UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
ANÁLISIS DE USO DE SOLUCIONES DATA LOSS PREVENTION PARA INSTITUCIONES FINANCIERAS COMO MECANISMO PARA EL CUMPLIMIENTO DE NORMATIVA PCI-DSS.
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Héctor Adrián Martínez Mena
Tutor:
MSc. Christian Patricio Vaca Benalcázar CPA

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, MSc. Christian Vaca con C.I: 1719368555 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de uso de soluciones Data Loss Prevention para instituciones financieras como mecanismo para el cumplimiento de normativa PCI-DSS.

Elaborado por: Hector Adrián Martínez, de C.I: 1721674594, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2022

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Héctor Adrián Martínez Mena con C.I: 1721674594, autor del proyecto de titulación denominado: Análisis de uso de Soluciones Data Loss Prevention Para Instituciones Financieras Como Mecanismo Para El Cumplimiento De Normativa PCI-DSS. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2022

Firma

Tabla de contenidos

Índice de figuras

Índice de tablas

INFORMACIÓN GENERAL

Contextualización del tema

A raíz de la pandemia por la Covid-19, nuevas necesidades y nuevas estrategias de comunicación se han presentado, que gracias al Internet y su globalización se puede cubrir para la continuidad de los distintos negocios en especial la industria financiera, colaboradores en teletrabajo, uso de nuevas plataformas y nuevas herramientas así como nuevas estrategias para la continuidad de los negocios, con esto; muchas vulnerabilidades y brechas de seguridad aparecen día a día, poniendo en riesgo la información sensible, tanto de las empresas como de los colaboradores y su información personal, ergo; resulta ser menester el uso de técnicas de seguridad o mejores prácticas para preservar la información que se pueda considerar sensible.

Cumplir con las normativas que las superintendencias de bancos exigen para el correcto funcionamiento de una compañía financiera, resulta ser un reto complejo para un profesional encargado de las tecnologías de la información (TI), teniendo la obligación de proteger la información y la continuidad del negocio, en este caso particular de estudio; las instituciones financieras con la data de sus clientes, cuentas bancarias, información de tarjetas de crédito, etc.

Problema de investigación

En la actualidad los atacantes informáticos apuntan en su mayoría hacia empresas con poder adquisitivo y económico, empresas que manejan grandes cantidades de data e información de usuarios, siendo las empresas financieras un blanco primordial para los ataques en búsqueda de robo de información, tanto intrusivo desde fuera como inclusive desde dentro con los colaboradores como ejecutores de la sustracción de data de formas ilegales, con base en lo mencionado y tomando en cuenta la necesidad de la aplicación de las normativas para la aplicación de tecnologías de Data Loss Prevention (DLP), en empresas donde la información sensible sea operada, desarrollada, manipulada, distribuida, o procesada de alguna manera por sus colaboradores y sobre todo, hoy en día, con nuevas modalidades de teletrabajo o trabajo en casa, y tomando en cuenta que; al ser información crítica resulta necesario y vital el uso de herramientas y técnicas que puedan asegurar que la información de la empresa no caiga en manos externas a la misma, o peor aún, que caigan en posesión de personas con baja moral y sin escrúpulos que puedan causar daños a la compañía como pérdidas económicas, problemas legales o incluso que pueda llevar a quebrar la compañía, bajo ésta problemática, la importancia de este documento. (AmericaEconomía, 2020)

Bajo esta premisa, se puede plantear el siguiente cuestionamiento:

¿Es acaso necesaria la implementación de una herramienta para la protección de datos y mitigación de fuga de información en las empresas financieras?

Objetivo general

Establecer criterios que permitan cumplir lo establecido por normativas PCI-DSS y leyes propias para instituciones financieras por medio del uso de tecnologías DLP.

Objetivos específicos

Revisar de forma sistémica de normativas PCI-DSS con relación a la fuga de información, para identificar las brechas de seguridad que se cubren con la solución DLP.

Realizar un análisis comparativo de soluciones DLP con la finalidad de establecer requisitos emitidos por la normativa PCI-DSS.

Realizar comparativas de algunas soluciones DLP open source y de paga, y así esclarecer las mejores opciones de acuerdo con las necesidades y recursos de la compañía.

Elaborar un informe con las recomendaciones de las mejores alternativas en cuanto a costo, calidad y rendimiento para el uso de DLP en las entidades financieras.

Vinculación con la sociedad y beneficiarios directos:

El presente documento va dirigido a las empresas financieras, las cuales se pueden tomar en cuenta para trabajar o mejorar en sus lugares de trabajo, ya que muchas suelen descuidar sus entornos de seguridad y más aún las seguridades internas para la fuga de información.

El control que deben tener las compañías financieras es importante en el funcionamiento de estas, por lo que una guía práctica puede colaborar con las pretensiones de protección de la data que manejan estas empresas. (Rider, 2021)

Se debe tomar en cuenta las normativas PCI-DSS para el cumplimiento de las configuraciones de seguridad en cuanto a la fuga de información de una empresa financiera resulta ser indispensable para la seguridad de los datos de clientes, usuarios, equipos y negocios.

Cabe mencionar con ejemplos clave o casos de uso aplicables, las leyes constitucionales y de protección de datos en entornos empresariales financieros, con las causas y formas más probables de delitos de fuga de información; se conseguirá concientizar al lector para el cumplimiento de las normativas y reglamentos internos de una compañía financiera para evitar percances y problemas legales. (Rider, 2021)

Con base en los Objetivos de Desarrollo Sostenible(ODS) de las Naciones Unidas el objetivo nueve literal a, menciona que «Facilitar el desarrollo de infraestructuras sostenibles y resilientes en los países en desarrollo mediante un mayor apoyo financiero, tecnológico y técnico, los países menos adelantados» (Naciones Unidas, 2022), el presente artículo pretende aportar a la seguridad de la información de las empresas financieras en cuanto a la mitigación de la fuga de información a través de herramientas DLP.

CAPÍTULO I – FUNDAMENTOS TEÓRICOS

1.1. Contextualización general

Para realizar el presente documento se han tomado en cuenta las opciones que se pueden tener para evitar la fuga de información o pérdida de información de las compañías financieras con base al nuevo método de teletrabajo implementado a partir de la pandemia mundial del SarsCov2 y las nuevas normativas laborales que se obligaron a efectuar para preservar la continuidad del negocio. (CEPAL, 2020)

Bajo esta perspectiva se desarrolla la idea de proteger los datos de la empresa y que, para ello, aplicar herramientas que sustenten la idea de la tecnología *Data Loss Prevention* (DLP), dentro de los equipos de los colaboradores de las empresas que requieran proteger su información sensible. (CEPAL, 2020)

Esta investigación se fortalece con base en un análisis comparativo de distintas herramientas DLP, donde analizando soluciones open source y de paga, además de utilizar indicadores como los cuadrantes de Gartner o SoftwareReviews para realizar las comparativas necesarias, y así comprender de mejor manera lo que hace la tecnología DLP, estableciendo así la importancia de la herramienta, las falencias de una u otra marca, y la capacidad de inferir resultados positivos para las compañías financieras interesadas. (ElPais, 2020)

Según indica el Instituto nacional de Ciberseguridad Española (INCIBE), las tecnologías DLP cuentan con inteligencia artificial además de opciones de configuración estableciendo políticas o directivas de seguridad, que se pueden implementar de acuerdo con lo que necesitemos proteger, ya sea, información de usuarios, números de cédula, correos electrónicos, números de tarjetas de crédito, etc., concatenando estas opciones tener una solución que permite adecuarse al tipo de documento o información confidencial que la organización necesite resguardar. (INCIBE, 2019)

Nuevas tecnologías y soluciones se desarrollan constantemente para combatir la ciberdelincuencia, con ello las empresas y las áreas encargadas de la TI evalúan asiduamente herramientas y combinaciones de estas para salvaguardar de mejor manera la información y continuidad del negocio, creando métodos para la prevención de fuga de información, DLP es una de las tecnologías más usadas e importantes para la prevención de fuga de información, ya que; dependiendo de la marca del producto, y según informa la empresa McAfee con relación a su producto McAfee DLP Endpoint (Nelson Diaz, 2020), pueden contener módulos de seguridad como:

- Protección de correo electrónico: Analiza la información que un usuario puede agregar dentro de los documentos adjuntos o redactado en un correo electrónico.

