ANÁLISIS DE SOLUCIONES DPL (PREVENCIÓN DE PERDIDA DE DATOS) COMO ESTRATEGIA PARA LA SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES COLOMBIANAS

CRISTIAN CAMILO GANTIVA RINCON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ACACIAS
2021

ANÁLISIS DE SOLUCIONES DPL (PREVENCIÓN DE PERDIDA DE DATOS) COMO ESTRATEGIA PARA LA SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES COLOMBIANAS

CRISTIAN CAMILO GANTIVA RINCON

Trabajo de grado presentado como requisito para optar al título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director: YENNY STELLA NUÑEZ
Ingeniera de Sistemas, Especialista en Seguridad informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ACACIAS
2021

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Dedicatoria

Dedico este proyecto de grado a una persona muy querida y amada por mí, mi tía Yolanda Rincón Moreno quien me ha apoyado y estado pendiente de mí en cada momento de mi vida, me ha empujado y motivado para crecer cada día no solo como profesional sino también como persona.

AGRADECIMIENTOS

Agradezco a todos mis familiares y a amigos que me apoyaron este proceso de formación para no desistir. A mi padre Marco Gantiva que me ha apoyado incondicionalmente en todas las decisiones que he tomado.

A mi asesora del proyecto de grado la ingeniera Yenny Stella Nuñez quien fue guía en este proceso de formación y aprendizaje.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTADO DE FIGURAS

Glosario

AMENAZA: acción que podría tener un potencial efecto negativo sobre un activo, puede afectar la disponibilidad, confidencialidad o la integridad.

CONFIDENCIALIDAD: Garantizar que la información sólo sea revelada a las personas con la autorización adecuada. (Previene contra la divulgación no autorizada de la información).

DISPONIBILIDAD: Garantizar que los usuarios autorizados tienen acceso a la información cuando lo necesiten. (Previene contra la denegación no autorizada de Información).

DLP: referente a seguridad informática, comprendida por un conjunto de herramientas destinadas a evitar que la información crítica o confidencial de una organización se filtre por sus usuarios para ser usada de forma indebida. Por medio de la motorización, detección y bloqueo de datos sensibles.

HARDWARE: componente físico de un sistema informático.

INFORME: presenta el resultado de la auditoría realizada al cliente, identificando las vulnerabilidades encontradas, resaltando los puntos que deben corregirse y aquellos en la que el tipo de seguridad es la correcta.

PROYECTO DE INVESTIGACIÓN: es un plan desarrollado anteriormente a un trabajo de investigación, su objetivo es presentar información mediante un conjunto de datos en base a un problema para generar una hipótesis con el fin de dar una solución. Se realiza en base a una metodología científica ejemplo, proyecto de desarrollo social, proyecto desarrollo tecnológico.

RIESGO: probabilidad de que ocurra un incidente de seguridad.

RIESGO Y CONTROL INFORMÁTICO: su propósito es analizar el funcionamiento y cumplimiento de las medidas que se toman o se piensan tomar junto con su efectividad.

SEGURIDAD EN REDES: Evita el ingreso de personal no autorizado a los quipos, impidiendo que se vulnera a la privacidad o tenga acceso a información confidencial, garantizando la protección contra amenazas ya sean de tipo externas o internas en la organización.

SEGURIDAD EN SISTEMAS OPERATIVOS: la seguridad en este tipo de sistema hace referencia a tres aspectos para los sistemas operativos los cuales son la confidencialidad, integridad y disponibilidad de la información. Esta seguridad en

los sistemas operativos se encarga de vitar la perdida de datos o el acceso a intrusos (personal ajeno) a los sistemas.

SEGURIDAD INFORMATICA: son medidas que se toman para evitar la ejecución de operaciones no autorizadas sobre un sistema informático, cuyos efectos pueden dañar la información de un sistema.

SNIFFER: son aplicaciones desarrolladas para analizar las redes y su principal función es la de capturar los paquetes de datos que viajan por una red, registrando información de los periféricos y las actividades realizadas en un dispositivo. Capturando cada paquete de información codificándolo y permitiendo a su propietario tener acceso a esta información.

SOFTWARE: es un proceso computacional que implementa una funcionalidad comunicativa, autónoma en una aplicación.

VULNERABILIDAD: es una debilidad presente en un sistema informático que puede ser usada por una persona ajena con el fin de causar daño, estas vulnerabilidades se pueden ser tanto en hardware como software. La existencia de esta vulnerabilidad no significa que se produzca un daño en un equipo, lo que quiere decir es que se presenta un tipo de debilidad que puede ser aprovechada por una persona para causar daño.

RESUMEN

Hoy en día la mayoría de organizaciones manejan datos sensibles y confidenciales, ya que esto puede causar pérdidas no solo monetarias sino de credibilidad, para evitar estos problemas existen herramientas de DLP que permiten configurar cuales son estos datos sensibles mediante configuraciones pueden otorgar permisos a los usuarios para el manejo de este tipo de información, teniendo en cuenta que esto no afecte el correcto funcionamiento de las actividades.

La información que manejan las organizaciones está expuesta frecuentemente a riesgos como pérdida o fuga de datos. Un DLP es un sistema que se encarga de monitorear los datos de una organización en tiempo real que se encuentran en uso, reposo o movimiento, realizando evaluación de estos mediante políticas definidas que le permiten tomar acciones predefinidas las cuales pueden ser, bloquear el tráfico, encriptar los datos, generar alertas a los usuarios o administradores.

El proyecto se desarrolla en base a la consulta de diferentes fuentes bibliográficas disponibles, con el objeto de conocer el funcionamiento, evolución y uso de los DLP, estableciendo los riesgos presentes en las empresas al momento de almacenar y compartir información y los factores que motivan a implementar este tipo de sistemas de prevención de perdida de datos. A su vez, se estructura las funciones, características, fases y recursos de un DLP identificando que tipo de estrategias y controles se pueden efectuar para prevenir la fuga de información en las organizaciones.

ABSTRACT

Today most organizations handle sensitive and confidential data, since this can cause losses not only monetary but also credibility, to avoid these problems there are DLP tools that allow you to configure which is this sensitive data allowing through configurations to grant permissions to users for the handling of this type of information, taking into account that this does not affect the correct functioning of the activities.

The information handled by organizations is frequently exposed to risks such as loss or leakage of data, a DLP is a system that is responsible for monitoring the data of an organization in real time that is in use, rest or movement, evaluating these through defined policies that allow you to take predefined actions which can be, block traffic, encrypt data, generate alerts to users or administrators.

The project is developed based on the consultation of different bibliographic sources available, in order to know the operation, evolution and use of DLP, establishing the risks present in companies when storing and sharing information and the factors that motivate implement this type of data loss prevention systems. At the same time, the functions, characteristics, phases and resources of a DLP are structured; identifying what type of strategies and controls can be carried out to prevent the leakage of information in organizations.

INTRODUCCION

La pérdida de información es una problemática que afecta a las organizaciones, pudiéndose presentar en cualquier momento cuando no se implementan los controles adecuados, lo que puede generar fuga de datos sensibles, causando un impacto negativo y en ocasiones esta problemática no es detectada. La mayoría de veces las organizaciones desconocen los métodos para proteger sus datos y la importancia que estos poseen. No se tiene un correcto manejo de esta información, no cuentan con buenas prácticas y no existen políticas para preservarlas, dándose fuga de información significando gastos más altos de funcionamiento, alteración en la continuidad del negocio, pérdida de clientes, junto con riesgos operativos legales y de reputación.

En ocasiones el desconocimiento de cómo proteger los datos sensibles hace que la información pueda ser extraída de manera fácil ya sea por personal que labora en la organización o personas externas a través de copias, alteración o eliminación, al no tener claro que datos son sensibles. La problemática consiste en saber ¿de qué manera deben ser protegidos los datos y por qué implementar un sistema de prevención de perdida de datos? debido que todos los datos no tienen el mismo valor para la entidad, es decir, los datos deben ser manejados y protegidos con un tratamiento distinto según su nivel de importancia dentro de la organización. En este sentido un sistema DLP permitiría lograr controles de seguridad, conociendo los datos sensibles y confidenciales, consiguiendo su clasificación en función de su relevancia y nivel de riesgo, buscando la creación de políticas para conservar la información y poder acceder a ella.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La pérdida de datos es un desafío en las organizaciones y empeora cada día. El estudio anual de Ponemon de 2019 sobre costos de violación de datos encontró que el costo promedio global de una violación de datos es de $ 3.92 millones, un aumento del 1.5% con respecto a 2018. Además, Ponemon informó que las organizaciones de todo el mundo están lidiando con un promedio de 20 incidentes de pérdida de datos por día.

Otros hallazgos son los actores malintencionados que apuntan a datos confidenciales, los ciberdelincuentes se dirigen a los datos confidenciales por una variedad de motivos, como el espionaje corporativo, la ganancia financiera personal y la ventaja política. Las violaciones de datos más graves están dadas por la incidencia de violaciones de datos que aumenta en magnitud cada año a nivel mundial. Por ejemplo, en 2018 en América del Norte, se registraron 1244 incidentes de filtración de datos con 446,52 millones de registros expuestos (un aumento del 126% con respecto al año anterior). Los datos confidenciales compartidos en la nube son otro factor importante hoy en día una gran cantidad de datos se comparten en la nube, por lo que se requiere de soluciones de DLP que brinden protección a este tipo de datos.

Los crecientes desafíos para proteger los datos están impulsando la demanda de soluciones DLP. El mercado de prevención de pérdida de datos se valoró en $ 1,21 mil millones en 2019 y se espera que alcance los $ 3,75 mil millones para 2025, a una tasa de crecimiento anual del 23,59%[1] . Los principales ataques que llevan a este crecimiento de la implementación de herramientas DLP en las organizaciones es el aumento de los ataques cibernéticos, un crecimiento masivo en la información manejada por las organizaciones, más unidades de almacenamiento en los puntos finales de red o la nube, falta de personal con conocimiento en seguridad informática y regulaciones más estrictas en cuanto a la confidencialidad de la información.

[1] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

1.2 FORMULACIÓN DEL PROBLEMA

¿Por qué es necesario y cuáles son los beneficios de implementar políticas y herramientas DLP en las organizaciones?

2. JUSTIFICACIÓN

En la actualidad el activo más preciado para una organización es su información y los datos que maneja, un DLP permite examinar, detectar, proteger, supervisar y administrar el contenido de los archivos, etiquetando la información confidencial y crítica, para que los usuarios no puedan divulgarla, eliminarla, alterarla, duplicarla o transferirla a terceras personas. Con el objetivo de gestionar su seguridad y políticas de uso en los diferentes sistemas de información dentro de la organización.

