OBJETIVO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tecnología

Magatem

18-03-2016

Susana Noemí Tomasi

INTRODUCCIÓN

Cada vez más los dispositivos de computación forman parte general en las diversas actividades del ser humano y de las organizaciones públicas y privadas y la documentación y archivos conteniendo información en los equipos de cómputo es tan importante y vital como el equipo de cómputo en sí.

Tal es el valor de la información que se la preserva como un activo personal y de las empresas y al mismo tiempo es un recurso invalorable, ya que sin él las organizaciones ya no pueden operar y por tanto es excesivamente significativo su gestión y resguardo.

El progresivo aumento de los negocios y la economía a nivel global, ha acrecentado la exigencia en las organizaciones a efectuar una apertura respecto al entorno que las rodea y por lo tanto de disponer de información íntegra y confiable en el momento adecuado, pero además esta información debe ser confidencial, no debe ser observada por ajenos a dichos negocios.

Debido al aumento en la diversidad de los movimientos económicos y negocios de los entes y a la respuesta requerida en forma inmediata, la única forma de disponer del recurso de la información es contando con sistemas de información seguros a los que se pueda acceder en el momento requerido, de manera tal que la organización se encuentre en la delantera tecnológica y garantice a los usuarios de estos sistemas, la seguridad necesaria respecto a su utilización y a los requerimientos de un mercado cada vez más profesionalizado.

Para lograr estas finalidades, todas las organizaciones, no importa el tamaño, deben contar con políticas debidamente desarrolladas respecto a la seguridad de la información.

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN – SU OBJETIVO

Es puntualizar las exigencias indispensables mínimas para la utilización eficiente y el resguardo de la información, de los archivos y equipos, de los sistemas, etc. y proporcionar el marco necesario para el desarrollo de todas las actividades relacionadas con la seguridad dentro de la Organización.

Que abarca, la seguridad integral, física, e informática tanto de los bienes y equipos como del personal que forma parte de la misma.

Como consecuencia de lo especificado anteriormente, un objetivo básico de las políticas de seguridad de la información es garantizar la

- Confidencialidad de la Información
- Integridad de la misma.
- Disponibilidad, para el momento en que sea requerida.
- No repudio.
- Legalidad
- Confiabilidad de la Información

CONFIDENCIALIDAD

Se debe cumplir con la ley 24766 de 1996, de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.

Según lo especificado en la misma, las personas físicas o jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honesto, mientras dicha información reúna las siguientes condiciones:

a) Sea secreta en el sentido de que no sea, como cuerpo o en la configuración, reunión precisa de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y

b) Tenga un valor comercial por ser secreta; y

c) Haya sido objeto de medidas razonables, en las circunstancias, para mantenerla, secreta, tomadas por la persona que legítimamente la controla.

Se considerará que es contrario a los usos comerciales honestos el incumplimiento de contratos, el abuso de confianza, la instigación a la infracción y adquisición de información no divulgada por terceros que supieran o no, por negligencia grave, que la adquisición implicaba tales prácticas.

La presente ley es de aplicación con respecto a la información que conste en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares.

Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información que reúna las condiciones enumeradas en el artículo 1° y sobre cuya confidencialidad se los haya prevenido, deberá abstenerse de usarla y de revelarla sin causa justificada o sin consentimiento de la persona que guarda dicha información o de su usuario autorizado.

Además por disposición 74/2006, se define respecto a Confidencialidad que se debe garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

INTEGRIDAD

En la misma disposición 74/2006, se define respecto al término integridad, que se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Microsoft, indica que “la integridad de datos se refiere a los valores reales que se almacenan y se utilizan en las estructuras de datos de la aplicación. La aplicación debe ejercer un control deliberado sobre todos los procesos que utilicen los datos para garantizar la corrección permanente de la información.

Es posible garantizar la integridad de los datos mediante la implementación escrupulosa de varios conceptos clave, como los que se incluyen a continuación:

- Normalizar datos: Explica el proceso que consiste en perfeccionar las definiciones de datos para eliminar grupos repetidos y dependencias innecesarias.

- Definir reglas de empresa, para el acceso a los datos: Explica la forma en que las reglas de empresa controlan la manipulación de los datos de la aplicación y pueden ser reutilizadas por otras aplicaciones.

- Proporcionar integridad referencial: Describe la forma en que la integridad referencial evita que se dañen los datos.

- Validar los datos: Explica la comprobación de intervalos, la validación de campos y formas más complejas de validación de datos.

DISPONIBILIDAD

En la misma disposición 74/2006, se define respecto al término disponibilidad, que se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Es la particularidad, condición o circunstancia de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos usados para recopilar y procesar la información, los exámenes y las revisiones de seguridad utilizados para resguardarlos y los conductos de transmisión válidos de que se disponen para acceder a dicha información deben estar funcionando en forma adecuada.

Se deben evitar las interrupciones del servicio debido a cortes de energía, fallos de hardware, actualizaciones del sistema, problemas técnicos o fallas humanas.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requieran. Tales mecanismos se implementan en infraestructura tecnológica,

servidores de correo electrónico, de bases de datos y de servicios web, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que se desee proteger y el nivel de servicio que se quiera proporcionar.

