ESTRATEGIAS PARA LA CLASIFICACIÓN DE LA INFORMACIÓN Y LA PREVENCIÓN DE FUGA DE INFORMACIÓN

Carlos Andrés León Tejada
Especialización en Seguridad Informática
Universidad Piloto de Colombia
Bogotá, Colombia andres.leon@hotmail.com
carlos.leon@softsecuritycorp.com

Abstract ---Protect information from unauthorized disclosure has become one of the most important concerns for companies worldwide. High profile cases where it has been seen as essential to protect intellectual property and confidential data. Taking into account legislative and regulatory requirements, such as Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Gramm-LeachBliley Act (GLBA), (ITAR), Payment Card Industry Data Security Standard (PCI DSS), and SB1386 among others, are the main guardians to implement solutions to prevent data loss.

Index terms **:** Data Loss Prevention (DLP), Lost Data, Prevention, Data Value.

Resumen ---Proteger la información de la divulgación no autorizada se ha convertido en una de las preocupaciones más importantes para las empresas de todo el mundo. Casos de alto perfil en donde se ha visto como fundamental proteger la propiedad intelectual y datos confidenciales.

Teniendo en cuenta requisitos reglamentarios y legislativos, como la portabilidad del seguro de salud y la ley de responsabilidad (HIPAA), la ley Sarbanes-Oxley (SOX), la ley Gramm-LeachBliley (GLBA), (ITAR), Payment Card Industry Data Security Standard (PCI DSS), y SB1386 entre otros, son los principales tutores para la implementación de soluciones de prevención de pérdida de datos.

Índice de términos : Data loss Prevention (DLP), Pérdida de datos, Prevención, Valor de los datos.

I. INTRODUCCIÓN

1. ¿Qué es la pérdida de datos?

La pérdida de datos es una condición de error en sistemas de información en el que la información se destruye por las fallas o negligencia en el almacenamiento, transmisión, procesamiento o simplemente por fuga de la información.

1.1. El valor de los datos.

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad. Además las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son resistentes a dedicar recursos a esta tarea.

1.2. Información en las empresas u organizaciones.

Respecto a la información en las organizaciones se han encontrado documentos que describen la valoración de la información y la administración de la información como herramienta básica en las organizaciones. En general, se detalla la propuesta de autores que consideran a la información como un activo.

1.2.1. La información como un activo. [1]

Respecto al valor de la información, Oppenheim, Stenson, & Wilson (2003a), identifican los atributos de la información y concluyen que a ésta se le puede considerar, Las cualidades que conforman la seguridad de los activos de información de una organización son: [2]

La **confidencialidad** tiene relación con la protección de información frente a posibles accesos no autorizados, con independencia del lugar en que reside la información o la forma en que se almacena. La información sensible o valiosa que la organización custodia o maneja, necesita ser protegida mediante estrictas medidas de control. La verificación y la autorización son dos mecanismos que se emplean para asegurar la confidencialidad de la información.

La **integridad** se refiere a la protección de información, datos, sistemas y otros activos informáticos contra cambios o alteraciones en su estructura o contenido ya sean intencionados, no autorizados o casuales. También es importante proteger los procesos o programas que se emplean para manipular los datos. La información se debe preservar y poner a disposición de sus propietarios y de los usuarios autorizados de una forma precisa, completa y oportuna.

La **disponibilidad** es la garantía de que los usuarios autorizados puedan acceder a la información y recursos cuando los necesiten.

1.3. Por qué se pierde la información [3]

La mayoría de las empresas utiliza salvaguardas para controlar la información sensitiva. Sin embargo, a menudo estos controles no son permanentes y se administran en diferentes puntos de la empresa con diferentes niveles de diligencia y eficacia. El resultado es que a pesar de sus esfuerzos, en empresas a todo lo largo y ancho del mundo se producen fugas de grandes volúmenes de información sensitiva. Estas fugas generan un riesgo considerable para las empresas, sus clientes y socios comerciales, y tienen el potencial de ejercer un impacto negativo sobre la reputación del negocio, su cumplimiento, ventajas competitivas, finanzas, confianza de los clientes y socios comerciales.