Se dará a conocer los beneficios que adquieren las organizaciones al implementar un sistema DLP como solución para proteger información sensible. Esta herramienta de seguridad de información ayuda a entender el significado de cada uno de los datos propios de la organización, identificando los riesgos que se presentan al momento de ser almacenados, manipulados y compartidos, clasificando y administrando cada uno de estos para el correcto manejo de la información.

El documento proporciona una descripción de la problemática que se tiene en la actualidad sobre el robo y pérdida de información en las organizaciones, los conceptos y antecedentes referentes a los DLP , los tipos que se pueden encontrar en el mercado, sus características, como contribuyen a la seguridad y cuáles son los más utilizados, además de la identificación de los requerimientos necesarios para que sean implantados de forma adecuada como solución para mantener la información a salvo en las empresas.

3. OBJETIVO GENERAL

Realizar el análisis de las distintas soluciones DPL como estrategia de seguridad de la información en las organizaciones.

3.1 OBJETIVOS ESPECÍFICOS

- Realizar el estado de arte sobre los distintos sistemas DLP de acuerdo a su evolución y uso en las organizaciones como solución de seguridad informática.

- Identificar los riesgos presentes en las organizaciones al momento de almacenar y compartir información y los factores que motivan a implementar sistemas de prevención de perdida de datos.

- Estructurar las funciones, características, fases y recursos de un DLP identificando que tipo de estrategias y controles se pueden implementar para prevenir la fuga de información en las organizaciones.

4. MARCO CONCEPTUAL Y TEÓRICO

Teniendo en cuenta la creciente evolución de la tecnología, de alguna manera hace que la protección de la información requiera ciertos niveles de seguridad eficientes con el fin de evitar y prevenir la pérdida, fuga, robo de información y uso indebido de los datos. Mediante el uso de la tecnología DLP se puede prevenir la perdida de información, salvaguardando el activo más importante de la organización y optimizando los recursos tecnológicos.

En general un Proyecto de DLP busca la correcta implementación de una plataforma que logre prevenir la fuga de información sensible utilizando herramientas de software perimetral y de cliente final, permitiendo atender los requerimientos de seguridad de la organización y los lineamientos de su administración.[2] La seguridad informática debe ser administrada según los criterios establecidos por los administradores y personal capacitado, previendo que usuarios externos y no autorizados puedan acceder a ella sin autorización[3]

Un DLP tiene como función detectar, identificar, supervisar y prevenir la fuga de información sensible en cada una de las organizaciones, protegiendo los datos mediante un ciclo de vida de la herramienta.
Los DLP se basan de acuerdo a los tipos de datos obtenidos:

- Datos en reposo: son los datos sensibles en que se verifica su almacenamiento en los medios de respaldo donde están contenidos.
- Datos de movimiento**:** se refiere a los datos que están en constaste observación por el proxy en el tráfico de la red, tales como la mensajería instantánea.
- Datos en uso: solo los datos manipulados por el usuario y son monitoreados por medio de las soluciones al punto final, como por ejemplo la extracción de información sensible en dispositivos extraíbles.

Tiene la ventaja que en una organización pueden elegirse los archivos a analizar para que en caso de intentar copiar o transferir la información estos archivos puedan bloquearse e identificar si la información ha sido duplicada.

[2] ALVARADO AVENDAÑO, Deiby. Diseño e implementación del proyecto de dlp (data loss prevention), para las direcciones (dirección administrativa, dirección finanzas, dirección de planeación y presupuestario y secretaria de gabinete) del ministerio de defensa nacional [en línea]. Bogotá. 2016. Disponible en http://alejandria.poligran.edu.co/jspui/bitstream/10823/918/1/DLP-%20Alejandro%20Alvarado.pdf

[3] CALCEDO CUCHIMBA, Mildred y PERAFAN RUIZ, John. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca [en línea]. Popayán. 2014., 27 p. disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

DLP (Data Loss Prevention o Prevención de Pérdida de Datos), son sistemas que tienen la principal función de identificar, clasificar, monitorear la información de las empresas [4]con el desarrollo de este trabajo se trataran los temas y palabras claves puntuales e importantes del proyecto.

Medidas de seguridad se suelen clasificar en cuatro niveles:

• Físico: impedir el acceso físico a los equipos informáticos, a los medios de transmisión (cables de argón, por ejemplo), etc.

• Vigilancia, sistemas de contingencia, recuperación.

• Lógico: establecer programas o algoritmos que protejan el almacenamiento, acceso, transmisión, etc. Contraseñas, Criptografía, cortafuegos.

• Administrativo: en caso de que se haya producido una violación de seguridad, ¿cómo se delimitan las responsabilidades? Publicación de la política de seguridad.

• Legal: ¿qué se hace en caso de ataques, violaciones, que hayan sido comprobadas? Normalmente, transcienden el ámbito empresarial y son fijadas por los gobiernos o instituciones internacionales.

Parida de información este tipo de perdida puede darse a diversos factores dentro de los cuales se encuentran fallo de hardware o sistema operativo, error humano, virus informático o desastres naturales entre otros. Sin los debidos mecanismos que permitan salvaguardarla de cualquier riesgo, amenaza o vulnerabilidad se puede ocasionar la pérdida de su confidencialidad, disponibilidad e integridad.

Filtración de datos en la evolución de la fuga de información, los cambios han sido las maneras y tecnologías por medio de las cuales se filtra o pierde, el problema de la fuga de información existe desde cuando los humanos manejan información.

El panorama en las empresas colombianas no es tan alentador el impacto en los incidentes de seguridad digital causan peritadas millonarias por daños a los activos e infraestructura, o sanciones, multas y gastos legales[5] debido a que no se gestionan debidamente las inspecciones de las tecnologías de información (TI). Lo que se debe hacer es la prevención y detección oportuna para evitar la pérdida de confidencialidad de la información, puesto que las amenazas tienen a

[4] ACOSTA ROBLES, Ximena, desarrollo de un modelo de seguridad para la prevención de perdida de datos DLP en empresas pymes [en línea]. 2015 17p. disponible en http://200.24.220.94/bitstream/33000/4476/1/UDLA-EC-TIERI-2015-02.pdf

[5] Portafolio; Hay empresas que pierden hasta $4.000 millones por ciberataques; [sitio web]; [consulta: 22 de noviembre 2020]; disponible en: https://www.portafolio.co/negocios/empresas/auditorias-ti-ahorran-perdidas-por-ciberataques-531817

incrementarse debido a la implementación de nuevos modelos de tecnología que se convierten en herramientas de uso empresarial.
en Colombia más del 60% de las organizaciones encuestadas incurrieron en costos cercanos al millón de pesos por daños relacionados con ciberataques, mientras que el 20% gastaron entre 1 y 15 millones de pesos, el 15% entre 15 y 235 millones y el 5% presentó valores desaforados de hasta 4.000 millones de pesos, como consecuencia de incidentes de vulneración tecnológica[6]

[6] Portafolio; Hay empresas que pierden hasta $4.000 millones por ciberataques; [sitio web]; [consulta: 22 de noviembre 2020]; disponible en: https://www.portafolio.co/negocios/empresas/auditorias-ti-ahorran-perdidas-por-ciberataques-531817

5. EVOLUCIÓN Y USO EN LAS ORGANIZACIONES DE UN DLP

5.1 Clasificación de los datos

Este proceso consiste en separar y organizar los datos en grupos relevantes "clases" en función de las características que comparten como su nivel de sensibilidad y los riesgos que estos presentan, junto con las regulaciones de cumplimiento que los protegen. Para proteger los datos confidenciales, debe ubicarse, luego clasificarse según su nivel de sensibilidad y etiquetarse. Luego, las empresas deben manejar cada grupo de datos de manera que garanticen que solo las personas autorizadas puedan obtener acceso, tanto interna como externamente, y que los datos siempre se manejen en total cumplimiento con todas las regulaciones relevantes[7].

Se debe tener en cuenta la importancia de realizar esta clasificación de manera adecuada ya que cuando se hace correctamente el uso y protección de datos será más eficiente. Esto puede pasarse por alto cuando las organizaciones no comprenden su propósito, alcance y capacidades por completo.

5.1.1 ¿Por qué llevar a cabo la clasificación de datos?

La seguridad y privacidad de los datos se ve afectado cuando las organizaciones desconocen los datos que maneja, incluidos donde se encuentran almacenados y la manera de protegerlos.
Es recomendable que toda organización sepa lo siguiente para poder llevar una correcta protección de información:

- Que datos existen.
- Donde residen.
- Su valor y riesgo para la organización.
- Normativa de cumplimiento que rige los datos.
- Quien está autorizado a acceder y utilizar los datos.

Esto permite la creación de atributos para los datos que prescriben como proteger a cada grupo de acuerdo a los requisitos impuestos. Conociendo donde se encuentran los datos las organizaciones pueden aplicar protecciones que reducen el riesgo de ellos, eliminando redundancias de protección pudiendo enfocar los recursos de seguridad en las acciones correctas.

[7] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

De esta manera, la clasificación agiliza y fortalece los programas de protección de seguridad y privacidad de datos de las organizaciones.

5.2 Beneficios de la Clasificación De Datos

Actualmente la mayoría de organizaciones no conocen la ubicación de sus datos confidenciales ni cómo protegerlos, al conocer donde se alojan sus datos las organizaciones pueden obtener diversos beneficios.

- Mejorar la seguridad de datos.
- Apoyar el cumplimiento normativo.
- Aumentar la eficiencia y reducir el riesgo de operaciones comerciales.

5.2.1 Mejorar la seguridad de los datos

La clasificación de datos permite a las organizaciones salvaguardar datos confidenciales corporativos y de clientes. Ofreciendo siguientes ventajas:

- Disminuye la huella de datos confidenciales, siendo la seguridad de datos más efectiva.
- Reduce el acceso a datos confidenciales a usuarios autorizados.
- Comprender la importancia de los diferentes tipos de datos para protegerlos de una mejor manera.
- Optimizar los costos sin desperdiciar recursos de datos críticos menos importantes.

5.2.2 Apoyar el cumplimiento normativo

La clasificación de datos ayuda a determinar dónde se encuentran los datos regulados en toda la organización, garantiza que se implementen los controles de seguridad adecuados y que los datos sean rastreables y buscables, según lo exigen las regulaciones de cumplimiento ofreciendo las siguientes ventajas:

- Garantiza que los datos confidenciales se manejen de manera adecuada para diversas regulaciones.
- Ayuda a mantener el cumplimiento diario de todas las reglas, regulaciones y leyes de privacidad.
- Admite la recuperación rápida de información específica dentro de un periodo de tiempo establecido.
- Mejora la oportunidad de aprobar auditorias de cumplimiento.

