ADMINSTRACION DE LA SEGURIDAD

Fuga de información la mayor amenaza para la imagen corporativa

Sandra Patricia Gordillo Contreras

Universidad Militar Nueva Granada

Especialización Administración de la Seguridad

Bogotá D.C.

2017

Resumen

La fuga de información es una vulnerabilidad que pone en riesgo la imagen de las empresas, estos incidentes pueden ser internos y externos, esta operación se ve afectada por los empleados infieles. La protección de la información se articula en torno a la protección de tres principios básicos: confidencialidad, integridad y disponibilidad, esto conlleva a que una buena seguridad de información debe también cumplir con tres elementos que son personas, procesos y tecnología.

"La fuga de información presenta una tendencia creciente en lo que refiere a pérdidas de información para las empresas, a partir de estadísticas de Data Breaches y del Indetify Theft Center se sabe que, solo en Latinoamérica, en los últimos dos años la cantidad de incidentes de fuga de información fue casi igual al 90% de los habitantes, lo cual sería como si en el último par de años se hubiera visto filtrada información sensible de 9 de cada 10 habitantes de la región". (Admin in seguridad informatica, Servicios, 2016).

Con el fin de prevenir la fuga de información es necesario crear cultura de seguridad de información con el fin que los empleados tomen conciencia de la importancia de mantener la información confidencial protegida, crear políticas de protección de datos, restringir el acceso a sitios no autorizados, utilizar medios seguros para el almacenamiento de la información, son algunas de las medidas más importantes.

Palabras claves: Controles - Fuga de información – Protección de información – Vulnerabilidades.

Abstract

The leak of information is a vulnerability that puts at risk the image of the companies, these incidents can be internal and external, this operation is affected by the infidel employees. The protection of information is based on the protection of three basic principles: confidentiality, integrity and availability, which means that good information security must also comply with three elements that are people, processes and technology.

"Information leakage presents a growing trend in terms of information loss for companies, based on data from Data Breaches and Indetify Theft Center, it is known that in Latin America alone, in the last two years the number of incidents of Information leakage was almost equal to 90% of the inhabitants, which would be as if in the last couple of years sensitive information had been filtered out of 9 out of 10 inhabitants of the region." (Admin in seguridad informatica, Servicios, 2016)

In order to prevent information leakage, it is necessary to create a culture of information security in order to make employees aware of the importance of keeping confidential information protected, create data protection policies, restrict access to unauthorized sites, Using secure means for storing information, this can be dataloker, airokei, etc., are some of the most important measures.

Keywords: Controls - Information leakage - Information protection –Vulnerabilities.

Introducción

Durante los últimos cinco años, las organizaciones han experimentado un aumento en el volumen de fugas de información intencionales o no. En este escenario conceptos como reputación corporativa o riesgo reputacional (Toda acción, evento o situación que podría impactar negativa o positivamente en la reputación de una organización) han ido ganando relevancia en el ámbito empresarial propiciado por los ataques a grandes firmas unidas al endurecimiento de las normativas. (Arantxa Calvo Moyano, directora de marketing de secura it).

Uno de los riesgos que se presentan en las empresas y que les ha costado mucha perdida de dinero e imagen es la fuga de información por cuenta de agentes internos y externos, una de las razones es la no realización de un buen estudio de confiabilidad por parte de talento humano y de igual forma la no capacitación en el momento del ingreso del empleado, con el fin de proporcionarles confianza y seguridad.

Es complicado medir el impacto que puede causar a una empresa la fuga de información porque puede ser diverso, dependiendo de la intensión del incidente. “En aquellos casos en que se trata de un accidente no intencional, el impacto en la empresa dependerá de qué ocurre con el nuevo poseedor de esa información. Si se supone que un gerente de la empresa pierde una computadora portátil, el impacto puede ser nulo si quién la encuentra ignora la información que allí se contiene y formatea el sistema; o puede ser alto si el nuevo poseedor identifica los datos y los utiliza para publicarlos, comercializarlos o cualquier otra acción dañina.” (¿Qué es la fuga de información? Sebastián bortnik, 2010).