NO REPUDIO

Garantizar el no repudio de mensajes o transacciones electrónicas y se encuentra estandarizado a través de la norma ISO-7498-2.

Proporciona la prueba ante una tercera parte de que cada una de las entidades que se comunican, puedan denegar el haber participado en parte o en toda la comunicación. Se han definido dos modalidades del servicio:

- Los servicios de no repudio con prueba de origen sirven para proporcionar al destinatario una prueba del origen de los datos.

- Los servicios de no repudio con prueba de destino sirven para proporcionar al emisario una prueba de que los datos se han entregado al destinatario.

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje.

LEGALIDAD

En la misma disposición 74/2006, se define respecto al término referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones.

O sea, dentro de los objetivos de las políticas de seguridad de la información se encuentran cumplimentar las siguientes leyes:

LEY 11723
Artículo1º — A los efectos de la aplicación del presente decreto y de la demás normativa vigente en la materia:

a) Se entenderá por obras de software, incluidas entre las obras del artículo 1º de la ley 11.723, a las producciones constituidas por una o varias de las siguientes expresiones:
I. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación;
II. Los programas de computación, tanto en su versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por el computador;
III. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.
b) Se entenderá por obras de base de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.
c) Se considerarán procedimientos idóneos para reproducir obras de software o de base de datos a los escritos o diagramas directa o indirectamente perceptibles por los sentidos humanos, así como a los registros realizados mediante cualquier técnica, directa o indirectamente procesables por equipos de procesamiento de información.
d) Se considerará que una obra de software o de base de datos tiene el carácter de publicada cuando ha sido puesta a disposición del público en general, ya sea mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente o mediante la oferta generalizada de su transmisión a distancia con fines de explotación.
e) Se considerará que una obra de software o de base de datos tiene el carácter de inédita, cuando su autor, titular o derechohabiente la mantiene en reserva o negocia la cesión de sus derechos de propiedad intelectual contratando particularmente con los interesados.
Art. 2º — Para proceder al registro de obras de base de datos publicadas, cuya explotación se realice mediante su transmisión a distancia, se depositarán amplios extractos de su contenido y relación escrita de su estructura y organización, así como de sus principales características, que permitan a criterio y riesgo del solicitante individualizar suficientemente la obra y dar la noción más fiel posible de su contenido.
Art. 3º — Para proceder al registro de obras de software o de base de datos que tengan el carácter de inéditas, el solicitante incluirá bajo sobre lacrado y firmado todas las expresiones de la obra que juzgue convenientes y suficientes para identificar su creación y garantizar la reserva de su información secreta.

LEY 25036:

ARTICULO 1° -Modifícase el artículo 1° de la Ley 11.723, el que quedará redactado de la siguiente manera:

Artículo 1°: A los efectos de la presente ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas; en fin, toda producción científica, literaria, artística o didáctica, sea cual fuere el procedimiento de reproducción.

La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.

Articulo 2° -Incorpórase como inciso d) del artículo 4° de la ley 11.723 el siguiente texto:

Artículo 4°:...

d) Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

Articulo 3° -Incorpórase como segundo párrafo del artículo 9° de la ley 11.723 el siguiente texto:

Artículo 9°:...

Quien haya recibido de los autores o de sus derecho-habientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo.

Dicha copia deberá estar debidamente identificada, con indicación del licenciado que realizó la copia y la fecha de la misma. La copia de salvaguardia no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

Articulo 4° -Incorpórase como artículo 55 bis de la ley 11.723 el siguiente texto:

Artículo 55 bis: La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción.

Articulo 5° -Incorpórase como artículo 57, in fine, de la ley 11.723 el siguiente texto:

Artículo 57, in fine: Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación.

LEY 24766 – De confidencialidad (30-12-1996) especificada anteriormente.

LEY 25326 - Que 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. Siendo que un dato personal es cualquier dato que pertenezca a una persona o a una persona jurídica.

DECRETO 1558/2001- A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

DISPOSICIÓN 2/2003- Habilita el Registro Nacional de Bases de Datos, que pasa a ser obligatorio para todas las bases de datos, por la Ley Nº 25.326 que 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.

DISPOSICIONES 1/2004, 3/2004, 6/2006, 8/2006, 5/2008, 6/2008, 12/2010, respecto a los Tratamientos de datos personales para la difusión pública.

LEY 26032:
ARTICULO 1° — La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión.

LEY 26388:
Artículo 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.
Articulo 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:
Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.
Articulo 3º — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:
"Violación de Secretos y de la Privacidad"
Articulo 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:
Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Articulo 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Articulo 6º — Sustitúyese el artículo 155 del Código Penal, por el siguiente:

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Articulo 7º — Sustitúyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Articulo 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Articulo 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:

Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Articulo 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Articulo 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente:

Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Articulo 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente:

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

Articulo 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

Articulo 14. — Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

Incluyo la legislación de Argentina, pero es válido para la legislación de cualquier país.