- Protección de USB: Protección de dispositivos extraíbles analizando los archivos que se copian a los USB o bloqueando directamente de manera física el uso de puertos USB.

- Protección de portapapeles: Esta protección analiza lo copiado en el portapapeles de Windows o Mac y con base en políticas bloquea la copia de información sensible.

- Protección de red: Analiza los archivos que un usuario puede copiar dentro de un entorno de red, carpetas o recursos compartidos.

- Protección de impresoras: Tanto para impresoras físicas como para impresoras virtuales, analiza el documento desde el cual se envía a imprimir para evitar fuga de información.

- Protección de capturas de pantalla: El producto analiza en las capturas de pantalla, posibles datos con información sensible de acuerdo con las directivas establecidas.

- Protección web: Esta protección analiza lo que se pueda subir a la web a través de los navegadores web o aplicaciones con conexión o salida a Internet. (McAfee, 2021)

1.2. Características Y Funcionalidades

De acuerdo con la información que McAfee (en la actualidad llamado Trellix) proporciona de su producto DLP indica que el software McAfee DLP Endpoint utiliza tecnología de reconocimiento avanzada, reconocimiento de patrones de texto y diccionarios predefinidos para identificar este contenido confidencial, e integra la administración y el cifrado de dispositivos para capas adicionales de control. (McAfee, 2020)

- **Optical character recognition (OCR)**

  Por sus siglas en inglés, «Reconocimiento óptico de caracteres», esta herramienta puede identificar y extraer el texto en archivos de imagen, esta información la compara con los extractores de texto, algoritmos y expresiones regulares configuradas dentro de la herramienta. (McAfee, 2021)

- **Extractores de texto**

El extractor de texto analiza el contenido a medida que se abren o copian los archivos y los compara con las plantillas de texto y las definiciones del diccionario de reglas de clasificación. Si se produce una coincidencia, los criterios se aplican al contenido.

- **Expresiones regulares**

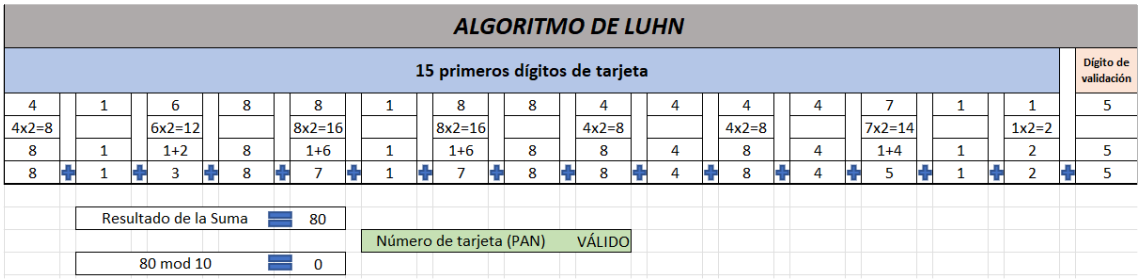
También conocidos como regex, le permiten filtrar texto para encontrar coincidencias, verificar la validez de datos, documentos de identidad o contraseñas, se pueden utilizar para calificar el texto de propiedades específicas para otros fines sustitutivos y muchas otras prestaciones. (McAfee, 2021)

- **Algoritmos de validación**

Si cuenta una secuencia de dígitos y desea saber si estos dígitos corresponden a un posible *Primary Account Number* (PAN), se utiliza el algoritmo de Luhn, cuyo resultado debe ser 0 (cero) si esta secuencia es válida. (Quobit, 2021)

Figura 1

Algoritmo de Luhn.



Nota. Esta figura muestra un ejemplo del uso del algoritmo de Luhn.

- **Diccionarios**

En las instituciones financieras no solo manejan números de cuentas, tarjetas de pago, cédulas y demás información sensible, si no que, además de eso, existe información de contractibilidad de los usuarios información que también debe ser protegida y para ello hacemos uso de los diccionarios, bloqueando palabras o frases clave en la herramienta e impidiendo que los usuarios hagan mal uso de esta data. (McAfee, 2021)

1.3. Comparativa herramientas *OpenSource* y de pago:

El precio de las herramientas de seguridad DLP de fabricantes de marca, las prestaciones que pueden dar las herramientas open source a diferencia de una con respaldo de licencia paga son las principales características por tomar en cuenta para la elección de una u otra opción en la implementación de una herramienta DLP.

1.3.1. Comparativa basada en investigación

Con base en lo que informa (Capterra, 2021), una empresa especializada en proveer soluciones de software y hardware para la seguridad de las compañías, además de recopilar opiniones con relación al uso que muchas empresas les dan a las distintas soluciones, tenemos que soluciones DLP como Safetica, McAfee y Symantec son los líderes de opinión de usuarios.

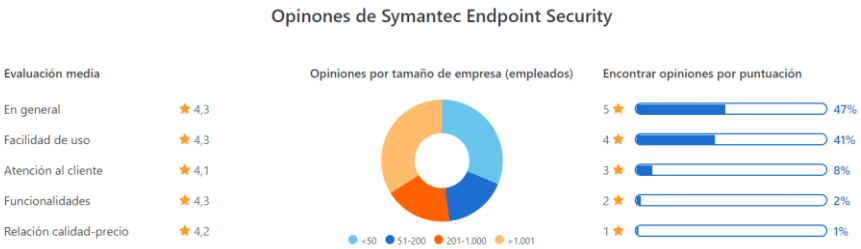
Figura 2

Opiniones de DLP Safetica.

Nota. Esta figura muestra la opinión de usuarios de la solución DLP Safetica. (Capterra, 2021)

Figura 3

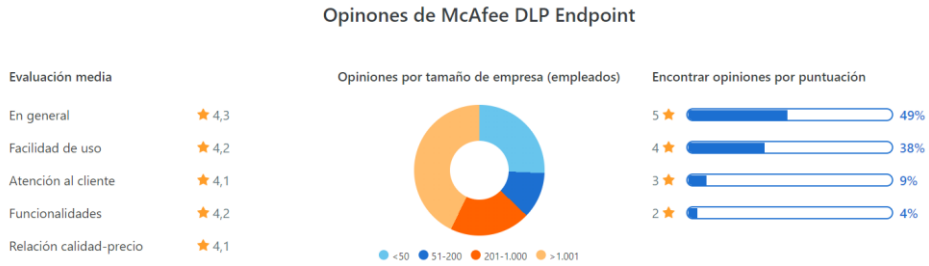
Opiniones de DLP Symantec Endpoint Security.



Nota. Esta figura muestra la opinión de usuarios de la solución DLP Symantec. (Capterra, 2021)

Figura 4

Opiniones de McAfee DLP Endpoint.



Nota. Esta figura muestra la opinión de usuarios de la solución DLP de McAfee. (Capterra, 2021)

Mediante encuestas e investigaciones se ha observado la relación y comparativa de soluciones de paga y open source, arrojando datos importantes como precios, complejidad para administrar el producto, robustes de la solución y características, además de su relación calidad precio.

Figura 5

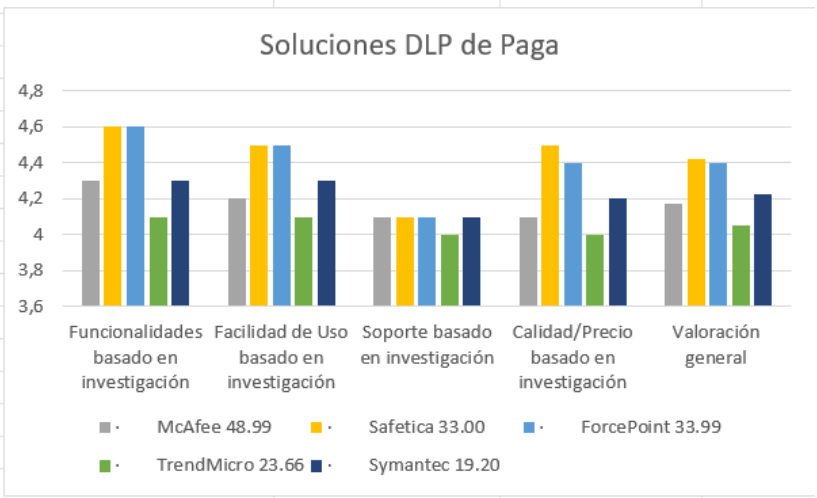
Cuadro comparativo de soluciones de paga y open source.

