INFORME DE INVESTIGACIÓN CIJUL

TEMA: SEGURIDAD DE LA INFORMACIÓN EN EL DERECHO COMPARADO

RESUMEN: En la siguiente investigación se examina el tema de la seguridad de la información en el derecho comparado. Específicamente se analizan los casos español, estadounidense y argentino, en cuanto a la normativa e información relacionada con el tema en estudio. Asímismo, se contempla información de carácter técnico relativa al manejo seguro de la información a través de la red internet.

Índice de contenido

DESARROLLO:

1. Normativa

España

a. Normativa sobre Protección de Datos

[SAN MARTÍN GARCÍA, José Miguel][1]

"La Agencia de Protección de Datos APD fue creada a partir de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, como órgano independiente encargado de velar por el cumplimiento de la misma. Dicho cometido implica el seguimiento de todas aquellas nuevas manifestaciones tecnológicas que puedan afectar al uso de los datos personales de los ciudadanos y a su derecho fundamental de protección de los mismos."

b. Datos Especialmente Protegidos

[SAN MARTÍN GARCÍA, José Miguel][2]

"DATOS ESPECIALMENTE PROTEGIDOS (ART. 7 Y 8 DE LA LEY ORGÁNICA 15/1999)

Existen tres niveles de protección de los datos:

• Datos con nivel de protección Básica: Son todos aquellos datos personales básicos, como nombre, DNI, domicilio, teléfono, e-mail, datos bancarios, datos legales (facturación, contabilidad…), actividades, negocios, licencias comerciales… Las medidas de protección aplicables en este caso son básicamente,la existencia de un Documento de Seguridad y el control de acceso mediante contraseñas a las bases de datos.

• Datos con nivel de protección Media: Son aquellos datos que se refieran a Información sobre infracciones administrativas o penales. Sólo podrán recabarse cuando por razones de interés general lo disponga una ley, o el afectado consienta expresamente (por escrito, salvo otra fórmula probatoria). En este caso, además de las medidas de Seguridad antes citadas, es necesario realizar auditorias periódicas a fin de verificar el cumplimiento de las medidas técnicas y organizativas de Seguridad.

• Datos con nivel de protección Alta: Son aquellos datos referentes a ideología,afiliación sindical, religión o

creencias,origen racial, salud o vida sexual. Nadie podrá ser obligado a declarar sobre estos datos, salvo que el afectado consienta expresamente y por escrito,salvo cuando sean absolutamente necesarios para los fines de una investigación concreta realizada por las Fuerzas y Cuerpos de Seguridad. Existe la obligación de advertir al interesado su derecho a no prestar su consentimiento. Existe la prohibición expresa de crear o mantener ficheros con la finalidad exclusiva de almacenar este tipo de datos. Además de las obligaciones antes citadas, es necesario garantizar en este caso, que la Información no es inteligible o manipulada."

c. Medidas de Seguridad

[SAN MARTÍN GARCÍA, José Miguel][3]

"SEGURIDAD DE LOS DATOS (ART. 9 DE LA LEY ORGÁNICA 15/1999)

El responsable de los datos deberá adoptar las medidas necesarias para mantener la Seguridad de los datos. Deberá evitar concretamente la alteración, pérdida y tratamiento o acceso no autorizado de los datos. Se prohíbe el tratamiento de datos en centros de tratamiento, locales, equipos, sistemas y programas que no reúnan las condiciones adecuadas para garantizar la integridad y Seguridad de los datos.

Por lo que se refiere a los ficheros automatizados de datos les será de aplicación lo previsto en el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

(...)

MEDIDAS DE SEGURIDAD Y REDACCIÓN DEL DOCUMENTO DE SEGURIDAD

El Responsable del Fichero y, en su caso, el Encargado del Tratamiento de los datos, deberán adoptar las medidas técnicas y organizativas necesarias para garantizar la Seguridad de los datos, de forma que se evite su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas que se adopten deben ser acordes con el estado de la técnica en cada momento, con la naturaleza de los datos de carácter personal almacenados en los ficheros y con los riegos a que estén expuestos tales datos, ya sean riesgos procedentes de la acción humana o del medio natural.

