PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

SANDRA LILLIANA ZULETA PULGARÍN
AUTOR

FERNANDO ANTONIO MORENO FORERO
ASESOR

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
DIRECCIÓN POSGRADOS
CONVENIO UPB MEDELLÍN
ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD
MEDELLÍN
2014

Resumen

Es usual la aparición de noticias en todos los medios, sobre empresas que han sufrido una pérdida de datos, sea de manera intencional o no. Las fugas de datos generan enormes pérdidas económicas, costos legales y sanciones. Además de costos indirectos como la pérdida de clientes, desventaja competitiva y el deterioro de la imagen y la reputación.

Las causas pueden ser; ataques maliciosos, hacking, errores u omisiones en el uso de los datos por parte de los empleados. Y a través de empleados cuando salen de la empresa también se filtran documentos confidenciales.

Para prevenir la fuga de datos; se debe crear una cultura de protección de la información, propendiendo para que los empleados tomen conciencia de la necesidad de mantener la información confidencial protegida, crear y monitorear políticas de protección, compartirlas con los empleados, y restringir el acceso a la información en las aplicaciones y servicios, son algunas de las medidas más importantes.

Palabras Clave: Fuga – Información – Protección – controles.

Introducción

El tratamiento de los datos personales por parte de entidades financieras requiere de sumo cuidado. Tanto en la recolección como en el tratamiento. Sólo se pueden recoger datos personales informando al usuario el uso que se les dará a estos y cumpliendo los requisitos establecidos por la Ley. Estos requisitos son un desafío por sus altos estándares de cumplimiento. Los altos directivos tienen la responsabilidad legal de evitar la fuga de datos, y pueden ser demandados, perder su trabajo, si no cumplen con sus responsabilidades. Adicionalmente Todos los empleados, son responsables de asegurar la información de los clientes, para cumplir con los pilares de seguridad en cuanto a confidencialidad, integridad y disponibilidad.

Ya se están tomando algunas medidas de protección requeridas para la empresa, independiente de su tamaño, siempre que tengan información personal de clientes. Un incidente llamó la atención a nivel mundial y demostró que ninguna empresa está a salvo porque la seguridad completa no existe, el efecto de las medidas de protección es minimizar el impacto y la probabilidad de los riesgos, Es el de Wikileaks ejemplo perfecto de cómo una fuga de información puede tener consecuencias impensadas y un enorme impacto, debido a la naturaleza de la información filtrada, el daño fue muy grande y puso en jaque al gobierno americano, el cual realizo grandes esfuerzos para minimizar el impacto del incidente.

PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

Un término importante en este tema es la fuga de información, se trata de salidas no controladas de información personal, donde esta puede llegar a personas no autorizadas y sucede cuando se revela parte de la información a procesar o transmitir debido a errores u omisiones en los procedimientos de uso de esta. El crecimiento de la información personal en una empresa sobrepasa su capacidad de protegerla y gestionarla.

Los datos personales; son los concernientes a las personas, que tengan carácter de privados, que estén ligados a su intimidad y que toquen temas susceptibles de discriminación como orientación sexual, religiosa, étnica, entre otros.

La protección de datos, **s**on todas las medidas que se toman, tanto a nivel técnico como jurídico para garantizar que la información de los usuarios de una empresa, entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas. La norma en Colombia indica que las empresas deben proteger esos datos.

Es importante también reconocer el auge que han tenido las redes sociales, pues generan otro riesgo de fuga de información para las empresas. Esto se traduce, básicamente, en más usuarios, más datos, más dispositivos y aplicaciones fuera del perímetro tradicional de seguridad interno.

Independiente de las políticas, procedimientos y herramientas que se tengan implementadas, el comportamiento inadecuado (intencional o no intencional) de algunos empleados pone en riesgo la información confidencial de las empresas.