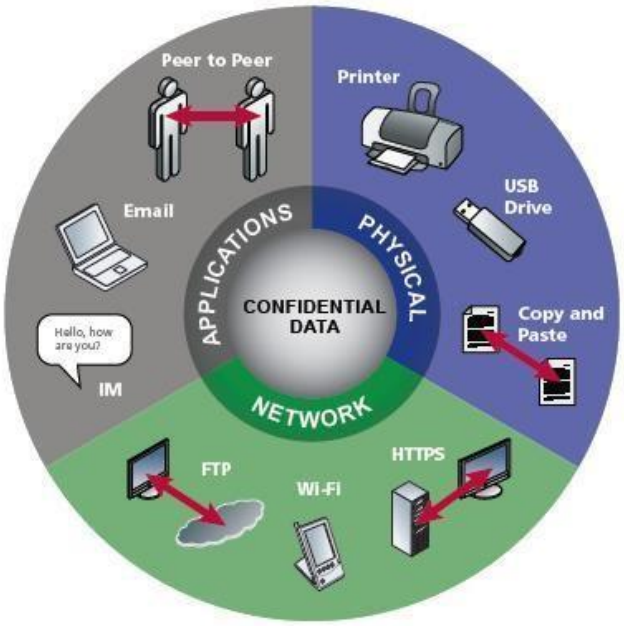
La preocupación y la necesidad de tener un mejor control y proteger información sensitiva han dado lugar a un nuevo conjunto de soluciones dirigidas a mejorar la capacidad de una empresa para proteger sus activos de información. Estas soluciones son variadas en cuanto a sus capacidades y metodologías, pero en conjunto se han ubicado dentro de una categoría conocida como prevención de fuga de datos (DLP).

Si bien todavía es una tecnología joven, la DLP se está adoptando cada vez más y un número creciente de productos está siendo lanzado al mercado. En un estudio publicado a principios de este año por la empresa de investigación en TI TheInfoPro, DLP se calificó como una primera prioridad para los presupuestos de seguridad de las empresas [4]

Cabe mencionar que si bien las soluciones de DLP tienen la capacidad de interceptar algunos intentos maliciosos o delictivos de robo de información, la tecnología todavía no está suficientemente desarrollada para impedir métodos más sofisticados de robo de datos.

Afortunadamente el consenso general es que estos casos constituyen una parte muy pequeña del riesgo general de la fuga de datos. En un informe publicado en marzo de 2009 por el Instituto Ponemon, [5] se estima que 88 por ciento de los incidentes relacionados con fuga de datos fueron debidos a negligencia por parte de los usuarios y 12 por ciento se debió a intentos maliciosos. No obstante este bajo porcentaje puede ser algo engañoso, pues normalmente un porcentaje mucho mayor de robos maliciosos de datos que de pérdidas accidentales conducirá a acciones adversas.

Los sistemas de seguridad de prevención de robo de datos típicos proporcionan protección razonable en contra de las amenazas externas mediante el uso de defensas perimetrales como cortafuegos y detección de intrusiones o prevención. Sin embargo estos sistemas no están diseñados para evitar el robo de información interna. Por lo que hay que diseñar medidas adicionales de seguridad que protegen la información interna, la mayoría de las empresas solo tienden a limitar el acceso de datos, sólo para el personal autorizado pero cuando tal acceso legítimo no da derecho al usuario para eliminar, copiar o extraer datos de la empresa, las soluciones existentes no protegen adecuadamente contra este riesgo.



Fuente [8] Data Loss Prevention – Part 3 – How DLP Technologies Work

FIGURA.. 1 NIVELES DE PROTECCIÓN DE LA INFORMACIÓN

Los sistemas de seguridad de prevención de robo de datos típicos proporcionan protección razonable en contra de las amenazas externas mediante el uso de defensas perimetrales como cortafuegos y detección de intrusiones o prevención. Sin embargo estos sistemas no están diseñados para evitar el robo de información interna. Por lo que hay que diseñar medidas adicionales de seguridad que protegen la información interna, la mayoría de las empresas solo tienden a limitar el acceso de datos, sólo para el personal autorizado pero cuando tal acceso legítimo no da derecho al usuario para eliminar, copiar o extraer datos de la empresa, las soluciones existentes no protegen adecuadamente contra este riesgo.

Según el estudio Magic Quadrant for Content-Aware Data Loss Prevention realizado por la consultora Gartner, en el año 2014 más del 50% de las empresas utilizará alguna característica en sus políticas de seguridad a la hora de realizar una prevención de fuga de información (Data Loss Prevention) en sus datos sensibles. Sin embargo sólo el 30% de estas dispondrá de una solución o estrategia DLP global basada en el contenido.