Las medidas de Seguridad adoptadas deben constar en el llamado Documento de Seguridad, que debe redactar el Responsable del Fichero. El Documento de Seguridad debe recoger todas las medidas técnicas y organizativas adoptadas en la empresa para garantizar

la Seguridad de los datos almacenados en el fichero. Dicho documento ha de estar a disposición de la Agencia de Protección de Datos,cuando ésta lo solicite."

d. La Seguridad en los Sistemas de Información de las Administraciones Públicas

[MEDINA, Manel][4]

Definición de la política de seguridad

En el caso de las Administraciones Públicas, existe un documento de referencia que puede ser de gran utilidad para definir una política de seguridad:

Criterios de Seguridad, Normalización y Conservación de la información, del MAP

La Secretaria de Estado para la Administración Pública del MAP publicó en Diciembre de 2001 la guía "Criterios de Seguridad de las aplicaciones, de Normalización y Conservación de la información".

El objetivo perseguido es fomentar entre las administraciones públicas el uso de mejores prácticas basadas en normas existentes, como la ISO/IEC IS 17799 "Código de buenas prácticas para la gestión de la seguridad de la información", que constituye una referencia fundamental sobre el tema. De esta forma se pretende que las organizaciones adopten medidas organizativas y técnicas que doten de un nivel de seguridad adecuado a sus sistemas. AENOR está redactando la versión española de esta norma (UNE 717799).

Estos criterios, además, contemplan la legislación aplicable en materia de protección de datos personales.

El documento se estructura en capítulos que siguen la estructura de la norma BS ISO/IEC 17799-2:2000; el contenido de estos capítulos concreta algo más el de la norma, al tratar los siguientes aspectos:

Requisitos de carácter normativo que obligan a aplicar distintas medidas de seguridad.

Criterios a considerar en la aplicación de las medidas, para satisfacer los requisitos anteriores.

Recomendaciones que complementan los criterios expuestos, desarrollando con descripciones de las medidas técnicas u organizativas concretas.

Los niveles de seguridad a que corresponden, según lo definido por el Reglamento de medidas de seguridad de los ficheros automatizados que contiene datos de carácter personal.

Referencias que permiten ampliar conceptos técnicos y organizativos en los que se fundamentan las medidas.

Legislación aplicable: LOPD, LSSICE

Estas políticas de seguridad deben cumplir con los reglamentos de seguridad publicados, para garantizar técnicamente los requisitos legales impuestos por las leyes de Protección de Datos Personales [LOPD] y de Servicios DE la Sociedad de la Información y del Comercio Electrónico [LSSICE= Ley 34/2002 de 11 de julio (BOE 12/VII/02)].

Como resumen debemos decir que la LOPD obliga a que todos los ficheros de datos personales tengan un documento de seguridad, en el que se describan los procedimientos empleados para proteger los datos de usos indebidos. Si dichos datos requieren unas medidas de protección de tipo alto (sanitarios, religión, políticos, etc.), además deberá ser necesaria una auditoria independiente tanto de la calidad de las medidas de protección declaradas, como de su cumplimiento.

La LSSICE exige que los datos publicados en Internet reúnan unas condiciones determinadas, como por ejemplo incluir datos de contacto, Registro Mercantil, etc. La no publicación, o inexactitud de estos datos, puede desencadenar la aplicación de sanciones, y por tanto los servicios de publicación de información en Internet deben cumplir los requisitos de Integridad que permitan garantizar que nadie podrá modificar o eliminar la información requerida por la LSSICE, para perjudicar la imagen de la organización.

Implantación de la política de seguridad

Una vez definida la política de seguridad y determinadas las medidas de protección que es necesario aplicarlas para reducir el riesgo en los sistemas por debajo del nivel de riesgo aceptado por la organización, es necesario planificar la puesta en marcha de estas medidas.

Sin ánimo de ser exhaustivos, a continuación repasaremos las herramientas - técnicas y organizativas - que comúnmente utilizan las aplicaciones de e-Government para ofrecer los servicios de seguridad que precisan.

Disponibilidad 24x7

Cuando se ofrece un servicio con altos requisitos de disponibilidad debe plantearse la necesidad de establecer contratos con varios proveedores de un mismo servicio, de forma que si no podemos disponer de uno por cualquier avería o fallo,

podamos restablecer la normalidad en el mínimo tiempo posible, sin depender de que ellos resuelvan su problema.

