Filtración de Información

Karol Abarca Cortés

Universidad Latinoamericana de Ciencia y Tecnología

Licenciatura en Ingeniería Informática con énfasis en Desarrollo de Software

¿Cuáles son los factores que interfieren en la filtración de la información en las organizaciones?

Resumen

Como menciona Francis Bacon “la información es poder” y esta es la base para uno de los problemas más complejos que se presentan en todo tipo de organización, la filtración de información, afrontar esta eventualidad o dejarla pasar puede sin duda cambiar todo el paradigma al que está sometida la empresa, ocasionar pérdidas monetarias e incluso problemas legales.

En la actualidad los problemas de fuga de datos dentro de las compañías se han convertido en uno de los daños más frecuentes a los que están expuestas en la actualidad. Por lo tanto es necesaria una investigación que aporte a los gerentes y personas de todas las áreas laborales el contexto suficiente para comprender cuáles son las principales causas de este problema, esto, tomando en cuenta los diferentes puestos dentro de la compañía, los niveles de escolaridad de sus empleados y otros factores que influyan en la situación.

Para el análisis de este problema, se plantea un estudio a 70 personas de distintos segmentos dentro de la jerarquía de diferentes organizaciones, este estudio de empleados se realiza mediante el uso de un cuestionario en el cual se desarrollan preguntas sencillas de responder que nos brindan una muestra general del comportamiento institucional, parcializando los resultados y evaluado las vulnerabilidades latentes.

El análisis de los resultados obtenidos ofrece posibles soluciones para aumentar los estándares de seguridad y la forma indicada en que se deben de desarrollar las prácticas empresariales dirigiéndose tanto a las características del personal como al equipo gerencial y de la empresa en general.

Palabras Clave

Filtración de información / Seguridad de la información / Riesgos / Confidencialidad / Ingeniería Social

Abstract

As mentioned Francis Bacon "information is power" and this is the basis for one of the most complex problems in all types of organization, information filtering, face this eventuality or pass it definitely can change the whole paradigm that this subject the company lost money and even cause legal problems.

At present the data leakage problems within companies have become one of the damages to which they are subjected more frequently. Therefore research is needed to provide managers and people of all work areas sufficient context to understand what are the main causes of this problem, that, taking into account the different positions within the company, education levels of employees and other factors affecting the situation.

To analyze this problem, we propose a study on 50 people from different segments within the hierarchy of different organizations, this study of employees is done by using a questionnaire which was developed to answer simple questions that give us a general sample of institutional behavior, biasing the results and evaluated the latent vulnerabilities.

The analysis of the results offers possible solutions to increase safety standards and the way in which they indicated must develop business practices addressing both the personal characteristics of the management team and the company in general.

Key Works

Information leakage / Information Security / Risk /

Privacy / Social Engineering

Introducción

Problema:

Actualmente la mayoría de las empresas e instituciones cuentan con la existencia de procesos que maximicen los niveles de seguridad, esto debido a que la información como es conocido se convierte en la fuente esencial de la productividad y eficacia de la industria, por lo tanto es necesario resguardarla, esto a la vez se convierte en una tarea complicada incluso con la existencia de políticas de privacidad.

La filtración de información organizacional no es propiamente una actividad que se lleve a cabo intencionalmente en todos los casos, la competencia o incluso atacantes sin un fin especifico se fundamentan en el uso de la ingeniería social para extraer datos de forma encubierta, demostrando la falta de ética de estas personas y evidenciando las vulnerabilidades latentes dentro de la institución tanto en materia técnica como humana.

Los agujeros en la seguridad propiciados por sus empleados suponen en algunos casos los bajos rangos educacionales de estos así como la falta de capacitación en el área, este ultimo aspecto la base desde la cual se ejecutan las fugas de información gracias al personal.

El hecho de que las empresas no tomen en cuenta como una prioridad para el negocio la capacitación de personas que no trabajan directamente en el área como secretarias e incluso personal de limpieza acrecienta la facilidad de terceros para obtener información, aunque no del todo funcional, si eficiente para dañar a la institución.

Todos estos problemas en muchos casos corresponden a una contradicción de la organización la cual es necesario analizarla, ya que por un lado se pretende que las personas resguarden la información pero no se invierte presupuesto en su formación.

Por otro lado, tampoco podemos omitir la otra cara de la moneda, es decir, la filtración de manera intencionada dada por empleados directos, la facilidad de acceder a la información posiciona en un juego de beneficios particulares al personal lo cual conlleva a ofrecer esta información a otros a cambio de dinero u otros incentivos .

Objetivo General:

Identificar y explicar las características que intervienen en la filtración de información.

Objetivos Específicos:

Definir las principales fuentes de fuga de información.

Analizar las razones para la filtración de la información.

Definir las fallas de seguridad dentro de las instituciones

Definir las consecuencias de filtraciones de datos.

