Uso de las bases de datos de la empresa por el trabajador

Carrasco Fernández, Felipe Miguel

2010

USO DE LAS BASES DE DATOS DE LA EMPRESA POR EL TRABAJADOR

Felipe Miguel Carrasco Fernández[1]

1.- Introducción:

El uso de la tecnología en ambientes laborales ha generado beneficios tanto a empleados como a trabajadores. ha permitido ahorrar tiempo en la elaboración de informes, bases de datos etc., sin embargo ha generado conflictos por el correcto uso que se le debe dar.

La tecnología está cambiando al mundo, la economía, la sociedad, la cultura y un sector social que está siendo especialmente sensible a estos cambios es el de las relaciones laborales. Siendo este un sector siempre sujeto a transformaciones y evoluciones aceleradas, en los últimos años se detecta una intensificación de este fenómeno, consecuencia, entre otros factores, de los cambios tecnológicos experimentados estos cambios han sido recibidos hasta ahora con cierta inseguridad y desconfianza, en cuanto se les considera fuente de nuevos problemas laborales, riesgos específicos, pérdida de puestos de trabajo. La sociedad global de la información, se tiende a comparar con las transformaciones sus formas, se puede convertir en la clave para el desarrollo.[2]

2.- Protección jurídica de las bases de datos

Considerando que la fabricación de una base de datos requiere una gran inversión en términos de recursos humanos, técnicos y económicos, y que éstas se pueden copiar o acceder a ellas a un costo muy inferior al necesario para crearlas de forma independiente la legislación protege a estas. Por lo tanto el uso cada vez mayor de la tecnología digital expone al fabricante de una base de datos al peligro de que el contenido de la misma sea copiado y reordenado

---

[1] Coordinador de Posgrados en Derecho de la Universidad Iberoamericana Puebla-México. Autor de la obra “Relaciones Laborales en la Globalización”. Académico de Número de la Academia Mexicana del Derecho del Trabajo y de la Previsión Social. Miembro de la Asociación Mexicana de Estudios de Trabajo. Miembro del Sistema Nacional de Investigadores Nivel II (CONACYT-México)

[2] Pumarino, Andrés. “Abuso de la Tecnología en el Trabajo”, Revista Identidad Robada. No.1. Año 2008. P. 3

electrónicamente sin su autorización con el fin de crear una base de datos de idéntico contenido, pero que no infringiría los derechos de autor respecto a la ordenación de la base original además de proteger estos respecto a la originalidad de la selección y disposición del contenido de una base de datos, pretende proteger a los fabricantes de bases de datos contra la apropiación de los resultados obtenidos de las inversiones económicas y de trabajo hechas por quien buscó y recopiló el contenido, ya que protege el conjunto o las partes sustanciales de la base de datos contra determinados actos que pueda cometer el usuario o un competidor.[3]

El objeto de este derecho es el de garantizar la protección de una inversión en la obtención, verificación o presentación del contenido de una base de datos para la duración limitada del derecho; que esta inversión puede consistir en la aplicación de medios financieros y/o en el empleo de tiempo, esfuerzo y energía;

Por lo tanto este derecho consiste en facilitar al fabricante de una base de datos la posibilidad de impedir la extracción y/o reutilización no autorizadas de la totalidad o de una parte sustancial del contenido de la base de datos; que el fabricante de una base de datos es la persona que toma la iniciativa y asume el riesgo de efectuar las inversiones.

El derecho específico de impedir la extracción y/o la reutilización no autorizadas se refiere a actos del usuario que excedan de sus derechos legítimos y que perjudiquen así la inversión; el derecho de prohibir la extracción y/o reutilización del conjunto o de una parte sustancial del contenido se refiere no sólo a la fabricación de un producto competidor parásito, sino también a los actos realizados por el usuario que perjudiquen sustancialmente la inversión, desde el punto de vista cualitativo o cuantitativo.[4]

Se entiende por extracción la transferencia permanente o temporal de latotalidad o de una parte sustancial del contenido de una base de datos a otro

---

[3] Parlamento Europeo y del Consejo. “Directiva 96/9/CE del 11 de marzo del 1996 sobre la Protección jurídica de las bases de datos” en línea. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri_CELEX:31996L0009:ES:HTML 29 de enero de 2009

[4] Idem. P4

[6] Idem. P4

soporte, cualquiera que sea el medio utilizado o la forma en que se realice; y por reutilización toda forma de puesta a disposición del público de la totalidad o de una parte sustancial del contenido de la base mediante la distribución de copias, alquiler, transmisión en línea o en otras formas.[5]

2.1.- Tipos de bases de datos.