Algunos ejemplos comportamientos inadecuados son; utilización de programas no autorizados en equipos de la empresa, compartir los equipos móviles de la empresa con personas ajenas a esta, traspaso de información entre equipos de trabajo y personales, compartir contraseñas, compartir información confidencial en redes sociales, entre otros. Los ataques en la mayoría de las veces son motivados por razones económicas y detrás de éstos hay empresas bien estructuradas que buscan obtener ganancias sin dejar el más mínimo rastro (crimen organizado).

Hoy las amenazas y ataques son más frecuentes, más complejos y están orientados principalmente a las aplicaciones y bases de datos para obtener información valiosa.

La protección de la información, evita la fuga y hace referencia a la protección desde tres pilares: confidencialidad, integridad y disponibilidad. La fuga de información es la pérdida de la primera, la pérdida de la confidencialidad, de forma que: termina siendo visible o accesible para otros que no están autorizados.

> Es por esto que, aun cuando una víctima de delitos bancarios tiene la percepción de que la obtención de su información financiera o de sus credenciales de autenticación fue provocada por una fuga de datos del banco, la verdad es que, en la gran mayoría de los casos, el origen de la pérdida se origina en el cliente mismo. (Cuéllar, 2013, p.5).

En la evolución de la fuga de información, los cambios han sido las maneras y tecnologías por medio de las cuales se filtra o pierde, el problema de la fuga de información existe desde cuando los humanos manejan información. El incidente de Wikileaks estableció un antes y un después en la historia. La fuga de información tiene una componente social y humano muy importante.

Detrás de una parte importante de los incidentes se esconden motivaciones personales, errores, omisiones en políticas y procesos entre otras. Este incidente en el año 2010 está considerado hasta la fecha, como la mayor filtración de información de la historia. Wikileaks, una empresa sin ánimo de lucro, publicó un total de 250.000 (cables) comunicaciones que se habían realizado entre el Departamento de Estado Estadounidense y sus embajadas repartidas por todo el mundo. Las consecuencias no se hicieron esperar. Este incidente supuso la confirmación de algo que ya se sabía: la gran dificultad de mantener la confidencialidad de la información, evitando filtraciones y también puso de manifiesto como ninguna empresa está a salvo, incluidas aquellas con altos niveles de seguridad, porque disponen de programas de capacitación y entrenamiento para el personal, procedimientos, políticas, herramientas y personal entrenado para manejar información confidencial. Más como ha quedado demostrado, la seguridad completa no existe y la información es manipulada por personas, y como es conocido en seguridad - las personas son el eslabón más débil de la cadena -.

Los medios por los que más de filtra información son: a través de malware, aplicaciones, dispositivos móviles, correo electrónico, y redes sociales. Diversos estudios han demostrado que aproximadamente un 10% de las pérdidas de datos se producen a través de dispositivos tales como portátiles, PDAs, unidades USB y otros dispositivos extraíbles, como CDs regrabables, e iPODs. Este tipo de fuga de datos es el más difícil de combatir.

Según informe hasta la mitad de 2014 se han expuesto 502 millones de registros de distintas bases de datos, superando con creces la primera mitad del año 2013 y marcando un récord absoluto en la fuga de información en Colombia, dos incidentes de hacking exponen una combinado 318 millones de registros, el sector de negocios representaron el 64,3 % del número de registros expuestos, seguida de

Gobierno (34,9 %), el 78,2 % de los incidentes reportados fueron el resultado de Hacking, que representaron el 78,7 % de los registros expuestos. (Risk Based Security, 2014).

Hacia finales del año pasado Symantec detectó una serie de ataques sin precedente en la historia, a los que denominó como una "mega fuga de información" en la cual los atacantes planean por más tiempo concretar algún tipo de amenaza. La firma de seguridad menciona a través de un comunicado que una mega violación de datos puede valer lo equivalente a 50 ataques pequeños, mientras tanto los niveles de sofisticación entre los atacantes también han registrado mejoría. (Symantec, 2013).

Las implicaciones de la fuga de datos si caen en las manos equivocadas son de alto impacto: especialmente por los costos financieros pueden dejar mal una empresa, el costo para resolver un problema de fuga de datos es muy alta.