Analizar el modelo de ingeniería social y maneras de disminuir ataques

Justificación:

Es importante comprender en función de las labores realizadas quienes son los empleados que ponen a disposición de otros la información laboral y las razones por las

cuales se da una mayor cantidad de este tipo de filtraciones, como las mejores maneras de evitarlas.

Con certeza no solo los empleados tienen que comprometerse a proteger la información sino que a la vez se debe de trabajar en conjunto con la empresa, propiciando las instrucciones correctas, control adecuado de la información confidencial y someter al personal a buenas prácticas laborales además de un adecuado análisis de riesgos, así como a un estudio de las actitudes laborales.

Revisión Bibliográfica

Filtración de Información

La filtración de información es uno de los principales problemas que enfrentan las empresas hoy en día, principalmente porque estas organizaciones se basan ante todo en los niveles de confianza a sus empleados y no hay una forma clara y cien por ciento efectiva de evitar la filtración de contenidos empresariales. Por lo tanto el recurrir a diseñar planes de acción que logren contener estas acciones en la medida de lo posible.

El definir el concepto centralizado de la filtración de información es relevante para comprender el problema principal de esta investigación y a partir de aquí desarrollar conjeturas que resguarden los datos empresariales. En un contexto globalizado y general la filtración "se produce cuando la información confidencial de una parte se libera" (Wikipedia 2012)

Ingeniería Social

La ingeniería social la podemos definir como "la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos." Debido a que los mismos son " son el eslabón débil" para una empresa (Wikipedia, 2012).

En general este tipo de herramienta social para adquirir distintos datos de interés y que puedan ser utilizados para fines de diferente índole, son técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros. (HackStory, 2012)

Privacidad y Confidencialidad

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, diferenciándose de lo público y de lo secreto". (Eset, 2012)

En general tanto la privacidad como la confidencialidad se rigen bajo un código en el cual existe información que debe ser accedida únicamente por personas autorizadas, delegando a determinados responsables el manejo de esta.

Contratos de Confidencialidad

Los contratos empresariales de confidencialidad no solo son una manera de demostrar la importancia de los mismos sino que a la vez son la mejor manera de crear estándares de seguridad dentro de la institución. Un estudio sobre la manera en la que trabajan estos acuerdos dentro de las empresas.

En la actualidad se vuelve indispensable que toda compañía cuente mecanismos jurídicos pertinentes, que permitan dentro del marco de la ley, defender los intereses en caso de que alguno de sus empleados comparta información con personas interesadas en dañar el negocio. (Ideas para PYMES, 2011).

Es así como es importante que todos los empleados tengan conciencia de su existencia dentro de las empresas que laboran al tiempo de que deben de conocer la existencia de leyes vigentes en cada país que reconocen consecuencias contra quienes las transgredan.

Formularios (Google Drive)

Google Drive "es un programa gratuito basado en Web para crear documentos en línea con la posibilidad de colaborar en grupo" (Wikipedia, 2012). Dicha herramienta posee dentro de sus opciones nos ofrece la creación de formularios, los cuales pueden ser aplicados como cuestionarios brindando la posibilidad de agilizar y mejorar los procesos de recolección y almacenamiento de datos para su futuro procesamiento, controlando las respuestas mediante el uso de una hoja de calculo nativa. (Soporte Google, 2012)

Administración de recursos

La administración de recursos consiste en el manejo eficiente de estos medios, que pueden ser tanto tangibles como intangibles. El objetivo de la administración de recursos es que estos permitan la satisfacción de los intereses. Asignar correctamente las funciones a cada uno de los recursos aumenta los niveles de eficacia empresarial, aumentando a la vez su rendimiento (Definicion.de, 2012)

Normativas

Las normativas "se refieren al establecimiento de reglas o leyes, dentro de cualquier grupo u organización", dichas reglas deben incluir modelos, métodos, estándares, y fusionarse dentro de una metodología que deba ser seguirá por todos los empleados, ya que dichas normas trabajan dictadas por la Administración Publica bajo las leyes correspondientes. (Wikipedia, 2012)

Administración de Riesgos

Un riesgo de un proyecto es un evento o condición incierto que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad, es decir, cuando el objetivo de tiempo de un proyecto es cumplir con el cronograma acordado; cuando el objetivo de coste del proyecto es cumplir con el coste acordado. Por tanto, la gestión de los riesgos es un proceso iterativo y recurrente a lo largo de toda la vida del proyecto. El propósito es minimizar la probabilidad y consecuencias de los riesgos negativos (o amenazas) y maximizar la probabilidad y consecuencias de los riesgos positivos (u oportunidades) identificados para el proyecto de tal forma que los objetivos de los proyectos se cumplan. (PMBOK, 2004)

Metodología

Para la recopilación de los datos referentes a la investigación se censaron distintas personas con cualquier tipo de relación laboral con el departamento de tecnologías de información, dichas personas son de distintas empresas tanto públicas como privadas y con distintos niveles educacionales, es decir, el diferente nivel académico obtenido en cada caso. El hecho de trabajar con distintos estratos sociales nos permite aumentar el rango de razones posibles además de definir claramente los aspectos específicos más relevantes de las fallas en la seguridad.