Existe un gran clasificación de las bases de datos atendiendo a diversos factores, entre las que encontramos las siguientes:

a).- Según la variabilidad de los datos almacenados: *Bases de datos estáticas y Bases de datos dinámicas.*

b).- Según el contenido: *Bases de datos bibliográficas Bases de datos de texto completo, Directorio* Base de datos y *Bases de datos o "bibliotecas" de información.*

c).- Modelos de bases de datos: Bases de datos jerárquicas, Base de datos de red, Base de datos relacional. Base de datos multidimensionales, Bases de datos orientas a objetos, Bases de datos documentales, Base de datos deductivos

2.1.1 Robo interno:

El 61% de los encuestados consideran que el filtrado de datos lo realiza personal interno. El 23% cree que las filtraciones son deliberadas. *Encuesta McAffee y DataMonitor sobre pérdida de datos, 2007)*

Una tercera parte de todos los robos de equipos en grandes empresas son efectuados por empleados. *Encuesta DTI sobre violaciones en la seguridad informativa, 2006, 1 de mayo de 2007*

Entre 2005 y 2006 se registró un incremento del 81% en el número de empresas que denunciaron el robo de ordenadores portátiles con información confidencial. *Estudio Anual 2006: El coste de las filtraciones de datos. Instituto Ponemos, LLC, 2007*

[5] Idem. P8

3.- Código de Conducta Empresarial y Base de Datos.

Algunas empresas han establecido a través del código de conducta empresarial diversas disposiciones referentes al uso adecuado de las bases de datos, por ejemplo la compañía Nestle ha establecido que: El éxito constante depende del uso de información confidencial y de su no divulgación a terceros, a menos que así lo exija la ley o lo autorice la dirección de la empresa, los empleados no revelaran la información confidencial ni permitirán su divulgación. Esta obligación subsiste una vez extinguida la relación laboral, además, los empleados deben utilizar sus mejores esfuerzos a fin de impedir la revelación no intencional de la información teniendo especial cuidado al guardar o transmitir la información confidencial.

Los empleados deben proteger los bienes de Nestlé y utilizarlos únicamente en forma adecuada y eficiente. Todos los empleados intentaran proteger los bienes de Nestlé contra perdida, daño, uso incorrecto, robo, fraude, malversación y destrucción. Estas obligaciones cubren tanto a los activos tangibles como a los intangibles, incluidos las marcas comerciales, el know-how la información confidencial o privilegiada y los sistemas informativos.[6]

Aunque también es cierto que muchas veces el personal de confianza no es directamente culpable del robo de información. Un estudio de Trusted Strategies, basado en los procesos judiciales relacionados con los ataques informáticos documentados desde 1999 hasta 2006 en Estados Unidos, plantea entre sus conclusiones que las mayores pérdidas de datos se producen por acceso no autorizado a través de cuentas privilegiadas.

Los atacantes se hacen con el usuario y la contraseña de alguien con derecho real de acceso a la información y los utilizan para obtener documentos sensibles, a los que habitualmente no tendrían permiso para acceder.

Parece que las organizaciones no han tomado conciencia todavía de la gravedad del problema. Los ojos empresariales parecen ciegos ante el hecho de

---

[6] Código De Conducta Empresarial De Nestle. Visible en www.**nestle**.com/Resource.axd?Id=4E4FCBB4-F08C-4474-95AB-C6513ADED84B Diciembre de 2008. P.6

que 88% de los ataques involucrados en el robo de datos, según el mencionado estudio, se derivaron de simples accesos de empleados con contraseñas robadas (o deducidas), cometidos desde sus casas

Frente a estos riesgos, una posible solución es implantar una política de control de almacenamiento portátil a lo largo de la empresa. Algunos expertos e investigadores sugieren técnicas como el bloqueo físico de puertos o medidas más drásticas, como la total prohibición de todas, dispositivos similares en el sitio de trabajo.

