SEGURIDAD JURIDICA EN BASES DE DATOS

España Paz, Gustavo., Leguízamo Avila, Yenny.
gespana26@gmail.com,yenny.leguizamoa@gmail.com
Universidad Piloto de Colombia

Resumen—Este artículo, presenta de manera general el tratamiento que se debe dar a la información personal almacenada en las Bases de datos de las empresas, de acuerdo a lo establecido en la Ley 1581 de 2012, mediante la cual se reglamentan los derechos y deberes para el uso y tratamiento de los datos personales almacenados por organizaciones públicas, financieras y de salud, entre otras.

Comúnmente los datos sensibles se encuentran almacenados en sistemas de administración de bases de datos como Oracle, Microsoft SQL y otros, que aunque cuentan con medidas de seguridad son vulnerables a ataques e intrusiones que pueden afectar la confidencialidad de esta información.

Abstract—This article provides an overview of the treatment to be given to personal information stored in the databases of the companies, according to the provisions of Law 1581 of 2012, by which regulates the rights and duties for the use and treatment of personal data stored by public, financial and health, among others.

Commonly sensitive data are stored in management systems such as Oracle databases, Microsoft SQL and others, although have security measures are vulnerable to attacks and intrusions that may affect the confidentiality of this information.

Índice de Términos— autorización, dato personal, protección de datos.

I. INTRODUCCIÓN

La ley colombiana 1581 de 2012 reglamenta las medidas de seguridad que deben adoptar las organizaciones, que almacenan datos personales para garantizar la seguridad de estos, con el objetivo de evitar perdida, adulteración, uso o acceso por fuera de la autorización expresa de la persona. Procedimiento que deberá ser mantenido en la transferencia, procesamiento o almacenamiento de datos personales.

El presente artículo está enmarcado sobre los principios de: *circulación restringida, seguridad y confidencialidad* del proyecto del decreto [12] que reglamenta el artículo 25 de la Ley 1581 de 2012, ofreciendo al lector una visión general de la ley a través de los ataques a los que puede estar expuesta la información, así como una guía básica de protección a las bases de datos frente a intrusiones y/o accesos no autorizados para fines ilícitos, que conllevan sanciones a las organizaciones que van desde 2000 salarios mínimos legales vigentes hasta el cierre temporal de las operaciones.

La participación masiva de la tecnología informática, especialmente Internet, en las actividades que cotidianamente se realizan en la sociedad actual, ha incrementado el interés y la clandestinidad de quienes buscan acceso no autorizado a información y sistemas privados.

II. RIESGOS Y AMENAZAS SOBRE DATOS PERSONALES

La importancia que se le ha atribuido a la información personal, atrae la curiosidad por conocerla con o sin autorización, de acuerdo a la necesidad de quien la consulte utilizando mecanismos como:

A. Ingeniería Social

Es común escuchar la inconformidad de las personas por recibir información acerca de productos y servicios no solicitados a través de: llamadas telefónicas, correspondencia o visitas a la dirección de trabajo o residencia, y, al correo

electrónico. Todo esto sin haber entregado de manera previa los datos de contacto a estos iniciadores de comunicación.

> *"La respuesta es clara. La entidad encargada que tuvo en sus manos la información de mis datos personales contenida en mi solicitud, y que tenía responsabilidad de salvaguardarla hizo una divulgación inapropiada y abusiva" como se cita en [1]*

En las actividades cotidianas se requiere el intercambio de información personal y pública para el establecimiento de relaciones comerciales y sociales de toda índole, sin embargo, las personas no siempre son advertidas del uso que se dará a esa información o dan su consentimiento sin conocer las condiciones de tratamiento que tendrán sus datos personales, cuando son custodiados por un tercero.

B. Redes Sociales

La información que se publica, almacena o intercambia a través de internet y/o redes de comunicaciones, es susceptible de ser interceptada, conocida o modificada por terceros no autorizados. Además, posibilita el seguimiento de costumbres o datos sensibles que suministren herramientas para acciones ilícitas tales como: extorsión, fraude, suplantación de identidad, entre otras.