El análisis continuo de datos recopilados para esta investigación no solo debe proceder de profesionales en informática sino de todas las esferas sociales dentro de la empresa, abarcar toda la jerarquía institucional es necesario debido a que se tiene que realizar un estudio detallado para demostrar desde que puestos laborales se incurre más en la filtración de información a terceros, así como a la vez es importante saber en que puestos se desempeñan y que otros factores externos conllevan a que se dé el trafico de información.

El encuestamiento a estas personas se aplicó tanto con el uso de una herramienta web como con el uso de cuestionarios impresos para quienes no tengan acceso regularmente a una cuenta de correo electrónico, recordando que también fue importante censar a empleados de limpieza que tenían acceso al personal y al área de trabajo de tecnologías de información y quienes no poseían acceso a una cuenta de correo electrónico desde la cuál fuera posible contestar el cuestionario.

De esta manera se coordinó no solo con gerencia, jefaturas y profesionales especializados sino a la vez con personal de bajo perfil. La versión digital así como la versión impresa cuentan con las mismas preguntas ya que se debe de rescatar que es de suma importancia la estandarización de los resultados obtenidos sin importar a quien se le aplique.

La aplicación de las encuestas se realizó como se mencionó anteriormente mediante la distribución de un correo electrónico o de la versión física, las personas sometidas a esta encuesta son en un sentido general son quienes brinden plena conciencia de estar incorporados al mercado laboral y posean cualquier tipo de relación con personal o departamento en sí, de tecnologías de información tanto desarrollo de sistemas como soporte técnico y demás áreas yuxtapuestas en la empresa.

Con base en las respuestas brindadas por los empleados a esta encuesta se evalúa cuantitativamente de acuerdo a la información obtenida, las características más representativas las cuales se valuaran como amenazas, vulnerabilidades y factores cualitativos para todo tipo de organización, esto hace factible el llevar a cabo un análisis que permita el desarrollo de hipótesis en las cuales se registren las maneras indicadas de crear planes de contingencia que prevengan el desenvolvimiento de estas eventualidades.

Al desarrollar un estudio sobre los datos obtenidos, se realiza un plan de riesgos, globalizando los problemas y permitiendo entender a los encargados dentro de las empresas la necesidad de elaborar este mismo plan dentro de sus propias instituciones.

Para el desarrollo general de los cuestionarios se hizo un diseño especifico apegándose a las recomendaciones brindadas por distintas fuentes bibliográficas estudiadas, de esta forma se consigue producir una herramienta que conserve el interés de los censados

brindando las opciones de respuesta en preguntas cerradas y parcializando los resultados a réplicas de fácil tabulación para posterior estudio y especificación.

El cuestionario cuenta con 16 preguntas de las cuales 13 son preguntas cerradas y las 3 restantes abiertas para poder obtener los pensamientos críticos e individualizados, posteriormente se trabajó en una serie de claves que nos permita brindar distintas perspectivas de comparación de los datos permitiendo graficar para facilitar la observación, se muestran los ejemplos más relevantes y adicionalmente se brindan por completo comentarios objetivos de la realidad nacional en el aspecto investigado

Resultados

Las personas evaluadas mostraron una claro desconocimiento del tema, mostrando las falta de información sobre el mismo, aunque es un tópico sencillo de comprender, la educación y/o normativas que se le otorgan a los empleados es muy baja y en la mayoría de los casos nula, es decir, el personal conoce acerca del tema gracias a elementos externos a la institución en la que laboran ya que en las mismas, aunque en el mejor de los casos, se les impongan protocolos para el resguardo de los datos, normalmente no se le da importancia a la capacitación de los empleados en estas áreas, o a metodologías sistemáticas que les demuestren las formas más recurrentes en las que cualquier clase de datos a los que tenga acceso puedan ser obtenidos por otros.

De los casos analizados cabe recabar que impresionantemente más de la mitad de la población encuestada asegura nunca haber recibido ningún tipo de asesoramiento sobre las maneras en los que terceros pueden acceder a información y así de esta manera poder desarrollar mecanismos que eviten estas fugas. Por otro lado, las personas que tienen conocimiento en el tema, aseveran que ha sido gracias a su educación universitaria o propia investigación, difícilmente dichas capacitaciones han sido proporcionadas directamente por sus empleadores.

Los protocolos sobre seguridad de la información están bien definidos en la mayoría de organizaciones pero la manera de cumplir con ellos se deja de lado como una labor a sus empleados, desestimando la necesidad de capacitación y enfocándose únicamente a desarrollar políticas globales de seguridad a nivel tecnológico.