Pero tomando en cuenta la popularidad y practicidad de las memorias USB, esta opción no resulta la más conveniente. Afortunadamente, existen medidas de control alternas, como la encriptación de documentos confidenciales o restringir el acceso a la información, con base en roles y perfiles; así como monitorear quién y cuándo accede a los datos y qué hace con ellos.[7]

Contu y Girard, analistas de Gartner advirtieron de los riesgos de seguridad asociados con el uso no controlado de dispositivos portátiles de almacenamiento dentro de las empresas. Hoy, el robo de información se ha convertido en una plaga de la sociedad moderna; fuga de información, cifrado de datos y revelación de información son algunos de los términos usados por los expertos de seguridad para referirse al robo de información. Sin embargo, el término más general hasta ahora es probable el término 'pod slurping' que fue inventado por el experto de seguridad de EE.UU. Abe Usher quien utiliza el término 'pod slurping' para describir como los reproductores MP3 tales cómo iPods y otros dispositivos USB de almacenamiento masivo pueden ser utilizados para el robo de información empresarial sensitiva.

Todos los dispositivos portátiles de almacenamiento pueden ser utilizados para "absorber" información; cámaras digitales, PDAs, dispositivos pequeños, teléfonos móviles o cualquier otro dispositivo "conectar y listo (plug and play)" que tienen capacidades de almacenamiento.

---

[7] Hernández, Paloma. "La Información Empresarial puede estar Fugándose a través de CD quemados o dispositivos USB". Empresa Segura. En Línea. http://www.bsecure.com.mx/articulo-58-6507-371.html 29 de enero de 2009. Pág. 2

La absorción de datos es un proceso automático simple y no requiere de conocimientos técnicos; un usuario puede conectar el dispositivo portátil de almacenamiento a una estación de trabajo de la empresa y en el tiempo que tomaría el escuchar a un MP3, todos los datos corporativos sensitivos de la estación de trabajo son copiados al dispositivo portátil de almacenamiento.

El robo de información se ha convertido ahora en una gran preocupación para cada empresa y así la prevención de fuga de información está tomando lentamente una mayor porción en el presupuesto tecnologías de información. Esta tendencia es atribuida a dos factores: La oleada de amenazas que están afectando a la industria y el incremento en requisitos regulatorios que demandan más protección y controles más estrictos sobre los registros de clientes y otra información confidencial. Más controles y castigos severos están forzando a las empresas a tomarlas seriamente.

Una concepción errónea compartida por muchas empresas es que las amenazas de seguridad son originadas principalmente desde afuera de la empresa. De hecho, muchos miles de dólares son gastados cada año en firewalls y otras soluciones que aseguren el perímetro de la empresa de amenazas externas.

Sin embargo, las estadísticas muestran que los huecos de seguridad interna están creciendo más rápido que los ataques externos y al menos la mitad de los huecos de seguridad se originan detrás del firewall corporativo. Infortunadamente, los empleados internos son los primeros.[8]

Algunos de los empleados internos les gustaría “absorber” información porque los datos corporativos puede ser rentable en diferentes maneras; modelos, planos de ingeniería, licitaciones, listas de precios, código fuente, esquemas de bases de datos, archivos de sonido, letras y mucho más, toda esta propiedad intelectual valiosa podría ser explotada por individuos o empresas para ganar ventajas comerciales sobre otros competidores. Resumiéndolos, la mal intención, la

[8] GFI Hispania. “Pod Slurping (Absorción pod), Una técnica sencilla para el robo de información”. En Línea. www.gfihispana.com 30 de diciembre de 2008. Pág. 3 y 4

ganancia monetaria y la curiosidad son probablemente los principales motivos detrás del robo de información.