Con esto podemos decir que depende del tipo de información que se haya extraviado y el valor que le representa a la empresa para así poder implementar un plan de acción inmediato.

La información es el activo más importante de una organización, es por eso que requiere especial atención en su cuidado y/o protección. Es la que guía a la empresa por la senda del éxito. Así que la configuración e instalación inicial de los sistemas de cualquier empresa es fundamental para su correcto funcionamiento, ya que constituye el punto de partida para evitar que se dejen vulnerabilidades, que al ser descubiertas por intrusos, afectarían la correcta funcionalidad de los sistemas.

El uso de las tecnologías de la información y la comunicación (TIC), ha creado en la sociedad espacios en donde cada vez se gestiona más información y también se convierte en un activo crítico en las organizaciones y los usuarios. “las tecnologías posibilitan un tratamiento de la información sin precedentes y a nivel global, de manera que es transmitida, procesada, copiada o almacenada con una rapidez y eficacia impensable hace algunos años, sumado al hecho de que es posible llevar a cabo dichas acciones, desde múltiples tipos de dispositivos, en cualquier lugar y en cualquier momento.” (Guía gestión de fuga de información, Mayo 2012).

Con el fin de ayudar a los empleados de las organizaciones a implementar buenas prácticas en la protección de la información es indispensable asumir la responsabilidad de: tener buen conocimiento en las políticas de la empresa con el fin que el empleado conozca que tan importante es la información que va a manejar, buen uso de las herramientas que le son instaladas en el computador, estar pendiente de los códigos maliciosos que pueden aparecer en el equipo, tener precaución en el transporte y almacenamiento de información, utilizar una conexión segura, etc.

Este documento tiene como objetivo mostrar mediante casuística como ha sido vulnera la infamación en las empresas los riesgos que implica a la imagen corporativa, fuentes de fuga de información, estadísticas empresariales. De igual forma se pretende determinar estrategias para poder neutralizar o evitar que ocurra la fuga de información de manera que se pueda tomar la mejor decisión con el fin de minimizar las consecuencias y el impacto de algún incidente y por último los controles que se deben llevar.

Fuga de información la mayor amenaza para la imagen corporativa

De qué forma es vulnerada la información en las empresas, y los riesgos que implica a la imagen corporativa?

Objetivo general

Determinar la naturaleza del problema especificando estrategias, controles, con el fin de minimizar y/o evitar que se siga presentando perdida de información en las empresas.

Fuga de información

La fuga de información es una vulnerabilidad que pone en riesgo la imagen de las empresas, estos incidentes pueden ser internos y externos, esta operación se ve afectada por los empleados infieles. La protección de la información se articula en torno a la protección de tres principios básicos: confidencialidad, integridad y disponibilidad, esto conlleva a que una buena seguridad de información debe también cumplir con tres elementos que son personas, procesos y tecnología.

Casos relevantes

En los últimos años es habitual la aparición de noticias en todos los medios, sobre empresas que han sufrido alguna pérdida de información, sea de manera intencional o no. La fuga de información genera enormes pérdidas económicas, costos legales y sanciones. Además de costos indirectos como la pérdida de clientes, desventaja competitiva y el deterioro de la imagen y la reputación.

Casos de ataques informáticos

Es importante tener en cuenta que el software malicioso ha revelado información confidencial fuera de la organización sin que el usuario se dé cuenta. Simultáneamente, las personas con acceso a información privilegiada, es aquella a la cual solo tienen acceso directo ciertas personas en razón de su profesión u oficio, la cual por su carácter, está sujeta a reserva, que de conocerse podría ser utilizada con el fin de obtener provecho o beneficio para sí o para un tercero. Por otro lado informantes han utilizado nuevos métodos para sacar conductas cuestionables a la luz pública mediante la difusión de datos confidenciales como el sitio web de ***wikileaks.org.***

(Instituto nacional de tecnologias de la comunicación , 2012). En el año 2010 se produjo, la que está considerada hasta la fecha, como la mayor filtración de información de la historia. Wikileaks, una organización sin ánimo de lucro, publicó un total de 250.000 (cables) comunicaciones que se habían realizado entre el Departamento de Estado Estadounidense y sus embajadas repartidas por todo el mundo. Las consecuencias no se hicieron esperar. Este incidente supuso la confirmación de algo que ya se sabía: la gran dificultad de mantener la confidencialidad de la información, evitando filtraciones, pero también puso de manifiesto que

ninguna organización está a salvo, incluidas aquellas que pertenecen al ámbito gubernamental o dedicadas a alguna de las múltiples ramas o ámbitos de la seguridad, que lógicamente se suponen preparadas, ya que disponen de procedimientos, herramientas y personal entrenado para manejar información considerada sensible y confidencial.

