FUGA DE DATOS, ¿AMENAZA INMINENTE O BENEFICIO COMÚN?

William Fernando Pinilla Pinilla

Universidad Piloto de Colombia
Bogotá, Colombia
williferpin@gmail.com

Resumen— Dado que el alto riesgo en pérdida de información radica en que la fuga de datos podría causar una fuerte pérdida de dinero en una organización o volvernos blanco a las acciones fraudulentas por los delincuentes frente a la pérdida de información, considerando que las personas que pertenecen a una organización, en general, hace que la fuga de información se pueda dar por distintos canales y, a la vez, que se dificulte la concientización, ya que muchas veces la fuga de datos no viene de nuestros propios perfiles sino de los de nuestros contactos, que inocentemente agregan información inocua, la cual, correlacionada con la de otros usuarios de nuestra confianza y los nuestros, puede generar un gran caudal de datos útiles para cualquier atacante. El escenario se torna más delicado si se considera que las organizaciones suelen tomar medidas técnicas en las que gastan mucho dinero y, en caso de concretarse un ataque de este tipo, ninguna medida de seguridad digital serviría para protegerlas. Una parte de las soluciones en los entornos organizacionales es el cumplimiento de normas y regulaciones internacionales que permiten asegurar un determinado nivel estándar de controles y auditorías.

Abstract— Since high risk in loss of data is that data leakage could cause severe loss of money in an organization or become white to fraudulent actions by criminals against the loss of information, considering that persons belonging to an organization in general are numerous, this causes the leakage of information can be taken for various channels and at the same time, the awareness is difficult, because many times the data leak is not coming from our own profiles but those of our contacts, added innocently innocuous information, which, correlated with other users of our trust and our own, can generate a wealth of useful information for an attacker. Scenario becomes more delicate when one considers that the organizations often take technical measures you spend a lot of money and, if realized an attack of this type, no action would serve to protect digital security. Some of the solutions in organizational settings is the fulfillment of international standards and regulations which ensure a certain standard level of controls and audits.

Palabras clave— Criminalística, computer y network forensics, forense digital, fuga de datos, BYOD, medios físicos, medio magnético, medio electrónico.

I. INTRODUCCIÓN

Los continuos informes acerca de vulnerabilidades en los sistemas de información, el aprovechamiento de falencias bien sea humanas, procedimentales o tecnológicas sobre instalaciones o infraestructuras de computo en el mundo, proporcionan un ambiente inigualable para que se practiquen algunas técnicas de ataque que a menudo son utilizadas para saltear uno o varios de los controles implementados como parte de la defensa, tendencias relacionadas con intrusiones informáticas. Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos de especiales investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, sólo es preciso

establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado. Es aquí donde la informática forense hace entonces su aparición no como una disciplina auxiliar de la justicia moderna, presenta desafíos y técnicas para enfrentar a los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Se busca ofrecer un panorama general de esta especialidad técnico legal, sobre los fundamentos generales y bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, originando así nuevos científicos que mediante una metodología, la formalidad de los procesos y la precisión de la técnica buscan decirle a los intrusos informáticos que están preparados para confrontarlos y procesarlos.[1]

II. FUGA DE DATOS

Se entiende por fuga datos a la salida de información no controlada o supervisada que hace que esta llegue a manos de personas no autorizadas o sobre la que su responsable pierde el control y hacer uso de esta de forma benéfica para sí mismo o para un tercero, pudiendo llegar a ser, la información, un gran negocio lucrativo. La pérdida de información comienza cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados, revela parte de la información que procesa o transmite debido a errores en los procedimientos de diseño o trabajo. Por ejemplo, un protocolo de comunicación por Internet sin cifrar que sea interceptado por un atacante puede ser fácilmente leído; un carta con información confidencial enviada en un sobre sin mayor medida de seguridad, puede ser abierta y leída por una persona no autorizada.[2]

La informática forense define el proceso de obtención de información digital sobre un incidente para posteriormente analizarla y determinar lo que realmente sucedió durante el mismo.[3]