Los empleados insatisfechos que creen que no son respetados o que son explotados por sus empleadores podrían aprovecharse de su posición de confianza y vender planes corporativos y otra información sensitiva a la competencia directa.

Los empleados que sienten que han sido despedidos injustamente podrían utilizar su conocimiento de la estructura interna o explotar las relaciones internas para acceder, robar y exponer públicamente información de clientes y así dañar a la empresa. Empleados internos de confianza pueden también convertirse en informantes pagados para realizar espionaje industrial, guerra de datos u otras actividades fraudulentas tales como “robo de identidad”.

Las empresas están constantemente en riesgo de perder información comparativa sensitiva. El uso no controlado de dispositivos portátiles de almacenamiento dentro de las empresas. Pasa un gran riesgo de seguridad incluyendo el robo de información. Esto es mayormente atribuido al hecho que las empresas tienden a enfocarse más en la seguridad de perímetro e ignoran completamente el enemigo interno, haciendo más sencillo para empleados internos de confianza el robar información corporativa importante.

Para asegurar los datos corporativos y prevenir la absorción de información, los administradores deben tener una forma para controlar tecnológicamente el uso de dispositivos portátiles de almacenamiento, soluciones que da a los administradores el poder para controlar y reportar el uso de esos dispositivos a través de su red.

Según el Instituto Ponemon, el 78% de las filtraciones de datos las cometen los empleados autorizados de una empresa. Tanto la pérdida de información corporativa como las cuestiones de propiedad intelectual son causa de multas, litigios judiciales, y deterioro de la imagen de las empresas algunas han implementado medidas de Protección (VPN, cortafuegos y monitores de red) para proporcionar registros de auditoría y evitar el acceso no autorizado de personas ajenas a la información corporativa. No obstante, estas soluciones no resuelven el problema de las amenazas emergentes causadas por usuarios internos. Un canal

principal para la filtración de datos, bien como consecuencia de la infracción deliberada de políticas o de la pérdida de datos confidenciales (p. ej. pérdida de dispositivos Con registros personales). Al tener acceso a los activos de datos, el personal Interno constituye para proteger la información confidencial, las empresas necesitan una solución eficaz para la prevención frente a la filtración de datos que supervise las posibles filtraciones de información en el momento de su uso. No obstante, la proliferación de sistemas de Mensajería, redes inalámbricas y dispositivos de almacenamiento USB hace que la protección de la información básica resulte cada vez más difícil. En consecuencia, las empresas experimentan actualmente un aumento de la pérdida o del robo de activos de datos por parte de empleados y personal subcontratado, los cuales filtran los datos de forma accidental o intencionada.[9]

Por lo tanto proteger los datos de clientes, pacientes y empleados, las filtraciones de datos que se pueden usar para el robo de identidades y otros delitos, evitar pérdidas y gastos para la subsanación de intrusiones y proteger su posición con respecto a la competencia evitando poner en riesgo la propiedad intelectual.

Entre las reocupaciones informáticas.de las empresas nos encontramos ofrecer controles de tecnologías de información efectivos para evitar que los datos en la actualidad salgan de la red de la organización, ya sea de forma accidental o intencionada, debido a un comportamiento criminal directo a través de: Reforzar la seguridad informática y las políticas de gestión de riesgos mediante la concienciación y la formación de los proveedores de seguridad quienes han creado una serie de productos que únicamente solucionan partes del problema.

Para el global del robo de información y la filtración de datos en las empresas se han implementado cortafuegos, redes VPN, monitores del tráfico de la red, sistemas de filtrado de contenidos de correo electrónico y agentes de

[9] Trend Micro. “Implementación de la Tecnología de Prevención frente a la Filtración de Datos para proteger los Activos Empresariales”. En Línea. http://es.trendmicro.com/imperia/md/content/es/whitepaper/wp01_leakproof_080123es.pdf 15 de enero de 2008. Pág. 1

seguridad. Sin embargo, estos componentes son solo parte de la solución de la ventaja de la prevención de filtraciones de datos

