Facultad de Ingeniería
Universidad de Buenos Aires

75.17 - Implantación de Sistemas
75.56 - Organización de la Implantación y el Mantenimiento

Trabajo Práctico:

Fuga de Información

Profesora titular: Vilma Bettini

Profesores: Lucrecia Brollo
Hernán Apud
Nicolás Ureta

Año y cuatrimestre: 2014 2°C

Grupo N°: 2

Integrantes:

Apellido y nombre	Padrón	E-mail	Código materia
Maraggi, Santiago	86062	smaraggi@gmail.com	75.56
Parnisari, María Inés	92235	maineparnisari@gmail.com	75.17
Schmidt, Miguel Angel	83144	schmidt.miguel.a@gmail.com	75.17
Zhang, Yi Cheng	92333	ycg.zhang@gmail.com	75.17
Zurita, Stephanie	91809	abigail.zurita@gmail.com	75.17

Índice

Enunciado

Enunciado particular

Fuga de información en empresas con desarrollo de tecnología de punta, inventos, nuevos diseños, avances tecnológicos.

Riesgos a los que están expuestos por ejemplo laboratorios, automotrices y empresas con centros de investigación y desarrollo.

Controles efectivos (preventivos y detectivos) para mitigar los riesgos. Cómo se protegía el activo de información en el Siglo XIX. Cómo se protege en el Siglo XXI.

Enunciado general

De forma:

- Carátula indicando el grupo, tema, integrantes, cuatrimestre y año.
- Todas las páginas deben contener un encabezado y pie de página.
- Cuidar la distribución de los títulos, párrafos, tipo de letra, interlineado, etc.
- Revisar el texto, corrigiendo errores sintácticos y semánticos.

De contenido:

- Introducción.
  Debe contener una descripción de los hechos y situaciones relevantes de los siglos analizados. Dado que la amplitud de cada siglo es de 100 años, describir al menos 3 períodos por cada siglo (por ej. del 1800 al 1830, del 1831 al 1860, del 1861 al 1899).

- Desarrollo.
  Debe situar el análisis de riesgo en un determinado país y década. Comparación con la situación de riesgo en un país de cada una de las siguientes regiones/continentes: América del Norte, Europa Occidental, África.

  Ser concretos en cuanto a los riesgos y controles existentes referidos y focalizados en la industria o área mencionada en el enunciado.

  Presentar las conclusiones/respuestas a lo planteado en cada enunciado.

Introducción

El activo más valioso de las organizaciones

Antiguamente, la economía de las empresas estaba dominada por los **activos tangibles**, pero en la actualidad la situación es distinta: lo más valioso son los **activos intangibles**. Ellos otorgan ventajas competitivas sobre otras empresas. Aquella organización que tenga procedimientos adecuados, conozca los clientes de su segmento de mercado, tenga el conocimiento para desarrollar un producto único, motive a sus empleados, esté a la vanguardia de las tecnologías e innove, tendrá más probabilidad de triunfar.

De esta forma, la **información** se ha convertido en el activo más importante que posee cualquier organización, es la moneda de cambio e instrumento de fuerza y presión, otorga ventaja a quien la posee, y hay toda una industria en torno a la gestión, tratamiento y por supuesto, **protección de la información**.

Existen dos conceptos asociados a información: uno es la **confidencialidad**, que se refiere a la característica que la información sea accedida solamente por usuarios autorizados, y otro es la **privacidad**, que habla de la garantía que tiene un usuario respecto a la información y al uso que se le da.

La fuga de información

La **fuga de información** es un tema que preocupa enormemente a las empresas, y es debido a ello que suelen tomar recaudas para proteger su información. A grandes rasgos, la fuga de información ocurre cuando algún dato que tiene valor para una organización pasa a manos ajenas, perdiendo la cualidad de confidencialidad que le fue asignada.[1]

En el caso de **Argentina**, las principales fugas de información en las organizaciones gubernamentales, empresariales y educativas en la Argentina no son por acción de un empleado o ejecutivo infiel o por el ataque de un delincuente informático sino por "desconocimiento y negligencia" de los propios directivos y dependientes[2]. Luego de las fugas por negligencia o desconocimiento, siguen las que se producen por "ataques internos", como se define en la jerga, de empleados infieles, que actúan motivados por diferentes intereses: represalia, venganza, conciencia cívica, robo de información y otros motivos económicos. Al final, y en mucha menor medida que las dos anteriores, se encuentran los delincuentes informáticos.

Los **sistemas de información** capturan, procesan y almacenan información en una gran variedad de dispositivos. Estos dispositivos pueden requerir tratamiento especial para mitigar el riesgo de divulgación de información no autorizada, y asegurar la confidencialidad de la misma.

Existen dos **tipos principales de dispositivos**:

- ❏ Dispositivos **físicos**: por ejemplo, papeles y facsímiles. Estos dispositivos suelen ser los más difíciles de controlar, ya que nada impide que una persona tenga acceso a ellos.
- ❏ Dispositivos **electrónicos**: son el contenido de discos duros, memorias, teléfonos, computadoras.

La clave para decidir **cómo manejar la información** en cualquier información es primero decidir qué tipo de información se está administrando de acuerdo al nivel de confidencialidad requerido, y luego dónde está

[1] *Fuga de información, ¿una amenaza pasajera?*, página 3: http://www.welivesecurity.com/wp-content/uploads/2014/01/fuga_de_informacion.pdf

[2] *Como evitar el robo de información clave de una empresa.* Infobae, 2013. http://www.iprofesional.com/notas/168083-El-caso-Manning-reaviv-la-polmica-cmo-evitar-el-robo-de-informacin-clave-de-una-empresa

almacenada. Para ello, se debe categorizar la información (por ejemplo, memorandums, presentaciones, listados de salarios, minutas de reuniones estratégicas).

La pérdida de valor de la información

El tiempo es uno de los calificadores más importantes para una pieza de información. Saber cuándo sucedió, cuándo fue escrita, hace cuánto tiempo, qué tan recientemente, a la qué fecha se refiere la información y si es obsoleta, oportuna, atemporal y así sucesivamente es esencial para ser capaz de evaluar con precisión lo valioso, útil o importante que es esa pieza de información.

Pero hay también otro efecto del tiempo en la información, y es que la información "oportuna" o "en tiempo real" tiende a perder su valor con el tiempo, mientras que (potencialmente más importantes) piezas atemporales de la información no pueden en realidad ser valorados cuando se produce pero crecen en valor con el tiempo.