Tipo de soluciones	Marcas	Precios aproximados por licencia(Anual)	Funcionalidades basado en investigación	Facilidad de Uso basado en investigación	Soporte basado en investigación	Calidad/Precio basado en investigación	Valoración general
Soluciones DLP de Paga	· McAfee	48.99	4,3	4,2	4,1	4,1	4,175
	· Safetica	33.00	4,6	4,5	4,1	4,5	4,425
	· ForcePoint	33.99	4,6	4,5	4,1	4,4	4,4
	· TrendMicro	23.66	4,1	4,1	4	4	4,05
	· Symantec	19.20	4,3	4,3	4,1	4,2	4,225
Soluciones DLP Open Source	· My DLP	NA	3,7	4,2	NA	NA	3,95
	· SecureTrust's DLP	NA	3	4	NA	NA	3,5
	· CoSoSys' Endpoint Protector	NA	3,3	3,6	NA	NA	3,45
	· NightFall	NA	3,1	3,6	NA	NA	3,35
	· Commvault´s Orchestrate	NA	3,1	3,2	NA	NA	3,15

Nota. Este cuadro muestra una comparativa de las soluciones de paga y open source.

Figura 6

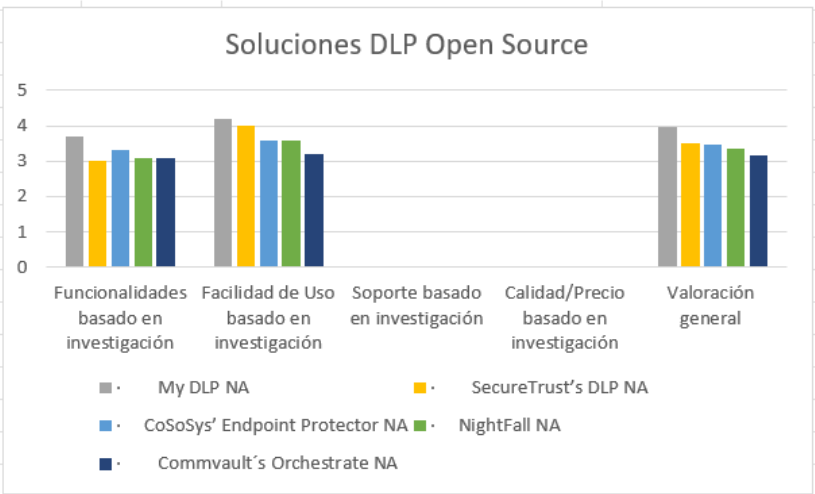
Comparación de soluciones DLP de paga.



Nota. Esta figura muestra la relación entre soluciones DLP de paga.

Figura 7

Comparación de soluciones DLP Open Source.



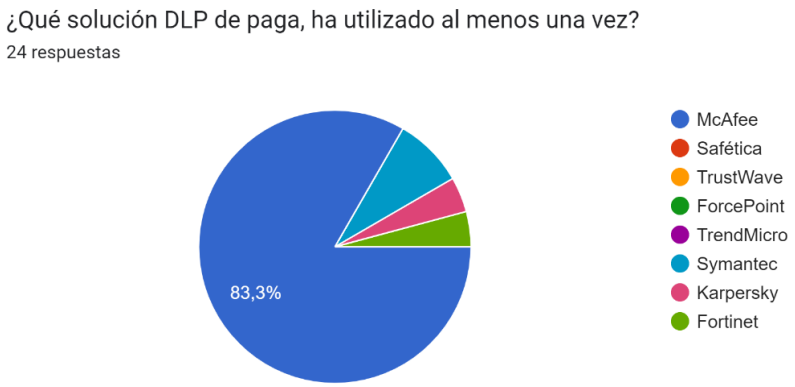
Nota. Esta figura muestra una relación entre soluciones DLP Open Source.

1.3.2. Comparativa basada en encuesta

Con base en la encuesta realizada (véase anexo 1) en su totalidad a profesionales del ámbito de seguridades de IT en empresas financieras, y una muestra de al menos 24 personas, hemos podido observar que la marca McAfee es la más utilizada en el medio con un 83% por sobre el resto.

Figura 8

Soluciones DLP de paga

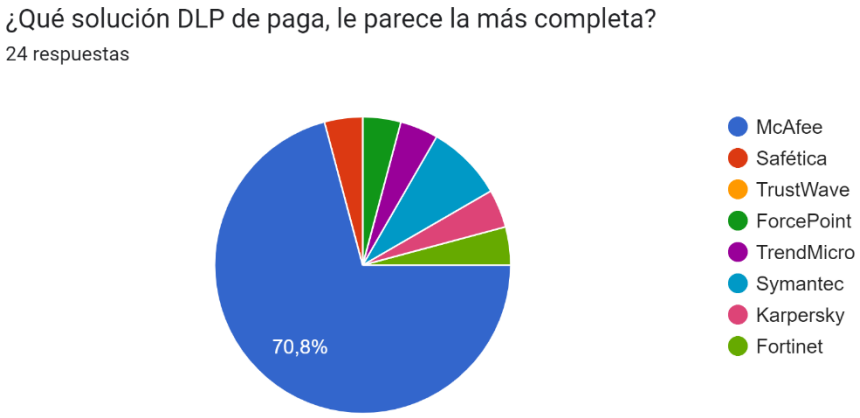


Nota. La figura representa el porcentaje de personas que han utilizado las distintas soluciones DLP de paga.

De igual manera la herramienta que consideran más completa y fácil de administrar McAfee lidera con un 70 y 66%, respectivamente.

Figura 9

Soluciones DLP de paga



Nota. La figura representa el porcentaje de soluciones DLP de paga que son más completas de acuerdo con los encuestados.

Figura 10

Soluciones DLP de paga

Nota. La figura representa el porcentaje de soluciones DLP de paga que son más fáciles de administrar de acuerdo con los encuestados.

Por el contrario, en las soluciones open source, vemos que se ha comprobado mucha más variedad de soluciones, y en algunos casos no han utilizado ninguna herramienta de las mencionadas.

Figura 11

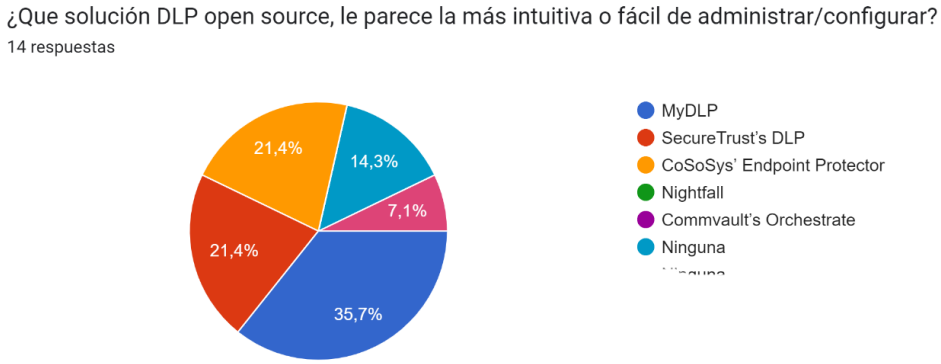
Soluciones DLP Open Source.

Nota. La figura representa el porcentaje de personas que han utilizado las distintas soluciones DLP Open Source.

Los encuestados consideran que la herramienta MyDLP es la más intuitiva y completa en cuanto a soluciones DLP OpenSource se refiere.

Figura 12

Soluciones DLP Open Source.



Nota. La figura representa el porcentaje de soluciones DLP open source que son más fáciles de administrar de acuerdo con los encuestados.

1.3.3. Comparativa de soluciones DLP según funcionalidades

Se realiza una comparativa entre soluciones DLP de paga y *Open Source*, para establecer las funcionalidades, prestaciones y falencias de una u otra, facilitando así la selección de herramientas de acuerdo con las necesidades y recursos de las compañías financieras grandes o pequeñas cooperativas.

Soluciones DLP Open Source

Son herramientas de código abierto que permiten realizar todas o algunas de las opciones que provee una herramienta de pago, la diferencia radica en el soporte, el respaldo de marca, el precio, la implementación, y con base en las necesidades de la empresa a la cual se va a aplicar la solución de seguridad, elegir la que más se adecúe al core del negocio.