4. Estadística.

Hoy en día, el activo más valioso de una organización son sus intangibles, la mayoría de los cuales se pueden encontrar en sus bases de datos. Estas bases de datos, que han tomado tiempo, esfuerzo y recursos en desarrollarse con frecuencia están libremente expuestas en la red interna al alcance de los usuarios, sin ningún tipo de restricciones, con la posibilidad de que estos se las "roben" sin que nadie se dé cuenta.[10]

En una investigación patrocinada por Mcafee el, 33% de los encuestados consideró que un incidente de pérdida de datos críticos y su distribución accidental o maliciosa pondría en riesgo la supervivencia de la empresa. Y no sólo eso: 61% de los participantes concluyó que la fuga de datos es responsabilidad de ésta. México y Centroamérica no están en mejor posición. De acuerdo a las estadísticas de Mattica, el robo de secretos industriales y de propiedad intelectual es el delito más común con 35% del total de los casos registrados. Le siguen amenazas y difamaciones (30%), fraudes y abusos de confianza (20%), fraudes financieros (10%), pornografía infantil y otros (5%).

Sólo 18% de los robos de secretos industriales y de propiedad intelectual los comenten agentes externos, mientras que 82% de los hurtos son ejecutados por los propios empleados de las empresas. Más que externo, el enemigo es interno.

Velázquez, le atribuye a este problema un porcentaje, 34% de los robos de secretos industriales y propiedad intelectual se pueden efectuar gracias al poco conocimiento que los usuarios tienen de los sistemas de cómputo que utilizan. Y es que un empleado poco capacitado resulta el blanco ideal para hacerlo abrir una página de Internet comprometida, ejecutar un archivo inadecuado activar un virus, desactivar un programa de seguridad o revelar una contraseña

---

[10] Caldas Lemaitre, Rodrigo. "Seguridad Informática ¿Una Política Eempresarial?". En Línea. http://www.acis.org.co/index.php?id=860. 29 de enero de 2009. Pag. 2

Carlos Lang, director de Damage Control, comenta: existen dos grandes grupos de compañías que realmente actúan respecto a prevenir el hurto de propiedad intelectual y secretos industriales, aquellas que verdaderamente tienen algo que proteger y a las que ya les robaron. Pero es poco frecuente encontrar organizaciones donde la información se proteja desde el inicio por su valor.

La forma de perpetrar los robos varía. Unas veces se utilizan dispositivos como USB o celulares con cámara, para registrar y sustraer datos, otras la información sale de las empresas vía mensajería instantánea o por sitios de correo Web gratuitos, menciona el directivo de Mattica.

De acuerdo con esta empresa, en México 63% de las empresas, tanto públicas como privadas, pierden anualmente archivos con información valiosa, en buena parte de los casos, porque el personal extravía equipos portátiles como laptops, smartphones y asistentes personales digitales o dispositivos de almacenamiento como discos compactos y memorias USB.

En el sector público, por ejemplo, lo anterior es ya una verdadera pandemia. De acuerdo con una investigación periodística realizada por Hiroshi Takahashi, entre el primero de enero de 2000 y el primero de mayo de 2007, 22 diferentes dependencias del gobierno federal perdieron 590 computadoras portátiles por extravío o robo.

De hecho, esto último se ha convertido en un verdadero riesgo, porque quienes buscan hurtar información de las empresas saben que una forma es adueñarse de los equipos portátiles.[11]

92% de las organizaciones no capacitan a su personal en materia de prevención y un código de ética a sus empleados 32% de las empresas han sufrido fraudes internos por colusión de sus empleados con clientes y proveedores. La administración de estas compañías reconoció que dichos fraudes detección de fraudes.[12]

En el último año, más de 50% de las empresas mexicanas no he han proporcionado e normalmente una empresa se protege de los de afuera cuando,

---

[11] Sandoval, Hugo. "¡Que no le extraigan su Inteligencia!". B:Secure. En Línea. http://bsecure.com.mx/articulo-53-6575-377.html 30 de Octubre de 2008. Pág. 5

[12] Lang Carlos. Citado por Hugo Sandoval. P. 15.

realmente las personas de las que tiene que cuidarse están dentro de la organización.