5.2.3 Aumentar la eficiencia y reducir el riesgo de operaciones comerciales

Desde el momento en que se crea la información hasta que se destruye, la clasificación de datos puede ayudar a las organizaciones a garantizar que se protejan, almacenen y gestionar sus datos de forma eficaz. Esto ofrece los siguientes beneficios:

- Proporcionar un mejor conocimiento y control de los tatos con los que cuentan las organizaciones y comparten.

- Permitir el acceso y uso más fácilmente de los datos que maneja una organización.

- Facilitar la gestión de riesgos evaluando el valor de datos de una organización, el impacto de su perdida, robo o uso indebido.

5.3 Concepto de DLP

La terminología DLP (Data Loss Prevention) que en español traduce como prevención de perdida de datos, es un sistema que se encarga de monitorear los datos de una organización en tiempo real que se encuentran en uso, reposo o movimiento, realizando evaluación de estos mediante políticas definidas que le permiten tomar acciones predefinidas las cuales pueden ser, bloquear el tráfico, encriptar los datos y generar alertas a los usuarios o administradores.

Se puede decir que es un conjunto de herramientas tecnológicas y procesos donde se garantiza que datos confidenciales no puedan ser robados o se pierdan.

5.4 Por qué se crean los DLP

Los DLP se lanzaron al mercado a mediados de las décadas del 2000 debido a que las organizaciones buscaban soluciones a los riesgos que enfrentaban en su momento, el cual era el aumento de la piratería externa, considerada la principal causa de perdida de datos.

Las herramientas DLP han evolucionado con el tiempo según las necesidades cambiantes del mercado. En sus primeras etapas se enfocaban en la seguridad de redes para proteger los datos de amenazas externas y extracción de datos externos. Ejemplo de esto son las pruebas de penetración, escaneo de vulnerabilidades, firewalls, sistemas de prevención de intrusos.

En un principio la adopción de esta herramienta fue escasa ya que las soluciones DLP eran implementadas para áreas limitadas como, el monitoreo de correos electrónicos y web, mas no se pensaba en soluciones integradas.

Cabe resaltar que las primeras iteraciones no podían capturar los riesgos de pérdida y fuga de datos internos, el cual era un problema que venía en aumento, lo que causo que el interés de las organizaciones por esta herramienta disminuyera, asimismo por su complejidad, su costo, y la incapacidad de la tecnología DLP para demostrar su verdadero valor en el mercado.

A finales de la década del 2010 se empezó a tener nuevamente interés por los DLP, debido a nuevas regulaciones y más estrictas donde se exigía mayor privacidad y seguridad en los datos de las organizaciones.
Otra constante es asegurar el universo de datos en expansión dentro de organizaciones que se vuelven complejas, tales como la computación en la nube, trabajo remoto y computación móvil.
Se implementaron tecnologías de seguridad de punto final con el fin de proteger los datos alojados en los PC y dispositivos móviles implementando técnicas de cifrado de datos.

La tecnología DLP también ha madurado convirtiéndose en soluciones integrales más efectivas, capaces de prevenir, detectar y responder a los riesgos de pérdida y fuga de datos confidenciales.

Se prevé que el mercado global de prevención de pérdida de datos empresariales será testigo de una tasa de crecimiento anual compuesta del 16,28% durante el período de pronóstico para crecer a US $ 2.546 mil millones para 2023, aumentando de US $ 1.198 mil millones en 2018[8]

5.5 FUNCIÓN DE LOS DLP

Se enfoca en detectar y prevenir la pérdida, fuga o uso indebido de datos a través de infracciones, transmisiones ex-filtración y uso no autorizado[9]

[8] research and marke; Mercado de prevención de pérdida de datos empresariales: tendencias, oportunidades y previsiones de la industria hasta 2023; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.researchandmarkets.com/research/npbpsp/global_enterprise?w=4

[9] crowdstrike; ¿QUÉ ES LA PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) ?; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.crowdstrike.com/epp-101/data-loss-prevention-dlp/?utm_campaign=dsa&utm_content=latam&utm_medium=sem&utm_source=goog&utm_term=&gclid=EAIaIQobChMItbS955fg7AIVFITICh17dgvNEAAYAiAAEgIPZPD_BwE

- Datos en uso (nivel del cliente): protegen los datos sensibles de una organización mientras estos se utilizan a diario. Los cuales son utilizados en ese momento y son modificados tales como la creación de un documento.

- Los DLP garantizan la autenticidad adecuada controla el acceso de estos datos a los usuarios, sus aplicaciones y procesos.

- Datos en movimiento (nivel de red): son datos que se mueven a través de la red. Se garantiza que los datos trasmitidos dentro de la organización mediante correo electrónico, web y transferencia de archivos no se dirijan a otros destinatarios para que sigan manteniéndose confidenciales, cumpliendo con las políticas establecidas para prevenir o detectar fuga de datos.

- Los DLP se enfocan en los movimientos de los datos de la red fuera de la organización, la información que se transmite de un punto a otro es monitoreada y en caso de ser necesario pueden ser bloqueados por el sistema en la red o puertas de enlace del correo electrónico.

- Datos en reposo (nivel de almacenamiento): es la protección de datos que reside en la base de datos de una organización, en cualquier ubicación de la red, incluida la nube, contando PC y dispositivos móviles. Estos datos son escaneados según reglas específicas mediante rastreadores que identifican sus ubicaciones, evaluando que tan sensibles son y si se encuentran ubicados idóneamente de acuerdo a las políticas establecidas.

5.6 FORMAS EN QUE SE PROTEGEN LOS DATOS

Las organizaciones deben proteger sus datos en las tres categorías que se describirán a continuación:

- Datos de identificación personal (PII): es cualquier dato que podría ser usado para identificar una persona en particular, un ejemplo de esto puede ser su nombre completo, número de identificación, dirección de correo electrónico entre otros.

- Información de salud personal (PHI): esta es cualquier pieza de información en un registro medico de una persona que se divulga durante el proceso de diagnóstico o tratamiento y puede ser usada para identificarla.

- Propiedad intelectual (PI): es considerara una categoría de propiedad de creaciones intangibles del intelecto humano, los cuales pueden ser marcas comerciales, patentes y derechos de autor.

5.7 OBJETIVOS DE UN DLP

Actualmente los DLP se enfocan en resolver cuatro objetivos los cuales son considerados los puntos débiles en una organización:

- Protección de la PII: permite administrar y establecer reglas comerciales para clasificar información confidencial y sensible, con el fin de que esta no pueda ser revelada de manera maliciosa o por accidente por los usuarios de la organización o personal externo. El DLP también puede proporcionar alertas, aplicar cifrado y aislar datos.

- Cumplir con las regulaciones: los DLP ayudan a cumplir con la normatividad que deben cumplir las organizaciones mediante la identificación, clasificación y etiquetado de datos confidenciales, monitoreando las actividades y eventos que rodean estos datos; son capaces de generar informes detallados los cuales son necesarios cuando se realizan auditorias de cumplimento de protección de perdida de datos

- Protección de la propiedad intelectual: con la combinación de políticas de seguridad, sensibilizando a usuarios y el uso de herramientas de seguridad, la implementación de un DLP garantiza que los usuarios de una organización no envíen información confidencial o sensible fuera de la red corporativa.

- Proporcionar visibilidad de datos: los DLP pueden ayudar a identificar riesgos y realizar seguimiento de los datos de una organización en los puntos finales, en su misma red, en dispositivos móviles y en datos almacenados en la nube. Facilitando conocer como los equipos interactúan con los datos, donde estos datos se alojan, quienes los usan y para que fines.

5.8 CÓMO FUNCIONAN LAS HERRAMIENTAS DLP

Las herramientas DLP toman medidas de seguridad informática de los datos de una organización como firewalls, endpoint, servicios de monitoreo y antivirus. Como también hace uso de la inteligencia artificial, aprendizaje automático y

automatización. Las tecnologías DLP suelen admitir las siguientes actividades de ciberseguridad:

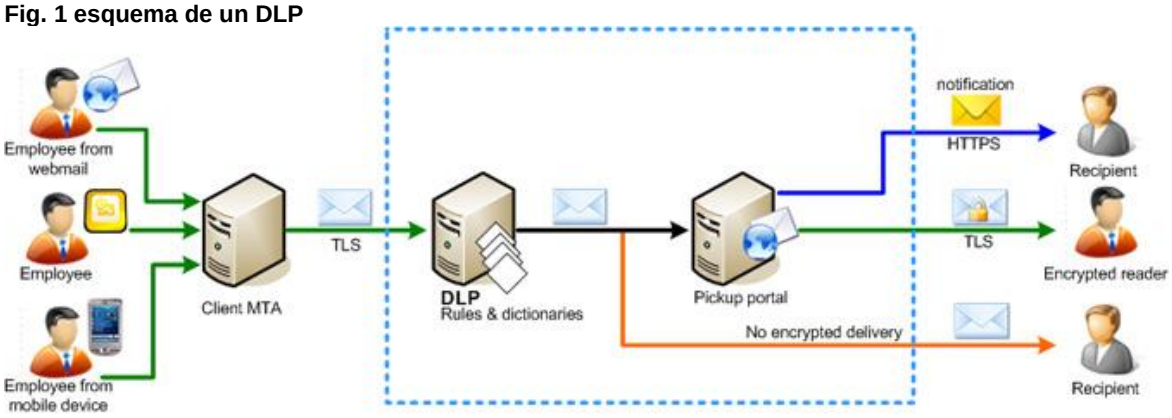
- Prevención: revisa en tiempo real los flujos de datos y restringe la actividad sospechosa a usuarios no autorizados.

- Detección: identifica actividad sospechosa mediante una visibilidad de datos y medidas de monitoreo.

- Respuesta: optimiza las actividades de respuesta ante incidentes mediante el seguimiento y la generación de informes de acceso y movimiento de datos en la organización.

- Análisis: contextualiza la actividad o el comportamiento de altos riesgos de los equipos de seguridad fortaleciendo las medidas de prevención.