Las sanciones financieras por las fugas de datos son cada vez más elevadas. Multas recientes en el sector financiero fueron en el 2009 que varias empresas HSBC salieron multadas con más de 3,3 millones de libras esterlinas, más el costo de la pérdida de clientes, la imagen negativa, la pérdida de reputación en el mercado y la pérdida de confianza por parte de los clientes.

Los costos legales de sanciones de la Superintendencia de industria y comercio en cumplimiento de Ley 1581 tienen las siguientes multas, primero; multas de carácter personal e institucional hasta por 2000 SMLMV, segundo; suspensión de actividades relacionadas con el tratamiento hasta por 6 meses. En acto de cierre se indicarán los correctivos, tercero; cierre temporal de las operaciones si no se adoptan los correctivos, cuarto; cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles. (Certicamara. 2013).

Los controles existentes para evitar la fuga de información son una oportunidad de mejora; pues previenen, detectan, corrigen y minimizan los riegos como son; los errores humanos, fallas de seguridad, de hardware, de software y la pérdida de dispositivos, los motivos más frecuentes de fugas. Para prevenir, las empresas deben monitorear, mejorar, mantener y optimizar el funcionamiento de sus sistemas de seguridad.

Una de las formas cómo se pierden los datos, puede ser; porque si antes, la mayoría de información era estructurada, con la seguridad de los controles en las aplicaciones y bases de datos de la empresa. En la actualidad, más del 80% de la información no es estructurada y tiene forma de mensajes de correo electrónico, documentos de texto, archivos PDF, presentaciones y hojas de cálculo entre otros. Este contenido poco estructurado circula libremente en el interior y el exterior de la mayoría de las empresas. Se estima que el 16% de las fugas de datos proviene del uso del correo electrónico externo y un 5% más lo hace del correo que circula dentro de la empresa.

El correo electrónico es difícil de controlar y se suman otras fuentes de fugas como; La mensajería instantánea, el correo Web, los foros, blogs, redes sociales, el uso y perdida de dispositivos de almacenamiento, abuso de privilegios de usuarios, distribución no intencional de información confidencial y hacheo de aplicaciones, todos estos han disparado el riesgo de fuga de datos.

La oportunidad de manejar información confidencial, la gran capacidad de almacenamiento de los sistemas tecnológicos de hoy y la movilidad, hacen cada vez más factible que esos documentos e información, de gran valor para las empresas, sufran una fuga.

La Prevención de Fuga de Datos, tiene como objetivo evitar la fuga de información sensible de la empresa por puertos (USB, WIFI), la web, el correo electrónico, chat, FTP, la mensajería instantánea, las redes sociales y las personas. En los puntos finales, la red, y las bases de datos mediante las siguientes recomendaciones que se implementan de acuerdo al tamaño y al tipo de empresa.

Recomendaciones para evitar la fuga de datos

La complejidad de Internet y de las comunicaciones hace que las empresas necesiten proteger numerosas puertas de acceso a datos y protocolos. Es fundamental encontrar una solución que proporcione distintos niveles de protección, para distintas amenazas, en distintos protocolos y servicios.

Es importante entender la realidad; y es necesario hacer lo posible para comprender las medidas a tomar. No se pueden controlar todas las acciones de todas las personas en todo momento, siempre habrá un margen de error y deberá reducirse al mínimo a medida que pasa el tiempo y se implementan nuevos controles para proteger los datos.

