**Título** Seguridad de la información en la actual sociedad del conocimiento

**Tipo de Producto** Ponencia (texto completo)

**Autores** Galmarini, Luciano; Lo Giudice, María Eugenia & Cuarterolo, Omar

XVI Congreso Nacional y VI Congreso Latinoamericano de Sociología Juridíca, Universidad Nacional de Santiago del Estero, (Santiago del Estero, Octubre 2015)

## Código del Proyecto y Título del Proyecto

A14S20- Espionaje comercial con robo de información confidencial

## Responsable del Proyecto

Lo Giudice, María Eugenia

## Línea

Derecho Informático

## Área Temática

Derecho

## Fecha

Octubre 2015

**INSOD**
Instituto de Ciencias Sociales y Disciplinas Proyectuales

UADE FUNDACIÓN UADE

Título de la ponencia :

"**SEGURIDAD DE LA INFORMACIÓN EN LA ACTUAL SOCIEDAD DEL CONOCIMIENTO**"

Autor/es:

Maria Eugenia Lo Giudice, Prof. Abog. Especialista en Derecho Alta Tecnología
Departamento de Derecho-Facultad de Ciencias Jurídicas y Sociales
Universidad Argentina de la Empresa (UADE)
mlogiudice@uade.edu.ar

Luciano Galmarini Prof. Abog. Especialista en Derecho Alta Tecnología
Departamento de Derecho-Facultad de Ciencias Jurídicas y Sociales
Universidad Argentina de la Empresa (UADE)
lgalmarini@uade.edu.ar

Omar Cuarterolo Prof. Licenciado en Sistemas
Departamento de Derecho-Facultad de Ciencias Jurídicas y Sociales
Facultad de Ingeniería y Ciencias Exactas
Universidad Argentina de la Empresa (UADE)
ocuarterolo@uade.edu.ar

Número y nombre de la comisión de trabajo:

Comisión Nro.1, "Globalización y Glocalización"

## I.- Introducción o estado del arte

***"… Cuando hablamos de riesgos, discutimos de algo que no está a la vista, pero que puede hacer su aparición si no se toman ahora mismo cartas en el asunto. Los riesgos creídos como tales, son la fusta con la que se puede hacer que el caballo del presente venga al galope. …"***
***Beck, Ulrich[1]***

Desarrollada la "sociedad de la información", actualmente transcurrimos la "sociedad del conocimiento", basada en los "datos" como unidad mínima de información.
Ahora bien, estos conceptos entendidos dentro de lo que Ulrich Beck dio en llamar la "sociedad del riesgo", donde se entiende que estamos en una fase de desarrollo de la sociedad donde los riesgos (de tipo social, económico, políticos, etc) tienden a diluirse del control de los órganos tradicionales encargados de velar por la protección.

Si entendemos que la información es un valor innegable y se convierte en un asset imperativo en el mundo empresario, debemos identificar los "riesgos" en cuanto al maenjo de los mismos. Tenemos que notar que repercute en los sujetos de derechos, desde el nivel personal al mundo de políticas públicas, las ONGs., etc.

Somos conscientes de la gran importancia del manejo de la información y la necesidad de tener el estrecho contacto con las personas que nos rodean en el ámbito laboral si lo enfocamos desde este ángulo, más allá del "dato personal".

Justamente en las organizaciones puede haber por diferentes razones ciertos niveles de disconformidad que podrían acarrear todo tipo de problemas relacionados con la confidencialidad.
Si bien puede ser dificultoso detectar estos casos, el hecho de conocer en profundidad al recurso humano de una organización, nos llevaría a comprender la situación general en que

[1] ¿Qué es la globalización?, Buenos Aires, Editorial Paidós, 2004 Pág.143

se encuentra una empresa y hacer posibles prevenir ciertos riesgos en el manejo de la información de los datos.

Debemos captar el ambiente en que se desarrollan las conductas laborales para comprender que se deben tomar medidas concretas y definir un plan de acción realista. Desde ya que que siempre habrá un margen de error que quedará abierto, porque donde hay tecnología hay posibilidad de errores en el manejo de la misma, pero un correcto tratamiento en el control de riesgos minimizará cualquier impacto que podría generar graves daños en lo que consideramos hoy el control de la seguridad informática.

Citando nuevamente a Beck, podemos distinguir ciertas características para poder reconocer estos cambios donde la "sociedad del conocimiento" se ve directamente influída por la "sociedad del riesgo". Así, debemos reconocer el daño sistemático que podría ocasionar el manejo no correcto de la "información". Por otra parte así como en la sociedad industrial moderna el problema era la distribución de la riqueza, hoy el problema lo tenemos en la distribución de esos riesgos, asociados muchas veces al proceso de "desigualdad social". Ante esta nueva situación, ya no son las instituciones de poder político las que legitiman los movimientos sociales sino que se hace necesario la alerta desde las ONGs especializadas y la comunidad global (superando el concepto tradicional de "Estado"), que nos advierten sobre los peligros de nuevas conductas sociales.