Fig. 1 esquema de un DLP



Fuente: ricardo-sb; Prevención de Pérdida de Datos (y IV). Pasos para implementar una solución DLP; [sitio web]; [consulta: 21 de noviembre 2020]; disponible en: https://ricardo-sb.blogspot.com/2017/05/prevencion-de-perdida-de-datos-y-iv.html

5.9 TIPOS DE DLP

Hay tres tipos principales de soluciones DLP entre las que las organizaciones pueden elegir en función de sus necesidades: [10]

[10] spirion. (31 de 10 de 2020). *spirion.com*. Recuperado el 31 de 10 de 2020, de spirion.com: https://www.spirion.com/data-loss-prevention/#phase-3

- **DLP de red:** rastrea, monitorea, analiza e informa sobre los datos en uso, en movimiento y en reposo, que fluyen mediante los puertos y protocolos que son utilizados en la red de la organización, esto con el fin de detectar datos que son considerados confidenciales por las políticas de seguridad implementadas. Se encarga de asegurar todas las comunicaciones de la red, correo electrónico y aplicaciones web, controlando y protegiendo el flujo de la información que pasa a través de la red mediante técnicas de cifrado automático de datos. Crea una base de datos la cual registra cuando se accede a datos sensibles o confidenciales, quien accede a estos y donde se mueven estos datos en la red.

- **DLP de punto final:** supervisa todos los puntos finales de la red de las estaciones de trabajo en una organización, como pueden ser computadoras, dispositivos móviles, discos duros externos. Con el fin de monitorear y prevenir la trasferencia de información confidencial, lo cual hace más fácil su protección independientemente de la red. Pudiendo controlar la trasferencia de información entre grupos de usuarios y partes externas consiguiendo bloquear los intentos de comunicación en tiempo real y enviar mensaje a los usuarios. Realiza un seguimiento de los datos almacenados en puntos finales tanto dentro como fuera de la red.

- **DLP de almacenamiento:** toma el control de la información con la que los empleados de una organización cuentan y comparten, enviando alertas al equipo de seguridad cuando esta información corre riesgos de quedar expuesta a personas ajenas, un ejemplo de esto son los datos que se almacenan en la nube. Proporciona vista de archivos confidenciales almacenados en la red, mantiene una lista de usuarios y aplicaciones que pueden ingresar a los datos confidenciales de la nube, mantiene registros de cuando un usuario accede a los datos confidenciales almacenados en la nube.

5.10 HERRAMIENTAS DLP MÁS POPULARES EN EL MERCADO

El mercado está lleno de herramientas de prevención de pérdida de datos y tratar de encontrar la adecuada puede resultar abrumador[11] a continuación se abordaran

[11] d dnsstuff; 10 mejores software de prevención de pérdida de datos en 2020; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.dnsstuff.com/data-loss-prevention-software

y darán a conocer las características de diversas herramientas de DLP que existen actualmente en el mercado para que en base a las necesidades de una organización se tome la mejor opción.

- **SolarWinds (SEM):** esta herramienta incluye USB Defender para proteger uno de los puntos más vulnerables en una red ya que son de las entradas más fáciles para robar datos, la herramienta permite proteger estos puertos con la supervisión de actividades sospechosas. Recopila, centraliza, monitorea y analiza los registros de actividad de los usuarios, para a obtener visibilidad de las acciones de todos los usuarios en la red, con informes en tiempo real si alguna de esas acciones viola las políticas de la organización. Sus respuestas automatizadas facilitan la reacción ante amenazas, aparte de contar con plantillas automáticas ante amenazas, también pueden crearse reglas propias de respuestas automatizadas ante posibles amenazas.

- **Symantec Data Loss Prevention:** está enfocado para la implementación en grandes organizaciones ya que puede resultar complicado para utilizarlo en pequeñas organizaciones. Cuenta con un sistema de protección de datos de terminales, proporcionando cobertura en la nube, dispositivos móviles y múltiples terminales incluyendo equipos de escritorio y servidores. Cuenta con un panel de administración siendo capaz de identificar aplicaciones que intentan acceder a los dados y bloquearlas, permite detener las transferencias de datos. Cuando se instala por primera vez la herramienta realiza un barrido para encontrar todos los datos confidenciales en la red solicitando si desean moverlos a un repositorio de datos central seguro, encripta los datos sensibles registrando el acceso a estos. acceso a información confidencial, incluso mediante la toma de huellas digitales de los destinatarios para confirmar que deben tener acceso a la información que se les envía[12]. Su desventaja es que no ofrece una versión de prueba gratuita, ni cuenta con una versión sencilla de informes para las auditorias

- **Digital Guardian Endpoint DLP:** cuenta con diversas herramientas que lo hace algo complicado de configurar, adecuado para grandes organizaciones. Funciona en diversos sistemas operativos como MAC, Linux y Windows monitorea datos tanto en la red como en la nube. Puede configurarse de tal manera que bloquee, justifique o cifre de manera automática datos confidenciales, sus configuraciones también permiten bloquear de manera automática la actividad de los usuarios de acuerdo a

---

[12] dnsstuff; 10 mejores software de prevención de pérdida de datos en 2020; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.dnsstuff.com/data-loss-prevention-software

políticas previamente determinadas como sospechosas, registrando y auditando el evento para un posterior análisis forense. Una desventaja es que usuarios de esta herramienta informan que puede dar falsos positivos en exceso generando alertas en eventos no críticos, con actualizaciones frecuentes para solucionar un problema puede causar otros.

- **McAfee Total Protection DLP:** cuenta con un conjunto de múltiples herramientas para la protección de datos, se centra en un análisis forense detallado es capaz de identificar y priorizar los datos más confidenciales en una organización. Garantiza que tenga las mismas políticas de seguridad empleadas en la red ya sean locales, de puntos finales o en la nube. Su desventaja es que es algo difícil de configurar.

- **SecureTrust DLP:** es una de las mejores herramientas de prevención de perdida de datos para organizaciones que tienen conocimiento en el tema, o que prefiere políticas preestablecidas, en cuanto a la infracción de comportamiento sospechoso ya que por defecto viene con más de 70 configuraciones de políticas y riesgos definidas. Supervisa todos los archivos adjuntos y documentos basados en la web, incluidos los correos electrónicos, las publicaciones en las redes sociales y los blogs, que ingresan a su negocio, verificando si hay violaciones del gobierno de la empresa, las políticas de uso aceptable y el cumplimiento [13]

- **Check Point DLP:** es una buena opción para las organizaciones que tienen poco conocimiento del uso de herramientas DLP, su interfaz es intuitiva y cuenta con políticas predeterminadas, por lo cual no es conveniente para organizaciones que tiene conocimiento en el tema puesto que puede que les parezca simple. Esta herramienta busca educar a los empleados de una organización sobre el riesgo de la pérdida de datos para que identifiquen y respondan manera adecuada a incidentes, el cual es uno de los factores relevantes y difíciles de prevenir con soluciones tecnológicas en este tema, siendo el sentido de que por desconocimiento pueden introducir virus al sistema o compartir información sensible con personal externo. La herramienta rastrea y controla datos confidenciales en todos los servicios como lo son, navegación web, correo electrónico y datos en reposo, gestionando toda la red desde una única consola.

- **Comodo MyDLP:** esta herramienta registra y protege datos confidenciales utilizando listas blancas y listas negras con el fin de determinar si los usuarios tienen acceso a datos confidenciales, determinando que acciones

[13] dnsstuff; 10 mejores software de prevención de pérdida de datos en 2020; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.dnsstuff.com/data-loss-prevention-software

pueden realizar estos con los datos. Protege los puntos finales con el resto de la red, pudiéndose configurar para bloquear el flujo de los datos que contienen información confidencial, evitando que salga del sistema, su interfaz es intuitiva lo que lo hace fácil de usar. se puede acceder a esta herramienta mediante la nube o instalarla en los equipos. La desventaja de esta herramienta es que no profundiza en el análisis de comportamientos sospechosos y riesgos de seguridad comparada con otras.

6. RIESGOS EN LAS ORGANIZACIONES Y QUE MOTIVAN A IMPLEMENTAR UN DLP

6.1 SEGURIDAD EN BASE DE DATOS

La seguridad en datos es un aspecto esencial en las TI de las organizaciones, el cual hace referencia a la protección de datos contra accesos no autorizados con el fin de protegerlos de una posible corrupción durante su ciclo de vida.

6.1.1 Vulnerabilidades que afectan la seguridad de las organizaciones

- Privilegios excesivos: Cuando a un usuario se le entregan privilegios que exceden los requerimientos necesarios para el desarrollo de sus labores, se crea un riesgo de pérdida de información innecesario.
- Abuso de privilegios: muchos usuarios pueden llegar abusar de los privilegios de acceso legítimo en el sistema que se les otorga, para fines no autorizados como por ejemplo suministrar información confidencial de un cliente o sustraer información sensible de la organización para su propio beneficio.
- Elevación de privilegios no autorizados: personas atacantes pueden aprovechar vulnerabilidades en el software de bases de datos para convertir los privilegios otorgados de bajo nivel, en privilegios de alto nivel, como por ejemplo aprovechar una vulnerabilidad de desbordamiento de búfer en la base de datos para que se le otorguen privilegios de administrador.
- Vulnerabilidades de la plataforma: vulnerabilidades en sistemas operativos pueden facilitar el acceso no autorizado a datos de una organización.

6.2 MEDIADAS A TOMAR PARA ASEGURAR LA INFORMACIÓN DE LA (ONASYSTEMS.NET, 2020) ORGANIZACIÓN

Aplicar las medidas que se mencionaran a continuación es de vital importancia para que las organizaciones puedan trabajar de manera correcta y puedan cumplir con la normativa vigente de protección de datos.

- Controles de acceso a datos más escritos: una de las medidas de seguridad a implementar es limitar el acceso a la información, ya que mientras menos personas tengan acceso a dicha información menor es el riesgo de que se dé fuga de está.

- Realizar copias de seguridad: se debe implementar un sistema para la realización de copias de seguridad de manera periódica, puesto que esto permite que una organización pueda recuperar información de una incidencia catastrófica, impidiendo la pérdida total de esta información.

- Utilizar contraseñas seguras: el acceso a las diversas plataformas con las que cuenta una organización como lo son (el correo electrónico, servidores de copias de seguridad, entre otros), se debe realizar mediante la implementación de claves de seguridad seguras, impidiendo que sean fácilmente descubiertas por personal ajeno. Estas es una de las medidas de seguridad más importante a implementar por parte de las organizaciones.

- Proteger el correo electrónico: hoy en día la mayoría de comunicaciones se realizan utilizando el correo electrónico, una mediada para protegerlo es utilizando filtros antispam y un sistema de encriptado de mensajes con el fin de asegurar la protección y privacidad de los datos trasmitidos.

- Contar con un software integral de seguridad: es indispensable que toda organización cuente con paquetes con paquetes de seguridad integral. Los cuales contienen antimalware, antispyware, antivirus, firewall entre otros. Con lo cual se pretende proteger la información de ataques externos que se pueden dar a través de internet.

- Utilizar software DLP: esos son programas de prevención de pérdida de datos los cuales pueden ser implementados como una medida de seguridad en las organizaciones, para asegurarse de que ningún usuario sin autorización este copiando o compartiendo información de datos que no debe.