Además de los impuestos, todas las organizaciones poseen información muy sensible que no debe ser vista por personas no autorizadas. Mientras que algunos documentos pueden ser destruidos minutos después de su impresión, las leyes pueden requerir que los mismos para ser archivados desde unos años a permanentemente. Pero entre estos dos extremos de la escala, cada empresa puede potencialmente tener un gran volumen de datos en papel que ocupa espacio.

Cómo deshacerse de forma segura de información

Dentro del proceso de gestión de la seguridad de la información, el ciclo de vida de la tecnología dentro de las organizaciones no es diferente que el de cualquier otro entorno. Las computadoras se compran, se utilizan, y se descartan con el tiempo. En muchos casos el hardware se dona a escuelas, ONGs o fundaciones, y en otros simplemente termina como chatarra. Pero ¿qué hay de los datos contenidos en esos equipos? En muchos casos se los tiene en cuenta, pero no en todos.

Con el fin de mantener los niveles de confidencialidad deseados de una organización, y más allá de las buenas prácticas, es indispensable además del cumplimiento de los procedimientos aplicables durante el uso de los equipos, que la información almacenada **sea efectivamente eliminada** cuando éstos o sus medios de almacenamiento son descartados por cualquier razón.

Existen cuatro categorías[3] de mecanismos para deshacerse de información:

1. **Desecho**: la información se elimina sin ningún tipo de tratamiento. Este procedimiento se utiliza cuando la información a eliminar no presenta riesgos a la organización si su contenido se divulgara. Por ejemplo, arrojar un papel a la basura.
2. **Limpieza**: la información se elimina de tal forma que se impide su recuperación mediante herramientas de recuperación de datos. Por ejemplo, eliminar un archivo en disco y luego sobrescribir la porción de disco donde el mismo solía estar.
3. **Purga**: la confidencialidad de la información se protege contra ataques de laboratorio que utilizan sistemas de procesamiento de señales y personal altamente especializado. Un ejemplo de este tipo de mecanismo es la desmagnetización de un disco magnético.
4. **Destrucción**: la información se elimina físicamente, de tal forma que no es posible recuperar la misma ni sus residuos. Incluye varios métodos, entre ellos se encuentran la desintegración, la incineración y la pulverización.

[3] *Guidelines for Media Sanitization*, página 7 *"Sanitization Types"*: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Riesgos existentes

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad.

El riesgo tecnológico puede verse desde tres aspectos[4]:

- ❏ A nivel de la infraestructura tecnológica (hardware o nivel físico).
- ❏ A nivel lógico (riesgos asociados a software, sistemas de información e información)
- ❏ Riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de estar conscientes que la administración del riesgo informático juega un rol crítico.

Las empresas afectadas por vulnerabilidades de seguridad pueden esperar el pago de un alto precio y sufrir las consecuencias de la erosión de la confianza, de la marca, pérdida de negocio y, en algunos casos, sanciones civiles e incluso criminales.

Tipos de controles para mitigar riesgos

Un **control** es un proceso que se lleva a cabo para proporcionar un grado razonable de confianza para el cumplimiento de los objetivos que sigue una empresa. Existen distintos tipos de controles, a saber:

- **Preventivos**: identifican el riesgo antes de que se produzca. Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
- **Detectivos**: se utilizan para detectar riesgos luego de que se materializan. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.
- **Correctivos**: ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

.

A lo largo del desarrollo del presente trabajo práctico, se analizará cómo se protege la información durante el siglo XIX y siglo XXI, y cuáles eran los riesgos a los que estaban expuestos.

Siglo XIX

Introducción

La ciencia y la tecnología entraron en una estrecha interacción durante el siglo XIX. Hacia la segunda mitad del siglo XIX, la ciencia estimuló muchas invenciones conduciendo al crecimiento de tecnologías e industrias basadas en la ciencia, como en el caso de la electricidad y la química.

[4] *Riesgo Tecnológico y su gran impacto en las organizaciones* http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

La Revolución Industrial que se había iniciado a mediados del siglo XVIII se consolidó durante el siglo XIX. Muchos fueron los avances técnicos que se produjeron durante este siglo en muchos campos de la ciencia y de la tecnología, los cuales sentaron las bases de lo que iba a ser el posterior desarrollo científico durante el siglo XX.

Otro factor de importancia en el desarrollo de los mecanismos legales de administración de la propiedad intelectual fue la política de la época. Tras la Revolución Francesa las monarquías europeas fueron cediendo a la presión por políticas más liberales por parte del nuevo empresariado burgués empoderado en nuevas posiciones políticas. En España Fernando VII copia el modelo de propiedad intelectual francés por presión de grupos liberales hacia 1820. En América la disgregación y separación de la corona española del Reino de Indias daba inicio a una serie de tensiones políticas entre diferentes actores que impulsaron la independencia. Guerras civiles y la fragmentación de territorios en Estados-Nación mantuvo ocupada la atención política la mayor parte de este siglo. La consolidación de los estados hacia la segunda mitad del siglo facilitó que estos participaran del marco internacional que se fue gestando a través de la firma de algunos convenios a fin de siglo.

El continente africano durante el siglo XIX estuvo influenciado por las potencias colonialistas europeas. En materia legal y de propiedad intelectual rigió la ley europea para las colonias, en tanto su aplicación era más o menos controlada según el alcance de los organismos de aplicación de las leyes que fueron surgiendo a lo largo del siglo. Muchas investigaciones de distintas ciencias en este siglo se desarrollaron en colonias africanas o en distintas expediciones incluso. Se destacaron campos de la biología y ciencias médicas, aunque también hubo descubrimientos en ciencias como la astronomía y matemáticas. La consolidación del marco legal europeo se intensificó a partir de la Conferencia de Berlín.

En América del Norte, en Estados Unidos, las posturas de los inventores Thomas Jefferson y Benjamin Franklin de que las ideas no pueden ser apropiadas por persona alguna fue perdiendo terreno por el arrollador avance del capitalismo y el progreso industrial que demandaba incentivos para nuevos desarrollos. Con la firma del Convenio de París en 1883 para la protección de la Propiedad Industrial y luego del Convenio de Berna en 1886 para regular los derechos de autor sobre obras artísticas y literarias se consolidó el marco jurídico internacional.

La locomotora de vapor y el barco de vapor vieron la luz en el siglo XIX. El automóvil o los buques con casco de hierro son algunos de los inventos que iban a revolucionar el transporte en décadas posteriores. En el campo de la electricidad hay que destacar la pila eléctrica, o la dinamo eléctrica que se inventaron en la primera mitad del siglo. El transformador de corriente alterna se inventó en 1885.

Durante este siglo se inventaron multitud de máquinas. La cosechadora, la cortadora de césped, la prensa rotativa, la máquina de coser, el refrigerador comercial, la grapadora, la turbina hidráulica, el ascensor eléctrico, el gramófono, el fonógrafo o la bicicleta de pedales son algunos de estos inventos. Daimler inventó la motocicleta en 1885.