Nos evidencia esta nueva etapa de transformación de la sociedad, una sensación de incertidumbre provocada por el efecto de las nuevas tecnologías, ante lo impredecible percibido a veces como una amenaza, lo que nos ha llevado a plantear en el derecho principios como el de un nuevo "orden público tecnológico" o el principio de "equivalencia funcional" o el principio de "neutralidad tecnológica".

Es común escuchar o leer noticias que nos relatan sustracción o robos de datos o información, como en el 2014 conocida a través de *Bloomberg News*, donde el banco JP Morgan fue victima de piratas rusos que atacaron cibernéticamente, provocando la pérdida

de datos sensibles. O aseveraciones como la de la firma de seguridad informática[2], Hold Security, nos arrojan cifras luego de un ataque entre 2013 y 2014, comprometiendo 1.200 millones de contraseñas y direcciones de correo electrónico en el mundo con lo que se permitía conectarse a unos 420.000 portales de internet. Hasta Adobe Systems fue afectada perjudicando a cerca de tres millones de personas, cuando piratas robaron sus datos personales y bancarios.

Otro ejemplo que sacudió la opinión pública dentro del ámbito ya del "dato personal", pero que nos muestra el fuerte impacto en la gestión de riesgo en el manejo de la información, es el conocido caso del hackeo sufrido en agosto de este año por el portal "Ashley Madison", de Canadá y que se identifica con el eslogan "la vida es corta, busca un amante". Sitio dedicado a realizar citas extramatrimoniales y que tiene usuarios de 46 paises operando desde el 2001. El gran impacto por la posible filtración de identidades y preferencias sexuales de más de 39 millones de personas, trajo una cantidad considerable de denuncias de chantaje y dos suicidios, un problema se seguridad que entró en crisis reflejando el poder que tienen los piratas informáticos y el peligro que corre la información circulando por bases de datos.

Estamos hablando de grandes volúmenes de información con velocidades de tratamiento que han dado en generar, el fenómeno del Big Data.
Donde quiera que haya una persona frente a este mundo tecnológico, habrá una información contenida en un dato que exigirá determinada seguridad en su tratamiento. Y es ahí donde se percibe de la "segunda modernización" que señale Beck, como propia de una sociedad globalizada y en un continuo desarrollo tecnológico.

Desde la Sociedad del conocimiento, somos como personas, un conjunto de datos e informaciones. Así como se habla del "habeas corpus" remedio constitucional que nos garantiza la libertad corporal de las personas, el "habeas data" introducido en la Argentina,

[2] http://www.infobae.com/2014/08/06/1585866-el-mayor-robo-contrasenas-la-historia-enciende-alarmas-la-web Noticia publicada en Infobae 06/08/2014, visitada on line: 14 Septiembre 2015

con la reforma constitucional de 1994, nos introdujo la idea del respeto hacia la privacidad, honor e intimidad de las personas, protegiéndoles justamente la información.

Pero más allá del dato personal, en este trabajo nos situaremos sobre la persona jurídica resaltando la importancia de la "seguridad de la información" que la misma le da tratamiento. Y trataremos de mostrar la importancia que tiene el "tratamiento del factor riesgo", entendido como aquella decisión previa que puede evitar la consolidación de una amenaza. Al decir de Luhmann, "las claves son las decisiones"[3] que se tomen y en esto debemos advertir el rol que juega el tratamiento de la información que podría derivar en conducta "disvaliosas" para el derecho, si no se minimizan los riesgos.

**II.- La "Inseguridad De La Información"**

Tratemos de identificar al menos en un principio, algunas de las causas genéricas que producen inseguridad en el resguardo de la información que disponen las distintas personas jurídicas.

Surge el temor latente de la "pérdida de control" sobre esa información disponible en algún Banco de Datos, y aquí se debe considerar el "tratamiento que se le da a la misma" por los responsables del manejo de "dato ajenos", así como los "datos dispuestos en la nube", es decir grandes cantidades de datos almacenados en forma gratuita u onerosa que guardan la información en internet.

Es infundado este temor? solo se trata de una percepción? Es cuestión de algún "malware"? entendido como aquel software malicioso que se introduce en nuestros equipos tomando control en diversas maneras (como virus, worm, spyware, bootnet, etc. etc.?).

De quién debemos estar prevenidos para no sufrir el "robo, secuestro o algún otro tipo de manejo inescrupuloso" de la información. Anuncios o redirección a sitios web con

[3] Reseña de "Sociología del riesgo" de Niklas Luhmann. Acevedo, Alberto, Vargas, Francisco. Estudios sobre las Culturas Contemporáneas [online] 2000, VI (junio) : Página visitada el 28/09/ 2015] http://www.redalyc.org/articulo.oa?id=31601109

publicidad que les reporta ciertos ingresos, obtención fraudulenta de datos financieros, controlar computadora y usuario como "zombi"[4] para atacar otros sistemas, fraudes, etc. Llegando incluso a generar la distribución de degradación del servicio.[5]

Pues parecería que no se trata de solo percepción…, la empresa "Sophos", especialista en ciberseguridad, recibe diariamente solo 1/3 de denuncias sobre los posibles virus existentes.. pero como quedamos en contacto con esos virus?...