- Trabajar en la nube: uno de los beneficios de trabajar en la nube es la protección de sistemas de seguridad adicional, que brindan los proveedores de este servicio además de que este es el responsable de posibles vulnerabilidades que puedan ocurrir.

- Involucrar a toda la organización en la seguridad: para que las medidas de seguridad implementadas funcionen se deben involucrar a todos los empleados de la organización, incluyendo clientes y proveedores. En diversas ocasiones estas cuentan con las respectivas medidas de seguridad que pueden ser vulneradas por el desconocimiento del personal.

- Monitorización continua y respuesta inmediata: se deben implementar sistemas que permitan monitorizar la gestión de los datos detectando

posibles fallos y acciones incorrectas, lo que permitirá actuar rápidamente para resolver cualquier incidencia minimizando su repercusión.

6.3 DESAFÍOS DE LA CLASIFICACIÓN DE DATOS

Toda organización cuenta con datos sensibles que son confidenciales, sin embargo, es muy posible que desconozcan donde se encuentran alojados estos datos y las múltiples maneras de acceder a ellos o comprometerlos. Por esta razón y otras, la utilización de programas de clasificación de datos efectivos dentro de las organizaciones enfrenta una amplia gama de desafíos.

6.3.1 Clasificación de datos engorrosa y costosa

Poscas organizaciones están en la capacidad de clasificar datos de manera manual, lo que incluye varios desafíos como:

- Los datos confidenciales pueden perderse con otros tipos de información y no están protegidos.
- La manera de manejar la información sensible puede resultar en pérdida de credibilidad e ingresos a futuro.
- Las organizaciones pueden resultar multadas y sancionadas por el mal manejo que brindan a los datos.

6.3.2 Falta de comprensión de prácticas para la clasificación de datos

Las malas prácticas en la clasificación de datos pueden generar una serie en cascada de fallas de seguridad y privacidad, lo que puede resultar en los siguientes desafíos:

- Las organizaciones no saben cómo localizar o identificar sus datos.
- Las organizaciones no cuentan con el pleno conocimiento con las regulaciones de cumplimiento que están en constante evolución.
- Las preocupaciones de proteger los datos sensibles no tienen la misma prioridad como los son el marketing y las ventas.

- Las organizaciones hacen que la clasificación de datos sea compleja, por lo que no se producen resultados prácticos.

6.3.3 Falta de aplicación de las políticas de privacidad de datos

Un problema en la mayoría de organizaciones radica en que tienen políticas de clasificación de datos que son más teóricas que operativas. Lo que quiere decir que las políticas corporativas no se aplican o se dejan a cargo de los usuarios y propietarios de datos para que las implementen.
El desafío surge de pasar por alto las respuestas a preguntas críticas como

- ¿Se están produciendo debates inapropiados sobre la privacidad de los datos en los niveles superiores de una organización?
- ¿Quién es en última instancia responsable de la privacidad de los datos?
- ¿Se comparte información sensible y confidencial con otras entidades?
- ¿Se están eludiendo las políticas de privacidad y cumplimiento?

6.4 CICLO DE VIDA DE DATOS

El clico de vida de datos proporciona una estructura que controla el flujo de datos de una organización, estas deben tener en cuenta la seguridad, privacidad y el cumplimento de los datos en cada paso. La clasificación de datos ayuda debido a que se puede promulgar en todos los estados, desde su creación hasta la eliminación.

Fig. 2 etapas del ciclo de vida de datos

Fuete: kumobe; Ciclo de vida del dato infografía; [consulta: 21 de noviembre 2020]; disponible en: https://kumobe.com/kumobe-datta/ciclo-de-vida-del-dato-infografia-2/

6.4.1 Etapas del ciclo de vida de los datos

1. Creación: Los datos confidenciales se crean en varios formatos, incluidos correos electrónicos, documentos de Excel, documentos de Word, documentos de Google, redes sociales y sitios web.

2. Uso basado en roles: esos controles de seguridad se aplican a todos los datos confidenciales mediante un etiquetado de acuerdo a las políticas de seguridad interna y reglas de cumplimiento.

3. Almacenamiento: después de cada uso los datos se almacenan con controles de acceso y cifrado.

4. Compartir: los datos se comparten constantemente entre los empleados de una organización, incluyendo clientes desde diferentes dispositivos y plataformas.

5. Archivar: la mayoría de los datos se archivan eventualmente dentro de los sistemas de almacenamiento de una organización.

6. Destruir permanentemente: es indispensable destruir cantidades significativas de datos con el fin de reducir el almacenamiento y mejorar la seguridad general de los datos.

Los datos deben clasificarse tan pronto como se creen. A medida que los datos pasan por las etapas del ciclo de vida de los datos, la clasificación debe evaluarse y actualizarse continuamente.

6.5 CLASIFICACIÓN DE DATOS

6.5.1 Tipos de sistema de clasificación de datos

Existen 3 opciones para crear programas de clasificación de datos:

1. Manual: los métodos tradicionales de clasificación de datos donde se requiere la intervención y el cumplimiento humanos.

2. Automatizado: solución impulsada por la tecnología que elimina el riego de intervención humana, el tiempo excesivo y los errores. La clasificación de datos se da las 24 horas del día.

3. Hibrido: la intervención humana proporciona un contexto para la clasificación de datos, mientras que las herramientas permiten la eficiencia y la aplicación de políticas.

6.5.2 Evaluación de los niveles de clasificación de datos.

Las organizaciones suelen generar sus propios modelos de clasificación de datos, pero deben tener cuidado con la utilización de procesos de clasificación demasiado complejos y desordenados. Es recomendable crear una clasificación de datos inicial con tres o cuatro niveles de clasificación de datos y luego agregar niveles más granulares según las especificaciones de la organización, los requisitos de cumplimiento y otras necesidades comerciales.

Los niveles de clasificación de datos en una organización comienzan con la determinación de la sensibilidad de los mismos. A medida que el impacto potencial se mueve de bajo a alto, la sensibilidad aumenta y, por lo tanto, el nivel de clasificación de los datos debería ser más alto y más restrictivo.

La clasificación de esta información se da de acuerdo a tres criterios clave:

- Confidencialidad: se conservan las restricciones autorizadas sobre el acceso y divulgación de la información, donde se incluyen los medios para proteger la privacidad personal y la información de propiedad.

- Integridad: protege contra modificación o destrucción inadecuada de la información, se garantiza la integridad de la información. Se puede esperar que la modificación o destrucción no autorizada de información tenga un efecto adverso.

- Disponibilidad: se garantiza el acceso y el uso oportuno y confiable de la información. Donde se espera que la interrupción del acceso, uso de información o un sistema de información tenga un efecto adverso limitado.

6.5.3 Tipos de datos a clasificar

La mayoría de organizaciones cuentan con datos confidenciales, los cuales debe conocer de antemano de manera que respalden la privacidad, la seguridad y el cumplimiento optimizados de los datos. Estos datos que deben clasificarse son denominados “datos confidenciales” lo que indica que, si se exponen dentro o fuera de la organización presentan riesgos de privacidad de seguridad, corriendo el riesgo de no cumplir con las regulaciones establecidas para la protección de datos los cuales se pueden clasificar en datos regulados y no regulados.

6.5.4 Información regulada

Los datos regulados por organizaciones de cumplimiento siempre son confidenciales, aunque en diversos grados, y siempre deben clasificarse. Esto incluye:

- Información de identificación personal (PII): son datos que pueden usarse para identificar o contactar a una persona especifica o distinguirla de otra, esto incluye número se seguridad social, direcciones y números telefónicos.

- Información de salud personal (PHI): es la información médica y de salud de una persona, como el estado de salud.

- Información financiera: como su nombre lo indica es la información financiera de una persona como el número de tarjeta de crédito, número de cuenta bancaria y contraseñas.

6.5.5 Información no regulada

En muchos casos, los datos no regulados son muy sensibles y críticos de proteger. Esto incluye:

- Información de autenticación: son datos utilizados para probar la identidad de una persona, como contraseñas, secretos compartidos, claves de cifrado y tablas hash.

- Propiedad intelectual corporativa: incluye información exclusiva de organizaciones, como sus planes comerciales, propiedad intelectual y registros financieros.

- Información gubernamental: es cualquier información que se clasifique como secreta o ultra secreta, restringida o que pueda catalogarse como una violación de confidencialidad si se es expuesta.

6.6 TIPOS DE PÉRDIDAS Y FUGA DE DATOS EN UNA ORGANIZACIÓN

La pérdida y fuga de datos en cualquier organización puede darse tanto como por fuentes externas como internas de manera intencionada o accidental. Los DLP

abordan todas estas áreas garantizando que se eviten estas amenazas las cuales son:

6.6.1 Violaciones de datos externos

Toda organización corre el riesgo de que ciberdelincuentes vulneren el sistema y capturen información sensible de sus datos, siendo este un problema exponencial a medida que se crean herramientas más sofisticadas para prevenir estos ataques, los delincuentes también desarrollan formas más sólidas de cometer estos ataques. Los atacantes penetran el perímetro de seguridad utilizando técnicas, como phishing, malware o inyección de código, y obtienen acceso a datos confidenciales, que luego utilizan para vender en la web oscura o para cometer aún más delitos cibernéticos[14]. En el 2019 este tipo de ataques el 51% de las filtraciones de datos.

6.6.2 Amenazas internas

Este tipo de ataque lo constituye ataques maliciosos por personas internas que cuentan con información privilegiada denominado extracción de ataques donde la filtración puede darse por sabotaje interno, fraude y robo realizado por empleados descontentos o malintencionados que intentan mover estos datos fuera de la organización.

6.6.3 Fuga de datos del sistema

Todos los días grandes cantidades de información fluyen fuera de las organizaciones a través de la red, mediante correos electrónicos, carga de datos, transferencia de archivos, mensajes instantáneos entre otros. Donde estos datos pueden perderse o filtrarse por procesos inseguros.

6.6.4 Infracciones humanas accidentales

La filtración de datos sensibles en una organización no siempre se da por personas internas malintencionadas, en muchos de estos casos se son accidentales. Un ejemplo de esto es enviar un correo electrónico a un destinatario incorrecto.

[14] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

6.7 QUE IMPULSA AL CRECIMIENTO DE LA INDUSTRIA DLP

6.7.1 Ampliación masiva de datos

Un informe de IDC predice que las empresas generaran 175 zettabytes de datos para el 2025 con una tasa anual de crecimiento del 61%. [15]Lo que quiere decir que todos los datos se almacenan en toda la infraestructura de TI en las organizaciones. A medida que se incrementa el volumen de datos hace que estos sean más difíciles de localizar, por ende, las organizaciones luchan por proteger sus datos, cumpliendo con las regulaciones establecidas, eliminar datos duplicados y redundantes.

