Fuga de información confidencial en las instituciones financieras y uso de data Loss Prevention

Leakage of confidential information in financial institutions and use of data Loss Prevention

(Entregado 20-agosto-2016 –Revisado 30-10-2018)

MSc. Marco Antonio Yandún Velasteguí
Ing. Eduardo Patricio Cando Salas
Msc. Damaris Elizabeth Mora Cuastusa

Universidad Politécnica Estatal del Carchi (UPEC - ECUADOR)

yandunmarco@gmail.com
patricio.cando@live.com
damarismora84@gmail.com

Resumen

En el presente artículo se expone una problemática existente en las Instituciones Financieras, la fuga de información, así también los posibles daños que pueda causar la falta de aplicación de políticas, procedimientos y controles para respaldo de información critica y el impedimento de la salida de información por múltiples medios lógicos o físicos, se hace una recopilación de datos referentes a la fuga de información disponible y verificada, se indica la clasificación de la información por su contenido y se muestra las estadísticas de los datos que los empleados suelen sacar de su lugar de trabajo, basado en los informes de seguridad de empresas proveedoras y fabricantes de herramientas de seguridad informática y en la investigación de campo realizada en una institución financiera presente en las provincias de Carchi, Imbabura y Pichincha, con estos resultados se puede analiza las ventajas y beneficios de utilizar herramientas Data Loss Prevention (DLP), que permitan mitigar la problemática de pérdida de datos confidenciales, en las empresas especialmente en el segmento Cooperativo Financiero que son las más afectadas por la información que generan y utilizan.

Palabras clave: *Fuga de información, Institución Financiera, Cooperativa Financiera, Seguridad Lógica.*

Abstract

In this article an existing problems in financial institutions, information leakage, so the potential damage that can cause lack of implementation of policies, procedures and controls for backup of critical information and the impediment of information output is exposed multiple logical or physical means, a compilation of data on the leak of information available and verified is made, the classification of information its content is indicated and statistics data shows that employees often take their place work based on safety reports of suppliers and manufacturers of computer security tools and field research conducted in this financial institution in the provinces of Carchi, Imbabura and Pichincha, these results can be analyzed the advantages and benefits using Data Loss Prevention (DLP) tools to mitigate the problem of loss of confidential data, especially in the business segment Financial Cooperative that are most affected by the information generated and used.

Keywords: *Information leakage, Financial Institution , Financial Cooperative, Security Logic.*

1. Introducción

La información es uno de los bienes más importantes que tiene una empresa en especial las Instituciones Financieras, la información incluso es considerada el activo principal y sin la cual la empresa no podría realizar su operaciones de forma normal, es más importante que la misma edificación o que todos los activos físicos juntos, proteger la información es una tarea que conlleva múltiples escenarios y responsables, ya que los datos correctamente protegidos ayudan a las empresas a levantarse, reconstruirse inclusive si no tuviera un espacio físico luego de un desastre, (Bravo, 2010) pero así también, si la información esta desprotegida contra fugas, sin respaldo; así se disponga de los mejores sistemas de seguridad física, electrónica e infraestructura la empresa no podría ejecutar su operaciones e incluso se encontraría en medio de una crisis mayor, su desaparición. (Quishpe 2007).

Así también, Según (Ernst & Young, 2012, pág. 5) "La información es poder. Los nuevos paradigmas de enfocar tanto el negocio como la tecnología han provocado el cambio de la protección del perímetro de seguridad hacía el aseguramiento y control a nivel de información y datos", esto conlleva a reunir los esfuerzos necesarios para proteger la información.

Erróneamente se cree que la seguridad de la información simplemente es mantener respaldados los datos realizando los procesos de respaldo establecidos y mantener en lugares restringidos, sin tomar en cuenta muchos riesgos existentes y brechas de seguridad que ocasionen perdida de información y que carezcan de controles físico y lógicos necesarios y adecuados. (Rojas y Vela 2011).

Es por ello que la fuga de información puede ser un problema común para los responsables de seguridad lógica y puede convertirse en un inconveniente muy grave con consecuencias desafortunadas si la información llegara a manos equivocadas. (López 2013). La fuga de información puede ser tratada como un incidente que puede ser causado ya sea de forma interna como externa, y a la vez intencional o no. Se puede mencionar múltiples causas, por ejemplo: algún funcionario de la empresa que venda información a otra, extravío de documentos en lugares públicos, documentos

que se arroja a la basura sin destruir, perdidas de laptops o dispositivos extraíbles que contengan información sensible, fuga por medio de programas de software malicioso o spyware instalados en equipos de cómputo infectados. (Bortnik, 2010).