Si se entiende que los programas maliciosos que nos perjudican en general entran por páginas web visitadas, bajando archivos seleccionados por el propio usuario, o incluidos en otros programas que se pretenden descargar de internet a través de archivos "peer to peer", etc.. y se le suma la advertencia de necesaria protección para este tipo de malware, "no abra archivos que vienen en mensajes de desconocidos", "use contraseñas que no sean tan simples", "tenga un buen antivirus", "no use sistemas wi fi ajenos para manejar datos sensibles", etc. etc., no será que debemos replantear el rol de la *"ingeniería social"* precisamente tanto como cuando se focaliza el rol de la *"ingeniería informática*"?

Es decir, queremos señalar que no se debe atribuir la "fuga de información" a solo y principalmente, fallas "informáticas", como comúnmente se presume. Sino atender al comportamiento social frente al manejo de la tecnología como vía de tratamiento de la información.

**III.- Causales Posibles De Fuga De Información o Datos**

Trataremos de analizar posibles factores que incidirían en estos riesgos:

1.- Negligencia o impericia en el manejo de la seguridad de la información: estadísticas nos señalan que gran parte de la fuga de información en empresas y organismos, se produce a

[4] Aquella computadora que es conectada a internet habiendo sido capturada por un hacker, virus de computadora o un "caballo de troya". Por lo general una computadora zombie ha sido tomada y se programa para realizar tareas maliciosas bajo un mando remoto. Ocurre muchas veces bajo la propia ignorancia de sus dueños. Según el Diccionario de Informática y Tecnología, http://www.alegsa.com.ar/Dic/computadora%20zombie.php, consultado on line 14 de septiembre 2015

[5] Distribuyen durante un tiempo y con determinada intensidad el ataque a un sitio web, intentando el colapso. http://www.alegsa.com.ar/Dic/computadora%20zombie.php#sthash.A1OlsaSi.dpuf

través de los propios empleados, por un estado de negligencia o impericia en el manejo de la seguridad de la información, entendiendo este concepto de una manera más amplia que lo estrictamente técnico.

Por ejemplo, el correo electrónico sin cifrar, o el envío de un correo a una dirección equivocada o el almacenamiento de archivos en servicios basados en "la nube", (Dropbox, Gmail, etc).

2.- Ataques internos: luego de las fugas por negligencia o desconocimiento, siguen las que se producen por **"**ataques internos**"**, cuando se trata de empleados infieles, que actúan motivados por**:** represalia, venganza, conciencia cívica, robo de información y otros motivos de tipo económicos.

3.- Delincuentes informáticos: Al final, y en mucha menor medida que las dos anteriores, se encuentran los delincuentes informáticos.

Existen técnicas capaces de robar información de dispositivos no conectados que se pueden producir de diversos modos, a través de interceptar la radiofrecuencia que emiten todos los dispositivos electrónicos (asimismo como uso de impresoras y escáneres) para acceder a redes aisladas, a través de espionaje electromagnético, el láser, la radio o el calor como para mencionar algunos ejemplos.

Podemos citar el caso del técnico Edward Snowden, de la Agencia de Seguridad Nacional norteamericana, CIA[6], acusado de revelar datos secretos de un programa de espionaje a ciudadanos de su país. Claro que en este caso hablamos de un técnico involucrado, respondiendo por ello a un accionar muy particular.[7]

[6] CIA, Agencia Central de Inteligencia, creada en 1947 con la firma del Acta de Seguridad Nacional por el Presidente Harry S. Truman

[7] Snowden trató de no ser objeto de control de sus comunicaciones depositando su celular en el refrigerador de su cocina, para que esta hiciera de «Jaula de Faraday», es decir bloqueando el escape de las señales electromagnéticas. No optó por la opción de apagar el dispositivo ya que muchos de los dispositivos actuales, no solo teléfonos, cuentan con estados a medias entre completamente encendidos y completamente apagados,

Según información del diario ABC de España, casi la mitad de las empresas españolas han sufrido en alguna ocasión un robo atribuido al negligente accionar del comportamiento de sus empleados[8]. El 50% de las empresas españolas ha restringido o prohibido el uso de servicios de intercambio de archivos.
El 47% ha impuesto reglas para regular la conexión de dispositivos externos en los equipos corporativos. Prácticamente la mitad de las empresas han sufrido un ataque de este tipo.
Es decir, controles insuficientes en términos de almacenamiento y comunicación de la información corporativa indican que es más probable que un empleado *provoque fugas de datos que de infectar su equipo mediante el acceso a redes sociales.*

**IV.- "Seguridad Informática", "Gestión De Riesgo"**

Por lo anterior expuesto la importancia de desarrollar estos conceptos, especialmente para los que no somos técnicos en informática.

La tecnología informática y en particular la Seguridad Informática son desde la óptica de un lego, como un proceso complejo que está fuera del alcance de todo profesional no especializado.

a) Si nos enfocamos desde el punto de vista de la "Empresa":

Muchas organizaciones entienden que la Seguridad Informática, por similitud es una especialización del área de Sistemas de Información. No estamos muy de acuerdo con esta visión dado que entendemos a la Seguridad de la Información requiriendo de la participación y compromiso de todas las áreas de la organización. Por lo general existe una división interna de las áreas de administración de la infraestructura y soporte técnico y el área de desarrollo de aplicaciones.