6.7.2 Más lugares para proteger datos

Los empleados utilizan múltiples canales de comunicación ya sean autorizados o no para transferir datos, como lo son correo electrónico, mensajes de texto, redes sociales, software colaborativo, capetas compartidas en línea entre otros. En donde los datos entran y salen de una organización y son enviados a sus socios, clientes usuarios legítimos y empleados remotos. También estos datos son almacenados en equipos de escritorio, teléfonos móviles, servidores, base de datos, en la nube. Toda esta actividad conduce a una falta de visibilidad de los datos y, por lo tanto, presenta un alto riesgo de pérdida y fuga.

6.7.3 Escases de talento en seguridad

A muchas empresas les resulta difícil cubrir puestos de trabajo relacionados con la seguridad. En las encuestas de ESG e ISSA, el 43% de las organizaciones se vieron afectadas por la escasez de talento en ciberseguridad. [16] Lo que constituye que las herramientas de DLP se conviertan en una alternativa para las organizaciones debido a que estas pueden realizar tareas de forma automática que antes era llevada por el personal de manera manual.

[15] Rydning, D. R.–J.–J. (01 de 11 de 2018). *www.seagate.com.* Recuperado el 03 de 11 de 2020, de www.seagate.com: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[16] Oltsik, J. (01 de 04 de 2019). *esg-global.com.* Recuperado el 03 de 11 de 2020, de esg-global.com: https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

6.7.4 Regulaciones de cumplimento más estrictas

En la actualizad los países se están preocupando por la preservación de la información con la que cuentan las organizaciones, por lo que han implementado nuevas leyes de protección de datos y modificaciones, con requisitos más estrictos a las ya existentes en las organizaciones que manejan datos confidenciales. Dentro de las cuales se incluyen sanciones importantes por el incumplimiento a estas regulaciones. Es en esto donde las herramientas DLP ayudan a mitigar y remediar la perdida de datos.

6.8 CUMPLIMENTO NORMATIVO EN DLP

Actualmente las personas exigen que sus datos personales que se encuentran contenidos en la red sean protegidos, debido a esto es que los gobiernos están respondiendo con regulaciones más estrictas para asegurar la confidencialidad de estos datos. Por ende, es importante que las organizaciones presten atención a las iniciativas de protección y privacidad de datos. Todas estas regulaciones tienen el objetivo de garantizar la privacidad, protegiendo la identidad y la información personal de cualquier persona. Las siguientes categorías representan las principales categorías de regulaciones de cumplimiento que afectan a las organizaciones actuales.

6.8.1 Normativa sobre datos sanitarios

Las organizaciones que se ocupen de PHI de las personas deben cumplir con estas regulaciones responsables de los proveedores de atención médica, los planes de salud y las empresas que recopilan datos de salud de los empleados.

- Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA): esta es una ley que se enfoca en la creación de estándares nacionales con el fin de proteger la información confidencial de salud de los pacientes en lo referente a diagnóstico y seguro médico, para que esta nos e divulgada sin su consentimiento.

- Ley de tecnología de la información sanitaria para la salud económica y clínica (HITECH): esta ley se creó con el fin de promover la adopción y el uso significativo de la tecnología en la información sanitaria.

6.8.2 Normativa sobre tarjetas de pago

Cualquier organización que acepte pagos con tarjeta de crédito o maneje datos de estas, debe tener encuentra los requisitos de seguridad de datos, incluido el control de acceso, firewalls, cifrado y seguridad de software y hardware, además de otros problemas como pruebas de penetración, skimming, phishing, evaluación de riesgos y violación de datos. Respuesta.

- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS): este es un conjunto de estándares de seguridad que garantiza que todas las organizaciones que aceptan, procesan, almacenan o transmiten información de tarjetas de crédito, mantengan su entorno seguro.

6.8.3 Regulaciones de datos geográficos

Las regulaciones geográficas más recientes pueden ofrecer a las personas la satisfacción de que los datos personales que las empresas recopilan sobre ellos son seguros y se mantienen privados[17]. Dicho esto, las organizaciones pueden presentar dificultades con la implementación de estos protocolos debido a que las regulaciones presentan diversos requisitos en diferentes países y en que estas regulaciones presentan objetivos, pero no es clara la forma de lograr el cumplimiento.

6.9 Leyes en Colombia prevención de perdida de datos

6.9.1 Ley Estatutaria 1581 de 2012

ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

ARTÍCULO 5o. DATOS SENSIBLES. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el

[17] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Referente al artículo 23 indica que la superintendencia podrá imponer sanciones a los responsables y encargados de los datos:
Multas equivalentes a 2000 SMLV. Suspensiones referentes al tratamiento de datos hasta por 6 meses. Cierre temporal relacionados con el tratamiento de datos y cierre inmediato y definitivo de las operaciones que involucren el tratamiento de datos sensibles.

6.9.2 Multas a organizaciones colombianas por violación de datos personales

En la última década se han implementado cerca de 800 sanciones a empresas colombianas por violación de datos personales con más de $30.000 millones. En el 2020 se han establecido más de 4000 denuncias por este delito.
El valor de las sanciones impuestas por la SIC a la compañía es de más de $30.000 millones y solo entre 2018 y 2019 el monto de las penalidades fue de $9.000 millones. [18]
Se recomienda que las empresas establezcan una política clara respecto al manejo de datos personales ya que este es un problema serio que puede dar hasta 8 años de cárcel. Actualmente la venta y el comercio de datos entre empresas son permitidos en Colombia. Se deben identificar qué tipos de datos que se manejan en las organizaciones para no incurrir en fallas o en contra la ley. Existen cuatro tipos de información que están estipuladas en la ley colombiana:

- Datos de carácter público: no tienen algún tipo de reserva como el nombre y la cédula.

- Datos semiprivados: es información que le interesa solo a un sector específico como la afiliación a fondos de pensiones o historial crediticio. La información puede ser revelada con autorización de una entidad menor como un ministerio o superintendencia.

- Información privada: son datos que solo pueden ser revelados por una autoridad judicial.

- [18] Dinero; Empresas han pagado más de $30.000 millones por violación de datos personales; [sitio web]; [consulta: 22 de noviembre 2020]; disponible en: https://www.dinero.com/economia/articulo/cuantas-empresas-han-sido-sancionadas-por-malos-manejos-de-datos-personales/305823

- Información sensible o reservada: son datos que pueden generar discriminación como, creencias políticas y religiosas. Esta información solo se puede revelar por una autoridad judicial en el marco de un proceso y cuando se requiere para la ejecución de un derecho

7. ESTRATEGIAS Y CONTROLES QUE SE PUEDEN IMPLEMENTAR PARA EVITAR LA FUGA DE INFORMACIÓN EN LAS ORGANIZACIONES

7.1 Como elegir la mejor herramienta DLP

Antes de seleccionar una herramienta de DLP para hacer uso de esta en una organización, es importante tomarse un tiempo para pensar cuales son las funciones que van acorde a las necesidades que se tiene y cuales son consideradas las principales amenazas a la seguridad de los datos, ya que los enfoques y puntos fuertes de cada herramienta DLP varían.

La implementación de un sistema DLP no es más que la reducción de riesgos, pero no la eliminación de amenazas, se debe conocer de antemano las políticas que van hacer definidas y las opciones con las que se cuentan para hacerlas cumplir.

Las herramientas de la prevención de fuga de datos no son necesariamente propensas a muchos falsos positivos, pero si se construye una mala política en una organización será inundada con malos resultados, o se pasará por alto importantes pérdidas[19]

7.2 Directrices para la clasificación de los datos

No existe un único enfoque para la clasificación de los datos completo e inteligente, sin embargo, este proceso puede dividirse en siete pasos claves, los cuales se pueden adaptar para satisfacer las necesidades de cada organización.

7.2.1 Realizar una evaluación de riesgos de datos sensibles

Se debe tener una comprensión por parte de la organización de los requisitos de privacidad y confidencialidad regulatorios y contractuales. Definiendo objetivos de clasificación de datos con todas las partes interesadas.

---

[19] evaluandosoftware; Consejos al implementar soluciones DLP; ; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.evaluandosoftware.com/consejos-al-implementar-soluciones-dlp/

7.2.2 Desarrollar una política de clasificación formalizada

La política de clasificación de una organización describe quién, qué, dónde, cuándo, por qué y cómo, para que todos comprendan el papel que desempeña la clasificación de datos en toda la organización.
En la que se incluyen los siguientes puntos:

- Objetivos: se establecen las razones por las que ha implementado la clasificación de datos y los objetivos que la organización espera lograr.

- Flujos de trabajo: se explica cómo se organiza el proceso de clasificación y como esta afecta a los empleados que utilizan diferentes categorías de datos confidenciales.

- Esquema: describe las categorías de datos que se utilizarán para clasificar los datos de la organización.

- Propiedades de datos: describe todas las funciones y responsabilidades de los involucrados en la gestión de clasificación de datos, como los datos se clasifican confidenciales y como se les otorga acceso a estos.

7.2.3 Categorizar los tipos de datos

Cada organización define sus datos confidenciales de maneras diferentes, determinando que tipos de datos sensibles existen dentro de la organización, teniendo en cuenta los siguientes interrogantes:

- ¿Qué datos de clientes y socios recopila la organización?
- ¿Cómo se utilizan los datos?
- ¿Qué datos de propiedad se crean?
- ¿Cuáles son los niveles de confidencialidad y riesgo de los datos recopilados en toda la empresa?
- ¿Qué normas de privacidad se aplican a los datos?

7.2.4 Descubrir la ubicación de todos los datos

Se catalogan todos los lugares donde se almacenan los datos de la organización

- Red
- Puntos finales
- Dispositivos
- Nube

7.2.5 Identificar y clasificar datos

Después de localizar los datos con el método de descubrimiento de datos se identificarán y clasificarán para que estén debidamente protegidos, asignando una etiqueta a cada activo de dato sensible para mejorar la política de clasificación de datos, este etiquetado puede automatizarse de acuerdo con el esquema de clasificación de datos o hacerlo manualmente.
Un sistema de clasificación automatizado inteligente ofrece las siguientes ventajas:

- Determinar automáticamente las clasificaciones adecuadas para todos los datos de la organización en función de las metodologías aprobadas por esta.

- Etiquetar los datos con la etiqueta de nivel adecuado.

- Asegurar de forma permanente que todos los datos se clasifiquen y actualicen a medida que avanzan por el ciclo de vida de los datos.