Para lo cual es necesario implementar controles necesarios que vayan de acuerdo a las recomendaciones de los estándares y buenas prácticas internacionales, el presente artículo aborda esta problemática y analiza controles básicos y controles gestionados por medio de sistemas especializados en prevenir la fuga de información. (Quishpe 2007).

2. MARCO TEÓRICO

a. Fuga de información lógica

Considerada como la salida no controlada de la información y que vaya a parar en manos equivocadas, así como la pérdida de control de los custodios de la misma, también la fuga de información es cuando un sistema informático tiene brechas de seguridad o se encuentra afectada su integridad permitiendo que atacantes en la intranet o desde internet intercepten los datos. Kelsey (2002).

Adicionalmente en las empresas existen herramientas de trabajo que contribuyen a la salida de información, las impresoras y copiadoras, en donde más del 80% de los empleados tienen acceso libre a estas, en un estudio de (López, 2013) indica que de 100 documentos encontrados en un basurero de una empresa, el 10% contenía información clasificada como confidencial es decir nombre de clientes , direcciones, teléfonos, entre otros, evidenciando que no se aplicaba el proceso de destrucción adecuada de documentos desechados y falta de aplicación de las políticas de seguridad física al momento de enviar los desechos fuera de la empresa especialmente papel utilizado en las oficinas.

Pero no solo la información sale por medios impresos, sale en forma lógica o digital por medio de: correo electrónico, dispositivos extraíbles USB, unidades de Red, dispositivos móviles conectados a un equipo de computación o a una red inalámbrica, copia de pantallas, sistemas de intercambio de archivos (P2P), mensajería simultanea, sitios alojamiento de archivos utilizando el protocolo ftp, almacenamiento en la nube, discos duros virtuales, discos externos, aplicaciones de internet móvil, internet por medio de blog y redes sociales, redes privadas virtuales (VPN), entre otros, existiendo en ocasiones en la empresa solamente controles básico de bloqueo de puertos en el sistema operativos, reglas en servidores de dominio o controles básicos por medio de gestores de antivirus. (Castrillón y Lescano, 2013).

b. Clasificación de la información en pública, privada y confidencial

Dentro de las empresas la información tiene su clasificación dependiendo del contenido y del público a donde está dirigida, según (Pacheco, 2011, pág. 3) “La confidencialidad se refiere a la característica que implica que la información sea accedida solamente por los usuarios autorizados. Por su parte, la privacidad habla más bien de una garantía de confianza respecto a la propia información y su uso”.

En el Ecuador existen Leyes que indican las pautas para que cierta información pueda considerarse como confidencial, privada o pública. Según la Ley Orgánica de Transparencia y acceso a la Información Pública, 2004 en su Artículo 6 menciona:

> "Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República"(Ecuador, 2004, pág. 4)

Este artículo legal se puede aplicar no solo a empresas publicas sino también privadas ya que se dispone de un marco legal, que se puede incluir en acuerdos de confidencialidad entre el empleado y la empresa para tratar de disminuir la salida de datos confidenciales y privados.

Otra de las definiciones para el desarrollo de este artículo es la que menciona el Instituto Nacional de Estadística y Censo del Ecuador, en la que se refiere a la información privada como la información que es relevante para el tratamiento interno de la empresa, que no debe ser revelada por ningún medio mientras no sea oficialmente publicada. (INEC, 2015).

Por el nivel de clasificación que la información obtiene, se establece las acciones a tomar así por ejemplo: para la información privada es necesario notificar al usuario, bloquear el intento de salida y auditar la información, para la confidencial se utiliza la remoción del dato, notificaciones, generar alertas y tratamiento de control por medio de herramientas de prevención de fuga. (Teymouri y Ashoori, 2010).

c. Formas comunes de fuga de información

Dentro de las empresa existen múltiples formas para que la información salga de forma no controlada, entre lo más común se puede mencionar la salida de documentos, datos o información a través de cualquier dispositivos externo de grabación, por medio impreso y por cualquier servicios o protocolo disponible en internet

Tabla 1.
Información que los empleados extraen de la empresa basado en el Estudio de Seguridad de la marca (Chek Point, 2015)