Con el paso del tiempo la tecnología ha avanzado a pasos agigantados y sin darnos cuenta ya es parte de la vida diaria de las personas, de las organizaciones, y por supuesto infiere en nuestras vidas al punto de darle toda la importancia, pues de ella se obtienen progresos en el desarrollo de una organización, pymes y en general todo un país; como es de saber y conforme existen los avances en las ciencias aplicadas de la informática y la gran capacidad de domino que tienen en todas las áreas de la vida social, han surgido acciones ilícitas que conocemos como delitos informáticos, los cuales con el desarrollo de la programación y el internet se han vuelto más frecuentes y sofisticados; por lo expuesto, se formula la siguiente pregunta: Ante un incidente informático y teniendo en cuenta que existen las herramientas, normas, políticas establecidas, etc., en cualquiera de los casos ya sea en una entidad u organización, ¿se encuentra preparado para atender un incidente informático?

Pero, no solo la pérdida de información o fuga de datos se da cuando un atacante irrumpe en nuestros sistemas, inconscientemente podemos tener acceso a la información cuando tomamos prestado un sistema, guardamos documentos en medios magnéticos o extraíbles generando entonces un incidente de seguridad. Sin embargo, a la hora de acercarse a esta definición es bueno recordar que la definición de incidente ha evolucionado, tiempo atrás, un Incidente de Seguridad en las TIC's, era definido como cualquier suceso adverso que tenía como consecuencia una pérdida de la confidencialidad, la integridad o la disponibilidad de los datos o sistemas. Hoy en día, un Incidente de Seguridad TIC se entiende como la violación o la amenaza inminente de violación de las políticas de seguridad o de los estándares o prácticas de la Organización.

---

1 Descubriendo los Rastros Informáticos, Jeimy J. Cano M., 2009.

2 Tomado de es.wikipedia.org

3 Fañanás Conte, Roberto, **CISA** ARMADA ESPAÑOLA, Aproximación a la Informática Forense.

Ante la necesidad que genera la actividad diaria, independientemente de los servicios o productos que se administren, se sustenta intensivamente en el soporte, en tanto que paralelamente el valor de los datos mantenidos es cada vez más importante, conformando ambos elementos entre otros, lo que hoy se denomina Activos Informáticos, por ello se origina el siguiente cuestionamiento:

¿Cómo las entidades u organizaciones de cualquier sector se acondicionan, localizan, dominan y destruyen, un incidente cuando se presenta y se interrelaciona en la fuga de datos?, ¿Existe un mecanismo de confianza que permita la recolección información?, ¿adquieren herramientas necesarias para manipular la información que contiene una entidad u organización?

III. FUGA DE DATOS MÓVILES

Desde el emblemático caso de WikiLeaks en 2010, se puso de manifiesto en las organizaciones y empresas de todo el mundo la imperiosa necesidad de analizar qué posibilidades tenían de ser víctimas de un caso de fuga de información, especialmente a la pérdida de confidencialidad de una determinada información que pertenece a una entidad, y es transportada hacia otro contexto, ya sea privado o público.

Los métodos para conseguir cualquier información son diversos, y se agrupan principalmente en tres categorías, basadas en la ubicación de la información: datos en tránsito (en las redes y conexiones), datos en uso (en las PC y dispositivos móviles) y datos almacenados (en los servidores de archivos). Consideraremos estos últimos como un caso particular de los datos en uso, a los fines del análisis, ya que nuestro foco es el rol que cumplen los dispositivos móviles en este escenario.