Inventos como el teléfono, la radio, o el automóvil serán fundamentales en el siglo XX. El desarrollo de motores como el de cuatro tiempos y posteriormente del motor diesel y del motor eléctrico compacto, serán esenciales para el desarrollo del automóvil, que se convertirá en el elemento básico de transporte en la centuria siguiente.

Otros inventos importantes de este período son la máquina de escribir, el periscopio, la esquiladora, el ventilador eléctrico o la tarjeta perforada. A final de siglo verán la luz el cinematógrafo de los hermanos Lumiere, la fotografía de colores, la cremallera, la grabadora de cinta o la estufa eléctrica.

Inventos del siglo XIX[5]

- ❏ Locomotora: 1804.
- ❏ Fonógrafo: 1878.
- ❏ Lámpara Incandescente: 1854.
- ❏ Fotófono: 1880.
- ❏ Cinematógrafo: 1894.
- ❏ Vitascopio: 1896.
- ❏ Gramónofo: 1888.
- ❏ Fotografía: 1826.
- ❏ Teléfono: 1854.
- ❏ Anestesia: 1846.
- ❏ Dirigible: 1863.
- ❏ Avión: 1890.
- ❏ Termómetro Clínico: 1866.
- ❏ Sensor de temperatura de resistencia de platino.
- ❏ Lente de Fresnel.
- ❏ Pastilla de jabón.
- ❏ Margarina.
- ❏ El método de la pasteurización: 1864.
- ❏ Coca-Cola, 1886.
- ❏ La aspirina Feliz Hoffmann,1899

[5] *Siglo XIX - Inventos* http://es.wikipedia.org/wiki/Siglo_XIX

Mecanismos de defensa

Esteganografía

La esteganografía se puede definir como el ocultamiento de la información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto.

Más de 400 años antes de Cristo, Heródoto ya reflejó en su libro Las Historias el uso de la esteganografía en la antigua Grecia. En dicho libro se describe como un personaje toma un cuadernillo de dos hojas o tablillas, raya bien la cera que las cubre, y en la madera misma graba un mensaje y lo vuelve a cubrir con cera.

Heródoto también narra la historia de un mensaje tatuado en la cabeza rapada de un esclavo de Histiaeus, oculta por el pelo que luego creció con él, y expuesta por afeitarse la cabeza. Este método posee dos desventajas, tales como la transmisión retrasada mientras se espera para que el cabello crezca, y las restricciones sobre el número y tamaño de los mensajes que pueden ser codificados en el cuero cabelludo de una persona[6].

En la China antigua se escribían mensajes sobre seda fina, que luego era aplastada hasta formar una pequeña pelota que se recubría de cera y que un mensajero se tragaba.

En el siglo XV, el científico italiano Giovanni della Porta explicó en su obra *Magia naturalis* una manera de hacer llegar un mensaje a los prisioneros de la Inquisición. El truco consistía en esconder el mensaje dentro de un huevo duro. Al parecer, la Inquisición era muy estricta en cuanto a lo que se entregaba a los prisioneros; sin embargo, no lo era tanto con respecto a los huevos, sobre los que no había sospecha posible. El método se basaba en preparar una tinta mezclando alumbre y vinagre, y con ella escribir el mensaje en la cáscara. Al ser ésta porosa, la solución penetraba por los pequeños agujeros y pasaba a la superficie de la clara del huevo duro. De esta sorprendente forma, al pelar el huevo se podía leer el mensaje[7].

Otra práctica es la de escribir con tinta invisible[8]. Los antiguos griegos y romanos ya usaban tinta invisible que extraían de la naturaleza, a partir de ciertos árboles y frutos. Por ejemplo, en el siglo I a.C., Plinio el Viejo tenía conocimiento de que la savia de la planta *Tithymallus* podía usarse como tinta invisible. Se utilizaban sustancias con alto contenido en carbono: leche, zumo de limón, jugo de naranja, jugo de manzana, jugo de cebolla, orina, etc. Básicamente, sin importar cuál de las tintas mencionadas se utilicen, al calentar la superficie donde se escribió el mensaje invisible, el carbono reacciona apareciendo el mensaje en un tono café.

A lo largo de muchos años, la esteganografía ha ofrecido ingeniosas ideas para garantizar las comunicaciones secretas. En muchos casos, estas técnicas han resultado ser muy útiles para ocultar la existencia de mensajes y cumplir con éxito su cometido. Sin embargo, la esteganografía tiene una debilidad básica: la estrategia para la comunicación secreta se basa simplemente en la ocultación del mensaje. Todo se reduce a que el mensaje pueda pasar inadvertido, ya que en el momento en que éste se descubre, el contenido de la comunicación se revela.

Criptografía

[6] *Esteganografía.* http://centrodeartigo.com/articulos-noticias-consejos/article_125403.html
[7] *Esteganografía: el arte de pasar inadvertido, Página 12* http://www.editorialterracota.com.mx/pdf/Criptografia.pdf
[8] *Esteganogafría, artículo de Wikipedia.* http://es.wikipedia.org/wiki/Esteganograf%C3%ADa

Al mismo tiempo que se desarrollaba la esteganografía, se produjo la evolución de la llamada criptografía. El objetivo de la criptografía no es ocultar la existencia de un mensaje (para eso está la esteganografía), sino ocultar su significado. Es decir, la criptografía se encarga de enmarañar la información de tal manera que el mensaje que se quiere transmitir no lo entienda nadie, excepto la persona a la que va destinado. De esta manera, aunque el mensaje sea interceptado, su contenido seguirá seguro.

Los primeros mensajes cifrados que conocemos datan del siglo V antes de Cristo, de procedencia espartana, que ponían en práctica un método simple y rudimentario que consistía en coger una vara (llamada escítala), se le enroscaba una cinta de cuero o papiro y posteriormente se escribía de forma longitudinal. Y por último se desenrollaba la cinta, con un puñado de letras sin sentido y se mandaba a través del mensajero de turno al trote.
Supuestamente solo se podía desencriptar la información con una vara del mismo diámetro que la original sobre la que se escribió[9].

A principios del siglo XIX Thomas Jefferson invento una máquina constituida por 10 cilindros que estaban montados en un eje de forma independiente, en donde se colocaba el alfabeto y al girar los cilindros, quedaba cifrado el mensaje.

En 1854 Sir. Charles Wheatstone diseñó un método de cifrado llamado Playfair, este método era parecido al de Polybios solo que ahora en vez de que cada carácter se sustituyera por dos caracteres sólo se sustituía por uno. Se trata de un cifrado digráfico formado por una matriz cuadrada de 5x5 elementos en los que se introducen las letras del alfabeto, utilizándose la misma celda para la I y la J[10].