DATOS ENVIADOS FUERA DE LA ORGANIZACIÓN POR LOS EMPLEADOS					
	2014	**2013**		**2014**	**2013**
Información del propietario	45%	35%	Información de la Red	13%	14%
Datos de tarjeta de crédito	30%	29%	Archivos protegidos con contraseña	10%	10%
Registros de datos de negocios	20%	21%	Mensaje de correo confidenciales	5%	5%
Información personal	25%	22%	Números de cuentas bancarias	5%	4%
Información sobre salarios	13%	14%	Otras	27%	31%

Fuente: Chek Point 2015

Para acotar los datos anteriores, Según (Ernst & Young, 2012) en una encuesta realizada por Dark Reading / Information Week (2011), el 73% de las fugas de información provienen de fuentes internas. En otra encuentas de MIS Training Institute at CISO Summit (2011) el 80% de los responsables de seguridad ve a los empleados como la mayor amenaza. Y el Informe de McAfee Datagate, sobre la encuesta realizada a 1400 profesionales de Tecnologia de la Informacion de Reino

Unido, Estados Unidos, Alemania y Australia, revela que el 77% de las empresas son incapaces de auditar o cuantificar la pérdida tras una fuga de información,tomando en cuenta un estudio de tal magnitud se puede considerar que el Ecuador la realidad no es diferente.

3. Resultados y discusión

Entre noviembre 2015 a febrero 2016, se realizó la investigación en una institución financiera cooperativa con influencia en las provincias de Carchi, Imbabura y Pichincha, con 129 funcionarios, se exponen las principales preguntas relacionadas con la fuga de información.

a.. La fuga de información lógica tiene relación con

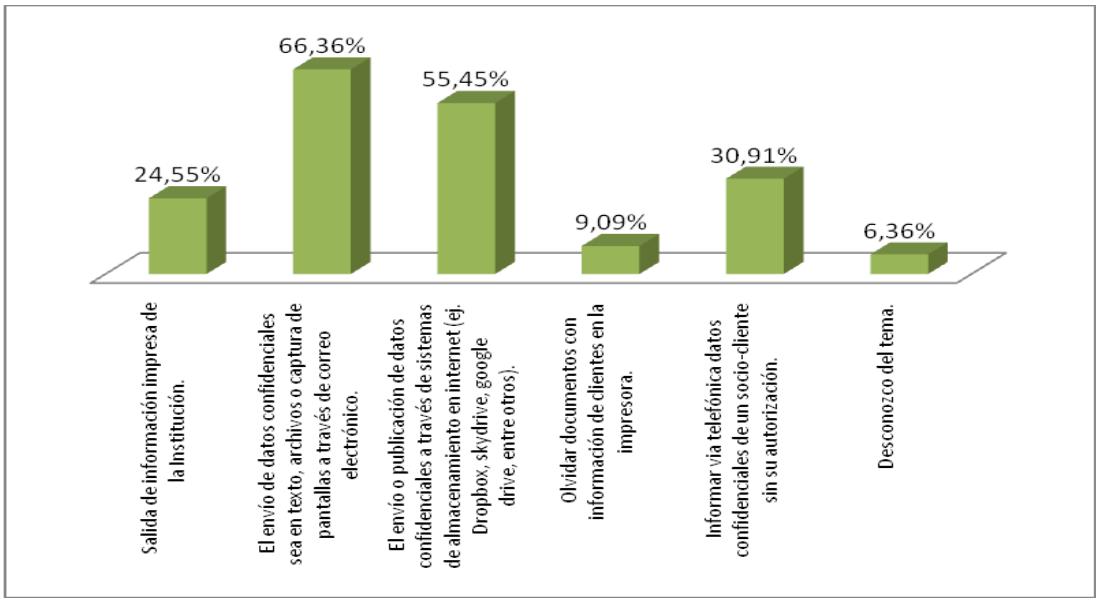

Figura1. Fuga de información lógica
Fuente Autores

Se evidencia que el envío de datos confidenciales sea en texto, archivos o captura de pantallas a través de correo electrónico es con lo que más relacionan con el término fuga de información con un 66%, luego con un 55% esta publicar información confidencial en sistemas de almacenamiento en internet como Dropbox, Google drive, etc. Con el 30% se considera fuga de información informar vía telefónica datos confidenciales

b. Medidas para mitigar la fuga de información que se ha implementado en la Institución investigada

