

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad

No. 24 - 2008

Contenido Cerrar Imprimir Página anterior Página siguiente



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 

Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

▶ Introducción

▶ ¿Qué es la privacidad?

▶ La Privacidad de la Información y su relación con el Robo de Identidad.

▶ Administrando la privacidad de la información en las Organizaciones

▶ Recomendaciones a nivel empresarial

▶ Recomendaciones a nivel personal

▶ Créditos / Suscribirse

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



Introducción

La información no es solo patrimonio con un valor económico, ni su acceso autorizado un problema que afecta únicamente a las empresas; en una sociedad donde las actividades económicas, profesionales y sociales involucran el uso de la tecnología, nos encontramos con amenazas como la violación de la privacidad y el robo de identidad, elementos que trascienden a la organización y que son inherencia de la sociedad.

Hasta hace poco tiempo, cuando un ladrón robaba la cartera, el dinero era su principal objetivo. Esto ha ido cambiando, y el impacto de la obtención de datos personales ha comenzado a representar un impacto mayor para el afectado. Las estrategias que usan los estafadores son cada vez más sofisticadas, y van desde la más común de robar documentos con información personal tirados a la basura sin antes ser destruidos, hasta refinadas técnicas informáticas

para vulnerar bases de datos de instituciones. Los internautas aún no han mostrado, en general, excesiva preocupación en lo que se refiere a la recopilación de datos.

Recientes estadísticas reflejan que “El 60% de los internautas no tienen ninguna preocupación acerca de la privacidad en Internet”¹, y que “El 59% de las personas que navega en Internet cree que si una empresa tiene políticas de privacidad, no compartirá información con terceras personas”²

Diariamente, las personas divulgan información sobre si mismas al hacer transacciones por teléfono, personalmente, o en portales de Internet para efectuar la adquisición de productos y servicios. La tenencia de esta información puede ser utilizada para forjar la identidad financiera de un individuo o efectuar actividades en su nombre.

¹ Pew Internet and American Life Project (Diciembre 2007).

² Annenberg Public Policy Center (Enero 2008)

La mayoría de las personas no tienen el conocimiento de cuándo han sido víctimas del robo de identidad, y sólo lo advierten cuando son asociados con actividades que no han realizado.

De acuerdo al informe anual –Consumer Fraud and Identity Theft Complaint Data– de la Comisión Federal de Comercio (Federal Trade Commission, FTC) en el cual se detallan las quejas de fraude y robo de identidad presentadas por los consumidores ante la agencia. Por octavo año consecutivo, el robo de identidad encabeza la lista registrando el 32 por ciento del total de 813.899 quejas recibidas entre el 1° de enero y el 31 de diciembre de 2007. (Ver Figura N°1)



Para visualizar la Figura No. 1 haga click en el icono.

Figura N°1: Principales Categorías de Quejas Presentadas por los Consumidores. Fuente: Federal Trade Commission

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



¿Qué es la privacidad?

La privacidad es el “ámbito de la vida que se tiene derecho a proteger de cualquier intromisión”³. Reconocidos investigadores se refieren a la privacidad de la información como un concepto dinámico y actual, citando:

“El concepto de privacidad esta cambiando de manera radical como resultado de nuestras vidas basada en la computadora. Antes la privacidad se lograba mediante la sola fricción de la vida cotidiana: distancia, tiempo y falta de registros. La información no viajaba bien y la mayoría de las personas que querían escapar de su pasado simplemente se mudaban a una nueva ubicación.

Ahora la perspectiva ha cambiado. Las personas pueden escapar de los que la rodean a través de Internet, pero sus acciones las pueden alcanzar fácilmente. Y no es solo

Internet, las operaciones con tarjetas de créditos, las base de datos de los vendedores, los registros de los teléfonos celulares y mucho más.”⁴

“La privacidad constituye un bien jurídico con proyección social, que enuncia el ejercicio de la libertad humana y, asimismo, impone un límite en la interrelación social”⁵.

El derecho a la privacidad y el derecho de la personalidad son fundamentales, en razón que su irrespeto puede exponer al afectado a exclusiones, negaciones, escarnio público o involucramiento en actividades ilícitas. Es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones o injerencias externas en estas áreas reservadas del individuo.

El derecho al respeto de la vida privada es reconocido como un derecho fundamental que protege al individuo contra las autoridades públicas u otros individuos. La comunidad internacional ha avanzado a grandes pasos en relación a fortalecer la protección al Derecho a la Privacidad. Como ejemplo de este planteamiento podemos mencionar el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de Naciones Unidas, el cual consagra lo siguiente:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

¹Real Academia Española. ²Investigación de Mercados – Carl Mc-Daniel y Roger Gates, ³The right to privacy - Warren y Brandeis

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



¿Qué es la privacidad? (continuación)

A su vez, el derecho a la privacidad es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas o injerencias externas en estas áreas reservadas del ser humano como son, entre otros:

- El derecho a la inviolabilidad a las comunicaciones privadas
- El derecho a la privacidad informática
- El derecho a no participar en la vida colectiva y a aislarse voluntariamente
- El derecho a la propia imagen

En Venezuela, la Ley Especial sobre Delitos Informáticos tiene como objetivo proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales

tecnologías (Gaceta Oficial N° 37.313 del 30 de octubre de 2001), contemplando acciones contra los siguientes delitos:

- Contra los sistemas que utilizan tecnologías de información
- Contra la propiedad
- Contra la privacidad de las personas y de las comunicaciones
- Contra niños y adolescentes
- Contra el orden económico

De igual manera, en la Ley de Telecomunicaciones se incorporan derechos de los usuarios tales como privacidad de las comunicaciones, acceso en condiciones de igualdad, facturación oportuna, compensación por interrupciones de servicio, así como parámetros mínimos de calidad de servicio.