La siguiente tabla muestra en datos brutos, la pérdida de control y seguimiento de la información ha accesos información expuesta por cada una de las empresas de seguridad. [6]

TABLA 1. TOTAL DE FUGA DE INFORMACIÓN.

Empresa	Nº de documentos	Usuarios	Directorios	Impresoras	Software	Correos	SSOO	Total metadatos
DLP1	1263	528	450	101	148	28	10	1265
DLP2	1247	323	330	47	101	10	6	817
DLP3	757	228	44	10	98	6	8	394
DLP4	214	93	115	30	42	0	4	284
DLP5	291	62	19	6	67	0	4	158
DLP6	154	18	7	1	42	0	1	69
DLP7	95	8	0	0	19	0	0	27
DLP8	61	20	1	0	13	0	0	34
DLP9	43	6	1	0	23	0	0	30
DLP10	18	4	0	0	12	0	0	16
DLP11	4	1	0	0	4	0	0	5
DLP12	1	0	0	0	1	0	0	1

Fuente [6] Fuga de información en empresas líderes en Data Loss Prevention

Por estos casos se recomienda realizar diseños de soluciones de seguridad de DLP donde se podrá tener autorizados y no autorizados.

Toda solución de DLP debe ser capaz de ofrecer una protección completa tanto en la información en reposo, en uso y la información en movimiento

FIGURA. 2 GRÁFICO DE LAS EMPRESAS LÍDERES EN DATA LOSS PREVENTION, SEGÚN GARTNER

Fuente [6] Fuga de información en empresas líderes en Data Loss Prevention

Las tecnologías están cambiando continuamente y, en consecuencia, la forma en que las personas hacen un uso

cotidiano de ellas. Cloud Computing, los medios sociales y los dispositivos móviles ya se encuentran integrados en mayor o menor medida en nuestras vidas.

¿A qué nuevos riesgos se enfrentan las compañías al implementar estas nuevas tecnologías para el uso de sus empleados y de sus clientes?

Podemos ver los riesgos a que se exponen las compañías ante estos cambios propiciados por la evolución tecnológica, y qué acciones recomendamos tomar para mitigarlos. Las empresas requieren adoptar estas nuevas tecnologías para seguir siendo competitivas. Sin embargo, este tipo de cambios en los modelos de negocio que aumentan la exposición al riesgo, siempre deben ser implantados de forma controlada y, en consecuencia, se han de adoptar las medidas necesarias para evitar los

nuevos problemas a los que se enfrentan las empresas

II. ESTRATEGIAS PARA LA IMPLEMENTACIÓN

Un asesoramiento experto asegura inversiones prevención de fuga de información (DLP) alcanzar los objetivos de negocio.

Un ciclo de vida completo para un proyecto de DLP incorpora las mejores prácticas, mejoras operativas y aplicación adecuada de herramientas. Como reflejo de las presiones empresariales del mundo real, se debe crear un programa considerando una protección completa de datos en el contexto de maximizar el retorno de la inversión.

Uno de los procesos más importantes dentro de la estructura de seguridad de la información, es el de la clasificación de la información. Estos procesos estarán asociados a la implementación de controles necesarios para dar la protección necesaria a la información de acuerdo con los niveles de clasificación establecidos.

La prevención de pérdida de datos protege los datos confidenciales y la propiedad intelectual contra transferencia no autorizada a través de varios medios de comunicación (intranet, internet, dispositivos externos, etc.).

Proteger informaciones confidenciales de divulgación no autorizada se ha tornado una gran preocupación para las empresas de todo el mundo. Algunos casos conocidos destacaron la necesidad urgente de que las empresas protejan sus activos principales, su propiedad intelectual y los datos confidenciales.

La pérdida de datos puede ocurrir por medio de varios canales de comunicaciones de datos:

- Aplicaciones (e-mail, webmail, screen capture o captura de pantalla, P2P, mensajes instantáneos, Skype)
- Red (HTTP, HTTPS, FTP, Wi-Fi)
- Física (USB, iPod, impresora, fax, CD, DVD y otros dispositivos removibles, discos duros)

La pérdida de datos puede tener consecuencias drásticas para las empresas, debido a las exigencias legales de tornar esas pérdidas públicamente conocidas. Hay innumerables factores del mercado que llevaron al interés por las soluciones de prevención de fuga de información:

- Exigencias legales y de gobernanza corporativa.
- Las empresas precisan adherir a una lista creciente de normas del mercado, legales y de privacidad, que exigen más control de la política corporativa.
- Amenazas de multas por incumplimiento de normas, procesos civiles y daños a la marca de la empresa.
- Pérdida de registros y datos confidenciales de clientes.
- Aunque no sea un problema reciente, la divulgación de la pérdida de datos para el público y el riesgo excesivo asociado a la falta de conformidad han destacado la necesidad de prevención.