En el caso del suministro eléctrico es una buena opción contratarlo a dos compañías diferentes, y alternar semanalmente el uso de una y otra, ya que así aseguramos que ambas conexiones funcionan y que nuestros técnicos saben cambiar de conexión sin problemas -reduciendo significativamente el tiempo de respuesta en caso de fallo-. Lo mismo puede plantearse con el suministro de climatización de los CPDs. En cuanto a los proveedores de red, mantener contratos con diferentes compañías es una manera rápida y efectiva de restablecer el servicio tras sufrir un ataque de denegación de servicio (DoS) sobre los servidores web. Pero podría ser que fueran nuestros sistemas los que fallaran; sabemos que los fallos técnicos de los elementos hardware son más frecuentes de lo deseado. Para ser capaces de restablecer -e incluso de no interrumpir- el servicio cuando eso ocurre es necesario mantener réplicas de los elementos críticos del sistema, preparados para entrar en funcionamiento en cualquier momento -o, como habitualmente se denomina, mantener redundancia HW-.

Cumplimiento con la LOPD

La LOPD no sólo establece cómo deben tratar las empresas privadas los ficheros que contienen datos de carácter personal, sino que también define cómo deben hacerlo las Administraciones públicas, y distingue ambos casos -siendo conscientes de que, con frecuencia, la información de carácter personal que éstas manejan es más sensible que la que acostumbran a gestionar la mayoría de las empresas privadas-. Así, por ejemplo, el órgano regulador para los ficheros de titularidad privada es la Agencia de protección de Datos -de ámbito estatal-, mientras que para los ficheros de titularidad pública se contempla la creación de Agencias autonómicas. En Cataluña se ha aprobado ya la creación de la Agencia Catalana de Protecció de Dades.

El cumplimiento con lo establecido en el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal plantea la necesidad de aplicar mecanismos de protección, entre los que cabe citar:

El Control de Acceso: hay que identificar a quien intenta acceder a la información, para poder determinar si tiene derecho a hacerlo, y para poder registrar (si la sensibilidad de los datos lo requiere) las operaciones que realiza sobre ellos.

Los mecanismos para identificar a un usuario son variados, como lo son los niveles de protección que ofrecen. Los más comunes (en orden creciente de seguridad) son:

El uso de un nombre de usuario y una contraseña. Este sistema

requiere una gestión de contraseñas adecuada -como exigir ciertas características sobre ellas: longitud, tipo de caracteres -numéricos y alfanuméricos- que contienen, que no sean palabras que puedan encontrarse en diccionarios, etc; y también sobre su protección: cifrado del fichero del sistema que almacena las contraseñas de todos los usuarios, renovación periódica o contraseñas de un solo uso, no revelación a compañeros, no anotarlos, etc.

El uso de certificados digitales blandos, que son aquellos que almacenan la clave privada en soporte disquete, en el disco duro de un ordenador, etc.

Habitualmente se realiza una comprobación de la identidad de la persona que solicita el certificado, y de su derecho a poseerlo; sin embargo, si alguien más que el titular del certificado tuviera acceso físico al soporte donde se almacena la clave privada, podría acceder sin problema a dicha clave y utilizarla para realizar operaciones en nombre del titular del certificado, suplantando su identidad.

Certificados de este tipo son los que la Agencia Estatal de Administración Tributaria (AEAT) emite a los ciudadanos que lo solicitan, para poder realizar trámites (como la presentación de declaraciones de IRPF, pago de impuestos, etc) a través de su Oficina Virtual.

El uso de certificados duros, que son aquellos que almacenan la clave privada en tarjetas chip (criptográficas o de memoria), teléfono móvil, PDA, etc. Para acceder a la clave almacenada en estos dispositivos es necesario que el titular introduzca un PIN de cuatro dígitos; así la protección depende de algo que el titular tiene y de algo que sabe. Certificados de este tipo son los emitidos por las Cámaras de comercio, o por la Agencia de Certificació Catalana.

El acceso seguro al sistema: hay que garantizar que un usuario solamente accede a la información a la que tiene derecho a acceder, a la información autorizada, y para realizar sobre ella las operaciones autorizadas. Para implantarlo puede pensarse en sistemas que gestionan los privilegios de los usuarios (o los poderes o derechos). El sistema desarrollado dentro del proyecto PERMIS -puesto en marcha por el Ayuntamiento de Barcelona para la gestión de multas de tráfico impuestas a conductores de coches de alquiler, es un ejemplo de aplicación que garantiza el acceso seguro a la información, gestionando los derechos de acceso de un grupo de usuarios amplio. La aplicación desarrollada permite que las compañías de alquiler de coches puedan consultar en los sistemas de información del Ayuntamiento si se ha impuesto alguna multa a un coche, para así incluir el importe de dicha multa en

la factura final que se cobra al conductor -en lugar de tener que asumir la multa las compañías de alquiler-.