Con la aparición de los medios extraíbles tales como diskettes, CD, USB, etc., extraer la información de un sistema era propio por estos dispositivos de almacenamiento, pero con la masificación de dispositivos MP3 y celulares; las empresas se enfrentaron a un gran dilema generando un interrogante: ¿se podrá evitar la conexión de estos dispositivos a los equipos de cómputo de la empresa? En muchas ocasiones la respuesta fue sí, generando políticas de control de acceso físico a los equipos, y prohibiendo la conexión de dispositivos externos y/o personales, como los mencionados anteriormente. Pero esta no fue una solución definitiva, dado que siempre existen brechas de seguridad que se pueden romper permitiendo entonces la fuga de información, aún con las políticas restrictivas para la conexión de dispositivos externos de almacenamiento la fuga continuó ampliándose, por ejemplo, un usuario que le interesa cierto documento o información en específico, pero que no lo puede copiar en un pendrive, lo que hace es subirlo a un servidor FTP o a alguno de los servicios Cloud (Skydrive, Box, Dropbox, etc.). La empresa pensaría en el problema y pondría restricciones de navegabilidad web, pero aún no estaría pudiendo evitar que un usuario se envíe por email el archivo a una cuenta personal y lo baje desde otra conexión. Incluso si los emails fueran auditados para determinar su destino (lo cual debería estar explicitado en la política de uso de recursos informáticos, en cuanto a la prohibición del uso personal de las cuentas corporativas) aún tendría que resolverse el gran problema de lidiar contra los teléfonos celulares.

El caso de los celulares, lleva hasta el límite la necesidad de protección, ya que en caso donde la empresa tenga políticas de BYOD (Bring Your Own Device - Traiga su propio dispositivo) ya está por defecto habilitando canales de uso de información corporativa a través de los dispositivos de los usuarios. Por ejemplo, si un usuario recibe un mail laboral con un documento confidencial adjunto en su dispositivo, podría descargarlo en su casa al sincronizarlo con la PC. Incluso en casos donde se hayan tomado medidas más restrictivas aún, podrían aprovecharse las conexiones inalámbricas o Bluetooth para transferir archivos desde y hacia celulares, y también de forma directa a las impresoras con tales capacidades.

IV. ESTADÍSTICAS EN LA PÉRDIDA DE INFORMACIÓN

El 2013 pasará a la historia como el año con la serie de ciberataques más dañina de la historia y una

fuga de datos que aumentó en un 62%, en comparación con el año anterior. Según el estudio más reciente de la empresa de seguridad Symantec, el aumento en la fuga de datos generó que más de 552 millones de identidades quedaran expuestas, lo que representó un crecimiento del 493%, aumentaron además los ataques de ransomware (utilizados para extorsionar y extraer dinero de las víctimas después de cifrar los datos) en un 500% y se volvieron más agresivos. El estudio evidenció la presencia de nuevas versiones encriptadas y secuestros de archivos. Fue el año de las vulnerabilidades y nuevas formas de obtener información ilegalmente.[4]

Los hackers fueron los protagonistas en la mayoría de las fugas de datos presentadas durante el año pasado (34%), pero también existieron otros factores para el robo de información. Datos publicados accidentalmente (29%) y el robo o extravío de equipos de cómputo o USB (27%) fueron algunas de ellas, explica Rodrigo Calvo, ingeniero de Symantec. "Muchos de los datos se publican accidentalmente. Las organizaciones deben identificar cuál es su información crítica, saber en dónde está almacenada, quién accede a ella, como está siendo utilizada y hacer copias de seguridad", recomienda Calvo.

La información que más robaron los hackers se relaciona con datos de tarjetas de crédito, números de teléfono, fecha de nacimiento y número de documento. Se filtró además información financiera y contraseñas y nombres de usuarios en casillas de e-mails.

Para llegar a ello se requiere conocer las necesidades de seguridad de una organización para establecer medidas que permitirán evitar una situación catastrófica mediante mecanismos de seguridad ante la presencia de un incidente, seguido de ello se hace una detección del incidente mediante revisiones operativas, revisión y correlación de eventos, revisión de alarmas, logrando lo anterior se contendrá el incidente para evitar que la eventualidad empeore y tener la certeza de que todas las medidas tomadas se aplicarán correctamente, llevando a la erradicación del incidente usando la información recopilada durante la identificación y contención, intentando aislar el ataque y determinar cómo fue ejecutado este.

V. ¿BENEFICIOS O DELITO?

Toda organización tiene intereses particulares, y muchas veces sus propios empleados ofician de atacantes internos (lo que llamamos en la jerga: insiders). Otras veces son entidades externas las que buscan contactos dentro de las empresas para motivar el robo de datos, o bien colocan a su propia gente pasando por los procesos formales de recursos humanos, en estrategias más avanzadas. Ya sea motivado por codicia, por dinero, por poder, o solamente porque les es posible, son los propios usuarios los que permiten la fuga de información.