Se suelen realizar inversiones importantes en lo que a infraestructura de seguridad se refiere.
Se está comprendiendo el cambio de paradigma que los nuevos comportamientos sociales plantean, pasando de una estructura con puntos de acceso con el exterior controlados, a otra

---

y la extracción de la batería tampoco sería suficiente ya que algunos dispositivos disponen de fuentes de energía adicionales en su interior.

[8] Según un reciente estudio de Kaspersky Lab, proveedor ruso de seguridad informática

donde existe la posibilidad de teletrabajo y más aún, cuando los dispositivos personales (Smart phones, Tablet, Notebooks) están fuera de la administración centralizada de la organización por motivos obvios.

En el caso del desarrollo de aplicaciones el tema es un tanto más dramático. Como ejemplo, hemos encontrado que existe una porción importante de las áreas de sistemas en las que el cumplimento de las normativas de seguridad (ISO 27000), ya sea por aplicación de mejores prácticas como por la regulación de la actividad de acuerdo a normativas externas, disponen de tres ambientes de trabajo, a saber: desarrollo, aseguramiento de la calidad (testing) y producción.

Difícilmente existan test que acredite la detección de vulnerabilidades de seguridad. No solamente esto, sino que el personal técnico afectado a desarrollo de aplicaciones no cuentan con capacitación apropiada en este aspecto. Consecuentemente, no hemos detectado una oferta de calidad en lo relativo a capacitación de profesionales que incluyan este aspecto, no solo en lo relativo a verificación de vulnerabilidades, sino también a la producción de software seguro. Es también entendible dado que esta capacidad no es una exigencia curricular para los empleados ni tampoco se incluyen dentro del programa de capacitación laboral. Esto demuestra la desconexión que existe entre las actividades propias de la infraestructura tecnológica y desarrollo de sistemas.

b) Si nos enfocamos desde el punto de vista del "Usuario final".
El tema de seguridad requiere una concientización específica en lo relativo a la misma. Un usuario entiende la necesidad de mantener en secreto el acceso a sus sitios personales, correo electrónico, home banking, sistemas de pago electrónico, etc. Sin embargo, mantener el secreto de sus claves de accesos a los datos de la organización es de aplicación un tanto más laxo.

Hemos observado que por ejemplo, en el caso de ausencia eventual (ya sea por enfermedad o licencia eventual) al lugar de trabajo, no tienen ningún tipo de inconvenientes en divulgar la clave a un compañero o superior que requiera acceder a datos que se encuentran bajo su tutela. Entendemos que este es un problema de administración de seguridad, dado que un superior debería poder acceder a los recursos de los subordinados en forma irrestricta. Esta es la única forma de determinar quién y en qué momento accedió a determinados datos.

Los métodos de autenticación consisten en la verificación de uno o una combinación de tres factores. Estos son: algo que "conozco", algo que "tengo" y algo que "soy".

1.- Definimos a “Algo que “conozco”, como por ejemplo una clave, “algo que tengo”, una credencial y “algo que soy”, referido a un aspecto biométrico del individuo, por lo general pasivo (huellas dactilares, iris, rostro, etc.) y no dinámico (forma de tipeo, cadencia de la voz, etc.).

No se entendería comprometer la seguridad de una organización mediante la divulgación o por el resguardo indebido de una clave. Tales conductas podrían ser evitables y no llegar a producir eventualmente un perjuicio irreparable.

Este tipo de comportamiento tiene varios matices que interesa analizar por separado:

a) -El sistema pide el cambio de clave en forma periódica: Método de oscuridad (psicológico) y no de seguridad (tecnológico)?
Una de la forma de asegurar el secreto más habitual consiste en solicitar el cambio de clave periódicamente. Esto se debe al temor de que el usuario divulgue o le sea extraída dicha clave, por lo que podría concretarse un acceso no autorizado al sistema.

Por esta razón, el usuario es obligado a recordar todas y cada una de las múltiples claves para los diferentes accesos que dispone, tanto personales, como ser Home banking, redes sociales, correos electrónicos, accesos laborarles, sitios de interés, tarjetas de crédito, por nombrar algunos de los más frecuentes. Dado que la memoria humana tiene límites específicos que varían de individuo a individuo, es común que los usuarios concluyan que la mejor practica consista en anotar las claves en un papel a modo de ayuda memoria, lo cual viola todo tipo de confidencialidad, o que utilicen una sola clave para absolutamente todos sus accesos. Alguno tal vez piense que mantener el resguardo ese “papel” sería suficiente, sin embargo, de acuerdo a los indicado por Shanon, este seria un método de oscuridad y no de seguridad, el primero es sicológico y el segundo tecnológico. No negamos su utilidad pero definitivamente negamos su eficacia. Un método alternativo es utilizar algún sistema de administración de contraseñas, local o WEB, los cuales son de dudosa confidencialidad.

b) -No existe una forma clara de detener el robo de claves
Existen varias formas de “robar” una clave. Una de ellas es mediante fraudes conocidos como “Phishing” en los que el usuario es inducido a utilizar su clave en un portal que se asemeja al de la organización. Otro de ellos es mediante el uso de “key loggers”, muy comunes en las terminales públicas donde se pueden registrar los tipeos de usuarios.