- **MyDLP:** Según indican (Purohit Singh, 2013), MyDLP es un proyecto de código abierto que como una buena solución de es capaz de monitorear, prevenir e inspeccionar la fuga de data sensible o que se considere sensible, gracias a políticas, directivas establecidas por los administradores de la herramienta.

Figura 13

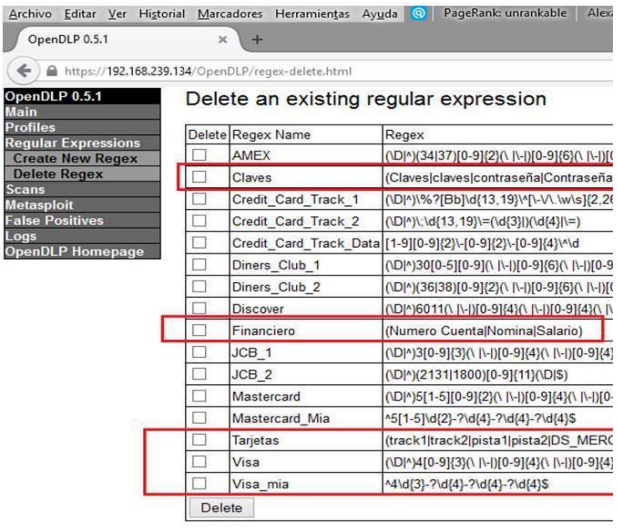
Pantalla de reglas de MyDLP.

Nota: Esta figura muestra una captura de la pantalla principal de la herramienta MyDLP.

- **OpenDLP:** (Raj y Abraham, 2019), afirman que la herramienta OpenDLP es una suite para evitar la fuga de información, bastante intuitiva con una interfaz centralizada que permite realizar los escaneos en un sistema determinado a través de un agente en el equipo y analiza procesos de bases de datos, sistema de archivos en busca de data confidencial, no es posible analizar data cifrada.

Figura 14

Expresiones regulares de OpenDLP.



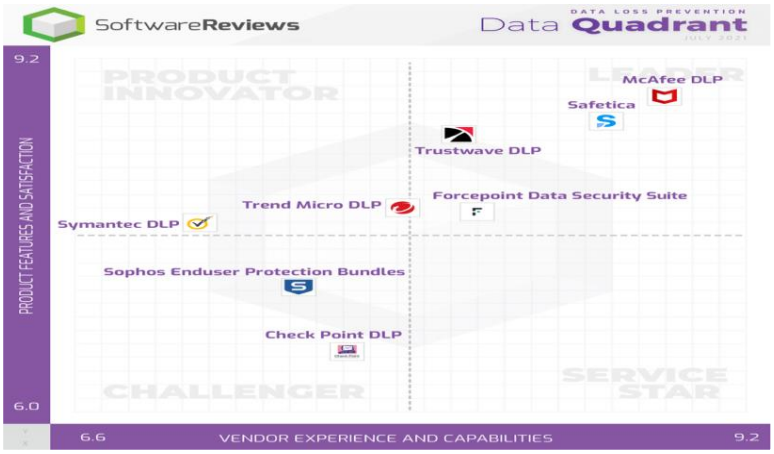
Nota. Esta figura es una captura de pantalla de la herramienta OpenDLP.

Soluciones DLP de Pago

Según la publicación del cuadrante *Software Reviews*, correspondientes a la tecnología DLP informan que McAfee y Safetica son las marcas mejor calificadas y para cubrir las necesidades de protección de datos e información sensible de una posible fuga de data. (Tecnozero, 2021)

Figura 15

Cuadrante SoftwareReviews



Nota. Esta figura muestra la clasificación del cuadrante de SoftwareReviews con respecto a la solución DLP. (SoftwareReviews, 2021)

Figura 16

Cuadrante Gartner

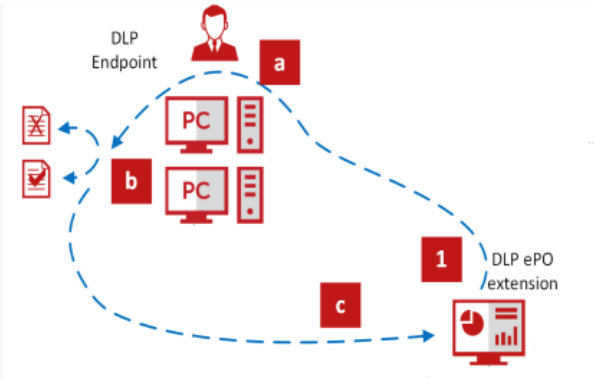
Nota. Esta figura muestra la clasificación del cuadrante de Gartner con respecto a la solución DLP. (Gartner, 2020)

- **McAfee DLP Endpoint**

De acuerdo con lo que la marca indica, McAfee® Data Loss Prevention Endpoint® brinda protección integral para todos los posibles canales de fuga de datos, incluidas las unidades extraíbles, la nube, el correo electrónico, la mensajería instantánea, la web, la impresión, el portapapeles, las capturas de pantalla, el uso compartido de archivos de aplicaciones, etc. (McAfee, 2020)

Figura 17

Funcionamiento de McAfee DLP



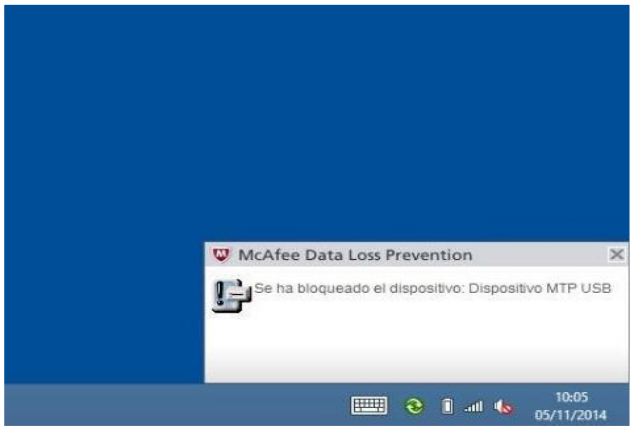
Nota. Esta figura muestra la forma de trabajo de la solución de seguridad McAfee DLP. (McAfee, 2020)

Ofrece directivas basadas en plantillas para las normativas, así como casos prácticos, para facilitar a las empresas el cumplimiento normativo. Además, los usuarios obtienen comentarios en tiempo real a través de ventanas emergentes que se basan en la directiva empresarial, que contribuyen a generar una cultura de seguridad empresarial más robusta. (PCI Security Standards Council, 2022)

Los siguientes, son ejemplos de la actividad de DLP y el trabajo que realiza cuando un usuario manipula información sensible o atenta contra las reglas y directivas especializadas y especificadas por la empresa para evitar la fuga de información.

Figura 18

Bloqueo de USB por McAfee DLP



Nota: El gráfico representa una alerta de regla DLP en ejecución para bloqueo de dispositivos USB.

- **Safetica DLP Endpoint**

Según informa SoftwareReviews en su publicación de comparativa de herramientas DLP, Safetica recibió las mejores calificaciones por la intuitiva forma implementación de su producto, así como la facilidad de integración de datos. Además, ocupó el segundo lugar en estrategia de productos y nivel de desarrollo y accesibilidad de soporte de marca y acompañamiento. (SoftwareReviews, 2021)

De acuerdo con sus manuales de configuración y gracias a la revista Revistabyte, Safetica funciona mediante la instalación de un agente (Safetica Endpoint Client) en las computadoras que van a ser monitoreadas y mantener una conexión regular con ellas a través del servidor (Safetica Management Service). Este servidor, a su vez, crea una base de datos de la actividad de esta estación de trabajo y despliega nuevas políticas y reglas para proteger la información en cada computadora. (Byte TI, 2018)

Figura 19

Características de Safetica DLP

Nota. La figura representa las características de la solución Safetica DLP desde el punto de vista de SoftwareReviews. (SoftwareReviews, 2021)

1.4. Principales Causas Para La Fuga De Información

Algunos ejemplos de fugas de información pueden provenir de la venta de un empleado información confidencial en la competencia, una secretaria que pierde un documento en algún lugar público o en la misma línea Pérdida de computadora portátil o llave USB y acceso remotamente a una base de datos en su organización o a una computadora infectada con software espía información a un criminal. (Lagua, 2021)

- **Servicios en nube**

  Hoy en día los servicios cloud, virtualizaciones y transacciones inmediatas han posicionado una situación, en la que las brechas de seguridad son más amplias.