De acuerdo con los datos obtenidos a partir de la experiencia de los encuestados en sus ámbito laboral, los empleados con funciones de secretariado e incluso limpieza poseen mucha información la cual puede ser fácilmente obtenida por personas con intensiones desleales como la competencia o empresas con que se podrían obtener ventaja de una u otra manera con la recopilación y/o divulgación de estos datos.

En el caso de este tipo de personal, que no tiene tareas especializadas propias del departamento no cuentan con un acceso directo a datos técnicos pero sin embargo poseen la capacidad, para calificarlo e alguna manera, de conocer al ambiente laboral a nivel personal, es decir, poseen conocimiento sobre las fallas habituales, el descontento del equipo con sus empleados y clientes, las fechas de entrega, reuniones por mencionar algunos de los ejemplos que ellos mismos nos contaron.

Toda información aunque no es la meta ideal de un hacker es sin un duda un gran beneficio para quien sea que quiera ocasionar un daño a la empresa, además por la naturaleza de dichos datos es más sencillo brindársela a terceros sin tener conciencia de lo que esto pueda ocasionar, dejando ir la información a la libre por simples errores.

Propiamente mediante el uso de la ingeniería social es que los interesados logran conseguir datos desde las fuentes principales, enfocándose al personal y dejando totalmente de lago el recurrir a procesos de ataque tecnológico.

El mundo de la información esta en jaque con el aumento de la globalización y el constante desarrollo por lo tanto las principales estrategias para obtener información confidencial o incluso información inter e intrapersonal de las áreas de trabajo se fundamental en la ingeniería social como se menciono en le punto anterior, así que aunque

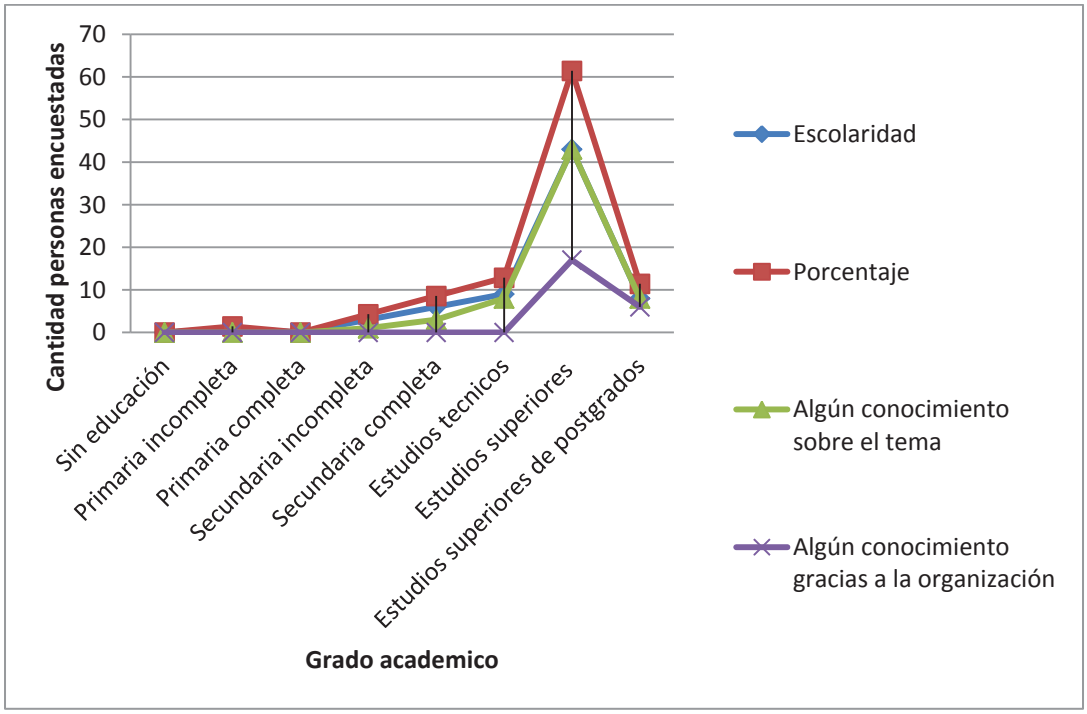
necesaria, la seguridad de las redes y equipos, dejar a la deriva el tema fundamental de culturización es un sesgo grave.

Por un lado es cada vez más común poder infiltrarse en los estándares técnicos de seguridad que se hayan definido, razón por la cual existen más y más herramientas para proteger los sistemas de información, esto mismo es lo que hace menos atractivo el panorama y conlleva por otro lado al aumento del enfoque direccional a los empleados, los cuales en charlas "inocentes" pueden dejar ir datos completamente relevantes.

Aunque no es posible determinar todas las formas en las cuales terceros pueden obtener información es importante enfatizar aspectos generales de relaciones humanas en las que se deje a descubierto las formas en las que se extrae la información para guiar las acciones a seguir, ya que como hemos visto es en este punto en el que se ahonda más profundo desde la visión externa.