Otra forma de conseguir que sólo los usuarios autorizados accedan a la información protegida es cifrándola, y distribuyendo los mecanismos necesarios para descifrarla e interpretarla sólo entre estos usuarios. Este último detalle (distribución de las claves para descifrar) hacen que este mecanismo sólo sea apropiado para gestionar los privilegios de un grupo reducido de usuarios autorizados. Por último, queremos recordar que este acceso seguro debe implementarse no sólo sobre la información que está en producción en el sistema, sino también sobre la información registrada en copias de respaldo y la de archivo, por lo que es necesario desarrollar sistemas de almacén seguro -de los que hablaremos más adelante-.

Un último mecanismo (este ya de carácter organizativo) que protege los datos de carácter personal manejados por las AAPP son los contratos que están obligados a establecer con terceras partes si se disponen a cederles estos datos. Haciéndolo de esta forma, el usuario puede confiar en que sus datos están bajo control, que solamente serán tratados por quienes sea necesario y con finalidades conocidas y lícitas.

Almacén seguro de información

Uno de los problemas de seguridad más claros que plantea la puesta en marcha de aplicaciones de e-Government es la necesidad de poder conservar a largo plazo gran número de documentos en soporte electrónico (cuando menos, los equivalentes a los que en la actualidad se archivan y almacenan en soporte papel); por ejemplo: expedientes, licencias, multas, permisos, censo, etc.

La solución apuntada es la puesta en marcha de un almacén seguro de información, que ofrezca los siguientes servicios de seguridad:

Confidencialidad de la información histórica, para que la solamente el personal autorizado tenga acceso a ella. Se consigue cifrándola y protegiendo adecuadamente (en caja fuerte, por ejemplo) las claves necesarias para descifrarla.

Integridad: para poder determinar si se ha alterado de forma ilícita la información almacenada podemos aplicar varios mecanismos de seguridad. El primero es recabar Registros de actividad (logs), que permitan analizar y reportar los accesos realizados sobre la información, conociendo quién accedió a ella, en qué instante de tiempo y qué operación (consulta, actualización o borrado) realizó.

Además pueden aplicarse herramientas que calculan un resumen (o hash) de la información y lo cifran con una clave que se protege

convenientemente, de forma que puede detectarse cualquier modificación de la información, puesto que al calcular de nuevo el resumen, el resultado obtenido es diferente al que se almacena cifrado. Otras herramientas, yendo más allá, permiten firmar electrónicamente las copias de respaldo.

Disponibilidad: el objetivo final de este almacén seguro es garantizar que, transcurridos unos años desde la creación de los documentos, si es necesario, podrán volver a consultarse. Para ello es imprescindible definir unos procedimientos de gestión de copias de respaldo (backups) adecuados, que tengan en cuenta el volumen de documentos a gestionar y su tamaño, las tecnologías de respaldo disponibles, y que no olviden que - en caso de cambiarse la aplicación que gestionaba los documentos- debe mantenerse en algún ordenador una copia de la aplicación reemplazada que permita restaurar y acceder a los documentos históricos.

Trámites seguros: Firma electrónica

Poco a poco va consolidándose la confianza de los ciudadanos en un mecanismo que les ofrece suficiente seguridad técnica y les parece de uso sencillo, y es la firma electrónica.

Este mecanismo de seguridad es la clave para poder establecer relaciones comerciales y contractuales a través de Internet, aunque es imprescindible que sea aceptada como la firma manuscrita, con las mismas condiciones legales y comerciales.

En ese sentido, tanto la Directiva Europea 1999/93/CE como el Real Decreto-Ley 14/1999 sobre firma electrónica consideran estos aspectos. En el caso de la ley española, se considera que una firma electrónica, basada en un certificado electrónico reconocido que cumpla las condiciones estipuladas (artículo 8 sobre los requisitos para la existencias de un certificado reconocido, y articulo 20 sobre normas técnicas), debe tener "...el mismo valor jurídico que la firma manuscrita... y será admisible como prueba en juicio" (artículos 3.1.y 3.2 de la misma ley). Por su parte, la Directiva Europea sobre firma electrónica contempla un formato de firma que pueda utilizarse como medio de autenticación, así como un formato particular de firmas electrónicas avanzadas (o cualificadas), cuya validez legal es equivalente a la de una firma manuscrita.Además, la aprobación del Decreto 324/2001 de la Generalitat de Catalunya, relativo a las relaciones entre los ciudadanos y la Administració de la Generalitat de Catalunya a través de Internet, destaca la firma electrónica como mecanismo clave para asegurar estas comunicaciones. Concretamente, el decreto establece que "...las comunicaciones y notificaciones telemáticas... serán válidas siempre que exista constancia de la transmisión y de la recepción, de sus datos y del contenido íntegro de las comunicaciones... y se identifique el remitente y