Para 1867 Wheatstone había ideado un nuevo disco de cifrado que en realidad se trataba de una versión mecánica del disco de Alberti; esta nueva versión ocupaba en el disco exterior el alfabeto inglés más un signo de "+" colocados de manera ordenada en sentido de las manecillas del reloj y el disco inferior tenía solamente 26 casillas con el alfabeto colocado de manera desordenada. Las agujas estaban engranadas de tal manera que cuando la externa giraba 27 posiciones, la interna lo hacía 26, estableciendo de esta manera una correspondencia entre los dos alfabetos.

En 1890 étienne Bazeries, tomando como base el cilindro de Jefferson creó un cilindro que constaba de 20 discos coaxiales con 25 letras en cada uno de ellos,, la diferencia con el cilindro de Jefferson es básicamente la manera de cifrar el mensaje, ya que el disco de Bazeries al tener un disco adicional con números impresos, el criptograma del mensaje en claro podía conformarse con letras de varias generatrices estableciendo el número de la generatriz con que se cifraba cada carácter del mensaje en claro.

Patentes de Invención

En la economía industrial, los activos físicos correspondían a la parte principal del valor de una empresa y eran determinantes para medir la competitividad de una empresa en el mercado.

Durante el siglo XVIII se desarrolló la discusión sobre si las invenciones e ideas podían ser propiedad o no de sus dueños, disputa propiciada por derechos entendidos de libre acceso al conocimiento humano y el de recibir beneficios el autor de un beneficio, cuando ese beneficio es generado justamente gracias a una idea. Grandes inventores como Thomas Jefferson y Benjamin Franklin eran partidarios de la no apropiación de las invenciones por parte de los inventores.

[9] Criptografía. http://bioestegoencript.blogspot.com.ar/2014/04/criptografia.html
[10] Historia de la Criptografía - Discos, cilindros y otros métodos de cifrado. http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/12-historia-de-la-criptografia?showall=&start=2

El desarrollo de la industria y la necesidad de fomentar nuevos inventos propiciaron que la política de patentes fuera configurándose en lo que es hoy. Las antiguas cédulas reales de privilegio de invención fueron siendo reemplazadas por patentes de invención basadas en un derecho natural, reclamable de forma evidente.

A comienzos del siglo XIX (1811, 1820 y 1826), las patentes como modalidad de Propiedad Industrial sustituyeron a las *Reales cédulas de privilegio de invención,* que venían concediéndose aleatoriamente, al menos desde 1478. A mitad de siglo, en 1850, se reguló la concesión de marcas de fábrica y comercio.

El impacto económico y los desarrollos que han propiciado todo tipo de invenciones provocaron, en un momento dado, la necesidad de establecer sistemas adecuados para la protección intelectual que las fomentasen y defendiesen.

Caja de seguridad

En la era donde los activos tangibles eran más importantes, la protección física de los datos era más relevante. Este potencial medio de protección de información (como también otros bienes tangibles, principalmente dinero, oro, joyas, etc.) es bastante auto descriptivo en su forma de salvaguardar: obstrucción física de acceso al elemento a proteger. A continuación veremos cómo fue evolucionando a través de la historia.

La caja fuerte más antigua apareció en el 700 AC aproximadamente, y pertenecía a Corinto de Cipselus. La caja consiste en un arcón de cedro con incrustaciones de marfil y oro, lo cual lo hacía valioso por sí solo, además de sus contenidos. La caja fuerte de hierro apareció por primera en el Imperio Romano. Gracias al desarrollo de la cerrajería y las técnicas de forja se lograron excelentes resultados en cuanto a la vulnerabilidad de estos elementos a mediados del siglo XIX.

La debilidad de las cajas fuertes es justamente la administración de las llaves que las abren y el factor humano que las administra.

Servicios tercerizados de guarda de bienes fueron ofrecidos desde tiempos del Imperio Romano bajo distintos marcos jurídicos. Pero el servicio de cajas de seguridad como hoy se lo conoce logra su gran evolución en la segunda mitad del siglo XIX. La fundación en el año 1861 de la *Safe Deposit Company* de Nueva York y en el año 1875 de la *National Safe Deposit Company Limited*, fue el origen de una vasta serie de empresas de difusión prácticamente universal, dedicadas a la prestación del servicio de custodia de bienes (Martorell, Ernesto Eduardo; “Tratado de los contratos de empresa”, T. II-Contratos Bancarios, pág. 499 y s.s.).

Riesgos

- ❏ Si las invenciones no eran patentadas, se corría el riesgo de que alguien más desarrollara la misma invención, y que incluso sea patentada antes que su inventor.

- ❏ Otro riesgo relacionado con no patentar las invenciones, es que otras organizaciones se aprovecharán de la invención, viéndose tentadas a fabricar el mismo producto.

- ❏ Las dificultades en el control del uso de una patente publicada, especialmente si el objeto de la patente era de relativa simplicidad para su desarrollo o aprovechamiento, podían perjudicar al dueño de la patente por lucro cesante.

- ❑ El desarrollo de objetos patentables en equipos de trabajo era delicado debido a que una persona o subgrupo de miembros del equipo podía adelantarse y patentar como propio el producto. Esto era particularmente delicado en grupos de trabajo más o menos informales que no tuvieran algún estatuto o código de sociedad formal.

- ❑ Robo de documentación. En este siglo toda la documentación de investigaciones estaba en soporte físico basado en papel. El conocimiento intermedio de una investigación, empero, podría ser aprovechable por un público especializado únicamente.

- ❑ Copia de patentes en el extranjero. Previo a la firma del Convenio de París, que dio un marco internacional a la protección de derechos de propiedad industrial, un invento patentado en un país podía ser copiado y patentado en otros países por otras personas. Aún luego de la firma del Convenio de París las patentes pueden ser copiadas a países que no lo suscribieron, pero la mitigación del riesgo con el convenio es ya muy importante.

Riesgos de no aplicar esteganografía y criptografía: Fueron métodos ampliamente utilizados en la antigüedad para salvaguardar la información clave que debía ser protegida del acceso enemigo. Por ejemplo se utilizaban para proteger datos de las batallas, de esta manera las estrategias a aplicar en el campo de batalla en caso de que cayeran en manos del enemigo no podían ser descifrados. Así mismo también podían usarse la criptografía para proteger planos de inventos en proceso.