En enero del mismo año tuvo lugar la Operación Aurora, un ataque masivo ocurrido contra más de 30 empresas como Google, Adobe y Juniper; destacado por ser uno de los ataques más importantes en materia de robo de información, aunque finalmente no tuvo éxito.

En julio de 2008 si bien no se dieron a conocer casos como los anteriormente mencionados, se produjo una importante cantidad de incidentes de seguridad basados en la vulnerabilidad del protocolo DNS descubierta por el especialista de seguridad Dan Kaminsky, que sirvió de base para realizar ataques de phishing, propagación de malware y otros. Ese año, según un informe de incidentes de Verizon, el 39% de los incidentes de seguridad involucraron a partners y terceras partes de las empresas, y el 31% de los ataques incluyeron algún código malicioso (en ese entonces el protagonista era el gusano Nuwar).

En agosto de 2007 el sitio global de búsquedas laborales Monster sufrió el robo de 1,6 millones de datos con información personal de los usuarios registrados. Los atacantes ingresaron a las bases de datos con contraseñas que habían sido obtenidas previamente mediante un troyano.

Casos fuga de información por empleados no confiables

"De las fugas, el 75% son accidentales. El 65% de los empleados que roban información deliberadamente ya tienen un puesto asegurado en otro puesto de la competencia. Un 20% han sido contratados por otra empresa en calidad de espías. El perfil más abundante es hombre de unos 37 años con un cargo técnico (científico, ingeniero, programador, etc). La mayor parte de

estos delincuentes tiene acceso autorizado a la información sensible. Además, no tienen la sensación de estar haciendo nada malo" (opinion)

Es el caso relevante el del banco HSBC, que en marzo de 2010 declaró la fuga de datos de 15.000 clientes suizos, luego de que un ex-empleado del área informática les llevará los datos a autoridades impositivas de Francia.

En diciembre de 2009, la red social Tuenti fue afectada por el robo de 4.000 cuentas de usuario y sus contraseñas, por parte de un atacante enojado con la empresa.

Por lo anterior nos podríamos preguntar por la magnitud de los eventos ocurridos, en cuanto a cantidad de registros robados y cantidad de incidentes ocurridos y que han filtrado por lo menos 30.000 registros. Sin dudas es en los últimos años cuando hemos empezado a ver las fugas de información con mayores pérdidas de datos, como lo podemos ver en el siguiente gráfico.