el destinatario de la comunicación" (artículo 14). Además, en el artículo 15 se especifica que "...para iniciar un procedimiento administrativo mediante un sistema telemático, los interesados deberán ser titulares de un certificado digital reconocido, que contenga la información y reúna los requisitos que prevé en los artículos 8 y 12 del Real Decreto-Ley 14/1999". A continuación, el artículo 15 indica que los certificados digitales "...podrán ser residir en cualquier dispositivo o soporte físico que permita almacenarlos con garantías de protección... y bajo el control exclusivo del titular del certificado digital". Finalmente, se reconocerán certificados emitidos por cualquier entidad prestadora de servicios de certificación digital acreditada o reconocida por la Generalitat de Catalunya.

Cuando se firma digitalmente un documento, su validez legal depende de tres aspectos fundamentales: El proceso de firma, El proceso de generación de certificados, El derecho del firmante a firmar el documento con la clave privada correspondiente

Evaluación de la eficacia de los mecanismos de seguridad aplicados

Una vez se han aplicado los mecanismos de protección según lo planeado, es recomendable evaluar por primera vez la eficacia de las medidas implantadas. Como referencia pueden seguirse los procedimientos recomendados por:

MAGERIT (Análisis de Riesgos Residual)

Esta metodología recomienda repetir ahora algunos de los procedimientos del Análisis de Riesgos: la estimación de las vulnerabilidades ante cada amenaza y la del impacto que la materialización de éstas tendría sobre el sistema, pero considerando las medidas de protección aplicadas (con la intención de reducir alguno de los tres factores del riesgo). Los riesgos así calculados son los denominados riesgos residuales. Comparándolos con los calculados al inicio del proceso (riesgo intrínseco) obtenemos una medida de la eficacia de las medidas aplicadas, tanto más real cuanto más acertadas sean las estimaciones realizadas.

Estas valoraciones pueden servir, por un lado, como argumento para justificar la inversión en medidas de seguridad y para calcular el retorno de la inversión (ROI); por otro, para determinar si, realmente, hemos conseguido el nivel de riesgo que esperábamos cuando decidimos cuáles iban a ser las medidas a implantar. De no ser así, debería revisarse si ello es debido a algún error durante la implantación (configuraciones incorrectas o incompletas, etc) o, simplemente, a un error en la estimación -optimista- de la eficacia de las medidas. Si se decide que ésta última es la causa, debe repetirse el procedimiento de interpretación del riesgo

-partiendo de la situación actual, del riesgos residual - y el de identificación y selección de salvaguardas, para luego planificar la implantación de nuevas medidas de protección complementarias.

Controles del BS 7799-2:2002

Esta norma ofrece, en su parte 2, una serie de controles que, agrupados por objetivos, contempla todos los aspectos que debe cubrir un sistema de gestión de la seguridad de la información. Es importante destacar que estos controles no son todos de carácter técnico, sino que hay varios grupos de controles referidos a medidas de protección que son de carácter organizativo.

Revisar un sistema de información contra esta norma revelará, no sólo si hemos aplicado las medidas de protección adecuadas -proporcionadas al riesgo calculado -sino que veremos también si estamos preparados para gestionarlas adecuadamente. Y este último detalle es la gran aportación, a nuestro entender, de la norma: incidir en el hecho de que los mecanismos de protección deben gestionarse, mantenerse, actualizarse, monitorizarse continuamente para asegurar que siguen siendo eficaces, y que se adaptan a la realidad siempre cambiante del sistema de información.

Por supuesto, la norma contempla la posibilidad de que esta gestión de la seguridad sea encargada a terceras partes, como parte de la externalización de servicios de una organización, siendo conscientes de que esta es la tendencia actual.