- **Malware**

  De acuerdo con una publicación de CISCO del 27 de julio del 2022, los malware comunes desplazan al Ransomware como principal ciber-amenaza, según el estudio de Cisco Talos, este cambio probablemente se deba a una serie de factores, como la suspensión de algunos grupos de Ransomware -debido a divisiones internas o acciones de las fuerzas de seguridad- y el resurgimiento de algunos troyanos basados en Remcos, Vidar, Redline y Qakbot/Qbot (este último es un conocido troyano bancario). Phishing, emails comerciales y Advanced Persistent Threats (APT) completan la lista de malware favoritos.

- **Movilización y Teletrabajo**

  El rápido cambio al trabajo remoto desafió a las organizaciones a brindar herramientas que protejan los datos y la necesidad continua de información sobre salud personal, ubicación y proximidad, y de contactos han obligado a las organizaciones y a los gobiernos a intentar equilibrar la necesidad de controlar el virus y mantener a las personas seguras respetando la privacidad. (Lagua, 2021)

  Cabe considerar que el fenómeno llamado BYOD (Bring Your Own Device), permitido por muchas empresas para que sus empleados puedan hacer uso de sus propios dispositivos, no es una opción que pueda ser tomada en cuenta en las entidades financieras, sobre todo en áreas críticas como en las áreas de impresión datacard. (Navarro, 2019)

- **Políticas de la Organización financiera**

  Políticas internas del manejo de la información sensible deben estar documentadas y aplicadas debidamente para controlar y evitar cualquier tipo de fuga de información considerada confidencial. (Navarro, 2019)

- **Accesos no autorizados**

  El acceso no autorizado a un sistema informático, según los autores chilenos (Huerta y Líbano, 1996), consiste en obtener acceso indebido, no vigilado o ilegal a un sistema de gestión de información con el fin de obtener satisfacción intelectual mediante el descifrado de códigos o credenciales de acceso.

1.5. Revisión de normativas y estándares.

Según (Navarro, 2019), el cumplimiento de las normativas es esencial para las empresas financieras, ya que estas se encuentran sujetas a auditorías constantes por parte de su ente máximo como la superintendencia de bancos, con esto de por medio, es importante el solventar todas las normativas que este ente máximo solicite, una de ellas es las normativas de *Payment Card Industry Data Security Standard* (PCI-DSS).

Todas las empresas independientemente del negocio al cual se encuentren orientados, y con más razón las empresas a las cuales se dirige el presente artículo, las financieras, se deben regir a un grupo de normativas con el fin de cumplir con las regulaciones que la ley y las organizaciones moderadoras exigen para calificar como confiables y puedan seguir ejerciendo el negocio al cual se dedican.

La transparencia de datos, el conocimiento de donde se almacena la información y un control del flujo de esta información resulta ser esencial, así como que personas tienen acceso a dicha información y que pueden llegar a hacer con la misma, ya que transferir, copiar, cargar o modificar data son una brecha de seguridad de la información si no se tiene bajo procesos controlados.

1.5.1. PCI-DSS

Dentro de la normativa que se aplica en este análisis: PCI-DSS, cuenta con tres puntos específicos los cuales son base para el desarrollo del presente artículo, en ellos se detallan cómo la información confidencial puede ser extraída a través de malwares o ataques de intrusión en nuestra red, por lo que se debe cumplir con la aplicación de técnicas de mitigación para la protección de la data.

- **Normativas referentes a la prevención de fuga de información**

Según el requisito 11 de la normativa PCI-DSS solicita poner a prueba constantemente el nivel de seguridades.

En su dependencia en el punto 11.5 se debe responder inmediatamente antes cambios imprevistos e intrusiones en la red.

Por su lado, en el punto 11.5.1.1 se exige, para los proveedores de servicios financieros, establecer técnicas de detección-intrusión e intrusión-prevención, alertando e impidiendo cualquier tipo de ataque, intromisión o fuga de información. (PCI Security Standards Council, 2022)

Dentro del anexo A3 de las normativas PCI-DSS, especifican la validación complementaria de Entidades Designadas (DESV), y solicita la revisión de los siguientes puntos:

Punto A3.2 el alcance PCI-DSS debe estar documentado y validado.

Por su parte en el inciso A3.2.6, se debe aplicar soluciones para detectar e imposibilitar que datos PAN no cifrados o enmascarados, abandonen el área de Cardholder Data Environment (CDE) por un canal, modalidad o proceso no acreditado, incluidos componentes como:

• Análisis permanente.

• Configuraciones para activar detecciones y evitar que los datos PAN no encriptados o enmascarados, abandonen el CDE sin autorización.

• Realizar registros de auditoría y alertas de eventos al detectar datos PAN no encriptados que salen del CDE sin autorización. (PCI Security Standards Council, 2022)

De acuerdo con el punto A3.2.6.1, las operaciones de respuesta se deben implementar para ser iniciados ante situaciones de detección de intentos para eliminar datos PAN no cifrados del CDE sin autorización. Los procedimientos de respuesta deben incluir:

• Procedimientos para la investigación de alertas por parte del personal encargado.

• Procedimientos para remediar fugas de información o procesos inestables, según sea necesario, para evitar cualquier pérdida de data. (PCI Security Standards Council, 2022)

Buenas Prácticas

Los métodos que pueden ayudar a detectar y abordar los canales de comunicación del malware incluyen el escaneo de puntos finales en tiempo real, el filtrado del tráfico de salida, una lista de "permitidos", herramientas de prevención de fuga de información y herramientas de supervisión de la seguridad de la red, como las tecnologías de detección de intrusos y los de prevención de intrusos, por sus siglas en ingles IDS-IPS, respectivamente.(PCI Security Standards Council, 2022)

La cobertura del mecanismo incluye, correos electrónicos, descargas a medios USB y salida a impresoras. Las soluciones para la detección y la mitigación de pérdida no acreditada de datos PAN sin cifrar, deben incluir el uso de soluciones apropiadas, como herramientas de prevención de fuga de información. (PCI Security Standards Council, 2022)

Los intentos movimientos de datos PAN, sin encriptar a través de medios no permitidos, podrían indicar un intento malicioso de secuestrar información, o podrían ser causados por las intenciones de un empleado autorizado, que no conoce los métodos correctos o simplemente no los siguió. Una revisión rápida de estos incidentes, pueden permitir identificar dónde se deben aplicar los parches y brindar información importante sobre el origen de las amenazas.(PCI Security Standards Council, 2022)

Las reglas y directivas que se aplican dependen de la necesidad de protección de la compañía, mediante plantilla preconfiguradas dentro de los productos, aunque muchas de las veces se necesita realizar una aplicación de regla con expresiones regulares para poder establecer de una manera más exacta lo que necesitamos bloquear o proteger, con base en normas y estándares como puede ser PCI-DSS utilizado para el sector bancario preferentemente. (INCIBE, 2016)

En resumen, y según (SkyhighSecurity, 2022), las normativas PCI-DSS en cuanto a la protección de fuga de información de una empresa financiera exige que:

- Se encripte la información almacenada de titulares de tarjetas, utilizando algoritmos admitidos. Se debe escanear continuamente los sistemas de almacenamiento y equipos involucrados que puedan revelar información sensible.

- Se proteja la información de los usuarios de tarjetas enviados a través de redes publicadas. La encriptación debe ser utilizada para preservar la data que viaja a través de redes publicadas.

- Se debe restringir el acceso a información de los usuarios de tarjetas. Todos los colaboradores dentro de una compañía financiera grande o pequeña, que no ocupan acceder a datos de los usuarios de tarjetas no deben tener acceso a ellas. Las personas que necesariamente deben hacerlo necesitan documentar y registrar todo tipo de acceso a esta data. (SkyhighSecurity, 2022)

1.6. Relación del análisis de DLP en función del aspecto legal.

La tecnología DLP además de ser preventiva, con el objetivo de evitar la fuga de información considerada sensible de una empresa financiera, puede ser una herramienta reactiva y además una herramienta de evidencia en caso de necesitar demostrar la fuga o el intento de fuga de información por parte de un colaborador empresarial.