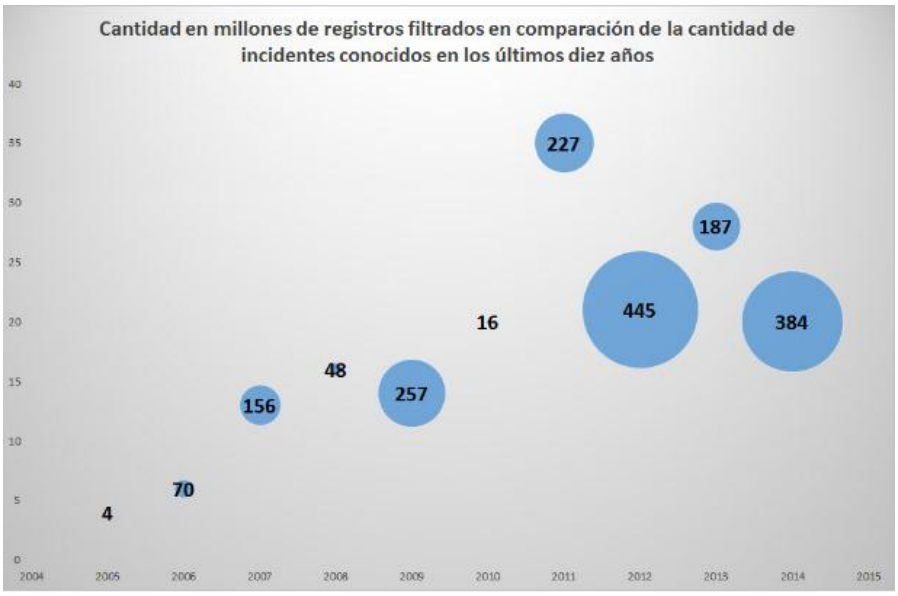
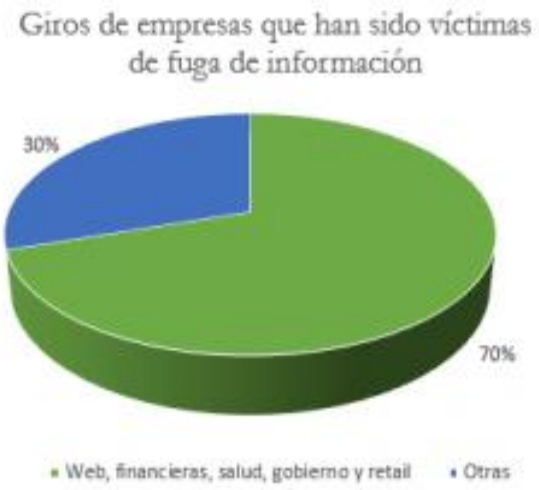


Grafico tomado de: 10 años de fuga de fuga de información – por Camilo Gutiérrez Amaya



El 70% de fuga de información está enfocado en empresas web, financieras, de salud, gobierno y retail
30% otras empresas

Grafico tomado de: Seguridad informática, servicios, Marzo 1 de 2016

Se puede ver que en los últimos cuatro años se concentra el 66% de las pérdidas de datos, Es decir que desde 2011 se han visto casi el doble de registros filtrados que en los seis años anteriores, sin lugar a dudas nos muestra cómo este incidente viene teniendo una tendencia creciente en lo que refiere a pérdidas de información para las empresas.

"De hecho, un dato curioso es que la cantidad de registros filtrados en los últimos dos años es casi igual al 90% de la cantidad de habitantes de Latinoamérica, lo cual sería como si en el último par de años se hubiera visto filtrada información sensible de 9 de cada 10 habitantes de la región.Vale la pena anotar que en la lista de empresas afectadas por estas brechas de seguridad encontramos a Gmail, eBay, Adobe, Sony, Target y AOL entre otras grandes empresas que llegan a manejar grandes volúmenes de información sensible". (Gutierrez Amaya, 2015)

Naturaleza del problema

La mayoría de los autores de robos de información a compañías son de aspectos técnicos, agentes externos y en ocasiones miembros de las propias organizaciones.

Desde el aspecto técnico el problema radica en la dificultad de administrar y gestionar la enorme cantidad de datos que procesan las organizaciones, en este sentido se tiene en cuenta el nivel de los usuarios en acceder a los distintos archivos y datos, los cuales deben viajar por redes y ubicados en distintas ubicaciones dentro y fuera de centros de cómputo, esto hace que lo que se deba proteger no esté centralizado y se requieran medidas y tratamientos diferentes para cada caso.

(Pacheco, 2011)En muchos casos uno de los aliados técnicos de la fuga de información es el malware, que en sus distintas formas y tipos permite acceder a equipos, explotar vulnerabilidades y afectar la privacidad de forma directa. De hecho, como caso particular, el spyware está diseñado para espiar los sistemas en los cuales se logra alojar, haciendo que, por ejemplo, las contraseñas de un usuario sean capturadas, o su información estadística de navegación sea tomada sin su consentimiento para fines económicos. En el mismo sentido, dentro del software malicioso que produce este tipo de resultados, existen los denominados keyloggers, que son dispositivos de software o hardware que capturan silenciosamente lo tecleado por el usuario. Si bien este aspecto técnico debe resolverse principalmente con un software antivirus adecuado, también es indispensable que el usuario conozca los peligros a los que se expone, dado que en muchos casos la falta de concientización es la que promueve la exposición directa a las amenazas.