Tabla 1. Recomendaciones para evitar la fuga de datos

Recomendación	Alcance	Tipo de control
Cifrado de datos	Datos personales que se encuentren en movimiento, en portátiles, dispositivos de almacenamiento y en correos electrónicos	Preventivo
Protección contra amenazas de software malicioso	Internet y correo electrónico	Preventivo Detectivo Correctivo
Implementación de Políticas	Se deben implementar de igual manera para todos, teniendo en cuenta que hay diferentes tipos privilegios de acceso y la política de clasificación de la información debe ser clara para facilitar su cumplimiento	Preventivo
Instalar herramientas de protección de datos	Un sistema de prevención de fuga de datos debe manejar una amplia variedad de identidades, desde clientes, terceros, consultores internos y directivos. Se debe dedicar el tiempo necesario para la definición de los requisitos de DLP, se debe conseguir una solución no intrusiva	Preventivo Detectivo Correctivo
Proteger los endpoints	Computadores de escritorio y portátiles, smartphones, PDAs, entre otros. Sin afectar su flexibilidad y facilidad de uso para la empresa.	Preventivo Detectivo
Proteger el correo electrónico	Correo interno, externo y servicio alojado en la nube	Preventivo
Tener buenos programas de capacitación y entrenamiento	Para los empleados de todas las áreas, enfatizando que es responsabilidad de todos proteger la información e incluyendo temas como el cuidado con el uso de las redes sociales por parte de adultos y niños	Preventivo Detectivo Correctivo
Realizar el inventario de los activos de información sensible	Activos críticos de información	Preventivo
Gestión de terceros seguros	Los terceros que intervengan en el tratamiento de los datos sensibles, tengan también implementados los controles mínimos de seguridad	Preventivo Correctivo
Gestión de seguridad sea centralizada en la medida de lo posible	Para aplicaciones, servicios y redes	Preventivo Detectivo
Realizar análisis de riesgos	Que contemple una revisión tanto de las nuevas tecnologías como de las aplicaciones y los riesgos que éstas implican.	Preventivo Detectivo Correctivo
Monitoreo, medición y gestión de controles	Todo control implementado debe ser medido periódicamente para evaluarlo e identificar puntos de mejora y retroalimentar el diseño e implementación de los controles	Preventivo Detectivo Correctivo
Seguir los mejores estándares y prácticas de seguridad	estándares internacionales de gestión de la seguridad, permiten disminuir el riego de fuga de información, algunos de ellos; (norma ISO/IEC 27001:2013 sistema de gestión de seguridad de la información, norma ISO 31000 gestión de riesgos:2009, ISO/IEC 20000, gestión del servicio, COBIT, marco de gestión y de negocio global para el gobierno, ITIL	Preventivo Detectivo Correctivo

Recomendación	Alcance	Tipo de control
	su objetivo es mejorar la calidad de los servicios TI ofrecidos	
Acuerdos de confidencialidad	para empleados, y terceros, aceptados y firmados	Preventivo
Procedimientos de seguridad	De gestión accesos de usuarios incluido el eliminado los derechos al finalizar la contratación, de almacenamiento de datos, y de contratación y desvinculación segura.	Preventivo Detectivo Correctivo
Infraestructura tecnológica adecuada	Principalmente para el hardware y software que soporta las aplicaciones y servicios críticos del negocio	Preventivo
Cifrado y contraseña en redes Wi-Fi	Para todas las redes Wi-Fi de la empresa	Preventivo

Fuente: Elaboración propia

Uno de los temas más importantes a tener en cuenta de la tabla anterior, en los programas de capacitación es del uso de contraseñas, para las que se deben tener en cuenta los siguientes elementos; debe ser personal e intransferible, secreta, fácil de recordar, difícil de averiguar, y con renovación periódica.

Se deben crear utilizando palabras poco comunes, sin que se vinculen a un dato personal, con al menos 10 caracteres, combinando letras mayúsculas, minúsculas, números y signos, para cada sistema, y no se deben escribir en otros lugares visibles.

Para el uso de las contraseñas, cuide que nadie observe cuando la escribe, no observe a otros mientras lo hacen, no comparta su clave con otra persona, no habilite la opción de recordar contraseña en las aplicaciones, no envíe su clave por correo electrónico ni la mencione en una conversación, no entregue la contraseña, ni siquiera al administrador del sistema o al personal de soporte de servicio, solo en caso de que personal sistemas autorizado la requerirla para realizar reparaciones del equipo o software, y luego de la reparación cambie la clave de acceso.