C. Clandestinidad

La comunicación entre las personas no requiere la presencia física de las mismas, puede llevarse a cabo por medios virtuales y no necesariamente en tiempo real. Lo que proporciona a un usuario mal intencionado, hacer uso de técnicas y conocimientos apropiados para borrar sus huellas del proceso de comunicación o direccionarlas a un usuario suplantado, dificultando o imposibilitando el rastreo de sus acciones.

.

D. Herramientas Gratuitas

Actualmente existe una gran variedad de herramientas comerciales que apoyan la implementación de medidas de seguridad en las redes de comunicaciones y sistemas de información, en la misma proporción, existe una diversidad de herramientas gratuitas que identifican y vulneran las medidas de seguridad implementadas, para lograr accesos y/o actividades no autorizados; estas herramientas pueden contar con redes de colaboración que capacitan al usuario en su uso adecuado.

III. PROTECCIÓN DE BASES DE DATOS

El Congreso de Colombia, implementó lineamientos para la protección de datos personales a partir de la Ley 1581 de 2012, en la que se establecen los derechos de las personas sobre el manejo de su información personal en manos de terceros.

En el ámbito de esta Ley se definen términos importantes a tener en cuenta., como son:

A. Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. Como en [11]

B. Base de datos

Conjunto organizado de datos personales que sea objeto de Tratamiento. Como en [11]

C. Dato personal

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

D. Encargado del tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. Como en [11]

E. Responsable del tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. Como

en [11]

F. Titular

Persona natural cuyos datos personales sean objeto de Tratamiento. Como en [11]

G. Tratamiento

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Como en [11]

La Ley se encuentra orientada a siete principios que deben ser acatados por todos aquellos que custodien información personal de terceros, como son: principio de veracidad o calidad del registro de los datos, principio de finalidad, principio de circulación restringida, principio de temporalidad de la información, principio de interpretación integral de derechos constitucionales, principio de seguridad y principio de confidencialidad. Estos principios pueden ser consultados en la Ley 1281 de 2012.

IV. ¿Quién gestiona el cumplimiento de la ley?

La Superintendencia de Industria y comercio ha sido designada para administrar el registro nacional de bases de datos, y, las entidades que custodien datos personales, deberán reportarle la adopción de un sistema de seguridad de información y las condiciones técnicas requeridas para proporcionar un nivel de seguridad razonable en la actualización de registros, pérdida, consulta y uso no autorizado.

V. ¿Cómo registrar una base de datos?

Para registrar una base de datos ante la Superintendencia de Industria y Comercio (SIC), se debe notificar la siguiente información: Datos del responsable del tratamiento de los datos, datos del encargado del tratamiento de los datos, canales dispuestos a los usuarios para ejercer sus derechos, nombre y finalidad de uso de la base de datos a reportar, vigencia de la base de datos, sistema y tratamiento que se aplicará a la base de datos, política de tratamiento de la información.

VI. Asegurar la base de datos

Se deben proporcionar medidas de seguridad a las bases de datos como: definir e implementar políticas de seguridad claras y acordes con las necesidades del negocio, apoyadas en la definición de procedimientos que permitan ejercer control sobre el entorno en que opera o interviene el manejo de las bases de datos, entre los cuales, controles de acceso en la red, condiciones del sistema operativo y las aplicaciones en las que procesa o maneja la base de datos. Así mismo, la ejecución de labores de auditoría y monitoreo periódico que permita ejercer acciones oportunas sobre eventos atípicos.

A. Identifique los datos sensibles

No se puede asegurar lo que no se conoce, para ello se debe elaborar un catálogo de tablas donde se almacenen los datos sensibles de sus instancias de base de datos.