Los datos confidenciales son el objetivo de muchos ataques y cualquier fuga puede resultar muy costosa, demás el almacenamiento de datos confidenciales en teléfonos inteligentes hace que los riesgos para la seguridad de las empresas estén aumentando a gran velocidad; aunque la fuga de datos se presenta en todo momento y lugar, el cual se denomina delito informático o ciberdelincuencia, que tiene como objeto el de recopilar, extraer, dañar o destruir la información de una empresa u organización. Aunque se piense que se va a sacar provecho de la información obtenida; en Colombia se modifica el código penal con la ley 1273 de 2009 creando un nuevo bien jurídico tutelado denominado "De la protección dela información y de los datos" y a su vez se divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones", donde se clasifican los tipos de delitos o actividades delictivas que se realizan por medio de sistemas e infraestructuras electrónicas que van ligadas a herramientas utilizadas por los ciberdelincuentes, para buscar, vulnerar y dañar todo lo que encuentren en el espacio informático, tales delitos pueden ser: ingreso ilegal a sistemas, interceptación ilegal de redes, interferencias (man in the middle), daños en la información (borrado, dañado, alteración o supresión de DataCrédito), mal uso de artefactos, chantajes, fraude electrónico,

[4] Fuente: http://www.elfinancierocr.com/tecnologia, http://bit.ly/19G9CVy

ataques a sistemas, robo de bancos, ataques realizados por crackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y entre muchos otros.

En Colombia existen instituciones de educación que promueven capacitaciones en temas relacionados con Delitos Informáticos, para el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e instruir en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas

VI. INCIDENTES DE SEGURIDAD

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por ejemplo Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La informática forense, aplicando procedimientos estrictos y rigurosos, puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

Incidentes de seguridad informática

Un incidente de Seguridad Informática está definido como un evento que atente contra la Confidencialidad, Disponibilidad e Integridad de la información y de los recursos tecnológicos. Cualquier evento adverso, real o potencial, vinculado a la seguridad de los sistemas informáticos o a las redes de computadoras o el acto de violar una política de seguridad explícita o implícita, son consideradas como un incidente de seguridad informática.

Según el FBI[5], la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso. Desde 1984, el laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional. Dentro de lo forense encontramos varias definiciones que se describen a continuación:

Computación forense (computer forensics): Esta expresión podría interpretarse de dos maneras: como la Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos, por tanto, esta disciplina aplica conocimientos técnicos y científicos relacionados al estudio de las computadoras, incluyendo: diseño, funcionamiento, métodos de almacenamiento y uso de la información presentada en internet combinando aspectos teóricos

[5] Federal Bureau of Investigation, (FBI) es la principal rama de investigación del Departamento de Justicia de los Estados Unidos. www.fbi.gov

y prácticos de la ingeniera, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano.

Forense en redes (network forensics): Seguridad en un contexto de TI abarca las técnicas de apoyo a tres objetivos fundamentales: mantenimiento de la disponibilidad de servicios y datos, velar por la integridad de la información y protección de la confidencialidad de la información, en la figura 1, se muestra como una red se puede ver afectada y se puede vulnerar cada uno de los puntos en los cuales se encuentran interconectados entre si: por tanto se ve la necesidad de mantener la disponibilidad e integridad de una red donde la seguridad debe prevalecer en todo momento.

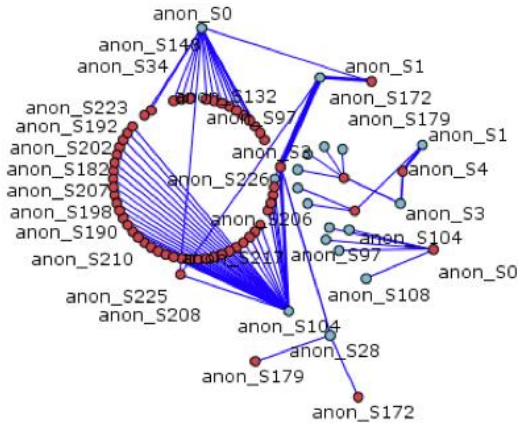

Fig. 1 Network Forensics.[6]

No es muy amplia la gama de enfoques para la consecución de estos objetivos. A medida que Internet crece y con la mayor dependencia de los sistemas de TI en los negocios, el valor de la información aumenta como también el número de amenazas se incrementan también. Las amenazas van desde física: el corte de cables e inundaciones en las salas de máquinas, por las acciones de los usuarios autorizados y otras amenazas internas.