Otra recomendación importante es implantar estándares como 27001, con la implementación de 27001, no solo protegerá los datos personales, sino que gestionara de manera integral la seguridad de toda la información confidencial de la empresa, la cual genera ventaja competitiva, porque expresa diferencia ante la percepción de los clientes y aliados estratégicos, se disminuyen los gastos generados por incidentes intencionales y no intencionales, se gestiona el acceso a usuarios, los activos de información, se gestiona la seguridad del personal antes, durante y después de la contratación, se gestiona la seguridad física, la de comunicaciones y operaciones, la segregación de funciones y el cumplimiento de varias normas sobre protección de datos.

También se obtienen garantías de continuidad del negocio, y en su mantenimiento se genera mejora continua a través de la metodología PDCA (Planificar, Hacer, Verificar y Actuar).

Cuando se encuentra en un nivel de madurez importante permite establecer una cultura de la seguridad y una gestión en el tratamiento de la información en todos los procesos de la empresa. Adicionalmente se puede interrelacionar con otras normas de gestión como norma ISO 31000 gestión de riesgos, ISO/IEC 20000, gestión del servicio, COBIT, marco de gestión y de negocio global para el gobierno, ITIL su objetivo es mejorar la calidad de los servicios TI ofrecidos.

Figura 1. Cumplimiento normativo relacionado con protección de datos en Colombia

Fuente: elaboración propia

Respecto a esta normatividad, en especial la ley 1581 la cual dicta disposiciones generales para la protección de datos personales en Colombia, que entre otros muchos beneficios disminuirá las llamadas a celular o fijo y los correos que llegan para vender un producto o servicio, para lo que

normalmente las personas no están interesadas. La reflexión es; como consiguieron los datos personales, en la mayoría de las veces fueron obtenidos de manera indebida.

En la ley se explica que, las empresas y entidades solo pueden utilizar la información para los fines para los que fue recogida. Las sanciones se aplicarán cuando las empresas hagan mal uso de la información que suministran sus clientes, vendan las bases de datos y cuando una empresa o entidad no le permita a un ciudadano actualizar su información personal incorporada en una base de datos en cualquier momento.

Su importancia radica en que la información personal puede ser utilizada para varios fines como la comercialización, la vida laboral e inclusive, para cometer delitos, porque su identidad puede ser suplantada en cualquier momento.

Los titulares de la información tienen derecho a encontrar de manera ágil y sencilla los datos suministrados por ellos y que se encuentra bajo la administración de otros. Cualquier persona puede consultar de manera gratuita sus datos personales, al menos una vez al mes. En caso de no recordar haberse inscrito en una base de datos, la persona puede solicitar una prueba de la autorización inicial por la que fue inscrito y también puede retirar sus datos.

El propietario de los datos tiene derecho a que se le describa para qué y cómo será utilizada su información y también tiene derecho a la actualización, rectificación y supresión cuando lo considere oportuno.

Las empresas que manejan información de clientes deben asignar una persona como responsable de protección de datos personales.

Herramientas del mercado de protección de datos

La adopción de una herramienta DLP (Data Loss Prevention), también llamada prevención de fuga de datos, prevención de pérdida de información, está siendo impulsada por amenazas internas de alto impacto y por las leyes sobre privacidad, muchas de las cuales tienen estrictos componentes de protección de datos.

Los productos de software de DLP utilizan reglas de negocio para examinar el contenido de los archivos y etiquetar la información confidencial y crítica, para que los usuarios no pueden divulgarla. El software puede ser útil para identificar y etiquetar contenido bien clasificado (como los números de tarjetas de crédito y datos personales en general), para implementar con éxito el software DLP se necesita involucrar activamente a toda la empresa.

Una vez que las herramientas de software DLP han sido implementadas, un usuario final que intente, de manera accidental o malintencionada, revelar información confidencial que ha sido etiquetada, será identificado y la información protegida.