La protección de derechos de propiedad intelectual siempre ha sido una prioridad crítica. Empresas de varios sectores están extremamente preocupadas en proteger patentes, marcas registradas o no, secretos comerciales, proyectos, arquitecturas, derechos de autoría, algoritmos,

códigos fuentes de software, esquemas de hardware, invenciones, procesos comerciales y otros recursos corporativos.

Las empresas con contratos de tercerización están preocupadas, principalmente con el aumento de informaciones en formato electrónico. Además el e-mail es el sistema principal de archivado de esas informaciones, lo que torna aún más importante la protección del flujo de salida de mensajes.

III. HÁBITOS BÁSICOS DE SEGURIDAD [7]

A continuación se brindan algunos consejos a tener en cuenta ante este escenario, de tal modo que sea posible evitar las principales causas de fuga de información, principalmente enfocados al ámbito corporativo:

1. ***Conocer el valor de la propia información.*** Realizar un análisis de riesgos y un estudio de valuación de activos para poder determinar un plan de acción adecuado que permita evitar posibles filtraciones.

2. ***Concientizar y disuadir.*** Diseñar una estrategia de concientización que incluya la responsabilidad en el manejo de la información, que funcione tanto para capacitar a las personas que podrían filtrar información por error u omisión, como para persuadir a las que deliberadamente intenten hacerlo, mostrando las potenciales consecuencias.

3. ***Utilizar defensa en profundidad***. Considerar el modelo de defensa en capas para tomar distintas medidas de diferente naturaleza a fin de no centralizar las soluciones ni promover puntos únicos de falla.

4. ***Incluir herramientas tecnológicas.*** En ámbitos corporativos resulta muy importante contar con una solución técnica de protección, por medio de hardware, software, o combinación de ambos, tanto a nivel de redes como de equipos (servidores y estaciones de trabajo). El crecimiento de amenazas como el spyware hace que los códigos maliciosos también sean potenciales puntos de fuga de información.

5. ***Seguir los estándares internacionales.*** Alinearse con estándares internacionales de gestión de la seguridad permite disminuir el riego de incidentes y evitar que el negocio se vea afectado por un determinado evento de filtración.

6. ***Mantener políticas y procedimientos claros.*** Relacionado con el punto anterior, se debe tener una clara definición y comunicación de las políticas de seguridad y acuerdos de confidencialidad, aceptados y firmados por todos los usuarios. Esto minimiza potenciales fugas de información, al contar con un consentimiento firmado del usuario para no realizar ciertas acciones.

7. ***Procedimientos seguros de contratación y desvinculación***. Tanto al momento de la contratación como en la desvinculación de una persona dentro de una organización, se produce la conexión o desconexión de una nueva pieza con el motor de la organización, por lo que deben tenerse en cuenta los métodos de acceso y registro de los usuarios en sus primeros o últimos momentos de trabajo.

8. ***Seguir procesos de eliminación segura de datos.*** Es fundamental que los datos que se desean eliminar sean efectivamente eliminados y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

9. ***Construir un entorno de confianza.*** Contar con personal capacitado y responsable para la gestión y administración de información sensible.

10. ***Aceptar y entender la realidad.*** Si bien el seguir estos consejos no garantiza de forma absoluta la seguridad de la información, estas prácticas ayudan a disminuir los riesgos de pérdida de información valiosa y resaltan la importancia de tomar medidas concretas y definir un plan realista, alejado de la paranoia innecesaria.

"*Es importante entender que no es posible controlar todas las variables y mucho menos todas las acciones de las personas que integran una corporación, por lo tanto,*

siempre habrá un margen de error en relación a la protección de la información. Sin embargo la idea es reducir ese margen al mínimo posible. Y esto se logra por medio de prácticas efectivas y adecuadas en torno a la Seguridad Informática. Por tal motivo en ESET trabajamos constantemente en capacitar a nuestros usuarios y brindar las herramientas tanto técnicas como educativas para evitar cualquier incidente informático", comenta Federico Pacheco, Education & Research Manager para ESET Latinoamérica. [7]

IV. METODOLOGÍA

La solución de prevención de fuga de información DLP, es una herramienta que permite el monitoreo, auditoria y bloqueo de información confidencial o privada que sale de la empresa o viaja a través de canales de comunicación autorizados y no autorizados tales como aplicaciones, dispositivos físicos y protocolos de red.