Otras métricas

Parece comúnmente aceptado que el tiempo y la actualización insuficiente de los sistemas de información y de sus mecanismos de protección, juegan en contra de la seguridad, y aumentan el riesgo de sufrir un incidente de seguridad. Y parece también cada vez más necesario contar con métricas para estimar el riesgo y la seguridad contra el tiempo y la inactividad de los administradores de sistemas.

En este sentido, la iniciativa Open Source Security Testing Methodology Manual (OSSTMM), define el concepto de RAVs (Risk Assessment Values) como la degradación de la seguridad dentro un ciclo de vida de gestión de esta seguridad que esté basado en mejores prácticas de revisiones periódicas. Esta métrica considera una serie de controles -definidos en el manual- que abarcan tanto aspectos técnicos como organizativos (procedimientos y políticas).

Matemáticamente los RAVs dependen de tres factores: El nivel de degradación de cada módulo (respecto al nivel de protección óptimo), el ciclo -o tiempo máximo que puede tardar en degradarse hasta alcanzar un nivel cero-, y varios pesos que dependen de las áreas de proceso de alarma, visibilidad, acceso, etc.

A partir de esto, definen una fórmula matemática para calcular el RA y, sobre cada uno de los módulos especificados en el manual, asignan un ciclo y un nivel de degradación. Así, por ejemplo, para el control que revisa la"Seguridad física" (y cuyo objetivo es determinar si es posible tener acceso a las instalaciones y activos de la organización aprovechando alguna vulnerabilidad de su localización o de sus medidas de protección física) se estipula un ciclo de 180 días, y un nivel de degradación del 7'9%; mientras que para el control "Búsqueda y comprobación de vulnerabilidades"- referido a seguridad en Internet-, cuyo objetivo es la identificación, comprensión y verificación de puntos débiles, configuraciones inapropiadas y vulnerabilidades de un host o red, el ciclo definido es de 3 días y el nivel de degradación es 3'6%.

Argentina

a. Ley de Protección de Datos Personales[5]

"Capítulo I

Disposiciones Generales

ARTÍCULO 1°.- (Objeto).

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

ARTÍCULO 2°.- (Definiciones).

A los fines de la presente ley se entiende por:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- Datos sensibles: Datos personales que revelan origen racial y

étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personal sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Capítulo II

Principios generales relativos a la protección de datos

ARTÍCULO 3°.- (Archivos de datos - Licitud).

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

ARTÍCULO 4°.- (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

ARTÍCULO 5°.- (Consentimiento).

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6º de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento

nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

ARTÍCULO 6°.- (Información).

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

ARTÍCULO 7°.- (Categoría de datos).

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones

respectivas.

ARTÍCULO 8°.- (Datos relativos a la salud).

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

ARTÍCULO 9°.- (Seguridad de los datos).

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

ARTÍCULO 10.- (Deber de confidencialidad).

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

ARTÍCULO 11.- (Cesión).

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el artículo 5° inciso 2;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

ARTÍCULO 12.- (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

(...)

Capítulo IV

Usuarios y responsables de archivos, registros y bancos de datos

ARTÍCULO 21.- (Registro de archivos de datos. Inscripción).

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

ARTÍCULO 22.- (Archivos, registros o bancos de datos públicos).

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de

aquéllas;

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Organos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

ARTÍCULO 23.- (Supuestos especiales).

1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquéllos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

ARTÍCULO 24.- (Archivos, registros o bancos de datos privados).

Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán

registrarse conforme lo previsto en el artículo 21.

ARTÍCULO 25.- (Prestación de servicios informatizados de datos personales).

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales

tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

ARTÍCULO 26.- (Prestación de servicios de información crediticia).

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

ARTÍCULO 27.- (Archivos, registros o bancos de datos con fines de publicidad).

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

ARTÍCULO 28.- (Archivos, registros o bancos de datos relativos a encuestas).

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

Capítulo V

Control

ARTÍCULO 29.- (Órgano de Control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

ARTÍCULO 30.- (Códigos de conducta).

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a

asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia."

b. Aspectos Técnicos de la Administración de la Seguridad

[SEGU-INFO][6]

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

Autenticación: se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización: es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Auditoría: se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda (proactividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados.

Sistemas de detección de intrusos: son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

Sistemas orientados a conexión de red: monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

Sistemas de análisis de vulnerabilidades: analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La

"desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.

Sistemas de protección a la privacidad de la información: herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red.