Este tipo de engaños hacen que el robo de las claves sea habitual y con los perjuicios que produce. Lamentablemente, las organizaciones que han sido víctimas de estas prácticas no publican sus estadísticas dado que supondría un descrédito en los clientes.
El uso de tarjetas de coordenadas permite mejorar la performance del método, dado que incorpora un segundo método ("algo" que tengo). Aunque requiere de la posesión de este "documento".

Estas situaciones pueden provocar el "repudio" por parte de un usuario al acceso indebido a datos.

Existiendo la posibilidad de "robar" una clave, sería normal que el usuario negara un determinado acceso, ya sea robo por descuido o simplemente un intento de negar un acceso indebido, y que no haya forma de demostrarlo. Si bien, cada transacción requiere del envío de la propia dirección de internet (ip address), también es sabido que tal sistema de direccionamiento, del mismo modo que una dirección postal, no es portable. Por lo cual existe una distribución geográfica global del sistema de direccionamiento que permite establecer la zona de donde se accede a los datos. Si bien existen formas sofisticadas de evitar este tipo de control, en una primera instancia es una contramedida que podría determinar el sitio desde donde se efectúa el ingreso.

El uso de tarjetas de coordenadas, al igual que el sistema de "Tokens" presenta algunas ventajas adicionales dado que solo el poseedor de estos elementos además de su nombre de usuario y clave recordada no solo hacen el sistema más robusto sino que también permiten evitar el eventual repudio.

Dada la aceptación general del uso de smartphones, algunos organismos gubernamentales están reemplazando el uso "Tokens" por el de una aplicación instalada en este que cumple las funciones de entregar un determinado código pseudo aleatorio para agregar a la clave de usuario como método de desafío- respuesta que mejora los costos de eventual reposición y programación de tokens. Ello así entendiendo que este sistema no supone disponer de un elemento extra, tomando en cuenta que un smartphone es, a la fecha, un dispositivo ubicuo.

Se debe actualizar estas políticas con la misma frecuencia que con la que avanza la tecnología y regularlas haciendo un control exhaustivo de su aplicación.

Recapitulando en un pequeño listado podemos resumir y completar los problemas de confianza en la seguridad por oscuridad (referido a lo psicológico):

- ✓ Los trabajadores de una entidad, a quienes se les confían los mecanismos internos de las redes de la compañía, pueden cambiar su rumbo laboral y abandonar la empresa dejando al descubierto esas contraseñas o scripts que hasta ese momento permanecían discretamente.
- ✓ Procesos de parches lentos o con efectos poco predecibles, son otros de los factores del éxito o el fracaso de un ciberataque. La dinámica en los parches rápidos y con efectos predecibles facilita el proceso resolutivo.
- ✓ Uso de comunicación inalámbrica sin autenticación ni cifrado
- ✓ Con el auge del BYOD[9] (el uso de dispositivos personales para el trabajo) promovidos por las empresas, cada vez con más frecuencia, los trabajadores utilizan dispositivos propios inalámbricos y/o sin cifrado que facilitan los ciberataques y posibilitan la entrada remota de usuarios a las redes de la compañía.
- ✓ Mecanismos deficientes para el aislamiento de redes y el control del tráfico no permitido.
- ✓ Con la introducción de los USB en las empresas cualquier trabajador puede transportar información de una red a otra pese a estar físicamente aisladas. Actualmente como dijo Karsten Nohl y Jakob Nell, investigadores de una firma de seguridad de Berlín, incluso ahora se puede cargar software malicioso en los firmware de los USB a través de pequeños chips que vienen en los dispositivos con USB, que no son detectables porque a ese nivel no hay escudos de protección, incluso cualquier periférico que querramos conectar podría contener software malicioso.
- ✓ Inexistencia de herramientas que identifiquen rápido actividad sospechosa
- ✓ Las empresas deben disponer de una plataforma resolutiva de incidentes que no solo integre alertas de cientos de soluciones puntuales, sino que dé respuestas a

[9] En el ámbito de la empresa se piensa que el BYOD (Bring Your Own Device) no representa una amenaza para su empresa y no tienen ningún interés en invertir en seguridad para dispositivos móviles, mientras que los empleados piensan que la responsabilidad de la seguridad es de la empresa, según un estudio realizado por Kaspersky Lab.
http://newsroom.kaspersky.eu/es/noticias/detalle/article/la-amenaza-del-byod-el-32-de-las-pymes-no-ve-peligro-en-que-el-trabajador-use-su-dispositivomovi/?no_cache=1&cHash=be1a761aa34b6d0e33eb8ac584d161e4

incidentes inteligentes y accionables y automatice los procesos, permitiéndoles enfocarse en los incidentes más urgentes.