En las distintas empresas clasifican su información y determinan que esta sea confidencial o crítica, dependiendo del círculo de negocio al cual se dedican, así como del público al cual prestan servicios, dentro del marco legal para la protección de datos, en el país existen distintas leyes las cuales pueden colaborar, primero para identificar qué información puede ser sensible, confidencial, o pública, así como para proteger la misma.

Según indica la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), vigente desde el año 2004;

> *«Art. 6.- Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República»* (LOTAIP, 2004)

En el caso de una investigación por parte de instituciones públicas autorizadas sobre la violación de los derechos humanos en la constitución política de la República, declaraciones, acuerdos, convenciones, documentos internacionales y el ordenamiento jurídico, no se puede presentar ninguna objeción. Se excluye el procedimiento determinado en investigaciones anteriores. (LOTAIP, 2004)

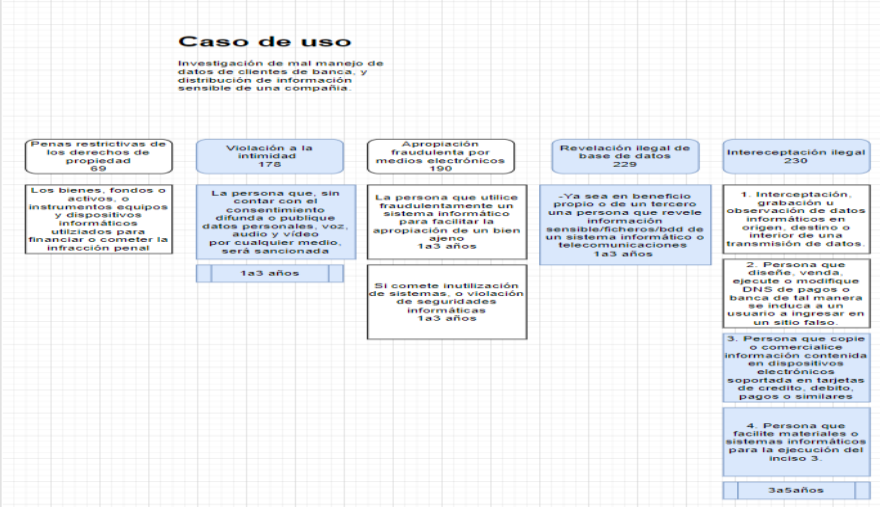
Este tipo de leyes pueden ser aplicadas, a través de un profesional de la ley, tanto a nivel de empresas del sector público como en el sector privado, en un eventual acuerdo de confidencialidad para establecer la importancia de la información que el colaborador o empleado puede manipular durante su estancia de ejercicio laboral, y de esta manera poder mitigar una posible fuga de información.

Como normativa interna de una compañía que busca preservar su información crítica, la cual manipula diariamente su personal, se deben aplicar normativas internas para su protección, como informar oportunamente de las sanciones a las cuales se pueden enfrentar, las personas que incumplan las normativas que contienen el acuerdo de confidencialidad y del Reglamento interno de la compañía, familiarizando las medidas que pueden llegar a tomarse en caso de ser necesario. (Castro, 2020)

Establecer e informar al colaborador las medidas para que, de modo disuasivo, contener la decisión mal tomada que pueda llegar a cometer un colaborador, con base en el COIP, en el apartado de Delitos contra la seguridad de los activos de los sistemas de información y comunicación. (GDPR Legal, 2021)

Figura 20

Caso de uso infracción de leyes fuga de información



Nota: En esta figura se observa los artículos del COIP que corresponden a delito informático, sombreando los artículos referentes al caso de uso del ejercicio de fuga de información.

Dentro del Código Orgánico Integral Penal, y con fines académicos, se tiene una idea de las sanciones que se pueden aplicar dentro de un hipotético caso de fuga de información, lo que indica una idea, como se había indicado líneas antes; disuasiva para con el personal que pueda tener acceso a una información confidencial, cabe recalcar que un profesional de la ley tiene la visión más clara para aplicar las leyes y normas que rigen el estado, el presente artículo únicamente trata de informar con base en lo investigado, la aplicación de leyes en caso de una posible fuga de información.

CAPÍTULO II – ARTÍCULO PROFESIONAL

1.1. Resumen

La información que poseen las empresas financieras y emisores de tarjetas de crédito en el país, como: Diners Club del Ecuador, Banred, Banco Pichincha, Banco Pacífico, Banco de Guayaquil y Pacificard e Interdin respectivamente, son empresas que trabajan con data extremadamente sensible, para lo cual necesitan proteger la información de posibles fugas, robos o secuestros de datos.

En la investigación se explica la utilidad de las soluciones *Data Loss Prevention* (DLP), mediante comparativas, análisis, encuestas e inclusive el aspecto legal en caso de posibles fugas de información o *Principal Account* Number (PAN), con el fin de esclarecer y socializar la importancia del uso de herramientas DLP para proteger los datos tanto de los usuarios internos de las compañías financieras como de los mismos clientes.

Se logró estudiar las distintas posibilidades y opciones para que, con base en la necesidad del cumplimiento obligatorio por parte de la Superintendencia de Bancos, y la normativa PCI-DSS, las personas, profesionales y encargados de compañías financieras elijan con mayor claridad una solución que se adecúe a sus necesidades y recursos.

Palabras clave:
DLP, PCI-DSS, seguridad, financiero, PAN.

1.2. Abstract

The information held by financial companies and credit card issuers in the country, such as: Diners Club del Ecuador, Banred, Banco Pichincha, Banco Pacífico, Banco de Guayaquil and Pacificard and Interdin respectively, are companies that work with extremely sensitive data, for which they need to protect the information from possible leaks, theft or data kidnapping.

The research explained the usefulness of DLP solutions, through comparisons, analysis, surveys and even the legal aspect in case of possible information leaks or PAN, in order to clarify and socialize the importance of using DLP tools to protect data. data both from internal users of financial companies and from the clients themselves.

It was possible to study the different possibilities and options so that, based on the need for mandatory compliance by the Superintendence of Banks, and the PCI-DSS regulations, people, professionals, and managers of financial companies choose more clearly a solution that suits your needs and resources.

Keywords

DLP, PCI-DSS, security, financial, PAN.

1.3. Introducción

En la actualidad, la industria financiera está considerada como un sector de los más atacados por ciberdelincuentes que buscan apropiarse de información sensible, con distintos fines, por lo que resulta necesaria la concientización de la protección de datos en este tipo de industrias, en américa latina un significativo número de entidades financieras aún no tienen establecidas herramientas, soluciones, inspecciones y procesos para mitigar este tipo de ataques. (OEA, 2020)

Muchos de los ataques sufridos por entidades financieras, en su mayoría pequeñas e inmaduras en términos de seguridad de la información, suelen ser desde adentro, trabajadores insatisfechos y con pocos escrúpulos optan por filtrar información, por lo que es en extremo necesaria la implementación de herramientas de seguridad para evitar la fuga de información.(OEA, 2020)

La superintendencia de bancos, ente regulador para todo tipo de compañía financiera, ya sea banco o emisor de tarjetas, realiza constantemente auditorías para analizar el nivel de seguridad y cumplimiento de estas empresas dedicadas a la banca, una de las normativas en las que se basa para analizar el cumplimiento es el conjunto de normas PCI-DSS, normativas específicas para grupos de empresas financieras, en su estándar de seguridad de datos y de requisitos y procedimientos de evaluación para entidades financieras establecen artículos específicos correspondientes a la fuga de información y la implementación de herramientas DLP, las cuales en el presente artículo se toman en cuenta para el análisis, comprensión y eventual aplicación del lector.