Después de haber ocurrido un fallo de seguridad puede ser muy difícil identificar lo que ha sido robado o manipulado. Este problema es especialmente cierto en las grandes organizaciones donde puede haber cientos de miles de servidores que ejecutan aplicaciones o servicios de red avanzadas, técnicas forenses, realizan un enlace con los datos de gestión de red para rastrear el comportamiento e identificar los problemas. Los enfoques tradicionales de forenses sólo son útiles en las investigaciones a pequeña escala.

Una habilidad fundamental en muchas circunstancias es comprender los tipos de ataques que pueden haber intentado por los delincuentes para poder poner a prueba el sistema, para aquellos que de una manera segura puedan informar a los equipos de seguridad en el cambio de una postura de seguridad.

Forense Digital (Digital Forensic): Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

VII. RIESGOS Y ERRORES COMUNES

Hoy en día las empresas son cada vez más distribuidas y móviles, lo cual les obliga a enfrentar desafíos en la protección de su información confidencial. Con el objeto de comprender esta situación, una compañía independiente de investigación de mercado, realizó un estudio que abarcara a empleados y profesionales de TI en diversos países[7]. Como parte del estudio, se realizaron encuestas en 10 países que Cisco seleccionó debido a las diferencias en sus culturas sociales y comerciales. En cada país, se encuestó a 100 usuarios finales y 100 profesionales de TI, cubriendo así a un total de 2000 personas. La

[6] Tomado de: http://www.sys-consulting.co.uk/web/Expertise_Security.html

[7] Cisco facultó a InsightExpress, quien se encargaría de realizar los estudios pertinentes. Fuente: Website www.cisco.com/go/offices

investigación descubrió que a pesar de las políticas, procedimientos y herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales. Tales conductas incluyeron:

- ✓ Uso de aplicaciones no autorizadas: el 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.
- ✓ Uso indebido de computadoras de la empresa: el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.
- ✓ Acceso no autorizado tanto físico como a través de la red: el 39% de los profesionales de TI afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.
- ✓ Seguridad de trabajadores remotos: el 46% de los empleados admitió haber transferido archivos entre computadoras del trabajo y personales al trabajar desde el hogar.
- ✓ Uso indebido de contraseñas: el 18% de los empleados comparte contraseñas con sus colegas. El porcentaje aumenta al 25% en China, India e Italia.

Para reducir la fuga de datos, las empresas deben integrar la seguridad en su cultura empresarial y evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios.

Muchas veces consciente o inconscientemente se adoptan conductas que ponen en riesgo la información y los recursos empresariales, a pesar de las políticas que establecen procedimientos correctos como por ejemplo el uso de aplicaciones no autorizadas pudiendo conllevar el riesgo de contagio de sitios maliciosos, uso indebido de los equipos de cómputo de la empresa (cambiar las configuraciones de seguridad y compartir carpetas e información confidencial con personas ajenas a la empresa.), los usuarios anulan las configuraciones de TI para descargar música, comprar en línea, pagar cuentas y, en algunos casos, acceder a juegos de azar y pornografía en línea. Estas conductas facilitan que propiedad intelectual de la empresa llegue a manos de personas que constituyen una grave amenaza para la seguridad y la rentabilidad empresarial, entre otras conductas está el acceso no autorizado tanto físico como a través de la red, permitiendo que personas desconocidas ingresen a dependencias de la empresa sin la supervisión necesaria; también la seguridad de trabajadores remotos aumentan el riesgo potencial de pérdida de información, conductas tales como transferir archivos de un dispositivo laboral a un computador personal que no esté protegido según las normas de TI; por último el uso indebido de contraseñas y procedimientos de inicio/cierre de sesión aunque parezca increíble cuesta pensar que existen usuarios que pasan por alto estos conceptos básicos de seguridad

Cualquiera de estas infracciones al protocolo de seguridad ofrece peligrosas oportunidades a los atacantes. En conjunto, no sólo dejan la puerta abierta a amenazas potenciales, sino que invitan el ingreso de atacantes. Por ejemplo, cuando un empleado deja un sistema con la sesión activa sobre un escritorio y con su contraseña adjunta, invita a que un intruso robe su computadora en ese momento e información confidencial en el futuro. Si el empleado utilizó dicha computadora para uso personal, el atacante también podrá acceder a dicha información.