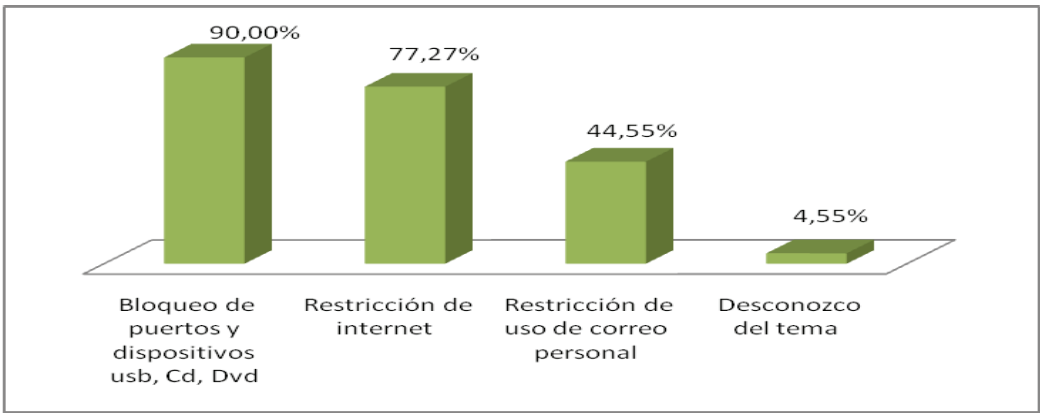

Figura2. Medidas para prevenir la fuga de información confidencial
Fuente Autores

Tomando en cuenta que los empleados tienen acceso a la información y la salida de información de socios y clientes es alarmante ya que el resultado de la información obtenida es muy alto, además la información sobre números de cuentas bancarios y salarios es confidencial y en un porcentaje alto sale de la Institución.

Formas de protección de información financiera

Para lograr una protección básica contra la fuga de información financiera se puede realizar con la ayuda de herramientas disponibles en el sistema operativo como: el bloqueo de puertos universal serial bus (USB), unidades de disco compacto (CD), disco de video digital (DVD), puerto paralelo (LPT), Bluetooh. Para lograr una protección más efectiva se puede usar herramientas tecnológicas de prevención de fuga de información avanzadas como Data Loss Prevention (DLP), la cual se considera una tecnología que está evolucionando y mejorando su forma de operar y la estadística en referencia a la demanda de estos productos lo demuestra ya que paso de 50 millones de dólares en el 2006 a 500 millones de dólares en el 2009 las ventas de soluciones DLP (Proctor & Ouller, 2007).

Por lo consiguiente las herramientas DLP ayudan de forma sustancial a prevenir y disminuir las fugas y perdida de datos aplicando los múltiples vectores o reglas de control y salida, cabe aclarar que los DLP no es lo último en tecnología de prevención, es una herramienta más, que conjuntamente dispositivos de protección perimetral de redes como los muros de fuego (Firewall), sistemas de detección de Intrusión (IDS), sistemas de Prevención de Intrusión (IPS), proporcionan los controles para ser una línea de defensa contra la fuga de información desde el interior de las empresas, (Castrillón y Lescano, 2013).

Entre los beneficios de disponer herramientas DLP es preservar la seguridad y mantener el cumplimiento de información confidencial de una forma simple, "El enfoque completo de Symantec para proteger la información abarca los perímetros de seguridad erosionados de la actualidad, los ataques dirigidos cada vez más frecuentes y los hábitos y las expectativas en constante evolución de los usuarios." (Symantec 2015)

Es por ello que las herramientas DLP ayudan a controlar el comportamiento de los usuarios frente a la información privada que utilizan, ya que disponen de configuración basada en reglas, grupo de palabras clave, diccionarios de términos considerados confidenciales, de auto aprendizaje para mejorar las configuraciones de seguridad y de alertas que se generan en línea y advierten al

usuario sobre la gestión de la información; las herramientas DLP modernas ofrecen una gama de servicios que incluyen la generación de log's o bitácora de auditoría, que pueden ser utilizados con un correlacionador de eventos y disponer de reportería en tiempo real de múltiples escenarios que soliciten los entes de control especialmente cuando se requiera el cumplimiento de normativas y disposiciones internas (McAffe 2015)

4. Conclusiones

La fuga de información es una problemática que está presente en las empresas y las estadísticas demuestran que los datos que se pierden son confidenciales como: numero de cuentas bancarias, clientes, información contable, entre otras y esta información sale sin inconvenientes mayores ya que no se aplica controles adecuados para prevenirlo, como pueden ser políticas y procedimientos establecidos referentes al tema, restricción de acceso a internet y sus servicios, bloqueo de puertos, aplicación de roles, credenciales de acceso a sistemas informáticos, segregación de funciones y el uso de herramientas de prevención de fuga de información.