Los requisitos de PCI DSS se aplican a entidades financieras con entornos que almacenan, procesan o movilizan datos de cuentas (tarjetas, cuentas, contactabilidad, etc.), así como a entidades con entornos que pueden afectar la seguridad del CDE. Ciertos requisitos de PCI-DSS también pueden aplicarse a entidades cuyo entorno no almacene, procese ni transmita datos de cuenta, como entidades que subcontratan operaciones de pago o administración de CDE. Las empresas que subcontratan entornos de pago u operaciones de pago a terceros son responsables de garantizar que el tercero proteja los datos de la cuenta de acuerdo con los requisitos PCI DSS aplicables. (PCI Security Standards Council, 2022)

1.4. Metodología

El enfoque de la presente investigación es de tipo cuantitativa, bibliográfica comparativa ya que estudia la realidad en su contexto natural, exactamente como se manifiesta, y trata de comprender los fenómenos o interpretarlos según los significados que tienen para las personas involucradas. En investigación se involucra el uso y recolección de una amplia gama de materiales, investigaciones, encuestas, experiencias laborales, comparativas, observaciones, imágenes, artículos legales y normativas, que describen la realidad del tema, además de un estudio de la solución DLP para así entender la importancia de la herramienta en relación con la mitigación de la fuga de información. (Rodríguez y Gil, 1996)

El estudio realizado a la herramienta DLP muestra conclusiones importantes basadas en la diferencia de cada marca o licencia para que, según las necesidades y recursos de las compañías financieras puedan optar por una solución u otra.

1.5. Conceptos Generales

Data Loss Prevention, es una solución de prevención de fuga de información, que sirve para monitorear, bloquear y aislar eventos que puedan ocasionar filtración de la información.

Emisor de tarjetas, son entidades financieras encargadas de imprimir tarjetas de crédito o débito para proveer a sus clientes.

PCI-DSS, Payment Card Industry Data Security Standard, conjunto de normas y reglas que establecen requerimientos mínimos para el funcionamiento de entidades financieras o emisoras de tarjetas.

PAN, Principal Account Number, como su traducción del inglés indica es el número principal de cuenta de un usuario en una entidad bancaria.

CDE, Cardholer Data Environment, es el entorno donde la data de un usuario de tarjeta se encuentra, y este entorno debe estar protegido con requisitos específicos establecidos en la normativa PCI-DSS.

LOTAIP, es la Ley Orgánica de transparencia y acceso a la información pública, la cual garantiza el derecho a acceder a las distintas fuentes de información.

BYOD, Bring Your Own Device, por su traducción del inglés “traer tu propio dispositivo”, es la práctica en la que un empleador incita a sus colaboradores a utilizar sus propios recursos o dispositivos con los que cuenten en casa.

CASB, Cloud Access Security Brocker, es una solución para garantizar la seguridad de la información en la nube, protegiendo la información entre el usuario y los servicios alojados en cloud.

1.6. Investigaciones previas realizadas

En el presente artículo se muestran las siguientes fuentes de investigación:

Con base en las publicaciones de (Capterra, 2021) acerca de las distintas soluciones de prevención de pérdida de datos, indica muchas soluciones DLP y las reseñas de los usuarios que han experimentado con las herramientas DLP.

En la publicación de (CEPAL, 2020), muestra el cambio de vida que el planeta sufrió por motivo de la Sars-Cov2 y las nuevas tecnologías que fueron, obligatoriamente aplicadas en muchas compañías para la continuidad del negocio.

El presente artículo se basa en la información emitida por entidades tanto gubernamentales como de normativas establecidas específicamente para empresas orientadas al ámbito financiero, estas entidades fueron (PCI Security Standards Council, 2022) y en el aspecto legal con las entidades gubernamentales.(LOTAIP, 2004)

Periódicos y publicaciones como (El Pais, 17 Jun 2020) aportaron al presente artículo, en el tema de la fuga de información y su repercusión en Latinoamérica siendo una de las zonas más afectadas por ataques cibernéticos y escenarios de pérdida de datos.

1.7. Análisis de resultados

Con base en la investigación realizada, se establece que existen muchas herramientas en el mercado, que colaboran para poder cubrir las necesidades de las compañías financieras en cuanto a la mitigación de fuga de información, la idea siempre será basarse en cuadrantes de análisis de productos, las necesidades del negocio, las funcionalidades de las herramientas, y las normativas que se deben cumplir; de esta manera, aplicando buenas prácticas y procedimientos documentados y metodológicos se puede implementar y robustecer una solución DLP de la manera más adecuada para nuestras compañías o clientes financieros, coadyuvando a la seguridad de la información, al flujo del negocio e incluso al cliente final con su información protegida, sirviendo así, no solo a las compañías si no, al país entero.

Tabla 1

Características de las soluciones DLP de paga.

Funcionalidades		**Soluciones DLP de paga**			
		McAfee DLP	Safetica DLP	ForcePoint DLP	Symantec DLP
Cumplimiento PCI-DSS	Restricción de acceso a data confidencial	☑	☑	☑	☑
	Cifra y protege información sensible	☑	☑	☑	☑
	Visión de información sensible publicada	☑	☑	☑	☑
Funcionalidades adicionales	Directivas de seguridad administrables	☑	☑	☑	☑
	Análisis forense	☑	☑	☑	☑
	Notificaciones y alertas	☑	☑	☑	☑
	Administración centralizada	☑	☑	☑	☑
	Protección de almacenamiento extraíble	☑	☑	☑	☑
Objetivo	PCI-DSS	☑	☑	☑	☑

Nota. La tabla representa las funcionalidades de las soluciones de paga y su cumplimiento con las normativas PCI-DSS.

Tabla 2

Características de las soluciones DLP Open Source.

Funcionalidades		Soluciones DLP *OpenSource*			
		MyDLP	SecureTrust DLP	NightFall DLP	CoSoSys DLP
Cumplimiento PCI-DSS	Restricción de acceso a data confidencial	☑	☑	☑	☑
	Cifra y protege información sensible	☑	☑	☑	☑
	Visión de información sensible publicada	☑	☑	☑	☑
Funcionalidades adicionales	Directivas de seguridad administrables	☑	☒	☑	☑
	Análisis forense	☒	☒	☒	☑
	Notificaciones y alertas	☑	☑	☑	☑
	Administración centralizada	☑	☑	☑	☑
	Protección de almacenamiento extraíble	☑	☒	☒	☑
Objetivo	PCI-DSS	☑	☑	☑	☑

Nota. La tabla representa las funcionalidades de las soluciones *open source* y su cumplimiento con las normativas PCI-DSS.

Con base en el análisis de resultados se determina que aún las soluciones *Open Source* tienen la capacidad de cubrir las necesidades para el cumplimiento de normativas PCI-DSS, lo que puede convencer al cliente o encargado de la implementación de estas soluciones para mitigar la fuga de información, serían las funcionalidades que tienen estas herramientas y las necesidades de la compañía en cuanto a la seguridad de la información sensible.

1.8. Resultados – Discusión

En la tabla 1, se muestra un resumen del análisis de uso de las soluciones DLP de acuerdo con la condición de paga u Open Source y las funcionalidades de las herramientas tomadas como muestras para dicho estudio.

En la tabla 2, se expresa la capacidad de las soluciones *open source* DLP para cubrir no solo las necesidades de las compañías financieras, sino que además, cumplen con la normativa PCI-DSS sin inconvenientes.

Se observa que las tecnologías disponibles tienen gran cantidad de prestaciones para la protección de datos sensibles de una compañía financiera, por lo que, el uso de estas dependerá de las necesidades de la compañía, así como de sus recursos.

En cuanto al cumplimiento de las normativas PCI-DSS, todas las soluciones tomadas como muestras tienen la capacidad de cumplir con la normativa, ergo, en caso de auditorías no debería existir inconvenientes al momento de ser examinados.

Cabe recalcar que las herramientas denominadas *Open Source,* suelen no tener un respaldo de soporte técnico, al mismo nivel que una solución de paga.

CONCLUSIONES

Con base en las normativas PCI, hemos podido reconocer las formas más comunes de fugas de información y así mismo las técnicas de mitigación para que una falla así pueda ocurrir, identificando las brechas de seguridad y aplicando normativa PCI para cubrirlas de la mejor manera.

Mediante las comparativas realizadas de ciertos productos o soluciones DLP, se puede objetivar el uso de las herramientas, enfocados al giro del negocio que en este caso son las industrias financieras, y que, con la normativa PCI aplicada, robustecer la seguridad en contra de la fuga de información.

Tomando en cuenta las soluciones DLP de paga y las herramienta open source o de libre uso, y con base en las necesidades y situaciones de la compañía dentro del presente documento, pudimos comparar las herramientas para comprender de mejor manera las utilidades de una u otra opción, los pros y contras para esclarecer el funcionamiento y uso que se les va a dar, de acuerdo a los análisis pudimos, en este documento colocar al líder de acuerdo a los cuadrantes como la mejor opción de DLP en el mercado, McAfee DLP.