- ✓ Contraseñas débiles
- ✓ La gestión deficiente de los controles de acceso puede abrir las puertas con facilidad a ataques externos.
- ✓ Utilización ineficiente del ancho de banda de red.
- ✓ Gestión deficiente de la memoria que puede derivar en "buffer overflow".[10] Esto constituye un fallo de programación. Poco fiable de los cambios de seguridad

Expertos en ciberseguridad estiman que "la permanencia media de los atacantes en redes corporativas antes" de ser detectados es más de un año, tiempo suficiente que combinado con las perspectivas nombradas anteriormente pueden resultar muy preocupantes. Debemos pensar en protección, en anticiparse al peligro para poder protegerse. En la "amenaza" que el sociólogo Ulrich Beck señaló. Por lo tanto, al hablar de seguridad informática queremos prever la forma de anticiparse al riesgo o peligro de dejar expuesta la información.

**V.- Aspecto Jurídico**

a) Ahora bien, jurídicamente hablando, la seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su

- ✓ confidencialidad,
- ✓ integridad
- ✓ disponibilidad

Casualmente hemos listado las características propias de los datos exigidas en la Argentina, por la ley de datos personales 25326. Es decir, nuevas pautas que me ayudarán a evaluar las conductas dentro de la nueva sociedad del riesgo dentro de la sociedad del conocimiento.

[10] El error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer). Si dicha cantidad es superior a la capacidad pre-asignada, los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria.

Considerar aspectos de seguridad para resguardar nuestro "asset", significa a) conocer el peligro, b) clasificarlo y c) protegerse de los impactos o daños de la mejor manera posible. Debemos identificar potenciales amenazas, agresores e intenciones dañinas (directas o indirectas) en contra de nosotros, y así tomar medidas de protección adecuadas.

Entonces, la Seguridad Informática jurídicamente considerada, sirve para la protección de la información en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

Algunas de estas herramientas jurídicas a tener en cuenta desde el punto de vista preventivo, en el caso de las empresas podrían ser:

- Contar con un Manual de gobierno corporativo, donde trate la protección de datos, teniendo en cuenta los principios de buena fe, compromiso y lealtad.
- Tener el control sobre el personal de la empresa, desde la selección y contratación del personal hasta el estado de satisfacción en la misma.
- Al momento de la contratación, incluir cláusulas en los contratos donde queden aclarados los parámetros exigidos en cuanto la seguridad de la información.
- Manual de uso y herramientas informáticas que contenga: Protocolos Jurídicos de Seguridad, clausulas de responsabilidad en el tratamiento de la información y el uso de las herramientas

- Desde el punto de vista de la empresa se puede aplicar los standares de seguridad como la aplicación de normas ISO 27000,.

b) Protección de Datos

En la Seguridad Informática[11] se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos.
Hasta ahora hablamos del aspecto "seguridad de la información", seguidamente nos enfocaremos en la "Protección de los datos".

[11] Gestión de Riesgo: glosario https://protejete.wordpress.com/glosario/#seg_inf

Ambos forman la base y justifican la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática de lo cual surgirá la obligación de su protección. No obstante lo cual, las medidas de protección aplicadas normalmente serán las mismas.

En un taller realizado en Centroamérica por una ONG europea, en el marco la capacitación y sensibilización para la seguridad de la información[12] se experimentó con los participantes, un interesante ejercicio al tratar de distinguir cuales serían las cuestiones de índole confidencial y de índole pública en una relación entre un particular y una entidad bancaria, involucrándose ambas en la seguridad informática. Cómo se vive ese concepto de "segunda modernidad", según Beck, donde a veces discrepa ese concepto de riesgos y control, del esquema tradicional de la sociedad industrial clásica. Se llegó a la conclusión que existe una percepción diferente de lo que sería el concepto de la información confidencial.

Se focaliza a la seguridad de la información, por el banco, y la otra perspectiva que se da desde la persona, a la protección de datos.

Dijimos que la seguridad informática se ocupa de la protección de los datos mismos, teniendo en cuenta los requisitos exigidos por la propia ley de datos personales, confidencialidad, integridad y disponibilidad pero especialmente debemos sumarle el requisito de "autenticidad".

- Si la seguridad debe entenderse como medida de prevención del daño a la información, en primer lugar debemos establecer procesos y medidas de protección, que garanticen un cumplimiento adecuado, de acuerdo con el principio de neutralidad tecnológica.

  Se debe implementar medidas de protección preventivas suficientes. Porque la gestión de riesgo informático con resultado negativo, no solo conllevará a pérdidas de tipo económicas

[12] Proyecto de Seguimiento al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras"
Durante los años 2007 y 2008, la Fundación Acceso de Costa Rica, en alianza con SIMAS (Servicio de Información Mesoamericana sobre Agricultura Sostenible) de Nicaragua y con el apoyo técnico de SEDEM (Asociación para el Estudio y la Promoción de la Seguridad en Democracia) de Guatemala, trabajaron en un proyecto, iniciado y financiado por HIVOS Holanda, para dar seguimiento al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras".

sino también a asumir responsabilidades jurídicas tanto civiles y penales, contractuales y extracontractuales.