Riesgos de no utilizar cajas fuertes: De no utilizar este medio de protección existía la posibilidad de que se produjera la pérdida o daño de información, o así mismo que cayeran en manos enemigas.
Esta protección externa, proporciona hasta la actualidad uno de los medios más utilizados por las personas con intenciones de proteger su propiedad tanto material como intelectual.

Riesgos de no patentar un invento o conocimiento: Siguiendo el desarrollo de esta época, encontramos dos ejemplos de los riesgos que puede ocasionar el no patentar un invento. Fueron los casos del inventor alemán Philipp Reis del teléfono quien a pesar de haber sido el primero en desarrollar un artefacto similar al que hoy conocemos como teléfono, por no haberlo dado a conocer públicamente y haberlo asentado en un registro de patentes hoy es Alexander Graham Bell a quien el mundo conoce como el inventor del teléfono.
Otro caso similar fue el del inventor de la lámpara de luz incandescente, a quien se atribuye su invento a Mr Edison pero sin embargo Humphry Davy fue quien realmente fabricó la primera luz incandescente al pasar la corriente a través de una delgada tira de platino.
Estos ejemplos claramente demuestran que el riesgo de no patentar un invento o conocimiento puede que sea adjudicado a otro.

Casos reales

Durante la Guerra Civil Americana, la Unión utilizó la sustitución de palabras seleccionadas seguida de una transposición de palabras mientras que los Confederados usaron Vigenère, el cual se consideraba irrompible. Los mensajes confederados fueron poco secretos, ya que los miembros de la unión rompían habitualmente los mensajes[11].

El 19 de Enero de 1917, el *Telegrama Zimmermann* fue interceptado y descifrado lo suficiente como para poder leer un esbozo de su contenido[12]. Un mensaje que desencadenaría en uno de los momento más trascendentes de la Primera Guerra Mundial.

El 1 de junio de 1944 la máquina Colossus interceptó un mensaje crucial: Hitler y su Alto Mando esperaban un ataque aliado masivo en Calais. Esto determinó que el general Eisenhower decidiera desembarcar sus tropas el 6 de junio en las playas de Normandia. El efecto sorpresa multiplicó el golpe sobre la defensa germana. Este hecho, junto al éxito descifrador de la máquina Colossus, supuso, según un artículo de *The Guardian*, de 1995, un acortamiento de la guerra de por lo menos dos años[13].

El automóvil
Supuesto Inventor: Henry Ford
Inventor Real: Karl Benz
Aunque a muchos nos dijeron que el inventor del automóvil era Henry Ford y, a pesar de que, ya varios ingenieros alemanes (incluyendo Gottlieb Daimler, Wilhelm Maybach, y Siegfried Marcus) estaban trabajando en el tema más o menos al mismo tiempo, Karl Benz es, en verdad, a quien se le atribuye la invención del automóvil moderno. Así, en 1885, Benz logró crear un vehículo propulsado por su propio motor de cuatro tiempos, que funcionaba a base de gasolina en Mannheim, Alemania. Se le otorgó la patente en enero del año siguiente, bajo los auspiciado por la empresa, Benz & Cie (fundada en 1883). Se trataba de un diseño integral, que, aunque sin la adaptación de los otros componentes existentes, desarrollados por los demás ingenieros, incluía elementos tecnológicos totalmente innovadores que lo hacían único. Estos lo hicieron merecedor de la patente y así, el primer auto moderno comenzó a venderse en 1888. Ford, en tanto, no se dedicó a la producción de estos hasta 1896, o sea once años después de que Benz hiciera el suyo.

La Radiografía o Fotografía de Rayos X
Supuesto Inventor: Thomas Alva Edison
Inventor Real: Wilhelm Röntgen
Si bien es cierto que fluoroscopio de Edison se convirtió en el artefacto estándar utilizado en Medicina, no fue el primero en conseguir Fotografías de Rayos X. El 22 de diciembre de 1895, Wilhelm Röntgen (profesor de física alemán) logró obtener una foto de la mano de su esposa en una placa fotográfica formada por rayos-X. Esta fue primera imagen de una parte del cuerpo humano con rayos-X. Su contribución a la Ciencia y Fotografía de rayos-X resultó tan importante que, actualmente, también se les llama “rayos Röntgen”.

Las Filmaciones o Imágenes en Movimiento
Supuesto Inventor: Thomas Alva Edison
Inventor Real: Louis Le Prince

[11] *Cifrado de Vigenère* http://jcabana-cripto.blogspot.com.ar/
[12] *Telegrama Zimmerman*n http://es.wikipedia.org/wiki/Telegrama_Zimmermann
[13] *La Criptografía Clásica, Página 21*
http://www.hezkuntza.ejgv.euskadi.net/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf

Otra vez, aparece Edison como supuesto inventor. Sin embargo, el clip de arriba (las primera imágenes en movimiento) fue registrado, a 12 cuadros por segundo por el inventor francés Louis Le Prince. Así, mientras que la primera filmación atribuida a Edison apareció en 1889 o 1890, Le Prince registró la suya el 14 de Octubre de 1888, en la casa de Joseph y Sarah Whitley, en Leeds, West Yorkshire, Inglaterra ; y las personas que aparecen son Adolphe Le Prince (hijo de Louis), Sarah y Joseph Whiteley, y Harriet Hartley. Ahora viene la parte oscura: diez días después de filmar, Sarah Whitley murió. Dos años más tarde Le Prince desapareció misteriosamente de un tren que viajaba entre Dijon y París. Otros dos años después, Alfonso (el hijo mayor), fue hallado muerto en Nueva York después de testificar en un juicio contra la patente de Edison por la American Mutoscope Company. Dejo estos datos a la consideración de cada uno, pero, en mi opinión, como dije en un post anterior, la mayor habilidad de Edison fue robar inventos ajenos antes de que lograran patentarse, mejorarlos o adornarlos un poco, hacerlos parecer como propios rápidamente y, finalmente, desacreditar o perseguir a sus verdaderos creadores.

Las Grabaciones de Sonido o Audio
Supuesto Inventor: Thomas Alva Edison
Inventor Real: Édouard-Léon Scott de Martinville
Acá hay que reconocer algo: Thomas Alva Edison concibió el principio de la grabación y reproducción de sonido, entre mayo y julio de 1877 como un sub-producto de sus esfuerzos para "reproducir", mensajes telegráficos grabados y automatizar los sonidos del habla para su transmisión por vía telefónica. El 21 de noviembre de 1877, anunció la invención del fonógrafo, un dispositivo de grabación y reproducción de sonido. Sin embargo, 17 años antes (1860), el francés Édouard-Léon Scott de Martinville inventó el fonoautógrafo, el cual podía grabar y registrar en Transcripciones el sonido, aunque no consiguió desarrollar los medios para reproducirlo una vez grabado. Esas transcripciones, conocidas como Fonautogramas, fueron reproducidas por primera vez con éxito, utilizando tecnología informática, en 2008 y se puede escuchar en ellas claramente la voz de una mujer cantando "Au clair de la lune", registrada hace más de 150 años.