Nos podemos referir a los niveles de escolaridad de las personas encuestadas en torno al conocimiento que poseen o que han logrado adquirir por distintas razones, ya sea mediante experimentación personal o gracias a la empresa para la cuál laboran en base al grafico correspondiente a la Tabla 1.

Tabla 1. Escolaridad vrs Conocimiento sobre el Tema



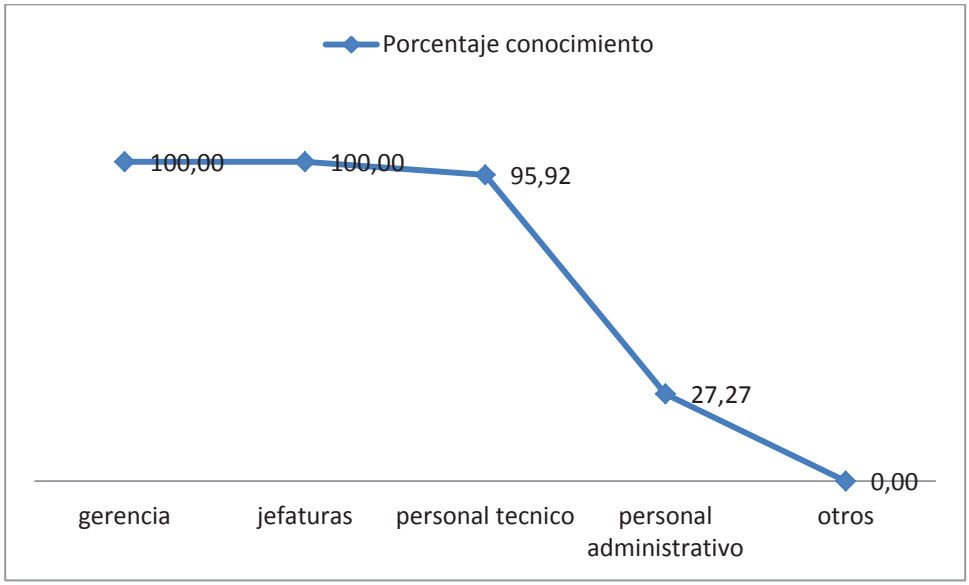
El grafico de la Tabla 1 no solo evidencia que entre más alto es el grado de escolaridad mayor la accesibilidad a información vital para una buena administración de los datos institucionales, sino que además demuestra que en para poder involucrarse en una empresa, los requisitos de ingreso incluso para puestos de bajo perfil son mucho mayores a los conocimientos que se necesitan para laborar.

Asimismo, es clara la tendencia de las empresas a no brindar ninguna clase de capacitación que permita a sus empleados familiarizarse con las fugas de información comprometiendo la integridad del área de trabajo.

Entre mayor sea el rango de la persona dentro de la jerarquía institucional, mayor es el conocimiento que se maneja sobre el tema en parte por la educación que ha recibido como las facilidades de capacitación que se les ofrece, dejando totalmente aislados a este conocimiento a personas que no hayan obtenido títulos universitarios y que se encuentren en los puestos inferiores de la jerarquía.

En el grafico posterior podemos ver como se evidencia lo anteriormente mencionado.

Tabla 2. Conocimiento del Tema de acuerdo a su Puesto Laboral



Los agujeros que se producen pueden ser prevenidos de distintas maneras basándonos en el espacio laboral y todos los aspectos anteriormente descritos, aunque pueda representar altos costos capacitar a todos, una buena alternativa es controlar más organizadamente y diseñar políticas donde sea estrictamente educando al personal de

primer grado para evitar que cualquier otro empleado tenga conocimiento alguno sobre los procesos, de esta manera, la inversión se reduciría.

Entre las personas de menor posición laboral que tienen mayor acceso a datos, el índice demuestra que es más normal que laboren para organizaciones publicas pero a la vez es consecuente que tanto en privadas como publicas se dan fallos en la seguridad, sin dejar que al igual es en ambas que se dan la misma cantidad de ataques, esto a causa de que en las empresas privadas se manera información relevante para la competencia pero en las instituciones públicas se espera lograr obtener información que pueda afectar al estado ya que sus acciones repercuten en la ciudadanía.

En cuanto al área técnica los ataques están estandarizados, las empresas cuentan tanto con medidas de prevención como con medidas de detección a intrusiones en sus sistemas, por lo tanto en la mayoría de situaciones es más difícil obtener información por estos medios.

En cuanto a los contenidos y accesos con los que cuentan los usuarios, en el 80% de las empresas se demuestra que están bien estandarizados, controlando los permisos de cada empleado en cuanto a acceso a paginas web, uso de dispositivos externos y permisos específicos para distinta información, sin embargo esto no cubre el área en la que cada persona puede hacer uso efectivo de redes sociales, paginas web propietarias, o blogs personales para publicar el contenido que deseen desde fotos hasta información que aunque no se rija siempre por normativas de confidencialidad, aún así conforman un conglomerado de datos que pueden afectar la imagen de la empresa o que puedan ocasionar daños corporativos, lo cual nos devuelve al punto trascendental que es la parte humana.