En el aspecto humano que puede ser externo o interno, si bien en el aspecto interno lo normal es que las personas no roben información intencionalmente, no podemos negar que exista la posibilidad. Es posible afirmar que si en algún momento existe fuga de información intencionalmente esto se debe a grupos de empleados disconformes con la empresa, o que se encuentren perjudicados por la misma, esto sin contar el espionaje interno que puede existir por parte de empleados que lo realizan en función de intereses externos, perjudicando a la propia organización a la que pertenecen.

Con esto podemos decir que "Algo tan simple como una infección de malware transportado en un pendrive podría introducir un riesgo importante en una empresa si no cuenta con un sistema que pueda prevenirlo de manera eficiente. En las empresas, para facilitar la trazabilidad de las acciones de los usuarios, se suelen incluir procedimientos mediante los que se garantiza que el uso de los activos de información es efectivamente auditado y que es posible generar registros (logs) de las acciones importantes que se hayan definido, que si bien es un proceso técnico, implica un conocimiento de los individuos respecto a su grado de responsabilidad en lo que realizan dentro de una empresa." (Pacheco, 2011).

Por eso tenemos que tener claro y definido los términos sobre fuga de datos y así evitar riesgos.

- ✓ Evento: cambio inesperado de un activo de información que indica que puede haberse infringido una directiva de seguridad.
- ✓ Incidente: evento de seguridad que compromete la integridad, confidencialidad o disponibilidad de un activo de información.

- ✓ Fuga: incidente que provoca la divulgación confirmada de datos (no solo su posible exposición) a destinatarios no autorizados.

Riesgos

- ✓ El uso de aplicaciones no autorizadas en las redes empresariales, constituye uno de los riesgos para la información empresarial confidencial e información personal del empleado, en el caso del correo electrónico personal esta aplicación no es autorizada pero es la que más utilizan, también los pagos en línea, compras en línea, entre muchas otras actividades de carácter personal que se están realizando dentro de la empresa y que conlleva a ser uno de los riesgos más importantes para la perdida de información por parte de los empleados y de robo de datos por parte de piratas informáticos debido a que con frecuencia no son supervisadas y no se adhieren a las normas de seguridad de la empresa, llevando a la empresa al riesgo de contagio de sitios maliciosos.

- ✓ Muchos empleados usan indebidamente los computadores de las empresas en contra de las políticas de seguridad de TI, en algunos casos se puede alterar las configuraciones de seguridad y compartir dispositivos laborales e información confidencial con personas ajenas a la empresa, estas conductas pueden facilitar que información personal de la empresa llegue a manos de personas que constituyan una grave amenaza para la rentabilidad de la empresa.

- ✓ Muchos empleados permiten que personas ajenas a la empresa ingresen a las dependencias o deambulen libremente por las instalaciones sin ninguna supervisión, hasta los empleados acceden a zonas no autorizadas de la red o a las instalaciones

empresariales, estas acciones pueden facilitar que el personal no autorizado roben recursos de la empresa o accedan a información confidencial.

- ✓ Los empleados móviles son un riesgo potencial en la perdida de información, puesto que el transferir archivos de un dispositivo a otro que no esté protegida con las normas del departamento de TI, el usar medios de comunicación personales que no tenga una seguridad adecuada, el hablar de temas confidenciales en lugares públicos y el no proteger debidamente los dispositivos de almacenamiento y los equipos portátiles que pueden perderse o ser robados, facilitan el robo de información.

- ✓ Uno de los métodos más antiguos de seguridad es usar contraseñas, cerrar sesión, bloquear el equipo al retirarse del puesto de trabajo el no almacenar datos de inicio de sesión y contraseñas en su computadora son pasos básicos de seguridad informática, pero aún hay empleados que los pasan por alto.