El Teléfono
Supuesto Inventor: Alexander Graham Bell
Inventor Real: Philipp Reis
Casi todos hemos escuchado la historia de Alexander Graham Bell, en la cual, supuestamente, al inventar el teléfono, lo habría usado por primera vez para llamar a su secretario, el Sr. Watson. Sin embargo el primer teléfono que funcionó, fue creado 15 años antes por Philipp Reis, un inventor alemán. Su dispositivo (que él llamó la Telephon Reis) fue exhibido públicamente en 1861. El Telephon Reis sólo era capaz de transmitir los tonos musicales con bastante claridad, y las voces humanas muy débilmente, pero eso no quita que la primera transmisión de esta por medio de cables haya sido a través del dispositivo de Reis. Bell, como muchos de los “inventores” de esta lista, simplemente, habría mejorado el diseño.

La Radio
Supuesto Inventor: G. Marconi
Inventor Real: Nikola Tesla
En 1895, Marconi presentó al público un dispositivo de radio en Londres, afirmando que era su invención. Pese a ello, el diseño del aparato era idéntico a las descripciones realizadas por Nikola Tesla en varios de sus artículos científicos traducidos a numerosos idiomas. Así el sistema de fabricación del mismo era igual al desarrollado por N. Tesla entre los años 1893 y 1895. A finales de ese último año, Marconi realizó la supuesta primera transmisión de señales desde una distancia de kilómetro y medio. Sin embargo, el ingeniero electromecánico Nikola Tesla, quien ha sido llamado el padre de la telegrafía sin hilos, ya había patentado una forma de emitir ondas de radio frecuencia. Es más, entre 1895 y 1899, Tesla dijo haber recibido señales inalámbricas de transmisión a larga distancia, aunque, hay que reconocerlo, no hay evidencia concreta para apoyar esto.

La Bombilla Eléctrica

Supuesto Inventor: Thomas Alva Edison
Inventor Real: Humpry Davy (concepto), Warren de la Rue
Y para terminar esta lista de inventos "robados", ¿quién mejor que Mr. Edison?. En fin, aunque a todos nos hayan enseñado que él fue el inventor de la Bombilla eléctrica, ya en 1802, Humphry Davy fabricó la primera luz incandescente al pasar la corriente a través de una delgada tira de platino. Es cierto, no fue lo suficientemente brillante ni duró lo bastante para ser un descubrimiento práctico; pero fue el precedente de todos los esfuerzos posteriores en este campo. Más tarde, en 1840, un químico y astrónomo inglés, llamado Warren de la Rue colocó un espiral de platino dentro de un tubo de vacío y logró hacer pasar electricidad a través de ella, creando la primera bombilla funcional. Recordemos que Edison recién “inventaría” su más famosa creación en 1879/1880.

Siglo XXI

Introducción

El siglo XXI se caracteriza por un cambio de la economía tradicional traída en la revolución industrial hacia una **economía basada en la información.** Durante esta era, la industria es capaz de explorar las necesidades personales de los consumidores, lo cual trae aparejado una reducción de costos tanto para los consumidores como para las empresas.

Algunos de los **eventos[14] que marcan esta era** son los siguientes:

- 2001: Nace Wikipedia, una enciclopedia gratuita y de acceso público.
- 2004: Nacen Gmail y Facebook.
- 2005: Nace YouTube, una plataforma de videos masiva.
- 2006: Nace WikiLeaks, un proyecto cuyo objetivo es publicar documentos confidenciales.
- 2007: Apple lanza el teléfono iPhone.
- 2011:
  - Egipto bloquea todo acceso a internet, en un intento de evitar que activistas organicen protestas contra el presidente Hosni Mubarak. El bloqueo es temporal y no tiene éxito.
  - Se publican 100 millones de contraseñas de usuarios de Sony en Japón.[15]
- 2013: Se produce una batalla legal entre Samsung y Apple por divulgación de información confidencial sobre un acuerdo de patentes entre Apple y Nokia.
- 2014: Se produce la divulgación de fotos privadas de 26 celebridades mediante la plataforma iCloud de Apple.

Durante este período, caracterizado por la miniaturización de las computadoras y la **proliferación de internet** desde el año 1990, la fuga de información se ve incrementada gracias a la rápida expansión de los medios de comunicación. Dado que existen más formas de comunicación que se utilizan dentro de las organizaciones, han emergido nuevas formas de fuga de información, como ser la mensajería instantánea, los correos electrónicos, la ingeniería social, etc.

En el campo de la **medicina**, la situación es crítica. La información clínica de los pacientes es almacenada electrónicamente, y esto permite que las autoridades envíen registros de enfermedades a investigadores; en muchas ocasiones esto incluye los nombres y direcciones de los pacientes, sin su consentimiento explícito.[16]

[14] *Timeline: Social Media. Key dates in the evolution and increasing influence of social media. 2000.* http://www.infoplease.com/science/computers/social-media-timeline.html
[15] http://thehackernews.com/2011/05/sonys-3rd-massive-leak-100-million.html
[16] *The future of the NHS (National Health System), 2000*, Artículo de la revista *The Guardian*, Reino Unido. http://www.theguardian.com/society/2000/jun/25/futureofthenhs.health

Algunos **números** reflejan la situación actual:[17]

- En 2013, se reportaron 1143 incidentes de pérdidas de información confidencial. Esto representa un incremento del 22% con respecto a 2012.
- Más de 561 millones de registros fueron comprometidos, incluyendo información personal y financiera. El 85% de los registros que se divulgaron incluyen datos personales.
- Los Estados Unidos ocuparon el primer puesto en cuanto a cantidad de incidentes. Rusia se encuentra en segundo lugar y el Reino Unido en tercero.
- Las organizaciones estatales y las instituciones médicas continuaron siendo la fuente principal de fugas de información.
- Las pérdidas financieras causadas por los incidentes alcanzaron un costo total, en 2014, de 7,79 billones de dólares.

El **principal capital de las empresas tecnológicas** lo conforman los bienes o activos intangibles: información, conocimientos, algoritmos, fórmulas, invenciones, procesos, estrategia comercial y bases de datos, entre otros. Las organizaciones del siglo XXI deben estar preparadas para los siguientes desafíos:

- Manejar y procesar grandes volúmenes de información diversa a alta velocidad.
- Analizar datos estructurados y no estructurados, tanto dentro como fuera de sus redes.
- Monitorear eventos en entornos de nube, móviles y virtuales.
- Adoptar acciones automáticamente cuando se detecta una amenaza.