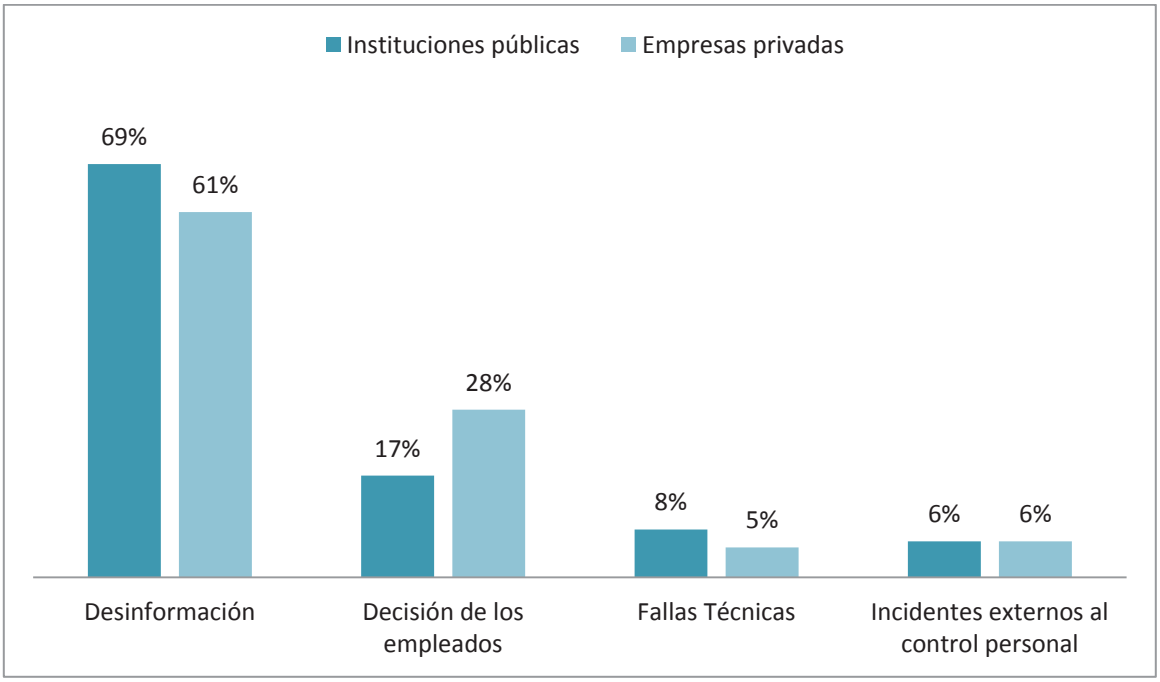
Al provocarse fugas en las cuales no existía la intensión directa de filtrar información, estos datos pueden llegar a fuentes potencialmente dañinas por simples actos como el acceso a las cada vez más frecuentes aplicaciones y herramientas para transferencia de archivos y compartición de datos, los cuales poseen políticas de eliminación de archivos dudosas y dejan abierta la brecha a interesados en obtener distinta información de personas gracias a las reglas implícitas a las cuales los usuarios acceden al afiliarse.

Para este tipo de filtraciones es importante informar de su existencia a todo el personal.

Cuando estos incidentes son provocados, es decir, que se dan conscientemente ya sea porque los empleados hayan decido brindar la información, o porque el ataque se haya dado directamente para conseguir los datos son la parte riesgosa y a la cual se le debe de hacer frente mediante planes de análisis de riesgos así como de medidas de contingencia ante altercados de esa índole.

En resumen gracias a la investigación desarrollada podemos intuir que las principales causas que ocasionan que la información de nuestros procesos empresariales tanto en instituciones públicas como privadas, llegue a otros son las que se exponen en la tabla 3.