Se trata de elaborar un plan de gestión de riesgo tal que nos permita anticipar el riesgo identificando el peligro, clasificándolo y de esta manera podremos efectivizar una adecuada protección de los posibles daños que de él surjan. Se debe involucrar todos los sectores de la organización, comprometiéndolos en lograr el objetivo de seguridad pues la falencia de cualquiera perjudicará a todos

Como dijimos antes es muy importante tener en cuenta el proceso que acarrea cumplir con el principio de neutralidad tecnológico para no quedar desactualizado. Este tipo de procesos es tan dinámico que implica una inversión en actualización y capacitación continua (bajo una estricta supervisación).

**VI.- Qué Involucra los "Datos Informatizados" en la legislación argentina respecto a las conductas sociales en la nueva estructura de la sociedad del conocimiento?**

Se refiere a los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. Donde encontramos como partes a considerar los siguientes recursos:

1) los datos en si,
2) la infraestructura de tratamiento,
3) el componente humano.

1) De acuerdo a nuestra ley, por datos personales se entiende: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

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

2) Deducimos que también está involucrado:

— las 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". Todo sostenido por un equipamiento que irá desde la propia estructura física de almacenaje pasando por simples memorias o discos, celulares, etc…

3) En cuanto al elementos humano, la ley nos hable de:

— 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.

— 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.

Conductas necesarias a adoptar:

Se hace necesario adoptar conductas que se anticipen a una posible producción de daño en vista de la protección de la seguridad de la informática (tanto para protección de los datos como para protección de la seguridad de la información). Es decir prever la posibilidad de un evento que ponga en peligro la información.

Debemos asegurarnos informáticamente, siguiendo el lineamiento de resguardo que nos exige la ley de datos personales y por consiguiente resguardando la responsabilidad jurídica.

El art.9 nos dice:

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.

Identifiquemos las posibles debilidades desde el punto de vista del responsable de archivo, registro, base o banco de datos físico, asi existirán las propias internas que pueden surgir en base a culpa, negligencia o impericia y otras que ya provendrían del hecho ajeno a la empresa y que serían de tipo

a) Humano (directamente relacionado con las conductas de las personas)
b) Físico (Serán amenazas que responden a lo relacionado con lo humano y lo natural)
c) Tecnológico (influye en la estructura misma del sistema que puede puede influir en los mencionados sentidos anteriores).

**VII.- Conductas humanas e ingeniería social**

Reconocemos de acuerdo a nuestra ley las "categorías de datos" porque dependiendo de esto, tendremos diferentes conductas en cuanto al tratamientos y acceso a la información. Es decir, reconoceremos diferentes niveles de autorización de acceso a la información. Así podremos realizar una valoración del daño o "impacto" en relación a su manejo, y por lo tanto que consecuencias de daño material y/o moral puede devenir.

Para definir un impacto recurriremos a conocer las políticas internas corporativas, identificación de personas autorizados (con o sin acceso a información), cumplimiento de clausulas convenidas, etc.

Dentro de las políticas empresarias se entiende que es mejor prevenir en la definición de los tipos de daños que se consideran y por lo tanto en las responsabilidades que se incurrirá, al violar los mismos.

La magnitud del impacto tendrá que ver con el daño que genere la pérdida de control de la información recayendo la posibilidad de la sanción sobre quien resulte involucrado e identificable.

Una cultura de seguridad debe ser cultivada de manera interna y en todos los niveles tanto administrativos como ejecutivos, no así confiada sólo a dispositivos electrónicos programados.

Para adoptar medidas de seguridad minimizando los riesgos, es necesario comprender los puntos críticos, o aspectos que generan mayores riesgos de filtro de información, y sin lugar a dudas el punto crítico es el comportamiento humano, lo que llamamos la "ingeniería social". Independiente de los hardwares, como ser el control biométrico o software, o los firewalls que se implementen en una empresa, el factor humano siempre será un punto crítico en la seguridad, las máquinas pueden ser programadas, pero no así el empleado.

Los sujetos que trabajan en una institución tomando en cuenta desde la alta gerencia, no pueden ser automatizados, por lo que tratar de comprender quién podría dar lugar a una falla de seguridad es casi imposible.

**VIII.- Conclusión**

Podemos inferir a lo largo de lo que se ha expuesto, que la tecnología es tan necesaria como una puerta que comunica entre ambientes, pero donde hay una puerta habrá posibilidades de violaciones al cierre del paso que se pretende con ella, simple analogía con la tecnología tan necesaria en nuestros días porque, donde hay tecnología y manejo de información, si no se extreman los cuidados puede haber "fuga" de datos, depende como se de el tratamiento de los mismos, y en gran parte hay responsabilidad de la ingeniería social.

Es innegable la necesidad de redefinir parámetros de comportamientos de conducta humana como atenuante de generación de riesgos, que hacen que percibamos una cierta "amenaza ante el nuevo mundo tecnológico", basado en la sociedad del conocimiento.