Además de ser capaces de monitorear y controlar las actividades de los puntos finales, las herramientas de DLP también pueden ser utilizadas para filtrar flujos de datos en la red de la

empresa y proteger los datos en reposo. Las marcas más reconocidas e incluidas en el cuadrante mágico de Gartner se muestran en la siguiente gráfica:

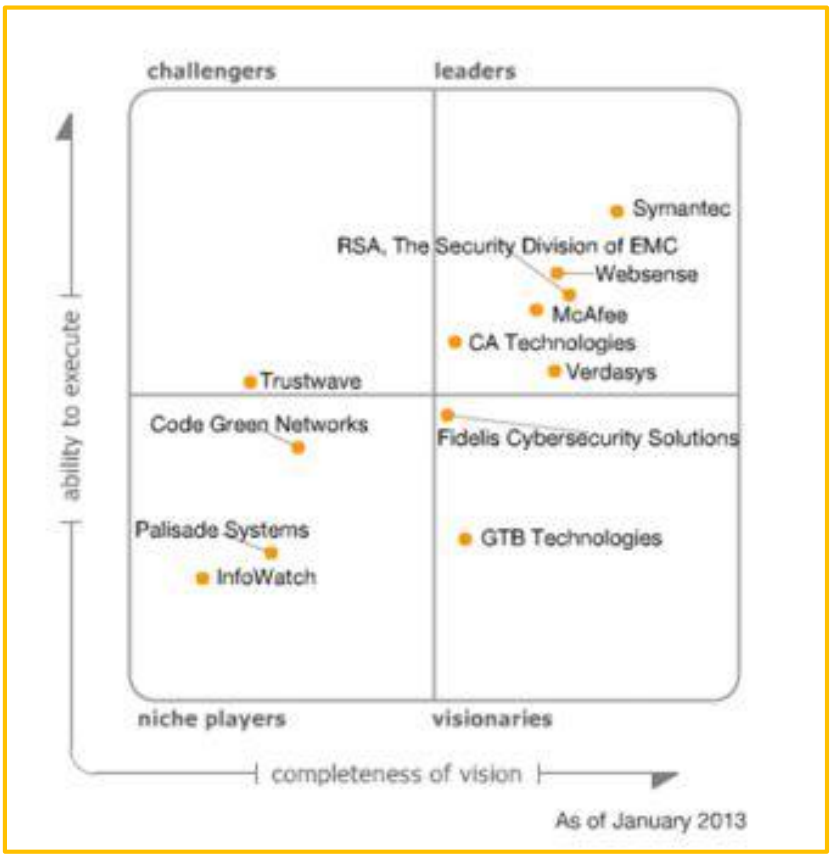

Figura 2. Magic quadrant for content-aware data loss prevention

Fuente: Gartner

Dentro de las herramientas de protección de datos incluidas en Gartner, las más conocidas son; McAfee, Websense y Symantec, todas proveen; auditoria y reportes centralizados de cumplimiento para diferentes módulos y/o grupos, despliegue y administración centralizada, políticas unificadas para datos en uso, en movimiento y en reposo, monitoreo y captura por

puerto o protocolo, descubrimiento de datos no estructurados, integración de contenido cifrado para datos en uso, en movimiento y en reposo entre otras funcionalidades.

Momento de la protección de datos en Colombia

Las dimensiones que está tomando la importancia de la protección de datos en Colombia es lenta, más hay que aprobar la entrada en vigencia de la ley 1581, ahora es importante que se le dé continuidad a su seguimiento y control. Apoyado en campañas y estrategias lideradas por la SIC y con el apoyo entidades como Asobancaria entre otras, donde enseñen a las personas de todas las edades a proteger sus datos personales, y se realice una buena gestión y trabajo en equipo con las empresas del sector público y privado para la debida protección de los datos, para así promover y mantener la confianza del público y la cultura del cuidado de los datos personales.

Cada persona debería proteger sus datos como un tesoro, porque en muchas ocasiones se genera perdida de datos por el mal uso que se le da, entregándola en cualquier lugar y por cualquier motivo como por ejemplo; para participar en la rifa de un supermercado o al momento de realizar alguna degustación de producto u obtención de un obsequio, que no ameritan que se les entregue; nombre, cédula, dirección, correo electrónico y hasta números de teléfono celular y fijo. Y de parte de las entidades públicas y privadas exigir que brinden igual responsabilidad con su protección.