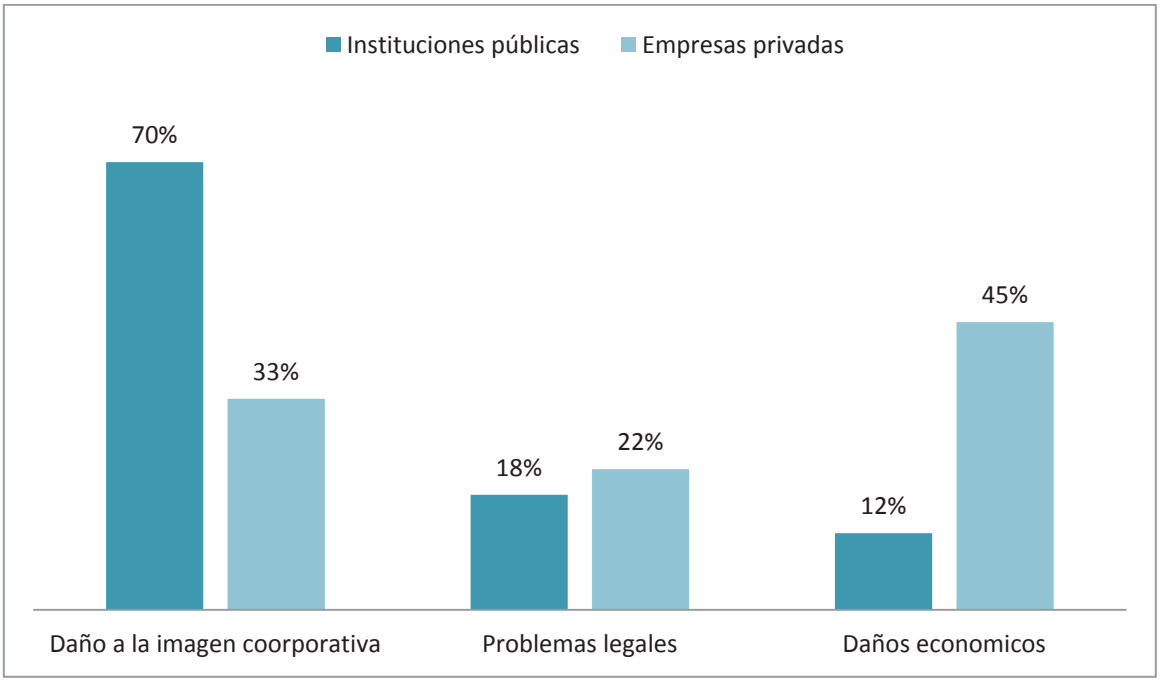
Tabla 3. Causas de las filtraciones



Y las consecuencias de mayor impacto las vemos divididas como se muestra en el grafico correspondiente a la Tabla 4, lo cuál destaca que mientras en las empresas privadas sus mayores perdidas son monetarias, este tipo de problema no afecta en gran medida a las instituciones del estado, ya que cuentan con presupuestos definidos y generalmente que se filtren datos no genera pérdidas en la rentabilidad, por otro lado vemos que los problemas de índole jurídico se encuentras a rangos semejantes en ambos con un nivel bajo promediado, dejándolos como la opción que se presenta con menos frecuencia.

Sin embargo, el gran margen de diferencia que vemos entre la perdida de credibilidad de los clientes en una organización gubernamental u autónoma del estado es mucho mayor a la que debe de afrontar por este mismo motivo una empresa privada.

Tabla 4. Consecuencias de las filtraciones



La ingeniería social expone la manipulación de las personas para obtener datos y esta misma la que conlleva de distintas maneras a que se desenvuelvan las consecuencias analizadas, es decir, por medios como conversaciones, correos electrónicos u otras formas de obtener mediante el uso de la confianza obtenida, ciertos privilegios, por esta razón es fundamental definir modelos de trabajo.

Conclusiones y Recomendaciones

La información es sin duda el activo más importante de cualquier empresa, por lo tanto para las miembros superiores en la jerarquía institucional debe ser prioridad y de vital importancia dedicarle atención a este aspecto, y conocer el valor de cada uno de los datos que se manejen internamente y a partir de esta clasificación tomar conciencia y difundir medidas que solapen cualquier actividad perjudicial.

La falta de educación, refiriéndonos al grado de escolaridad de las personas, acentúa los problemas de filtración, demostrando que entre menos sea este nivel, las personas son más propensas a liberar información sin cautela, por lo tanto es necesario capacitar a todo el personal dentro de una institución y no solo a los empleados que intervengan en primer grado con el desarrollo de los proyectos.

Como alternativa a este alto gasto operacional se pueden crear políticas institucionales donde se trate de manera totalmente cerrada todo lo relacionado a procesos de cada proyecto, así cualquier persona que no este involucrada en primer plano no tendría acceso a ningún dato que pudiera ser ventajoso para un ente externo a dicho proyecto, además esto conllevaría a que las necesidades de capacitación se redujeran únicamente al personal directo.

Es de suma importancia definir protocolos, normativas y buenas prácticas de trabajo, así como mantener informados y capacitados a los empleados ya que como se sabe los hacker hacen énfasis principal en el ataque a los empleados y no así al área técnica como se esperaría, es decir, el control del recurso humano es esencial para cubrir los

espacios más importantes y minimizar las fugas, claramente sin dejar de lado que la seguridad de los sistema es también una prioridad en general.

La filtración de información es uno de los elementos más complejos de seguridad, esto debido a todos los factores que intervienen, así como todos los causantes y las diferentes consecuencias que producen, por lo tanto es importante considerar los aportes que se le den a esta área como una necesidad primordial para toda institución enfocando presupuesto a la misma y generando las medidas preventivas necesarias.