Sin embargo, la garantía final de este derecho a la privacidad, es el establecimiento de hábitos en nuestras vidas que minimicen el riesgo al robo de

identidad y controle la inseguridad de la información que presentamos tanto en el ámbito privado como en el estatal, tomando responsabilidad sobre lo que se dice, publica y las acciones ejecutadas. El 70 por ciento de los consumidores en línea manifiestan preocupación sobre la privacidad, sin embargo, la conducta tiende a indicar otra cosa: En una encuesta realizada por la Privacy Leadership Initiative, sólo 3% de los consumidores leyeron cuidadosamente las políticas de privacidad y 64% las revisó superficialmente. Estas cifras pueden sobrestimar la atención que le presta las personas a las políticas de privacidad: por ejemplo, sólo el 0.3 por ciento de los usuarios lee la política de privacidad de Yahoo!, según el New York Times⁶.

⁶ Investigación de Mercados – Carl McDaniel y Roger Gates

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



¿Qué es la privacidad? (continuación)

En el mundo lógico en el que nos desenvolvemos a diario, el anonimato en Internet se ha disipado y debemos establecer en consecuencia hábitos para la entrega de información en servicios de uso cotidiano como:

- Servicios gratuitos de la Web, en donde se requiere la entrega voluntaria de datos, se realizan seguimientos de los hábitos de navegación mediante la instalación de cookie's y utilitario, web bugs, entre otros
- Uso de correo electrónico gratuito y sitios de alojamiento de documentos
- Acceder a la suscripción a servicios de mercadeo

- Mensajería instantánea
- Redes sociales.
- Blogs, foros de discusión y agrupaciones.

Por otra parte, hábitos de cuidado en la gestión de la información manejada en nuestro contexto físico, nos aportará mayor privacidad, estableciendo criterios y controlando servicios como:

- Entrega y recepción de correspondencia
- Gestión de desperdicios (Empresas Privadas e Instituciones Públicas)
- Páginas amarillas

La Privacidad de la Información y su relación con el Robo de Identidad.

Diariamente aumentan nuestras actividades que involucran el intercambio de información personal: Desde portales en Internet hasta la simple emisión de una factura, se va dejando una estela de datos susceptibles de ser recolectados y analizados para fines contrarios a los que fueron proporcionados.

En la obtención de datos e información privada se centran los esfuerzos actuales de los atacantes, y uno de los crímenes en esta materia que ha cobrado mayor importancia es el Robo de Identidad, sobre el cual se observa un crecimiento a nivel mundial.

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad

La Privacidad de la Información y su relación con el Robo de Identidad. (continuación)

De acuerdo a un estudio de la Comisión Federal de Comercio (FTC), 8.3 millones de adultos en los Estados Unidos, se convierten en víctimas de robo de identidad cada año. El estudio de la FTC clasifica el robo de identidad en tres categorías: Utilización de cuentas existentes de tarjetas de crédito, cuentas de otros servicios (tal como cuentas corrientes, de ahorro y de teléfono) y creación de cuentas nuevas u otros tipos de fraude que emplean el uso de información personal robada.

El robo de identidad es un crimen en el cual el impostor obtiene piezas claves sobre la información que identifica a un individuo, y los usa para forjar o suplantar su identidad, en su beneficio o perjuicio de otro. Puede empezar con el robo o

extravío de carteras y/o billeteras, intrusión en cuentas de correo, brechas de datos, virus en computadoras, phishing⁷, pharming⁸ o documentos dejados al alcance de terceros. Este crimen varía ampliamente y puede incluir fraude con cheques, fraude con tarjeta de crédito, robo de identidad financiera, robo de identidad criminal, gubernamental o simplemente fraude de identidad.

Métodos:

1. Robo de documentos personales
2. Ingeniería social
3. Empleados deshonestos con acceso información sensible
4. Robo de identidad perpetrado por familiares y/ o amigos
5. Usurpación de correo electrónico
6. Cambio de dirección de correspondencias
7. Phishing y pharming



⁷Phishing: Capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios.

⁸Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad

Administrando la privacidad de la información en las Organizaciones

Administrar la privacidad de la información, es una labor que amerita no sólo dispositivos o sistemas de control de acceso a los medios de almacenamiento, sino también la implantación efectiva de la gestión de seguridad de la información, que exija regular el uso de los mismos y adaptarse a la dinámica organizacional, de los negocios y de la tecnología.