VIII. RECOMENDACIONES Y CONSEJOS BÁSICOS PARA PROTEGER LA INFORMACIÓN

Las amenazas contra la seguridad de la información continúan evolucionando. La piratería informática se está convirtiendo de manera creciente en una profesión delictiva y la colaboración adversaria es una actividad con fines de lucro. Gran parte del peligro proviene de Internet, y en este entorno peligroso, se generan fugas de información por parte de los usuarios a pesar de los grandes esfuerzos que realizan los profesionales de TI para impedirlo. Si bien los productos comerciales denominados DLP (Data Loss Prevention) avanzan en el mercado, de momento se considera que no es

posible administrar una única medida para mitigar la fuga de información. Se debe elevar el nivel general de seguridad de las empresas analizando todos los frentes posibles, ya sean técnicos, físicos o administrativos, para enfrentar problemas y amenazas como parte de un ciclo continúo en el marco de una planificación estratégica.

Para lograr la seguridad de nuestro sistema, claramente no existe una solución mágica para salvaguardar la información, especialmente cuando las empresas y sus datos se tornan cada vez más móviles y operan con límites virtuales en vez de físicos. La forma más eficaz de prevenir la fuga de información es mediante un esfuerzo continuo y generalizado que sea estratégico de concientización.

Los incidentes de fugas de datos se producen por diversos motivos y los daños pueden ir mucho más allá de las multas impuestas por los organismos reguladores, por esta razón se deben tener normativas, herramientas y claros criterios de seguridad, algunas recomendaciones como:

- Protección de datos almacenados en dispositivos portátiles así como las herramientas para la seguridad de los datos.
- Poner medidas para proteger la información personal.
- Conocer los datos, el núcleo de la protección debe estar en la información, no en el dispositivo o el centro de datos. Se debe saber dónde se almacena la información confidencial y por dónde circula para identificar las mejores políticas y procedimientos necesarios para protegerla.
- Educar al equipo, compartir con los colaboradores la información y realizar las respectivas recomendaciones respecto a la protección de datos, en especial sobre políticas y procedimientos existentes para proteger la información confidencial en dispositivos personales y corporativos.
- Implementar medidas de seguridad sólidas, es necesario fortalecer la seguridad de la infraestructura de TI con prevención de pérdida de datos, seguridad de redes, cifrado, autenticación.
- Para los usuarios finales: asar los conocimientos de seguridad y tecnología. El uso de contraseñas es relevante. Utilizar un software de administración de contraseñas para crear claves seguras para mantener los dispositivos, incluyendo Smartphone, actualizados con el último software de seguridad, además crear una política de cambio periódico de contraseñas.
- Si se manejan cuentas bancarias, revisar con frecuencia los movimientos de la cuenta y tarjetas de crédito en busca de irregularidades, conjuntamente se debe prestar atención a los correos electrónicos no deseados o sospechosos y sobre todo se debe desconfiar de ofertas en línea o lo que hoy se denomina phishing.
- Cuando se hagan compras en línea, previamente se deberían conocer las políticas de las tiendas y servicios en línea que soliciten información bancaria o personal. Si hay que compartir algún dato, preferiblemente habría que ir directamente al sitio oficial de la compañía.

Con la presencia cada vez mayor de los teléfonos inteligentes, tabletas y otros dispositivos móviles en nuestras vidas, es importante estar al tanto de algunas opciones de privacidad y seguridad a las amenazas comunes, ya que estas son muy amplias y variadas, por lo que el nivel de privacidad y seguridad que se busca probablemente dependerán de la información que está en juego.