Cada empresa debe de realizar un análisis detallado de la información que manejan sus empleados, especialmente porque un departamento como lo es tecnologías de información, maneja toda la información de los procesos de su empresa así como de las empresas de sus clientes en caso de que brinden servicios profesionales a otras instituciones.

El hecho de que exista un porcentaje importante de fugas de información debido a empleados descontentos o simplemente empleados que hayan tomado la decisión de brindar información confidencial del negocio, no solo se debe de tomar como una posibilidad sino que es necesario definir buenas practicas de contratación, evaluando seriamente al profesional que intente incorporarse.

Un análisis de los riesgos permite evitar que las consecuencias de un incidente de fuga de información pueda incluso causar un importante daño de imagen o mermar la confianza de los clientes de la entidad, lo que puede llegar a afectar el negocio y ocasionar demás problemas éticos, legales y financieros. Al estimar el impacto que tendría cada riesgo que se llegue a materializar es más sencillo desarrollar un plan para gestionar estos procesos.

Desarrollar el plan de contingencia, por su parte, es la principal manera de tener un respaldo para actuar en caso de alguna incidencia y evitar que se sumen un mayor numero de problemas consecuentes.

Finalmente es necesario establecer mecanismos jurídicos que velen por que después de que los empleados estén capacitados y establecidas todas las políticas necesarias, estas sean cumplidas y existan sanciones para quienes las infrinjan.

Bibliografía

Ideas para PYMES (Agosto, 2012). Proteja su negocio con los 7 contratos básicos para su PYME. Obtenido el 18 de octubre del 2012 desde http://investigacion.uct.cl/v4/form_inv/convenio_conf.pdf

Microsoft PYMES y autónomos (07 de julio, 2011). Los acuerdos o pactos de confidencialidad. Obtenido el 17 de octubre del 2012 desde http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=313

Sistema Costarricense de Información Jurídica (21 de noviembre, 2008). Ley de Información no Divulgada. Obtenido el 18 de octubre del 2012 desde http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=41810&nValor3=74709&strTipM=TC

Wikipedia (04 de agosto, 2012). Filtración. Obtenido el 17 de octubre del 2012 desde http://es.wikipedia.org/wiki/Filtraci%C3%B3n_(Internet)

Wikipedia (21 de septiembre, 2012). Fuga de Información. Obtenido el 17 de octubre del 2012 desde http://es.wikipedia.org/wiki/Fuga_de_informaci%C3%B3n

Scribd (15 de noviembre, 2010). Filtración de Información. Obtenido el 15 de octubre del 2012 desde http://es.scribd.com/doc/97777059/Guia-Gestion-Fuga-Informacion

Hack Story (21 de septiembre, 2012). Ingeniería Social. Obtenido el 17 de octubre del 2012 desde http://hackstory.net/Ingenier%C3%ADa_social

Definición (21 de septiembre, 2012). Administración de Recursos. Obtenido el 17 de octubre del 2012 desde http://definicion.de/administracion-de-recursos/

Wikipedia (21 de septiembre, 2012). Normativa. Obtenido el 17 de octubre del 2012 desde http://es.wikipedia.org/wiki/Normativa

PMBOK Guide(21 de septiembre, 2012). A Guide To The Project Management Body Of Knowledge. Obtenido el 17 de octubre del 2012 desde http://www.pmi.org/en/PMBOK-Guide-and-Standards/Standards-Library-of-PMI-Global-Standards.aspx

Google (21 de septiembre, 2012). Formularios Google Drive. Obtenido el 17 de octubre del 2012 desde http://support.google.com/drive/?hl=es

Eset (21 de septiembre, 2012). Privacidad y Confidencialidad, Fuga de Información. Obtenido el 17 de octubre del 2012 desde http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf

Anexos

A nombre del GRUPO IDEA, cédula jurídica 3-102-10976714, hace constar que se realizó la revisión del presente trabajo, se analizó la construcción de párrafos, vicios del lenguaje, ortografía, puntuación y otros relacionados a la Corrección de Estilo, sin alterar la intencionalidad del autor y el enfoque del tema. Por lo tanto CERTIFICA, la revisión y corrección de este documento para optar por el Grado Académico de:

LICENCIATURA EN INFORMÁTICA CON ÉNFASIS EN DESARROLLO DE SOFTWARE
UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

Tema:
¿CUÁLES SON LOS FACTORES QUE INTERFIEREN EN LA FILTRACIÓN DE LA INFORMACIÓN EN LAS ORGANIZACIONES?

Elaborado por: KAROL PAOLA ABARCA CORTÉS
Cédula: 1 14660945

Se extiende la presente en San José, el 11 de diciembre del 2012

Atentamente:

JACQUELINE RÍOS A.
COORDINADORA GENERAL DE FILÓLOGOS
EDUCATESIS
C616F258