Mediante encuestas se validó el uso de las herramientas y marcas open source o de paga, para tener una muestra de que herramienta es más usada en el ámbito laboral profesional, la encuesta demuestra que la marca McAfee es la más usada en el medio financiero, con al menos 30 personas encuestadas que se desarrollan y laboran en empresas relacionadas a banca.

Las comparativas realizadas con base en su uso, facilidad de configuración, precio y prestaciones dan una idea de que solución puede ser la más conveniente a tomar en cuenta para cubrir la necesidad de mitigar la fuga de información, para el encargado de un área de seguridades en una entidad financiera y que pueda cumplir con las normativas establecidas para este tipo de compañías.

RECOMENDACIONES

Se recomienda que todas las instituciones, tanto públicas como privadas, socialicen el conocimiento de la información que procesan, con el objetivo de que el equipo interno la organización genere una cultura del compromiso y peligro de una posible fuga de información.

En las instituciones financieras directamente, es recomendable establecer planes de implementación y mejoramiento de un Sistema De Gestión De Seguridad De La Información (SGSI) y la respuesta que se necesita para tratar los incidentes en caso de existir una posible fuga de información y así desarrollar el nivel de seguridad de la información.

Es recomendable el análisis de herramientas DLP a nivel de cloud, con el fin de proteger las arquitecturas en nube como azure o incluso el mismo Ofice365, herramientas tipo Cloud Access Security Brocker (CASB), resultan ser importantes ahora que los servicios en nube son lo más utilizado.

Sobre todo, en las entidades financieras, se recomienda el uso de soluciones DLP de pago y con licenciamiento, ya que las características con las que cuentan coadyuvan a la protección de data importante y confidencial, propiedad de la compañía o de los mismos usuarios o clientes.

BIBLIOGRAFÍA

AmericaEconomía. (2020). *La fuga de información es una de las razones por las que las empresas pierden más dinero*. https://www.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di

Byte TI. (2018). Safetica DLP Suite. *Byte*. https://revistabyte.es/analisis/safetica-dlp-suite/

Capterra. (2021). *Software de prevención de pérdida de datos*. https://www.capterra.ec/directory/31106/data-loss-prevention/software

CEPAL. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad*. https://doi.org/1564-4227

CISCO. (2022). El malware común desplaza al Ransomware como principal ciber-amenaza. *27 Julio 2022*, 1. https://news-blogs.cisco.com/emear/es/2022/07/27/el-malware-comun-desplaza-al-ransomware-como-principal-ciber-amenaza/

Claudio Líbano Manzur; Marcelo Huerta Miranda. (1996). *Delitos informáticos*. https://isbn.cloud/9789562380928/delitos-informaticos/

ElPais. (2020). *Fuga de información: cómo evitar poner en riesgo los activos de las empresas con el teletrabajo*. https://elpais.com/retina/2020/06/15/innovacion/1592217009_535570.html

Gartner. (2020). *Gartner*.

Gregorio Rodríguez Gómez, Javier Gil Flores, E. G. J. (1996). *METODOLOGIA DE LA INVESTIGACIÓN CUALITATIVA*.

Lagua, A. (2021). *HERRAMIENTAS DATA LOSS PREVENTION (DLP) OPENSOURCE, PARA LA SEGURIDAD DE LA INFORMACIÓN*. https://repositorio.pucesa.edu.ec/bitstream/123456789/3121/1/77287.pdf

LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA, (2004). https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf

LOTAIP. (2004). *LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA*. https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

McAfee. (2020). *McAfee Data Loss Prevention Endpoint*. https://www.mcafee.com/enterprise/es-es/assets/data-sheets/ds-dlp-endpoint.pdf

McAfee. (2021). *Guía del producto de McAfee Data Loss Prevention*. https://docs.trellix.com/bundle/data-loss-prevention-11.4.x-product-guide/page/GUID-8BDBB6D0-CD54-418A-AF4A-6B414F0488A7.html

NacionesUnidas. (2022). *ODS 9- INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURA*. https://ecuador.un.org/es/sdgs/9

Navarro, J. (2019). *Desarrollo de un modelo de seguridad utilizando herramientas Data Loss Prevention (DLP), en las instituciones de Educación superior (IES). Caso Universidad ECOTEC*. http://repositorio.uees.edu.ec/bitstream/123456789/1437/1/Trabajo de titulación Johanna Navarro.pdf

Nelson Diaz. (2020). *Administración y Gestión de McAfee DLP*. https://www.mcafee.com/enterprise/en-us/assets/guides/gd-dlp-administration-and-management.pdf

OEA. (2020). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe*. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

PCI Security Standards Council. (2022). *Payment Card Industry Estándar de Seguridad de Datos*.

Purohit, B., & Singh, P. P. (2013). *Data leakage analysis on cloud computing*.

Quobit. (2021). *Así funciona el Algoritmo de Luhn para generar números de tarjetas de crédito*. https://www.quobit.mx/asi-funciona-el-algoritmo-de-luhn-para-generar-numeros-de-tarjetas-de-credito.html

Rider, J. (2021). *Como cumplir con PCI*. http://cumplirpci.blogspot.com/

Rosana Castro. (2020). *ACUERDO DE CONFIDENCIALIDAD*. https://derechoecuador.com/acuerdo-de-confidencialidad/

SkyhighSecurity. (2022). *PCI DSS Compliance Requirements*. https://www.skyhighsecurity.com/en-us/about/cloud-compliance/pci-dss-compliance-requirements.html

SoftwareReviews. (2021). *SoftwareReviews 2021 DLP Quandrant*.

Surya R Raj, Asha Cherian, A. A. (2013). A Survey on Data Loss prevention Techniques. *International Journal of Science and Research (IJSR)*.

Tecnozero. (2021). *Safetica líder en el cuadrante DLP de SoftwareReviews 2021*. https://www.tecnozero.com/dlp/safetica-lider-en-el-cuadrante-dlp-de-softwarereviews-2021/

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

Formato de entrevista hacia profesionales de seguridades de IT en empresas del sector financiero, Diners Club del Ecuador, Banred, Seguros Pichincha, Bco Bolivariano, Bco Pichincha, etc.

Comparativa soluciones Data Loss Prevention (DLP)

¿Qué solución DLP de paga, ha utilizado al menos una vez?

- McAfee
- Safetica
- Trustwave
- ForcePoint
- TrendMicro
- Symantec
- Otra….

¿Qué solución DLP de paga, le parece la más completa?

- McAfee
- Safética
- Trustwave
- ForcePoint
- TrendMicro
- Symantec
- Otra….

¿Qué solución DLP de paga, le parece la más intuitiva o fácil de administrar/configurar?

- McAfee
- Safética
- Trustwave
- ForcePoint
- TrendMicro
- Symantec
- Otra….

¿Qué solución DLP de paga, le parece la mejor opción en relación costo/beneficio?

- McAfee
- Safética
- Trustwave
- ForcePoint
- TrendMicro
- Symantec
- Otra….

¿Qué solución DLP open source, ha utilizado al menos una vez?

- MyDLP
- SecureTrust's DLP
- CoSoSys' Endpoint Protector
- Nightfall
- Commvault´s Orchestrate
- Otra…

¿Qué solución DLP open source, le parece la más completa?

- MyDLP
- SecureTrust's DLP
- CoSoSys' Endpoint Protector
- Nightfall
- Commvault´s Orchestrate
- Otra…

¿Qué solución DLP open source, le parece la más intuitiva o fácil de administrar/configurar?

- MyDLP
- SecureTrust's DLP
- CoSoSys' Endpoint Protector
- Nightfall
- Commvault´s Orchestrate
- Otra…

¿Qué solución DLP open source, le parece la mejor opción costo/beneficio?

- MyDLP
- SecureTrust's DLP

- CoSoSys' Endpoint Protector
- Nightfall
- Commvault´s Orchestrate
- Otra…

¿Cree usted que una solución de prevención de fuga de datos (DLP) sería importante en su compañía?

- MyDLP
- SecureTrust's DLP
- CoSoSys' Endpoint Protector
- Nightfall
- Commvault´s Orchestrate
- Otra…

ANEXO 2

Tabla de aspectos legales en la protección de datos.