Hay límites aún por la falta de compromiso de algunas empresas, porque en general se están implantando medidas de seguridad importantes y utilizándolas para competir con este plus en el mercado.

Desde mi punto de vista todos debemos poner nuestro granito de arena para aportar a este cuidado y ser un país confiable en el manejo de datos personales, para así contribuir con una buena imagen nacional respecto a la protección de datos personales. Y estar preparados para no recibir sorpresas como en otros países.

Conclusiones

Para considerar que una empresa es segura, debe implementar controles de seguridad en toda la empresa; de personal, de procesos, de aplicaciones y herramientas tecnológicas, para así poder minimizar los riesgos de fuga de información. Siendo muy relevante la capacitación a los empleados y la gestión de las salvaguardas o controles implementados.

La protección de la información tiene grandes desafíos y a medida que las empresas deben cumplir normativas locales e internacionales, las cuales regulan el tratamiento de información confidencial. Es mejor estar preparados para cumplir legalmente, proteger la información y minimizar la probabilidad e impacto de un posible incidente. Que exponerse al riesgo de fuga de datos con todas sus implicaciones.

Por medio de un sistema de gestión de seguridad de la información, se pueden controlar los riesgos a los que se encuentra expuesta la información personal, en la actualidad se está empezando a dar la importancia que se merece la protección de los datos en una empresa, Se puede concluir que si no existe un sistema de gestión de seguridad, difícilmente se lograra un buen nivel de protección de datos en la empresa, siendo muy importante en este sistema el fomento de la cultura en seguridad dirigida a todos los empleados.

Referencias

Asamblea Nacional constituyente. (1991). *Constitución Política.* http://blog.iso27001standard.com/ ISO 27001 & ISO 22301

Certicámara. (2013). *ABC Para Proteger Los Datos Personales Ley 1581 De 2012 Decreto 1377 De 2013*. http://goo.gl/F4iHbU

Cobit. (2012). *Marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa.* http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

Cuéllar, M. (2013). *VII Congreso De Prevención De Fraude Y Seguridad*, 5-15. http://www.asobancaria.com/portal/pls/portal/docs/1/3794047.PDF

Deloitte. (2013). *Cómo sobrevivir a los APTs*. http://www.inteco.es/sessions/enise/ponencias/listado_talleres_plenarias/T12Po2 12_ miguel rego.PDF

Icontec. (2013). *Norma técnica NTC-ISO-IEC 27001 Sistema de gestión de seguridad de la información.* Bogotá: editada Icontec

Icontec. (2009). *Norma ISO 31000 Gestión de Riesgos*. Bogotá: editada Icontec

Icontec. (2011). ISO/IEC 20000 *Tecnología de la información y Gestión del servicio.* Bogotá: editada Icontec

ITIL. (2011). *Calidad de los servicios TI ofrecidos.* http://www.osiatis.es/formacion/Formacion_ITIL_web_version3.pdf

Kosutic Dejan, (2012). *Ciberseguridad en 9 pasos.* http://www.iso27001standard.com/es/free-ebooks/9-steps-to-cybersecurity-managers-information-security-manual-es

Microsoft. (2012). *La Protección de datos personales*. http://www.videosinformatica.es/biblioteca/doc/libros/proteccion_datos.pdf

Ministerio de comercio industria y turismo. (2012). *Ley 1581*. http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Superintendencia de Industria y Comercio. (2009). *Ley 1273* http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Superintendencia de Industria y Comercio. (2009). *Ley 1266*. https://www.uiaf.gov.co/?idcategoria=20630

Symantec. (2014). *Tendencias De Seguridad Cibernética*. http://goo.gl/bV59xl

Risk Based Security. (2014). *Data Breach QuickView* https://www.riskbasedsecurity.com/reports/2014-MidYearDataBreachQuickView.pdf