Análisis de la normativa vigente y si se cumplimenta:

1. Que todo el software utilizado en la organización ha sido adquirido legalmente o corresponde a software libre, si no se cumplimenta en la actualidad, verificación de la manera de cumplimentarlo.

2. Si la confidencialidad se encuentra verificada en su totalidad, como marca la legislación vigente, que el personal de la firma, no tenga posibilidades de vulnerar la misma.

3. Si las bases de datos han sido registradas en el Registro Nacional de Bases de Datos, en caso contrario manera de implementarlo.

4. Si se verifica que el personal empleado no viola la legislación de Delitos informáticos, y si no se cumplimenta en la actualidad, procedimiento para cumplimentarlo.

CONFIABILIDAD DE LA INFORMACIÓN

En la misma disposición 74/2006, se define respecto al término es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

PARA CUMPLIR LOS OBJETIVOS SE DEBEN PROPORCIONAR:

INSTAURACIÓN, ORDENACIÓN Y METODOLOGÍA DE LA SEGURIDAD

Conducente a proporcionar seguridad de la información dentro cada organización y establecer un marco gerencial para controlar su instauración, ordenación e implementación de la misma.

CATEGORIZACIÓN Y OBSERVACIÓN DE ACTIVOS

Propuesto para salvaguardar los activos de cada ente. Para ello se deberán tener auditados los mismos y clasificados en su nivel de riesgo a fin de evaluar las medidas de seguridad necesarias al respecto.

PROTECCIÓN DE ERRORES O ILÍCITOS DEL PERSONAL

Orientado a reducir los riesgos de error humano, comisión de ilícitos o uso inadecuado de instalaciones del ente, por parte del personal propio o de terceros que interactúen en la organización.

SEGURIDAD FÍSICA Y AMBIENTAL

Destinada a impedir accesos no autorizados, daños e interferencia a las sedes del ente. Abarca además la seguridad física del personal que trabaja en la organización sea propio o terceros, y clientes, proveedores, etc. Que se encuentren en la misma en el momento de algún suceso que interfiera en la seguridad.

CUIDADO DE LAS COMUNICACIONES Y LAS OPERACIONES

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

OBSERVACIÓN DE ACCESO

Conducente a controlar el acceso a la información y a los lugares físicos desde donde la misma es transmitida.

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Encaminado a garantizar la incorporación de medidas de seguridad en los sistemas de información.

GERENCIAMIENTO DE LA GESTIÓN DE CONTINUIDAD DE LAS ACTIVIDADES DEL ENTE

Enfocado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

El objetivo general de las políticas de seguridad de la información es facilitar el cumplimiento de las metas de cada organización, sin interrupciones, ni complicaciones legales, salvaguardando todos los activos de cada ente.

Y ante sucesos inesperados contar con las medidas necesarias para que el organismo pueda continuar sus actividades en el menor plazo posible, sin afectarlo económicamente.

BIBLIOGRAFÍA

Decreto 1558/2001, (29/11/2001) Protección de datos personales, reglamentación de la Ley Nº 25.326, Argentina.

Disposición 2/2003 (27/11/2003) Registro nacional de bases de datos, su creación - primer censo nacional, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 1/2004, (26/02/2004) Protección de datos personales. Primer censo nacional de archivos, registros y bases de datos, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 3/2004, (30/04/2004), Tratamientos de datos personales para la difusión pública, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 6/2006, (31/03/2006), Tratamientos de datos personales para la difusión pública, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 8/2006, (24/05/2006), Tratamientos de datos personales para la difusión pública, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 74/2006, (02/11/2006), Consejo Nacional de Coordinación de Políticas Sociales, en el Manual de Políticas de Seguridad de los Sistemas de Información del Sistema de Identificación Nacional Tributario y Social (SINTyS) y sus Procedimientos, Argentina.

Disposición 5/2008, (29/05/2008), Normas de Inspección y Control de la Dirección Nacional de Protección de Datos Personales, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 6/2008, (04/07/2008), Tratamientos de datos personales para la difusión pública, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Disposición 12/2010, (18/06/2010), Tratamientos de datos personales para la difusión pública, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina.

Ley 11723 – Régimen legal de propiedad intelectual, (30/09/1933), adaptada por Decreto 165/1994 a la Protección de Software (03/02/1994), modificada por Ley 25036 (14/10/1998), modificada por Decreto 165/1994, Argentina.

Ley 24766, (20/12/1996), Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos, Argentina.

Ley 25036, (11/11/1998), Propiedad Intelectual, Argentina.

Ley 25326 (30/10/2000) Protección de los datos personales- Decreto 995/2000, Argentina.

Ley 26032, (17/06/2005), Difusión de información, Argentina.

Ley 26388, (04/06/2008), De delitos informáticos (Modificación del Código Penal), Argentina.

Norma ISO-7498-2 (1989), Sistemas de procesamiento de información - Interconexión de sistemas abiertos - Modelo de referencia básico - Parte 2: Arquitectura de Seguridad, The International Organization for Standardization, Suiza.