7.2.6 Habilitar controles de seguridad de datos efectivos

Se deben establecer medidas de ciberseguridad de referencia y definir controles de política basados en cada etiqueta de clasificación de datos con el fin de garantizar que se implemente soluciones de seguridad adecuadas.
Al comprender dónde residen los datos y el valor organizativo de los datos, puede implementar controles de seguridad adecuados en función de los riesgos asociados. Además, los metadatos de clasificación pueden ser utilizados por DLP, ILP, cifrado y otras soluciones de seguridad para determinar cómo deben protegerse.[20]

7.2.7 Monitorear y actualizar el sistema de clasificación

Las políticas de clasificación deben ser dinámicas para que puedan adaptarse a la naturaleza cambiante de la privacidad de los datos y el cumplimiento de datos, teniendo en cuenta de que los archivos se crean, copian, mueven y eliminan todos los días. Establecer un proceso de administración consistente para garantizar que

[20] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

el sistema de clasificación de datos funcione de manera óptima y continúe satisfaciendo las necesidades de la organización.

7.3 ROLES DE CLASIFICACIÓN DE DATOS EN LA ORGANIZACIÓN

La clasificación de datos es una función que involucra a todos los miembros de una organización, para optimizar los programas de clasificación de datos, las organizaciones deben designar personas que serán responsables de llevar a cabo tareas específicas. Esta tarea de clasificación puede darse de seis formas:

- Campeones de datos: una persona es la responsable del uso de datos en la organización con fines comerciales. Este rol puede presentarse en diferentes formas, como un Jefe de Oficina de Privacidad (DLP) que es responsable de la estrategia de datos, incluida la calidad, la gobernanza y la monetización. Se debe garantizar que la parte interesada identificada respalde e impulse los esfuerzos de clasificación de datos como parte de la estrategia general de datos de la organización.

- Propietarios de datos: son las personas responsables en última instancia de los datos y la información. si los datos residen y se utilizan principalmente dentro de su grupo, son de su propiedad. El objetivo es que los propietarios de los datos proporcionen una capa adicional de contexto para la clasificación, como acuerdos con terceros, que algunas de las herramientas automatizadas actuales aún no pueden hacer.

- Creadores de datos: la responsabilidad de identificar nuevos fragmentos de datos recién creados (incluidas copias de datos existentes) como confidenciales o no recae en su creador. Cualquiera dentro de una organización puede ser un creador de datos. Los creadores de datos pueden hacerse una pregunta simple para determinar la sensibilidad.

- Usuarios de datos: cualquiera que tenga acceso a los datos de la organización es considerado un usuario de estos, los cuales deben usar los datos de manera coherente con el propósito previsto y cumplir con esta política y todas las políticas aplicables al uso de datos.

- Auditores de datos: se encarga de revisar la evaluación del propietario de los datos de la clasificación y determinar si cumplen con los requisitos de socios comerciales y las regulaciones. También revisa la retroalimentación de los usuarios de datos y evalúa la alineación entre el uso de datos real o deseado y las políticas y procedimientos actuales de manejo de datos.

- Custodio de datos: los técnicos de las tecnologías de información y los oficiales de seguridad de información son los responsables de realizar copias de seguridad del sistema, base de datos y servidores donde se alojan los datos de la organización, además de ser los responsables de que se cumplan todas las reglas establecidas por los dueños de los datos asegurándose de que estas estén funcionando.

7.4 COSTO-BENEFICIO DE IMPLEMENTAR UN DLP

Las organizaciones pueden asegurarse de que están haciendo bien en implementar una herramienta DLP realizando un análisis del costo-beneficio de esta, comparado el costo de la inversión con la solución, la perdida de datos y los beneficios que se pueden obtener evitando que se filtre información sensible.

Los beneficios que se pueden obtener al implementar el sistema DLP son:

- Tener la capacidad de proteger los activos de la empresa, incrementando la confianza de los accionistas y clientes.
- La identificación y análisis de problemas de una manera eficaz.
- Evitar la mala utilización de los datos en la organización.
- Disminuir el costo de perdida de información en la empresa.

Un ejemplo de esto es la herramienta “ESET Endpoint Security” la cual ofrece una versión de prueba gratis y está disponible a partir de US$ 38,00 por el cual se cuenta con asistencia en línea, puede instalarse en Mac, Windows, la nube y web. Cuenta con formación en personas, línea, documentación y seminarios web.

Tabla 1FUNCIONES DE ESET ENDPOINT SECURITY

ESET Endpoint Security	**FUNCIONES DE ESET ENDPOINT SECURITY**
Herramientas de seguridad en equipos informáticos	Antivirus – análisis de comportamiento - cifrado – correspondencia de firmas - gestión de amenazas web – gestión de dispositivos – lista blanca/negra – registro de actividades – seguridad en aplicaciones.
Herramientas para teletrabajo	Acceso remoto
Programas para hacer copias de seguridad	Almacenamiento seguro de datos – cifrado – copia de seguridad continua – copia de seguridad de almacenamiento en la nube –

	opciones de servidor local y remoto – programación de copias de seguridad – registro de copias de seguridad.
Sistemas de seguridad informática	Antispam – antivirus – control de acceso de archivos – protección contra vulnerabilidades – supervisión en tiempo real.
Software de ciberseguridad	Análisis de comportamiento - gestión de incidentes – gestión de puntos de terminación – inteligencia artificial y aprendizaje automático - lista blanca/negra.
Software de copias de seguridad para servidores	Cifrado – comprensión – copia de seguridad continua – copia de seguridad diferencial – programación de copias de seguridad – recuperación de desastres.
Software de prevención de perdida de datos	Creación de informes de conformidad – gestión de amenazas web – gestión de incidentes – gestión de políticas – identificación de datos sensibles – lista blanca/negra.
Software de seguridad en la red	Análisis de vulnerabilidades – control de acceso - cortafuegos – creación de informes/análisis – respuesta a amenazas – sistema de detección de intrusiones – supervisión de actividades – VPN.
Software para la monitorización y gestión remota	Gestión de recursos informáticos – supervisión de redes.

Fuente el autor

7.5 DESARROLLAR POLÍTICAS DE SEGURIDAD DE UN DLP EN UNA ORGANIZACIÓN

Una política DLP contiene una o más reglas para monitorizar y controlar el flujo de datos confidenciales, las cuales pueden ser excepciones, condiciones y acciones en relación a los datos, archivos o mensajes para detectar y prevenir fuga de información.
Mediante las políticas de DLP las organizaciones pueden definir los datos que se pueden enviar, restringir, publicar, cargar, mover, o copiar.
Estas políticas también instruyen a la herramienta DLP sobre el cómo actuar para proteger el contenido cuando se cumple una serie de condiciones. Por lo general las herramientas DLP cuentan con políticas predefinidas, pero también las organizaciones pueden definir las suyas.

Para tener una seguridad de datos efectiva es necesario que las organizaciones creen políticas de DLP, estableciendo mejores prácticas con el fin de manejar y almacenar datos confidenciales, siendo capaces de tratar violaciones de seguridad. Se debe tener en cuenta que la tecnología de las herramientas DLP es solo un componente integral para mitigar la fuga de información.

A continuación, se realizarían sugerencias que pueden ser aplicadas en las organizaciones para configurar una política de DLP eficaz.

- Clasificar e interpretar datos: las organizaciones deben identificar que datos deben ser protegidos mediante una evaluación de factores de riesgo y la vulnerabilidad de los datos, ya que esto ayudara a implementar una política de prevención de datos adecuada.

- Seguimiento de dispositivos no administrados: realizar un seguimiento a los puntos no administrados que contienen información confidencial. En estos dispositivos se incluyen servidores, puntos finales, dispositivos de almacenamiento extraíbles, y almacenamiento en la nube. Los cuales son considerados como punto de partida para la información confidencial.

- Asignar roles: es importante involucrar a personas adecuadas con roles y responsabilidades desde el inicio de la implementación de un sistema DLP. Desarrollar derechos y deberes de DLP basados en roles proporcionará controles y equilibrios. El equipo de DLP debe incluir representantes que sean responsables de la protección de datos, propietarios de datos y personas de funciones clave, TI y varias unidades comerciales.

- Educar a los usuarios: se debe asegurar que todas las partes involucradas y los usuarios de datos conozcan el programa DLP y que deben hacer para proteger los datos de la organización. Las políticas y los procedimientos deben proporcionar una guía clara a los empleados sobre las prácticas de prevención de pérdida de datos apropiada e inapropiada.

- Documentar la estrategia DLP: hacer esto proporcionara claridad tanto a nivel individual como de la organización, referente a los requerimientos y como aplicar las políticas de seguridad.

- Asegurar primero los datos más sensibles: lo primero que se debe hacer es identificar los datos más sensibles, que generan mayor riesgo en una organización. La implementación inicial del DLP debe limitarse a un área o división de la organización. Luego, un enfoque por fases, que prioriza los módulos y apunta a los puntos finales clave, brinda la oportunidad de aprender de la experiencia antes de una implementación más amplia. Se debe planificar una hoja de ruta de implementación, con hitos y puntos de control apropiados para revisar el progreso[21]

[21] spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#

- Automatizar todo lo que sea posible: es recomendable que se automatice todo lo posible el uso de la herramienta DLP. Debido a que los procesos manuales están limitados en su alcance y la cantidad de datos que pueden cubrir, mientras que los sistemas automatizados brindan capacidades ilimitadas.

- Establecer métricas de éxito: Determinar los indicadores clave de rendimiento (KPI) que deben medirse y controlarse de cerca para determinar el éxito del programa DLP, incluido el porcentaje de falsos positivos, el número de incidentes y el tiempo medio de respuesta. Compartir estas métricas con el liderazgo de la organización para mostrar el impacto positivo de DLP y reforzar su valor comercial.

- Elegir soluciones de seguridad complementarias: hoy en día una sola herramienta no es suficiente ante la amenaza de pérdida de información sensible que puede sufrir una organización, se debe tener en cuenta realizar la protección en redes, los puntos finales, la nube y los usuarios. La mejor manera de lograr este objetivo es implementando un enfoque de seguridad de múltiples capas que incluyan varias soluciones integradas.