Quisiera cerrar con los consejos principalmente enfocados al ámbito corporativo, que nos deja Eset[13], empresa que trabaja con la seguridad informática, evitar las principales causas de fuga de información:

1. Conocer el valor de la propia información. Realizar un análisis de riesgos y un estudio de valuación de activos para poder determinar un plan de acción adecuado que permita evitar posibles filtraciones.
2. Concientizar y disuadir. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales.
3. Utilizar defensa en profundidad. Considerar la aplicación del modelo de defensa en capas a fin de que las distintas medidas que se toman cubran todos los aspectos del acceso a la información (físico, técnico y administrativo) y así evitar centralizar las soluciones o promover puntos únicos de falla.
4. Incluir herramientas tecnológicas. En ámbitos corporativos, contar de ser posible con una solución técnica de protección, por medio de hardware, software, o combinación de ambos, tanto a nivel de redes como de equipos (servidores y estaciones de trabajo). Además, las soluciones contra el malware son particularmente indispensables.
5. Seguir los estándares. Alinearse con estándares internacionales de gestión de la seguridad permite disminuir el riego de que puedan ocurrir incidentes, así como también de que el negocio se vea afectado por un determinado evento de filtración.
6. Mantener políticas y procedimientos claros. Relacionado con el punto anterior, se debe tener una clara definición y comunicación de las políticas de seguridad y acuerdos de confidencialidad, aceptados y firmados por todos los usuarios. Esto minimiza potenciales

[13] ESET, compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas (oficinas centrales en Bratislava, Eslovaquia, y de Coordinación en Estados Unidos, Argentina y Singapur).
http://www.eset-la.com/centro-prensa/articulo/2011/eset-10-mandamientos-seguridad-informacion-empresas/2566

fugas de información, al contar con un consentimiento firmado del usuario para no realizar ciertas acciones.

7. Procedimientos seguros de contratación y desvinculación. En estos dos momentos se conecta o desconecta una nueva pieza externa con el motor de la organización, por lo que deben tenerse en cuenta de manera muy particular, controlando especialmente los accesos y registros de los usuarios en sus primeros o últimos momentos de trabajo.

8. Seguir procesos de eliminación segura de datos. Es fundamental que los datos que se desean eliminar sean efectivamente eliminados, y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

9. Conocer a la propia gente. Se recomienda tener presente que en las organizaciones puede haber personas conflictivas o disconformes, que podrían ser foco de cierto tipo de problemas relacionados con la confidencialidad. Si bien puede ser dificultoso detectar estos casos, el hecho de conocer en profundidad al propio personal ayuda a entender la situación general en que se encuentra una empresa y los posibles riesgos.

10. Aceptar y entender la realidad. Es necesario hacer lo posible para comprender que se deben tomar medidas concretas y definir un plan realista. No se pueden controlar absolutamente todas las acciones de todas las personas en todo momento, por lo que siempre habrá un margen de error que quedará abierto, y que deberá intentar reducirse al mínimo a medida que pasa el tiempo.

## IX.- BIBLIOGRAFIA


1. http://www.infobae.com/2014/08/06/1585866-el-mayor-robo-contrasenas-la-historia-enciende-alarmas-la-web Noticia publicada en Infobae 06/08/2014, consultada on line: 14 Septiembre 2015
2. http://www.alegsa.com.ar/Dic/computadora%20zombie.php, consultado on line 14 de Agosto 2015
3. Kaspersky Laboratory. http://newsroom.kaspersky.eu/es/noticias/detalle/article/la-amenaza-del-byod-el-32-de-las-pymes-no-ve-peligro-en-que-el-trabajador-use-su-dispositivomovi/?no_cache=1&cHash=be1a761aa34b6d0e33eb8ac584d161e4 Consultado on line 4 de Julio 2015

4. Taller Centroamericano Ampliando la Libertad de Expresión: “Herramientas para la colaboración, información y comunicación segura” , Fundación Acceso, Costa Rica 2007 /2008
5. ESET, http://www.eset-la.com/centro-prensa/articulo/2011/eset-10-mandamientos-seguridad-informacion-empresas/2566 Consultado on line 23 de Mayo 2015
6. Reseña de "Sociología del riesgo" de Niklas Luhmann. Acevedo, Alberto, Vargas, Francisco. Estudios sobre las Culturas Contemporáneas [online] 2000, VI (junio) : Página visitada el 25/09/ 2015] http://www.redalyc.org/articulo.oa?id=31601109
7. Entrevista Al Sociólogo Ulrich Beck: "En la globalización necesitamos tener raíces y alas a la vez", Periódico on line Clarin.com, http://edant.clarin.com/suplementos/zona/2007/11/11/z-04015.htm Consultado on line 27/09/ 2015
8. Beck, Ulrich ¿Qué es la globalización?. 2004, Buenos Aires. Editorial Paidós.
9. Castells, Manuel. La sociedad red: una visión global. 2006, Madrid. Editorial Alianza.

Legislación consultada:

10. Ley de Protección de los Datos Personales, Nº 25.326 y su Decreto Reglamentario Nº 1558/2001
11. Ley de Delitos Informáticos Nº 26388
12. Ley de Defensa al consumidor Nº Ley 24.240
13. Ley de Confidencialidad Nº 24.766
14. Constitución Nacional argentina