Mecanismos de defensa

Controles informáticos

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático. Existen varios mecanismos que permiten sustentar la seguridad informática, donde uno sólo de ellos no es suficiente para garantizar el éxito, ya que es necesario complementarlos para obtener un buen resultado. Entre ellos se destacan:

- Restricciones de acceso físico
- Utilización de contraseñas seguras
- Uso de firewalls y software antivirus
- Encriptación de las comunicaciones confidenciales
- Copias de seguridad de la información
- Encriptado de las copias de seguridad
- Distinción de niveles de acceso según autorización formal en perfiles de usuarios
- Registro de operaciones en bitácoras automatizadas
- Registro de accesos en bitácoras automatizadas
- Redundancia de datos
- Localización múltiple y distante de estructuras de datos redundantes
- Políticas de recuperación ante catástrofes

Utilización de patentes

Una patente[18] es un conjunto de derechos que se le otorgan a un inventor por un período limitado de tiempo (20 años), a cambio de la divulgación de los detalles del mismo. Las patentes son una forma de

[17] *InfoWatch Global Data Leak Report, 2013*
tps://infowatch.com/sites/default/files/report/InfoWatch_Global_data_leak_report_2013_ENG.pdf
[18] *Patent*, Artículo de Wikipedia. http://en.wikipedia.org/wiki/Patent

propiedad intelectual, y le proporcionan al dueño la garantía de que otras empresas no podrán producir, utilizar o vender el producto patentado sin permiso.
El sistema de patentamiento fue creado en Venecia en 1450, pero fue durante la revolución francesa que se creó el sistema moderno. En general, las patentes sólo pueden materializarse durante litigios, y puede ser dueños de ellas tanto empresas como personas, aunque en ciertos casos los empleadores pueden exigirles a sus empleados que las patentes le sean adjudicadas a ellos.

De acuerdo a un ranking[19] de las patentes poseídas por distintas áreas geográficas, encontramos que:

- En Europa, los tres grupos económicos con mayor número de patentes registradas son Siemens y Alcatel (empresas de tecnología), Daimler y Volkswagen (industria automotriz), Bayer y Basf (laboratorios farmacéuticos), con un total aproximado de 93000 patentes.
- En Norteamérica, el listado lo encabezan empresas pertenecientes a la industria tecnológica: Hewlett Packard, General Electric, Intel, Microsoft, Motorola y Kodak, con un total aproximado de 75800 patentes.
- En Asia (particularmente Japón y Corea del Sur), empresas tecnológicas como Hitachi, LG, Canon, Samsung y Sony totalizan casi 1 millón de patentes.
- El resto de los continentes no figuran en el ranking.

Entre las críticas a este sistema, se encuentran los altos costos asociados al mantenimiento de patentes (por ejemplo, en Estados Unidos el mismo puede alcanzar los 30 mil dólares por patente), y el hecho de que no promueven la innovación, al limitar el uso de las nuevas tecnologías.

Utilización de estándares internacionales

Para la mayoría de las actividades es necesario basarse en estándares, normalmente de alcance internacional, y normativas vinculadas a lo que se quiera organizar. La fuga de información está contemplada dentro de la gestión de la seguridad, y como tal se describen contramedidas y técnicas en distintos estándares. Así pues, se apela con frecuencia a la serie de normas ISO 27000, que está especialmente dedicada a seguridad de la información. Dentro de esta familia se encuentran específicamente algunas normas como lo son la 27001, referida a los requisitos para implementar un sistema de gestión de seguridad, la 27002 que define las mejores prácticas, la 27004 que habla sobre las métricas, la 27005 que trata sobre la gestión de riesgos, entre otras.

Auditorías

En las empresas, para facilitar la trazabilidad de las acciones de los usuarios, se suelen incluir procedimientos mediante los que se garantiza que el uso de los activos de información es efectivamente auditado y que es posible generar **registros (*logs*) de las acciones importantes** que se hayan definido, que si bien es un proceso técnico, implica un conocimiento de los individuos respecto a su grado de responsabilidad en lo que realizan dentro de una empresa. El conocimiento de la vinculación entre las personas y sus accesos puede evitar en gran medida la fuga de información, ya que en caso de filtrarse hacia el exterior, se podría señalar de manera directa a todos aquellos que tuvieron acceso y se podría analizar su uso previo al incidente, obteniendo posibles conclusiones y responsables. De cualquier manera, dada la imposibilidad de monitorear a las personas más allá de la esfera laboral, es estrictamente necesario que exista un alto grado de concientización y que las políticas de seguridad estén correctamente aplicadas para garantizar que quienes manejen información confidencial tengan asumidos los riesgos relacionados con su filtración.[20]

[19] *Ranking of the group's invention by geographical areas:* ttp://www.corporateinventionboard.eu/en/corporate-rankings
[20] *Fuga de información, ¿una amenaza pasajera?, 2011*, página 7: http://www.welivesecurity.com/wp-content/uploads/2014/01/fuga_de_informacion.pdf

Uso de *code names* para los proyectos

Este mecanismo de defensa solo se aplica a empresas comerciales, particularmente tecnológicas[21]. Gigantes como Microsoft y Apple suelen utilizar nombres clave para los productos que están en fase de desarrollo y aún no se han lanzado al mercado. Como ejemplos podemos mencionar al proyecto Blackcomb (Windows 7).

Las razones para su uso son varias:

- Permiten a los trabajadores de dichos productos hablar sobre los mismos sin revelar de qué se trata a terceros. Al utilizar nombres neutrales, se obliga a enfocarse en el producto y prevenir la generación de asociaciones basándose en el nombre.
- Permiten crear un impacto positivo en los potenciales consumidores, al utilizar nombres que atraen al mercado.

[21] *3 reasons why you should use project codenames.* http://blog.bonusbox.me/bonusbox-blog-english/2014/8/10/xtbg7jxrjx8tdjzaxa7nmul2rttn09

Riesgos

- ❑ Personal deshonesto con niveles de autorización de acceso sensibles. Lo único que cambia respecto del siglo XIX es la mayor importancia que tiene en un mundo globalizado el impacto de la información.

- ❑ Políticas de administración de accesos inapropiada puede facilitar robo, alteración o pérdida de información.

- ❑ Espionaje industrial. Debido a la mayor conciencia sobre la importancia de la información el espionaje industrial, como concepto amplio, es un factor a tener en cuenta en sí mismo, y en combinación con todos los demás riesgos. En esta categoría se puede encontrar desde el hurto técnicamente más sencillo hasta equipos sofisticados de hackeo y crackeo en distancias remotas, financiados por servicios de inteligencia gubernamentales u otros organismos clandestinamente.