Tabla 2analisis DLP disponibles en el mercado

	DG Data Protection Platform	**McAfee DLP Endpoint**	**MyDLP**	**Symantec Data Loss Prevention**
Prueba gratis	no	no	No	No
Ideal Para	Sin información del proveedor	Herramienta local que ayuda a los equipos de seguridad de redes a proteger datos confidenciales, rastrear el comportamiento del usuario y garantizar el cumplimiento normativo.	Sin información del proveedor	Profesionales de seguridad de TI: Organizaciones pequeñas, medianas y grandes empresas
Funcionalidades	*Gestión de amenazas web *Gestión de incidentes * Lista blanca/negra	*Gestión de amenazas web	*Creación de informes de conformidad *Lista blanca/negra	*Control de acceso *Descubrimiento de datos * Gestión de almacenamiento * Gestión de correo electrónico

				* Gestión de procesos * Gestión de roles
Plataforma	*Dispositivo móvil ios y android *PC *Windows y MAC	*Dispositivo móvil ios y android *Windows y MAC	*Dispositivo móvil ios y android *Windows y MAC	*Dispositivo móvil ios y android *Windows y MAC
Formación		*Documentación * Seminarios web		
Asistencia		*En línea * Horas laborables		
Enfoque	Sistema de protección de datos para Windows, Mac o Linux. Analiza los datos entrantes y salientes y detiene la penetración de malware.	Herramienta local que ayuda a los equipos de seguridad de redes a proteger datos confidenciales, rastrear el comportamiento del usuario y garantizar el cumplimiento normativo	Sistema que protege las aplicaciones de oficina ante la pérdida de datos internos o externos, detecta datos privados y alerta sobre posibles fugas.	Profesionales de seguridad de TI: Organizaciones pequeñas, medianas y grandes empresas

Fuente el autor

7.6 OPCIONES DE INTEGRACIÓN DE UN DLP

Las herramientas DLP para tratar la fuga de información en las organizaciones se pueden dividir en cuatro categorías generales: medidas de seguridad estándar, sistemas DLP designados, medidas de seguridad inteligente y control de acceso y cifrado. Idealmente, las organizaciones adoptan un enfoque en capas para DLP.
Estas soluciones DLP son adecuadas para monitorear el flujo de datos y protegerlos de amenazas conocidas. Pero se debe tener encueta que hay varias funciones de seguridad critica en cuanto a seguridad de datos que no pueden ejecutar.
Las siguientes aplicaciones son soluciones complementarias que las empresas pueden integrar en sus programas DLP para desarrollar un programa completo de seguridad y privacidad de datos.

- Sistema de detección de intrusos (IDS): protege a las computadoras de ataques internos y externos, enviando alertas sobre intentos de acceder a datos confidenciales.

- Gestión de eventos e información de seguridad (SIEM): detecta eventos que pueden constituir una fuga de datos.

- Monitorización y filtrado de contenido (CMF): se encarga de detectar el contenido malicioso de sitos webs que por lo general es pasado por alto por los programas antivirus y antispyware.

- Protección y control de la información (IPC): se encarga de la gestión digital de los derechos de acceso a la información, el control y la integridad de los datos.

- Sistema de prevención de extrusión (EPS): detiene la fuga de información con un filtrado del tráfico de red saliente y evitando que los paquetes no autorizados se muevan fuera de la red.

- Análisis de comportamiento de usuarios y eventos (UEBA): se encarga de detectar a los intrusos y atacantes malintencionados que debido a patrones poco comunes de actuar no son reconocidos por los controles de seguridad de un DLP.

- Soluciones de seguridad de archivos: se encarga de proteger los datos en reposo y en uso, y detecta fugas de datos basados en archivos.

- Software antivirus: su función principal es evitar que los atacantes pongan en peligro los sistemas sensibles.

- Cortafuegos: bloquea el acceso de cualquier parte no autorizada, a los sistemas que se encargan de almacenar los datos confidenciales, también evita el acceso a personas externas a la red interna de una organización.

Tabla 3aplicaciones soluciones complementarias

	Ventajas	**Desventajas**
Sistema de detección de intrusos (IDS)	*detecta intrusiones en la red *detecta ataques para los cuales no tienen un conocimiento especifico *tienen un impacto pequeño en la red no interfieren en sus operaciones habituales	*Se debe actualizar constantemente ya que solo detecta ataques que conoce *produce gran número de falsas alarmas

Gestión de eventos e información de seguridad (SIEM)	*Certificación de la información de seguridad. *automatización de tareas *mejor manejo del riesgo *métricas de seguridad	* alto coste de implementación *integración limitada con el resto del sistema *es necesario entrenar al personal para esta tarea
Monitorización y filtrado de contenido (CMF)	*****Desarrollo y tiempo de implementación rápidos. *****Funcionalidades avanzadas de formularios, encuestas etc. *****Fácil de usar. *****Fácil mantenimiento	*Consumo de recursos en el servidor *Tener conocimientos previos de un CMF *Mantenimiento constante *Soporte técnico difícil de encontrar
Protección y control de la información (IPC)	*archivar información en caso de eliminación accidental o daño al original * protección contra el spam y virus * reducción del tráfico inadecuado	
Análisis de comportamiento de usuarios y eventos (UEBA)	*Detecta instalación de archivos maliciosos *Detecta creación de cuentas falsas * Detecta ataques de fuerza bruta * detecta cambios en permisos y creación de superusuarios * Detecta violación de datos protegidos.	* Costo económico más elevado apara ser adurido por pequeñas empresas *los datos que genera son más complejos lo que hace difícil su comprensión *permite detectar comportamiento inusual pero no detiene a los intrusos

Fuente el autor

8. CONCLUSIONES

- Toda organización tiene información sensible ya sea de clientes, proveedores, del personal que labora en esta o simplemente financiera que al darse a conocer puede generar pérdidas económicas y de credibilidad, por lo cual es necesario implementar herramienta y políticas de seguridad que se encargue de disminuir el riego de pérdida o filtración de datos confidenciales.

- Las organizaciones deben conocer de antemano los datos que manejan y el valor de los mismos, donde se almacenan y como protegerlos, ya que con esto se pueden implementar protecciones reduciendo el riesgo en ellos, eliminando redundancias de protección pudiendo enfocar los recursos de seguridad en las acciones correctas. Las malas prácticas en la clasificación de datos pueden generar una serie en cascada de fallas de seguridad y privacidad.

- La pérdida y fuga de datos en cualquier organización puede darse tanto como por fuentes externas como internas de manera intencionada o accidental. Los DLP abordan todas estas áreas garantizando que se eviten estas amenazas.

- Una de las mejores maneras de mitigar el riego de perdida y filtrado de información en las organizaciones es la implementación de un DLP puesto que su objetivo principal es gestionar la seguridad y políticas de uso en diferentes sistemas de información pudiendo examinar, detectar, proteger, supervisar y administrar el contenido de los archivos, etiquetando la información confidencial y crítica, para que los usuarios no puedan divulgarla, eliminarla, alterarla, duplicarla o transferirla a terceras personas.

- Los DLP ayudan a cumplir con las regulaciones establecidas por los gobiernos, identificando. Clasificando y etiquetando datos confidenciales, generando informes detallados para auditorias de cumplimiento de protección de perdida de datos.

9. RECOMENDACIONES

- Se recomienda capacitar al personal que labora en una organización respecto los peligros informáticos a los que están expuestos a diario por parte de los ciberleincuentes y cómo afrontar estas amenazas.

- Es aconsejable que las organizaciones al momento de generar su modelo de clasificación de datos tengan cuidado es este proceso ya que puede resultar en una clasificación compleja y desordenada. Es recomendable crear una clasificación de datos inicial con solo dos o tres niveles e ir agregando niveles gradualmente según los requerimientos.

- Se recomienda la instalación de un DLP ya que esta herramienta de seguridad de información ayuda a entender el significado de cada uno de los datos propios de la organización, identificando los riesgos que se presentan al momento de ser almacenados, manipulados y compartidos, clasificando y administrando cada uno de estos para el correcto manejo de la información.

- Es indispensable que desde un inicio las organizaciones tengan definidas de la mejor manera las políticas de seguridad y se hagan revisiones periódicas a las mismas, para evitar redundancia de estas con el fin de que se optimice la herramienta DLP que tienen implementada.

- Se debe realizar un análisis exhaustivo en toda la organización para determinar cuáles son las necesidades que se quieren cubrir al antes de implementar una herramienta DLP, puesto que en el mercado se encuentra un sinnúmero de estas herramientas y cada una cuenta con características especiales. No es lo mismo que una pequeña organización invierta en una herramienta diseñada para grandes empresas ya que no se verá reflejado el costo-beneficio de su inversión.

10. BIBLIOGRAFÍA

- capterra; Software de prevención de pérdida de datos; [sitio web]; [consulta: 21 de noviembre 2020]; disponible en: https://www.capterra.co/directory/31106/data-loss-prevention/software

- crowdstrike; ¿QUÉ ES LA PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) ?; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.crowdstrike.com/epp-101/data-loss-prevention-dlp/?utm_campaign=dsa&utm_content=latam&utm_medium=sem&utm_source=goog&utm_term=&gclid=EAIaIQobChMItbS955fg7AIVFITICh17dgvNEAAYAiAAEgIPZPD_BwE

- datos101; las 9 medidas de seguridad informática; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.datos101.com/blog/las-9-medidas-de-seguridad-informatica-basicas/

- Dinero; Empresas han pagado más de $30.000 millones por violación de datos personales; [sitio web]; [consulta: 22 de noviembre 2020]; disponible en: https://www.dinero.com/economia/articulo/cuantas-empresas-han-sido-sancionadas-por-malos-manejos-de-datos-personales/305823

- dnsstuff; 10 mejores software de prevención de pérdida de datos en 2020; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.dnsstuff.com/data-loss-prevention-software

- evaluandosoftware; Consejos al implementar soluciones DLP; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.evaluandosoftware.com/consejos-al-implementar-soluciones-dlp/

- kumobe; Ciclo de vida del dato infografía; [sitio web]; [consulta: 21 de noviembre 2020]; disponible en: https://kumobe.com/kumobe-datta/ciclo-de-vida-del-dato-infografia-2/

- onasystems; Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas; [sitio web]; [consulta: 01 de noviembre 2020]; disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

- Portafolio; Hay empresas que pierden hasta $4.000 millones por ciberataques; [sitio web]; [consulta: 22 de noviembre 2020]; disponible en:

https://www.portafolio.co/negocios/empresas/auditorias-ti-ahorran-perdidas-por-ciberataques-531817

- research and marke; Mercado de prevención de pérdida de datos empresariales: tendencias, oportunidades y previsiones de la industria hasta 2023; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.researchandmarkets.com/research/npbpsp/global_enterprise?w=4

- ricardo-sb; Prevención de Pérdida de Datos (y IV). Pasos para implementar una solución DLP; [sitio web]; [consulta: 21 de noviembre 2020]; disponible en: https://ricardo-sb.blogspot.com/2017/05/prevencion-de-perdida-de-datos-y-iv.html

- spirion; Guía de prevención de pérdida de datos; [sitio web]; [consulta: 31 de octubre 2020]; disponible en: https://www.spirion.com/data-loss-prevention/#