Podemos considerar que estas capas son:

Política de seguridad de la organización.

Auditoría.

Sistemas de seguridad a nivel de Router-Firewall.

Sistemas de detección de intrusos.

Plan de respuesta a incidentes.

Penetration Test.

Penetration Test, Ethical Hacking o Prueba de Vulnerabilidad

"El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos." (*)

El objetivo general del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas

puntuales sobre algunos ámbitos particulares de la empresa.

El Penetration Test se compone de dos grandes fases de testeo:

Penetration Test Externo: el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

Pruebas de usuarios y la "fuerza" de sus passwords.

Captura de tráfico.

Detección de conexiones externas y sus rangos de direcciones.

Detección de protocolos utilizados.

canning de puertos TCP, UDP e ICMP.

Intentos de acceso vía accesos remotos, módems, Internet, etc.

Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.

Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.

Prueba de ataques de Denegación de Servicio.

Penetration Test Interno: este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

Análisis de protocolos internos y sus vulnerabilidades.

Autenticación de usuarios.

Verificación de permisos y recursos compartidos.

Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).

Test de vulnerabilidad sobre las aplicaciones propietarias.

Nivel de detección de la intrusión de los sistemas.

Análisis de la seguridad de las estaciones de trabajo.

Seguridad de la red.

Verificación de reglas de acceso.

Ataques de Denegación de Servicio

HoneyPots-HoneyNets

Estas "Trampas de Red" son sistemas que se activan con la

finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural.

Actualmente un equipo de Honeynet Project (**) trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

"Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos (...). Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los 'fascinantes programas' que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen", dijo Dan Adams. "Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas" (***).

Esta última frase se está presentando a menudo en el tema de la investigación (y vigilancia) electrónica. Este es el caso del ex-director del proyecto Honeynet J. D. Glaser, quien renunció a su puesto después de aclarar que está convencido "que la vigilancia electrónica no es correcta, aunque se utilice en aras de la investigación (...). Ampliar un Honeynet es parecido a entrampar los derechos de otros, aunque sean los derechos de un delincuente."

Estados Unidos

a. Federal Information Security Management[7]

“TITLE III—INFORMATION SECURITY.

301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the Federal

ormation Security Management Act of 2002.

(b) INFORMATION SECURITY.—

IN GENERAL.— Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

SUBCHAPTER III—INFORMATION SECURITY

541. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(...)

§3546. Federal information security incident center

(a) IN GENERAL.—The Director shall ensure the operation of a central Federal information security incident center to—

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;

and

(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) NATIONAL SECURITY SYSTEMS.— Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

§3547. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.”

FUENTES CITADAS:

1 SAN MARTÍN GARCÍA, José Miguel. La Seguridad de la Información. Lagislación Actual de Seguridad de la Información. Consultada el 16 de mayo de 2007. Disponible en: https://www.icai.es/contenidos/publicaciones/anales_get.php?id=223

2 SAN MARTÍN GARCÍA, José Miguel. La Seguridad de la Información. Lagislación Actual de Seguridad de la Información. Consultada el 16 de mayo de 2007. Disponible en: https://www.icai.es/contenidos/publicaciones/anales_get.php?id=223

3 SAN MARTÍN GARCÍA, José Miguel. La Seguridad de la Información. Lagislación Actual de Seguridad de la Información. Consultada el 16 de mayo de 2007. Disponible en: https://www.icai.es/contenidos/publicaciones/anales_get.php?id=223

4 MEDINA, Manel. La seguridad en los Sistemas de Información de las Administraciones Públicas. ¿Qué medidas aplicar? ¿Cómo gestionarlas? Gobernanza y Seguridad Sostenible. Consultado el 16 de mayo de 2007. Disponible en: http://www.iigov.org/ss/article.drt?edi=13547&art=13721

5 Ley Número 25326. República Argentina, 4 de octubre de 2000. Asociación de Seguridad de la Información de la República Argentina. Consultada el 16 de mayo de 2007. Disponible en: http://www.asira.org.ar/07bas_protec_ley25326.htm

6 SEGU-INFO.COM. Consultada el 16 de mayo de 2007. Disponible en: http://www.segu-info.com.ar/proteccion/vulnerar.htm

7 Federal Information Security Management, Act of 2002 (FISMA). Consultada el 16 de mayo de 2007. Disponible en: http://www.cms.hhs.gov/InformationSecurity/12_Laws_Regs.asp