4.1 Perdida de datos

EbErnst & Young en una encuesta a 500 empresas mexicanas e internacionales que el 90% acepto haber sufrido algún tipo de fraude y el 80% de ellos fue cometido por empleados internos.[13]

En México el 65% de las empresas ha sufrido ataques informáticas pero el 73% de estas no midió el impacto inmediato o futuro en sus procesos de negocios. El 70% de las pruebas de penetración desde el exterior, realizadas a corporativos y empresas por parte de especialistas, fue un éxito.

En el 99 de ellas se obtuvo acceso de administración en sus sistemas críticos.

El 80% de las empresas que sufren ataques no los denuncia por evitar el detrimento de su imagen o una producción de desventaja frente a sus competidores.[14]

5.- Legislación Mexicana

El Código Penal Federal, en su última reforma publicada en el Diario Oficial de federación del 28-06-2007, establece lo siguiente:

"Artículo 210.- Se impondrán de 30 a 200 jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial

---

[13] Alcántara Castro, María Elena. "La información no tiene Precio". Revista Red. En Línea. http://www.red.com.mx/tema11.php 29 de enero de 2009. Pág. 2

[14] Alcántara Castro, María Elena. Op. Cit. P. 2

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días de multa

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de 100 a 300 días de multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de 50 a 150 días de multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de 300 a 900 días de multa.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de 100 a 600 días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de 50 a 300 días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de 100 a 600 días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que conténgalas penas previstas en este artículo se

incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero".

Algunas recomendaciones adicionales para mantener seguros los datos críticos son:

1.- Ubicar primero donde está la parte a proteger (patentes, fórmulas, derechos de autor, listas de clientes, nóminas de empleados, bases de datos y toda la información que pueda ser considerada como estratégica).

2.- Medir el impacto del robo de la información, para poder determinar cuánto debe invertirse en seguridad. El problema es no contar con métricas o indicadores de ningún tipo para hacerlo.

3.- Elegir una estrategia de protección a seguir, donde se puedan determinar quiénes son los responsables.

4.- Entender que la relación entre seguridad física y seguridad informática no es lineal. De nada sirve contratar policías para resguardar el acceso físico a las instalaciones, si no se cuenta con un esquema de seguridad informática adecuado, les de acceso a la información, y utilizar medidas apropiadas como la encriptación de correos y el manejo de códigos de acceso

5.- El nuevo paradigma de la seguridad tiene que incluir un componente legal. No se puede pensar en una protección al 100% sólo con tecnología. Es necesario, por tanto, proteger la confianza que se deposita en los empleados, mediante la firma de acuerdos de confidencialidad.[15]

[15] Sandoval Hugo. Op. Cit. P. 3

Bibliografía.

1) Absolute. “Estadísticas Sobre el Robo de Ordenadores y su Recuperación. En línea. http://www.absolute.com/EMEA/spanish/computer-theft-statistics-details.asp 29 de enero de 2009 Pág. 1-3
2) Alcántara Castro, María Elena. “La información no tiene Precio”. Revista Red. En Línea. http://www.red.com.mx/tema11.php 29 de enero de 2009. Pág. 1-4
3) Blanco Vigo, Alberto. “Detectives Vigueses investigan el robo informático de datos de empresas”. En Línea. Faro de Vigo. http://www.farodevigo.es/secciones/noticia.jsp?pRef=3119_2_165124_Gram-Vigo-Dete 29 de enero de 2009. Pág. 1-2
4) Caldas Lemaitre, Rodrigo. “Seguridad Informática ¿una política empresarial?”. En Línea. http://www.acis.org.co/index.php?id=860. 29 de enero de 2009. Pag. 1-3
5) Carlton. Jim. “La demanda tecnológica empresarial apunta hacia mas espacio y seguridad”. El Periódico de México. En línea. http://www.elperiodicodemexico.com/nota.php?fecha=2007-10-12&id=140708 29 de enero de 2009. Pág. 1-3
6) Código de Conducta Empresarial de Nestle. www.**nestle**.com/Resource.axd?Id=4E4FCBB4-F08C-4474-95AB-C6513ADED84B 20 de diciembre de 2008. Pág. 1-8
7) “El éxito empresarial, el derecho de autor y el entorno digital”. En Línea. http://www.estudio-juridico.cl/pil.htm 29 de enero de 2009. Pág. 1-4
8) GFI Hispania. “Pod Slurping (Absorción pod)- Una técnica sencilla para el robo de información”. En Línea. www.gfihispana.com 30 de diciembre de 2008. Pág. 1-9
9) Hernández, Paloma. “La Información Empresarial puede estar Fugándose a través de CD quemados o dispositivos USB”. Empresa Segura. En Línea. http://www.bsecure.com.mx/articulo-58-6507-371.html 29 de enro de 2009. Pág. 1-3