La clasificación de la información es una propuesta que cuenta con una amplia aceptación y marcos referenciales para su implantación, como es el caso de las estrategias sugeridas por la Norma ISO27001⁹ y la Gestión de Seguridad de la Información dentro del marco CobIT¹⁰. Estas mejores prácticas se mencionan estrategias aplicables a los procesos en las Organizaciones, con el fin de aumentar los niveles de protección

de la información; pero para proteger la información de una manera coherente y eficiente, es necesario incorporar estas estrategias dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).



⁹ UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información.

¹⁰ COBIT: (Control Objectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada). Marco de trabajo conformado por dominios y procesos para la gestión de los sistemas de información en las organizaciones.

Recomendaciones a nivel empresarial

La mayoría de las empresas mantienen información personal, bien sea de sus empleados, clientes o del negocio, las cuales se utiliza en las operaciones diarias de la organización. , El impacto que conlleva una violación a la protección de dicha información, plantea la necesidad de esfuerzos suficientes en la gestión de acceso y definición de prácticas confiables en su utilización. A continuación se presentan algunas recomendaciones de tener en cuenta:

- Clasificar y controlar los accesos a la información.
- Unificar los sitios para el almacenamiento de información sensible y documentar los procedimientos para su acceso
- Realizar evaluaciones de cumplimiento de los controles relacionados a la clasificación de información, identificación de brechas de seguridad y auditorías de cumplimiento de mejores prácticas.

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



Recomendaciones a nivel empresarial (continuación)

- Definir políticas de acceso a la información.
- Establecer capas intermedias de software, que permitan establecer políticas de acceso a la información sensible, a modo de transacciones, evitando el número de usuarios y ocasiones en los que se requiera acceder directamente a los repositorios.
- Realizar campañas de concientización en cuanto a la privacidad, que involucre a los usuarios con las políticas en materia de privacidad y sean partícipes del control sobre el acceso a esta información.
- Establecer procedimientos de monitoreo sobre el acceso a los repositorios de información sensible
- Definir políticas y procedimientos para la destrucción de información sensible y acceso a los datos.

Con base en lo mencionado anteriormente, la documentación que se elabore para establecer formalmente la seguridad, debe considerar los diferentes niveles de gestión de la información. A continuación se describen estos documentos:

- **Política de seguridad:** documento el cual establece las necesidades y requisitos de protección entorno a la organización, sirve de guía para crear la norma de seguridad la cual es otro tipo de documento más detallado. La política de seguridad establece formalmente los objetivos perseguidos por la gestión de seguridad y que pretende la misma. Para el logro de los objetivos puede apoyarse en documentos de menor jerarquía los cuales permiten materializarlo en hechos tangibles.
- **Norma de seguridad:** documento el cual establece que hay que proteger y bajo que condiciones, pero para situaciones más concretas. Debe ser clara y concisa. Establece

requisitos que se apoyan en la política y que reglamentan determinados aspectos de seguridad.

- **Procedimiento de seguridad:** documento el cual establece las acciones o tareas a realizar en la ejecución de un proceso concerniente a la seguridad y las personas o grupos responsables de su desempeño. Los procedimientos de seguridad especifican una serie de pasos en relación a la ejecución de un proceso o actividad que cumple con una norma o garantiza que en el cumplimiento de actividades se tomara en cuenta determinados aspectos de seguridad.
- **Instrucción técnica de seguridad:** documento el cual establece las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento en específico sobre una parte determinada del sistema de información.

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad



Recomendaciones a nivel empresarial (continuación)

- **Política de uso:** documento destinado a usuarios finales, con la finalidad de establecer un reglamento específico sobre la utilización de un sistema, recurso o tecnología. Se debe documentar las normas de conducta que deben cumplir los usuarios en el uso de los sistemas de información o los aspectos que se desean regular, adicionalmente se debe considerar los usos autorizados y los que no son aceptables.

Recomendaciones a nivel personal

Es posible establecer acciones para minimizar los riesgos, pero es importante entender que cualquier acción ejecutada a partir de un momento determinado, no protegerá necesariamente al individuo por la divulgación de información entregada en el pasado, o por exposiciones de la misma ocurridas por situaciones ajenas a las empresas recolectoras. En todo caso, el robo de identidad puede disminuirse mediante el uso cauto y prudente de la información personal, y estando informado sobre el tema. Debe considerarse:

- Controlar información personal publicada por terceros, tales como Redes sociales, correos masivos, blogs y otros
- No responda a e-mails o llamadas que pidan información personal.
- Desarrollar hábitos de seguridad sobre información que se entrega.

- Consolidar la correspondencia en un lugar seguro donde la reciba oportunamente.
- Deshágase de una manera apropiada de los papeles que contengan información personal. Rompa los recibos de pagos, los saldos de sus cuentas bancarias, las tarjetas de crédito vencidas.
- Ser escéptico en cuanto a cuando y a quien proveer información y cual es el destino de la misma.

Boletín de Asesoría Gerencial*

Privacidad de la información y robo de identidad

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666



© 2008. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3

Figura N°1: Principales Categorías de Quejas Presentadas por los Consumidores.

Fuente: Federal Trade Commision - FTC

Regresar al boletín Aumentar Imprimir