Las empresas del segmento Cooperativo Financiero no están exentas de esta problemática, es mas pueden verse inmersas en situaciones adversas por el hecho de que la información se fugue es crítica. Por ello se plantea alternativas para mitigar este problema la más efectiva pero que necesita de financiamiento es la de implementar herramientas Data Loss Pevention que Previenen que los datos salgan sin control.

Las herramientas DLP han sido poco explotadas o aplicadas en el Ecuador razón por la cual existe poca información científica que pueda aportar con un análisis profundo sobre el tema, queda abierta la puerta para realizar una investigación en base al análisis de las herramientas en las empresas especialmente los DLP que lideren el mercado de este producto.

5. Referencias bibliográficas

Bortnik S. (2010). *Comunidad de seguridad de ESET ¿Qué es la fuga de información?*. Obtenido de: Welivesecurity http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Bravo Sandoval, Y. B. (2010). *Importancia de la gestión de servicios de tecnología de información basada en ITIL*. Obtenido de: http://cdigital.uv.mx/bitstream/123456789/29464/1/bRAVO%20sANDOVAL.pdf

Castrillón Cadavid, M. A., & Lezcano Gallego, M. A. (2013). *Metodología para prevenir la fuga de información aplicando un sistema DLP en las empresas del sector financiero.* Obtenido de: http://bibliotecadigital.usbcali.edu.co/jspui/bitstream/10819/1607/1/Metodologia_Fuga_Informacion_Castrillon_2013.pdf

Chek Point. (2015). *2015 Chek Point Report.* Obtenido de https://www.checkpoint.com/resources/2015securityreport/CheckPoint-2015-SecurityReport.pdf

Ecuador. (2004). *Ley Orgánica de Transparencia y acceso a la Información Pública.*Obtenido de:http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Ernst, & Young. (2012). *Prevención de Fugas de Información Soluciones DLP – Data Loss Prevention.* Obtenido de: http://www.andorratelecom.ad/c/document_library/get_file?uuid=28bc3e82-0a1f-44f8-a688-1909deb3f363&groupId=10156

INEC.(2015).*Norma Técnica de confidencialidad estadística y buen uso de la información*

estadística. Obtenido de: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Resoluciones/2015/resolucion_no._001-inec-diju-nt-2015.pdf

Kelsey, J. (2002). Compression and Information Leakage of Plaintext. Fast Software Encryption. Obtenido de: http://www.iacr.org/cryptodb/archive/2002/FSE/3091/3091.pdf

López Argüello, M. E. (2013). La cultura en seguridad de la información y su relación con la confidencialidad en UNIFINSA de la ciudad de Ambato. Obtenido de: http://repositorio.uta.edu.ec/bitstream/123456789/3661/1/TMGF004-2013.pdf

McAffe. (2015). *McAffe for Bussines*. Obtenido de McAfee DLP Endpoint: http://www.mcafee.com/es/products/dlp-endpoint.aspx

Pacheco F. (2011).*Fuga de información: ¿una amenaza pasajera? Buenos Aires Argentina*. Obtenido de:http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf

Proctor P, MogullR. y Oullet E., (2007).*Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, 2007 Gartner Inc.*

Quishpe Reinoso, P. V. (2007). Definición e implementación de un modelo de respaldos de información en la compañía Transelectric SA. Obtenido de: http://bibdigital.epn.edu.ec/bitstream/15000/1475/1/CD-0990.pdf

Rojas Urguilés, J. L. y Vela Veintenilla, J. J. (1998), *Planificación estratégica y plan de seguridad informática de FABRIL FAME S.A*. Obtenido de: http://repositorio.espe.edu.ec/bitstream/21000/5167/1/T-ESPE-033137.pdf

Symantec. (2015). *Symantec Corporaciones.* Obtenido de Symantec Data Loss Prevention: http://www.symantec.com/es/mx/data-loss-prevention/

Teymouri, M., Ashoori, M, (2010).*The impact of information technology on risk management.* Published by Elsevier Ltd.