http://www.elperiodicodemexico.com/nota.php?fecha=2007-10-12&id=140708 29 de enero de 2009. Pág. 1-3

6) Código de Conducta Empresarial de Nestle. www.**nestle**.com/Resource.axd?Id=4E4FCBB4-F08C-4474-95AB-C6513ADED84B 20 de diciembre de 2008. Pág. 1-8

7) "El éxito empresarial, el derecho de autor y el entorno digital". En Línea. http://www.estudio-juridico.cl/pil.htm 29 de enero de 2009. Pág. 1-4

8) GFI Hispania. "Pod Slurping (Absorción pod)- Una técnica sencilla para el robo de información". En Línea. www.gfihispana.com 30 de diciembre de 2008. Pág. 1-9

9) Hernández, Paloma. "La Información Empresarial puede estar Fugándose a través de CD quemados o dispositivos USB". Empresa Segura. En Línea. http://www.bsecure.com.mx/articulo-58-6507-371.html 29 de enro de 2009. Pág. 1-3

10) Iglesias, Gonzalo. "Régimen Jurídico de los Bancos de Datos. Bases de datos y Marketing Directo: Un análisis de la igualdad de la comercialización de datos de referentes a terceros en el derecho comparado." En línea. Biblioteca Electrónica. http://www.aaba.org.ar/bi130017.htm pág. 1-13

11) López Pulido, Joan Pere. "Marco jurídico de los servicios de la sociedad de las información y el conocimiento, el comercio electrónico. La firma electrónica". En línea http://www.uoc.edu/dt/20156/index.html 29 de enero de 2009. pág. 1-24

12) Mashevsky, Yury. "El robo de propiedad virtual en las redes informáticas, parte II". En Línea. Virtualist.com http://www.virtualist.com/sp/analysis?pubid=207270890 29 de enero de 2009. pág. 1-4

13) Parlamento Europeo y del Consejo. "Directiva 96/9/CE del 11 de marzo del 1996 sobre la Protección jurídica de las bases de datos" en línea. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri_CELEX:31996L0009:ES:HTML 29 de enero de 2009 pag- 1-11

14) Pumarino M., Andrés. "Marco Jurídico de las bases de Datos".

15) Salellas, Luciano. “delitos cibernéticos”. En Línea. http://www.cabinas.net/informatica/delitos_informaticos.asp 29 de enero de 2009. Pág. 1-7

16) Sandoval, Andrés. “Fraude. Una Amenaza Permanente”. Revista empresarial PyMes. En línea. http://www.revistaempresarial.com/phum/index.php?option=com_content&ta sk=view&i 29 de enero de 2009 pág. 1-3

17) Sandoval, Hugo. “¡Que no le extraigan su Inteligencia!”. B:Secure. En Línea. http://bsecure.com.mx/articulo-53-6575-377.html 30 de Octubre de 2008. Pág. 5

18) Trend Micro. “Implementación de la Tecnología de Prevención frente a la Filtración de Datos para proteger los Activos Empresariales”. En Línea. http://es.trendmicro.com/imperia/md/content/es/whitepaper/wp01_leakproof_080123es.pdf 15 de enero de 2008. Pág. 1-11.