(Vásquez Cruz, 2016) Hoy en día los ataques cibernéticos son técnicamente más complejos y usan regularmente la información que puede conseguirse en redes sociales para ser más creíbles, sin embargo las acciones realizadas por las amenazas son las mismas desde hace tiempo, ya que se sigue utilizando el hacking, el malware y los ataques de ingeniería social, los cuales, por cierto, continúan creciendo a más velocidad que el resto. Quizá lo más sorprendente respecto al robo de datos es que el 40% de los hurtos sigue realizándose mediante medios físicos, es decir que se utilizan computadoras portátiles y unidades USB. Además, los tres principales métodos utilizados para filtrar datos son los protocolos web, las transferencias de archivos y el correo electrónico.

Razones para alterar la configuración de seguridad

Grafico tomado de: fuga de datos a nivel mundial riesgos y errores comunes de los empleados

Reglas de prevención

La norma técnica que rige en Colombia para la seguridad de la información es la NTC-ISO/IEC27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

La piratería informática se está convirtiendo en una actividad delictiva, la colaboración de las personas tanto internas como externas hace que esta actividad con fines lucrativos tome más fuerza y riesgo para la imagen corporativa. Por esto es bueno implementar algunas prácticas con el fin de proteger la información en las organizaciones, como es:

- ✓ Lo ideal es que las empresas cuenten con una política de seguridad, con el objetivo que todos los empleados tengan el conocimiento de cuán importante es la protección de la información para la empresa, la política debe ser entregado y explicado al empleado al momento del ingreso a la compañía, de igual forma se debe solicitar un compromiso para el cumplimiento de la política de seguridad.
- ✓ Realizar un buen uso de las herramientas instaladas en los equipos, como es mantenerse atento a las alertas de sus soluciones como lo es antivirus, firewall y antispam.
- ✓ No ignorar los códigos maliciosos como el malware, software malicioso, los cuales son uno de los ataques más comunes de la actualidad. Aunque este tipo de incidentes no pareciera impactar en el trabajo cotidiano, puede representar un riesgo de pérdida de información, de tiempo y también de dinero.
- ✓ Los desarrolladores de códigos maliciosos y atacantes informáticos suelen utilizar distintos medios para engañar y así comprometer la seguridad de la empresa, entre los más comunes está el fraude vía correo electrónico, la utilización de falsas noticias sobre temas relevantes con el fin de despertar la curiosidad y lograr que descarguen alguna aplicación maliciosa.
- ✓ Al momento de transportar o almacenar la información se debe tener precaución, porque un incidente de fuga de información puede ser generado por un mal accionar de las personas.

- ✓ Se recomienda no compartir el dispositivo móvil de la empresa, debe contar con una contraseña de acceso, descargar aplicaciones solo desde sitios de confianza, cifrar la unidad de almacenamiento de los dispositivos con el fin de evitar accesos no autorizados a la información.
- ✓ Es importante no utilizar las mismas contraseñas en los servicios laborales y personales, para que una contraseña sea fuerte debe ser fácil de recordar y difícil de descifrar.
- ✓ Evitar correos electrónicos que no provengan de un remitente de confianza, esto con el fin de minimizar la posibilidad de infectarse con códigos maliciosos y ser víctimas de robo de información personal, financiera a través de la falsificación de un ente se confianza.
- ✓ Hay que cuidar la información de la empresa cuando se traslada la documentación de importancia para trabajar fuera de la empresa, además los documentos deben ser manipulados teniendo en cuenta el nivel de confidencialidad que requieren.
- ✓ Utilizar conexiones seguras, no acceder a archivos con información confidencial en equipos públicos, no realizar conexiones sensibles como accesos al correo corporativo, esto con el fin de aumentar la seguridad en la transmisión de los datos.

Para enfrentar los problemas derivados del aspecto técnico aparecieron mecanismos, conocidos con distintas siglas, entre las que se encuentran: Data Loss Prevention (DLP), Data Leak Prevention (también DLP), Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) y Information Protection and Control (IPC). Todos estos mecanismos tienen como objetivo el monitoreo y control de los datos digitales que circulan en una infraestructura tecnológica, ya sea por medio de filtrado de contenidos web, por aplicación de políticas en el uso de determinados datos

previamente identificados como sensibles, o por el bloqueo de la conexión de dispositivos no marcados como confiables. (Pacheco, 2011)

Controles

Con el fin de reducir el riesgo en el robo de información, las compañías tienen la obligación de pasar auditorias cada cierto tiempo, podemos mencionar la:

La **LOPD** (Ley Orgánica de Protección de datos) se ocupa de velar por el derecho a la privacidad de las personas. Todas las empresas que manejen archivos (texto u ordenador) con datos personales tienen obligación de declarar estos archivos ante la AEPD (la Agencia de Protección de Datos) y de proteger dicha información. Como ejemplo de estos ficheros estaría el fichero de nóminas de la empresa y los historiales médicos de un hospital.