- ❑ Dependencia de sistemas informáticos. Con el desarrollo de la tecnología muchas empresas dependen absolutamente de sus sistemas de información para desarrollar sus procesos vitales.

- ❑ Capacitación de los operarios. La informatización abrupta de los procesos operativos genera el riesgo de una demanda de personal con capacidad de llevarlos adelante con las herramientas informáticas implicadas y la contemplación de las particularidades y casos de excepción al proceso típico. Este riesgo se menciona desde el punto de vista de la exposición de la información por la capacitación del personal.

- ❑ Calidad e implementación de un sistema informático. Programas desarrollados a medida o grandes sistemas mal implementados pueden generar situaciones de riesgo para la administración de la información.

- ❑ Administración de perfiles de usuario y contraseñas. Sin una política apropiada de para control de perfiles de usuario y usuarios con sus niveles de acceso podría generarse exposición indeseada o vulnerabilidad de la información.

- ❑ Dependencia de empleados clave. La centralización de estas funciones vitales para cualquier organización genera una dependencia muy directa y una vinculación de este personal con la alta gerencia. Por otro lado el poder que mantienen estos empleados sobre el resto del personal implica la necesidad de una política clara que administre las relaciones laborales de manera adecuada.

- ❑ Confianza y comodidad excesiva. La facilidad con que a veces se implementan sistemas y se resuelven cuestiones administrativas tediosas con poco trabajo puede degenerar en un acomodamiento de los actores y la pérdida de agilidad para resolver situaciones nuevas. En el peor de los casos se puede estar incurriendo en riesgos no contemplados, como por ejemplo de seguridad de accesos o falta de una política apropiada de back ups, que por ignorarlos tanto tiempo pueden estallar algún día de la peor manera.

- ❑ Generación de información residual. La interacción de los sistemas informáticos con otros sistemas informáticos, el uso de Internet a través de proveedores del servicio sujetos a sus propios riesgos, y la generación de archivos automatizada son agentes de riesgo por cuanto pueden dar información a quien la pueda captar e interpretar sobre actividades o situaciones del dueño.

- ❑ Administración del soporte físico de la información. Un empleado que lleva su computadora portátil del trabajo a reparar o la pierde, envío de soportes físicos de información a ámbitos poco seguros, entre otras cosas, pueden generar problemas.

Casos reales

Empresas relacionadas con la salud

En el año 1996 se promulgó en Estados Unidos la ley HIPAA (Health Insurance Portability and Accountability Act), cuyo objetivo es asegurar la privacidad de los pacientes y la seguridad de la información relacionada a ellos[22]. En el año 2004 se produjo el primer caso de violación a esta ley, cuando un empleado de una asociación de enfermos de cáncer utilizó información de pacientes para obtener tarjetas de crédito.

En el año 2005, empleados de un hospital fueron descubiertos mientras obtenían información de la internación por maternidad de la cantante pop Britney Spears.

Empresas tecnológicas

Uno de los casos con mayor repercusión fue el de Wikileaks, una organización sin fines de lucro que desde 2006 permite que personas que tengan cierta información sensible de interés público puedan publicarla en dicho sitio web, preservando el anonimato y garantizando la publicación tal cual esta fue ingresada. El sitio llegó a los grandes medios en noviembre de 2010, cuando comunicó a la prensa internacional una colección de más de 250.000 cables entre el Departamento de Estado estadounidense y sus embajadas por el mundo, transformándose en la mayor filtración de documentos secretos de la historia, además de haber afectado al país.

En los últimos años se han dado a conocer otros casos relevantes, como el del banco HSBC, que en marzo de 2010 declaró la fuga de datos de 15.000 clientes suizos, luego de que un ex-empleado del área informática les llevará los datos a autoridades impositivas de Francia.

En enero del mismo año tuvo lugar la Operación Aurora, un ataque masivo ocurrido contra más de 30 empresas como Google, Adobe y Juniper; destacado por ser uno de los ataques más importantes en materia de robo de información, aunque finalmente no tuvo éxito.

En diciembre de 2009, la red social Tuenti fue afectada por el robo de 4.000 cuentas de usuario y sus contraseñas, por parte de un atacante enojado con la empresa.

En julio de 2008 si bien no se dieron a conocer casos como los anteriormente mencionados, se produjo una importante cantidad de incidentes de seguridad basados en la vulnerabilidad del protocolo DNS descubierta por el especialista de seguridad Dan Kaminsky, que sirvió de base para realizar ataques de phishing, propagación de malware y otros. Ese año, según un informe de incidentes de Verizon, el 39% de los incidentes de seguridad involucraron a partners y terceras partes de las empresas, y el 31% de los ataques incluyeron algún código malicioso (en ese entonces el protagonista era el gusano Nuwar).

En agosto de 2007 el sitio global de búsquedas laborales Monster sufrió el robo de 1,6 millones de datos con información personal de los usuarios registrados. Los atacantes ingresaron a las bases de datos con contraseñas que habían sido obtenidas previamente mediante un troyano.

[22] *Health Information Leaks, 2012.*
http://www.ocf.berkeley.edu/~issues/articles/20.1_Mock_L_Patient_Health_Information_Leaks_HIPAA.html

Conclusiones

La amenaza más grande para las organizaciones probablemente no sean los ataques de terceros (*crackers*, *phishers*, o ingenieros sociales), ni los empleados maliciosos, sino los empleados descuidados que de forma inintencionada divulgan información sensible. Una combinación de protección tecnológica, políticas y procedimientos actualizados, y educación de los usuarios deberían contribuir a paliar los efectos que causan estas fugas.

El procedimiento básico para desarrollar una estrategia de protección consiste en lo siguiente: clasificar la información a proteger, entender los datos que se manejan –qué representan y cuánto valen para el negocio–, establecer políticas sobre el manejo de la información y capacitar al personal en las herramientas. Luego, se debe implementar seguridad a nivel físico; por ejemplo, mediante el uso de firewalls y software antivirus. Para organizaciones más pequeñas y con un presupuesto limitado, se puede considerar el uso de servicios de terceros. No debe olvidarse de ejecutar revisiones periódicas, para mantener las políticas actualizadas y en conformidad con los requisitos y las tendencias tecnológicas.

A pesar de que los ataques maliciosos son una minoría, no deberían ser ignorados. Es claro que, hoy en día, existen múltiples vías de escape de información que deben ser monitoreadas. Si bien no existen soluciones que protejan los activos intangibles de forma 100% segura, se puede minimizar la probabilidad de que ocurran pérdidas mediante la aplicación de varios métodos complementarios.