La metodología recomendada para la implementación de la herramienta está basada en un ciclo de vida de seis pasos aplicables a la organización:

FIGURA. 3 FLUJO DE TRABAJO DE MCAFEE DLP ENDPOINT

Fuente [9] McAfee Data Loss Prevention Endpoint Guía de producto

1. ***Descubrir y Aprender:*** En esta fase se realiza la monitorización de la información relacionada con las diferentes jefaturas, información recopilada por la solución McAfee DLP.
2. ***Evaluar el Riesgo:*** Evaluación del riesgo asociado a la información por parte del perfil funcional.

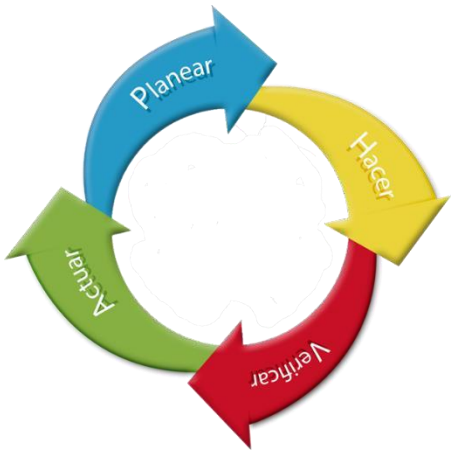
   Refinamiento de los niveles de impacto asociados a cada categoría de clasificación basados en la retroalimentación realizada por los usuarios funcionales.

   Análisis Política Base DLP con base en la información recopilada y la gestión de riesgos asociada.
3. ***Afinamiento de Política:*** Personalización de Política Base DLP con base en la información analizada por parte de los usuarios funcionales.
4. ***Aplicar Controles:*** Creación de Grupos de usuarios a los cuales se aplicaran las políticas, asociación de las diferentes políticas a los grupos de usuarios y replicación de la política definida para las diferentes jefaturas en ambiente producción.
5. ***Monitorizar, Reportar y Evaluar:*** Monitorización de los eventos generados por la solución, "SOC".

   Evaluación resultados aéreas o procesos involucrados y definición de planes de Acción.
6. ***Prevenir:*** Paso a modo prevención para las áreas con base en la definición de los planes de acción.

Posterior a esto se pasara a "Perfeccionar y Verificar" la política implementada bajo Ciclos PHVA.

FIGURA. 4 EL CICLO PHVA O CICLO DE DEMING



Fuente [10] OSHAS 18001: En el corazón de la Gestión

REFERENCIAS

[1] Studies on information as an asset I: Definitions. Journal of Information Science , 29(3), 159-166. | Oppenheim, C.,Stenson, J. & Wilson, R. M. S. (2003a).

[2] Seguridad de la información en las instituciones financieras| Ing. Paola Katherine Macías Anchundia.Disponible en Internet:http://repositorio.maeug.edu.ec/bitstream/123456789/183/2/10392999871338782948485686142557749202 6.pdf

[3] Fuga de información en las organizaciones. | Newnetsa -July Calvo. Disponible en Internet: http://www.newnetsa.com/2009/08/fugade-informacion-en-las-organizaciones/

[4] SC Magazine; "Security Spending, DLP Projects to Increase," www.scmagazineus.com/security-spending-dlp-projects-toincrease/article/164337/

[5] Informe DLP: Prevención de fuga de información http://blog.seguinfo.com.ar/2011/06/informe-de-dlp-prevencion-de-fuga-de.html

[6] Fuga de información en empresas líderes en Data Loss Prevention http://blog.elevenpaths.com/2013/08/fuga-de-informacion-enempresas-lideres.html

[7] http://www.eset-la.com/centro-prensa/articulo/2010/consejosevitar-fuga-informacion/2376

[8] Data Loss Prevention – Part 3 – How DLP Technologies Work http://blog.skodaminotti.com/blog/data-loss-prevention-part-3how-dlp-technologies-work/

[9] McAfee Data Loss Prevention Endpoint Guía de producto https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24536/en_US/dlp_930_pg_TP000036-a00_en-us.pdf

[10] OSHAS 18001: En el corazón de la Gestión https://seguridadindustrialgt.wordpress.com/tag/oshas-18001/