Por esto hay que pensar en la información de un dispositivo móvil y generarnos los siguientes interrogantes ¿Qué valor tiene esta información? ¿Estaría molesto si alguien accede a él sin consultarlo? ¿Qué pasaría si se pierde o es robado? Aparte de robo físico, amenazas como el malware y el spyware son cada vez más sofisticados. La buena noticia es que hay algunas cosas fáciles que se pueden hacer para reducir las probabilidades de ser víctimas. A continuación, se indican algunas cosas que se pueden pensar, y algunos consejos para ayudar a mitigar los riesgos.

- Proteger con contraseña el dispositivo (o usar otro medio de autenticación) y configurar el dispositivo para que se bloquee automáticamente después de un período determinado de tiempo.
- Usar contraseñas únicas y seguras y cambiarlas con frecuencia.
- Desactivar la opción Bluetooth cuando no se esté utilizando.
- Utilizar software de seguridad de confianza.
- Instalar aplicaciones solo del sitio de descarga de mayor confianza.
- Mantener actualizado el equipo, esto incluye actualizar las aplicaciones instaladas en el dispositivo.
- Para la protección de la información tanto personal como de la empresa que se maneje en el dispositivo, lo más recomendable es el tratar de no utilizar redes Wi-Fi públicas.
- Comprobar los ajustes de privacidad y seguridad del dispositivo, así como los permisos de las aplicaciones.

REFERENCIAS

[1] ©SYS Consulting Ltd., Company No. 04045713. Disponible en Internet en: http://www.sys-consulting.co.uk/web/Expertise_Security.html

[2] CANO, Jeimy. Computación Forense – Un reto técnico-legal para el próximo milenio. Diapositivas de la conferencia Presentada en el marco del I congreso internacional de Ing. de Sistemas y Ciencias de la Computación. Universidad Industrial de Santander. Bucaramanga. 2000.

[3] COLOBRAN, Huguet Miguel; ARQUÉS Soldevila Josep María; MARCO Galindo Eduard. Administración de sistemas operativos en red. Primera edición. Editorial UOC. 2008. 307 pág. ISBN: 978-84-9788-760-1

[4] FAÑANÁS, Conte, Roberto, Aproximación a la Informática Forense, Peritaciones y Arbitrajes, nº 4 julio-agosto 2006. Disponible en Internet en: http://www.revista-ays.com/DocsNum04/Peritaciones/Roberto.pdf

[5] Informe Symantec 2013: http://bit.ly/19G9CVy.

[6] Dispositivos móviles y fuga de información. Disponible en http://club.globallogic.com.ar/dispositivos-moviles-y-fuga-de-informacion/.

[7] Grupo de Trabajo Científico en la Evidencia Digital (SWGDE), Organización Internacional para las pruebas digitales (IOCE). Evidencia Digital: Normas y Principios. Abril 2000 - Volumen 2 - Número 2. Disponible en: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.

[8] Incidentes De Seguridad Informática, Disponible en Internet en: http://portal.aerocivil.gov.co/portal/page/portal/Aerocivil_Portal_Intranet/seguridad_informatica/mejore_seguridad_informacion/incidentes/incidente_seguridad_informatica

[9] REYES CALDERÓN, José Adolfo. Introducción al estudio de la criminología. 2da. edición México D.F. Editorial Porrúa S.A. 2010. 360 Pág.

[10] U.S. Department of Commerce. National Institute of Standards and Technology. Computer Security Incident Handling Guide. Special Publication 800-61 Revision 1. USA. March 2008. 147 Pág.

[11] ZUCCARDI, Giovanni, Gutiérrez, Juan David. Noviembre de 2006. Informática Forense. 17 Pág. Disponible en: http://pegasus.javeriana.edu.co/~edigital /Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

[12] JARA, Héctor y Pacheco Federico G. Ethical Hacking 2.0. Implementación de un sistema para la gestión de la seguridad. Colección: Manuales USERS. 352 Pág. ISBN 978-987-1857-63-0

[13] Fugas de datos y normativas. Disponible en: http://www.sophos.com/es-es/security-news-trends/security-hubs/data-loss-and-regulations.aspx.