La PCI-DSS se encarga de garantizar la seguridad de las operaciones realizadas con tarjetas de crédito. Esta auditoría trata de garantizar que todo punto por donde pasen tarjetas de crédito es seguro: seguridad física, cifrado de las comunicaciones, segmentación de la red, logs centralizados, gestión de usuarios y paswords, formación de empleados, existencia de WAPs, gestión de eventos de seguridad, detectores de intrusos, antivirus, etc.

Conclusión

Se puede concluir que el robo de información por parte de informantes corporativos representa una amenaza real con consecuencias a largo plazo para las compañías dañando la imagen corporativa, esto causa la interrupción de las operaciones y un daño profundo a la reputación de la compañía. Se deben tomar las medidas preventivas con el fin considerar los distintos motivos para que estas sean verdaderamente eficaces.

En algunos casos el robo de información se debe a que las personas estén motivadas por varios factores, incluidas la conciencia social o el deseo de obtener un beneficio personal. Las empresas deben estar convencidas que sus integrantes están comprometidos a erradicar cualquier comportamiento poco ético, y también que sus acciones serán reconocidas públicamente. Una vez que haya ganado la confianza de los posibles informantes, ellos se sentirán apoyados y seguros de poder levantar sus denuncias dentro de la organización, y usted evitará la publicidad negativa que acompaña a las fugas de información.

Por otro lado la prevención de pérdida de información, ataques, penetración y detección de software malicioso comprenden la localización, el entendimiento, la clasificación y protección de información confidencial.

Algo que se debe tener claro es capacitar a los colaboradores sobre las prácticas líderes de seguridad cibernética aumentará el grado de consciencia sobre seguridad y les brindará herramientas para combatir la ingeniería social. Por otro lado, contar con un programa de respuesta de incidentes robusto le permite a las empresas tener una reacción rápida y correctamente cuando eventos o individuos no previstos amenacen sus operaciones comerciales.

También el conocimiento de la vinculación entre los empleados y sus accesos puede evitar en gran medida la fuga de información, ya que en caso de filtrarse hacia el exterior, se podría señalar de manera directa a todos aquellos que tuvieron acceso y se podría analizar su uso previo al incidente, obteniendo posibles conclusiones y responsables. De cualquier manera, dada la imposibilidad de monitorear a las personas más allá de la esfera laboral, es estrictamente necesario que exista un alto grado de concientización y que las políticas de seguridad estén correctamente aplicadas para garantizar que quienes manejen información confidencial tengan asumidos los riesgos relacionados con su filtración.

Bibliografía

10 años de fuga de información: conoce los incidentes para no repetir la historia; Gutiérrez Amaya, Camilo; https://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

Archivo portafolio. Co; 25 de Junio de 2012; http://www.portafolio.co/mis-finanzas/ahorro/prevenir-evitar-fuga-informacion-empresarial-100890

Fuga de información en la empresa; http://blog.jmacoe.com/gestion_ti/fugas-de-informacion-en-la-empresa/

CISCO; http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf

BBITS Tecnología y opinión; https://borrowbits.com/2013/11/el-problema-de-las-fugas-de-informacion-tus-empleados-te-roban-datos/

Revista Vínculos; ciencia tecnología y sociedad: un enlace hacia el futuro; http://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/10518/11605

Admin in seguridad informática; Servicios, 2016

Fuga de información, la mayor amenaza para la reputación corporativa; Arantxa Calvo Moyano, directora de marketing de secura it; http://www.redseguridad.com/especialidades-tic/dlp-y-fraude/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa.

¿Qué es la fuga de informacion?; Bortnik, Sebastian, 2010; https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Guia gestión de fuga de informacion; Inteco; https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf