transmisión y almacenamiento, en consonancia con las políticas de seguridad implementadas. Esta solución integral proporciona a los administradores de TI una gestión y control eficaz del flujo de datos, eliminando la necesidad de integrar y configurar herramientas adicionales. Estas soluciones requieren licencia para su operación, lo que no solo implica un costo monetario significativo sino también consideraciones de seguridad. Al ser de código propietario, representan una caja negra que podría ser utilizada con fines malintencionados. Aunque su desarrollo es complejo, el autor sostiene que las ventajas de implementar una solución DLP personalizada superan los desafíos. El diseño modular propuesto, que responde a una necesidad real no cubierta por soluciones externas, es una innovación clave en la tecnología propuesta. Este enfoque incluye un cifrado del dispositivo completo sin intervención del usuario y un nuevo método donde la organización establece la contraseña para el cifrado, manteniendo al usuario en la oscuridad. Además, se abordan aspectos teóricos y prácticos como el manejo de eventos de conexión y desconexión a nivel del sistema operativo, entre otros resultados del desarrollo de la investigación presentada.

RECEIVED: DECEMBER, 2023.
REVISED: MAY, 2024.

REFERENCIAS

[1] BARRAGÁN. (2018). **Memorias USB: riesgos, protección y acceso a los datos**. Obtenido de https://www.securityartwork.es/2018/01/24/memoricas-usb-riesgos-proteccion-acceso-los-datos/
[2] BBC NEWS MUNDO. (2018). **Cuáles son los riesgos de usar memorias USB en el trabajo y por qué IBM se las prohibió a sus empleados.** Obtenido de https://www.bbc.com/mundo/noticias-44082644
[3] BROADCOM. (2021). **Symantec Endpoint Encryption**. Obtenido de https://techdocs.broadcom.com/es/es/symantec-security-software/information-security/encryption/11-3-1/about-v98443569-d1666e6.html
[4] CENTRO CRIPTOLÓGICO NACIONAL. (2021). **Guía de Seguridad de las TIC CCN-STIC 1507**. Obtenido de Procedimiento de empleo seguro Forcepoint On-Premise Security 8.5: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/6305-ccn-stic-1507-pes-forcepoint-on-premise-security-8-5/file.html
[5] CLODFLARE. (2020). **¿Qué es un punto de conexión?** Obtenido de https://www.cloudflare.com/es-es/learning/security/glossary/what-is-endpoint/
[6] COMPUTER SECURITY RESOURCE CENTER. (2021). **FIPS 140-2**. Obtenido de https://csrc.nist.gov/projects/fips-140-3-transition-effort#

[7] CORPORATION, K. T. (2018). **Requisitos de ciberseguridad del Departamento de Servicios Financieros del estado de Nueva York (NYDFS); sección 500 del título 23 de los Códigos, Reglas y Regulaciones de Nueva York (NYCRR).** Obtenido de https://www.kingston.com/latam/solutions/data-security/nydfs-23-nycrr-500
[8] CORPORATION, K. T. (2021). **Protección de datos**. . Obtenido de https://www.kingston.com/es/solutions/data-security.
[9] DANIEL M. S. (2013). **Implantación, creación de un laboratorio de pruebas y casos**. Alcalá, España: Universidad de Alcalá.
[10] DIWAN, S. (2018). **Complete Security Package for USB Thumb Drive**. 5. Obtemido de https://iiste.org/Journals/index.php/CEIS/article/view/14682
[11] EMILIO, A. (2017). **La Privacidad en entornos Data Loss Prevention.** Obtenido de http://www.redseguridad.com/opinion/articulos/laprivacidad-en-entornos-data-loss-prevention.
[12] ENISA. (2018). **Secure USB Flash Drives**. EEUU. Obtenido de https://www.enisa.europa.eu/publications/archive/secure-usb-flash-drives-en
[13] FORCEPOINT. (2017). **Forcepoint dlp endpoint detenga las amenazas avanzadas y proteja la información confidencial de los usuarios remotos**. Obtenido de http://www.forcepoint.com
[14] GARTNER Inc. (2021). **Gartner peerinsights**. Obtenido de Enterprise Data Loss Prevention (DLP) Reviews and Ratings: https://www.gartner.com/reviews/market/enterprise-data-loss-prevention/vendors
[15] GEEKFLARE. (2021). **Las 8 mejores soluciones de prevención de pérdida de datos que podrían ahorrarle millones**. Obtenido de GEEKFLARE: https://geekflare.com/es/data-loss-prevention-solutions/
[16] GOYVAERTS, J. (22 de Noviembre de 2019). **Regular-Expressions. Info**. Obtenido de http://www.regular-expressions.info/quickstart.html.
[17] GREENBERG. A. (2018). **Why the Security of USB Is Fundamentally Broken**. Obtenido de https://www.wired.com/2014/07/usb-security/
[18] HONEYWELL. (2020). **USB security-myths vs.reality**.Latest USB Security Threats & Best Practices to Follow.
[19] HUET, P. (2022). **OpenWebinars**. Obtenido de Arquitectura de software: Que es y que tipos existen: https://openwebinars.net/blog/arquitectura-de-software-que-es-y-que-tipos-existen/
[20] INBEST.SOLUTIONS. (2018). **iNBest.solutions**. Obtenido de https://inbest.solutions/que-es-prevencion-de-perdida-de-datos-dlp/
[21] OSTEC. (2019). **Data Loss Prevention-DLP ¿Qué es y como funciona***?*. Obtenido de https://ostec.blog/es/seguridad-perimetral/dlp-que-es-y-como-funciona/
[22] IT DIGITAL SECURITY. (2019). **DLP, o cómo prevenir la fuga de datos**. Obtenido de https://www.itdigitalsecurity.es/reportajes/2019/01/dlp-o-como-prevenir-la-fuga-de-datos
[23] TORRES MARTÍNEZ, M. Á. (2015). *DLp: prevención de fuga de información (data loss prevention), Especialización en* **Seguridad Informática**, Universidad Piloto de Colombia.
[24] MCAFEE . (2019a). **McAfee Total Protection for Data Loss Prevention**. Obtenido de http://www.mcafee.com
[25] MCAFEE. (2019b). **McAfee Data Loss Prevention Endpoint**. Obtenido de http://www.mcafee.com/es
[26] MYSERVERNAME.COM. (2021). **myservername.com**. Obtenido de Las 11 MEJORES soluciones DLP de software de prevención de pérdida de datos en 2021: https://spa.myservername.com/11-best-data-loss-prevention-software-dlp-solutions-2021
[27] NATALIE. (2020). **USBKey**. Obtenido de http://www.meet-electronics.com/products/usbkey
[28] NIST. (2021). **Security Requirement for cryptographic modules**. Obtenido de https://csrc.nist.gov/publications/detail/fips/140/2/final
[29] OLIVEIRA. (2018). System protection agent against unauthorized activities via USB devices.
[30] OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN. (2015). **Recomendaciones de Seguridad en el Desarrollo de Software.** Argentina. Obtenido de https://www.argentina.gob.ar/sites/default/files/onti/onti/83_recomendaciones_de_seguridad_en_el_desarrollo_de_software_ver_1_0.pdf

[31] PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. (2018). Reglamento (Ue) 2016/679 Del Parlamento Europeo Y Del Consejo, **Reglamento General de Protección de Datos**. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
[32] PARRILLA, J. A. (2018). **Bienes Difigtales. Una Necesidad Europea**. Madrid: Dkinson, S.L.
[33] RAMIÓ, D. J. (2022). **Criptografía para Ingenier@s**. España : Prólogo Dr. Alfonso Muñoz .Obtenido https://derechodelared.com/libro-gratuito-criptografia-para-ingenieros/
[34] RED HAT, INC. (2022). **Seguridad en el ciclo de vida de desarrollo del software**. Obtenido de https://www.redhat.com/es/topics/security/software-development-lifecycle-security
[35] RODRIGUEZ, L. (2018). **Symantec Team**. Obtenido de Symantec Endpoint Encryption, con la Tecnología PGP: https://www.teamnet.com.mx/blog/symantec-endpoint-encryption-con-la-tecnolog%C3%ADa-pgp
[36] SYMANTEC CORPORATION. (2018). **Symantec Data Loss Prevention, Drive total protection of your sensitive data**. Obtenido de http://www.symantec.com
[37] SYMANTEC CORPORATION. (2019). **La solución de prevención contra la pérdida de datos líder del mercado**. Obtenido de http://www.symantec.com/es/mx/data-loss-prevention
[38] Techopedia. **Human Interface Device** (HID). (20 de 2 de 2021). Obtenido de https://www.techopedia.com/definition/19781/human-interface-device-hid
[39] DAST @2018 - DISTRIBUIDOR ELITE PANDA SECURITY EN ARGENTINA (2020). **¿Qué es la DLP o Data Loss Prevention?** Obtenido de https://dast.com.ar/que-es-la-dlp-o-data-loss-prevention/
[40] UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO (2018). DGTIC. Obtenido de Seguridad Cultura de prevención para TI: https://revista.seguridad.unam.mx/numero25/dlp-tecnolog-para-la-prevenci-n-de-la-fuga-de-informaci-n
[41] VERITY. (2022). **Verity Voted Best Data Provider Overall** . Obtenido de https://verityplatform.com/