B. Evalué las vulnerabilidades de configuración

Revise que no existan vulnerabilidades de seguridad en la configuración de sus bases de datos y los procedimientos para accederla u operarla. De existir, verifique que cuenta con controles adicionales para mitigar el riesgo o implementé las medidas necesarias para robustecer las medidas de seguridad en la configuración.

C. Aseguramiento

Resultado de la evaluación de vulnerabilidades se obtendrá un listado de recomendaciones o acciones a implementar, defina un plan de trabajo para analizar e implementar las medidas necesarias para cumplir con las recomendaciones.

Defina e implemente una lista de verificación que le permita evaluar de manera periódica las condiciones de las bases de datos y asegúrese de actualizarla cuando se apliquen modificaciones o actualizaciones a los procedimientos o parámetros de las bases de datos.

D. Monitoreo

Defina e implemente tareas de monitoreo (automáticas, manuales) que le permitan conocer en tiempo real, las desviaciones de las condiciones normales de operación de las bases de datos y tomar las acciones necesarias de manera oportuna para limitar la exposición a riesgos.

E. Realice Auditorias

Una vez implementada la configuración recomendada a las bases de datos y las medidas de aseguramiento, realice autoevaluaciones periódicas para verificar que las medidas de seguridad son funcionales y pertinentes a la situación real de la organización, de ser posible acuda a expertos para la evaluación y analice las recomendaciones recibidas.

F. Pistas de Auditoria

Genere la trazabilidad de las actividades ejecutadas sobre las bases de datos, que puedan afectar la integridad de los datos o exponer la confidencialidad de estos.

Recuerde la importancia de mantener los registros de auditoría activos, los cuales deben generar alertas en tiempo real y la información que generen debe ser lo más clara y funcional posible para facilitar las tareas de detección y corrección del incidente, o, rastreo e investigación forense.

G. Autenticación

Establezca medidas de gestión de acceso a través de mecanismos automáticos de autenticación, teniendo en cuenta que no todos los datos tienen el mismo grado de sensibilidad y que no todos los usuarios tienen las mismas necesidades de acceso y operación sobre esta información.

H. Cifrado de Información

Analice la posibilidad de hacer ilegibles los datos sensibles, complique el trabajo de los atacantes, implementando mecanismos de cifrado de los datos en tránsito, imposibilitando al atacante la oportunidad de escuchar en la capa de red y tener acceso a los datos cuando se envía al cliente de base de datos.

I. Copias de Respaldo de Información

Las organizaciones que manejan información personal, están sujetas a implantar medidas de seguridad de alto nivel para proteger estos datos y a su vez, asegurar la disponibilidad, confidencialidad e integridad de los mismos durante su tratamiento. Lo que incluye la ejecución de toma de copias de respaldo periódicas, que deberán ser custodiadas en medios de almacenamiento y sitios idóneos.

VII. Herramientas que apoyan la protección de bases de datos

En el mercado existen variedad de herramientas que facilitan la protección de las bases de datos entre las cuales, las que se mencionan a continuación:

A. Oracle Audit Vault and Database Firewall [14]

Realiza inspección del tráfico de red en busca de amenazas a la seguridad y análisis de auditoria de datos. También añade la capacidad para auditar sistemas operativos, directorios y otros recursos, más allá de la base de datos Oracle y sistemas de bases de datos de terceros, puede monitorear el tráfico SQL en la base de datos de Oracle así como en SQL Server de Microsoft, MySQL y DB2 de IBM.

B. InfoSphere Guardium Data Encryption(IBM) [15],

Cifra información de la Organización, sin sacrificar el desempeño de las aplicaciones o crear complejidad en la administración como la encriptación de la base de datos a nivel de columnas.

C. Dynamic Data Masking [16]

Software de enmascaramiento de datos escalable y de alto rendimiento, para bloquear o enmascarar información sensible o confidencial e impedir el acceso no autorizado a bases de datos de producción

o cercanas a la producción.

D. McAfee Vulnerability Manager for Databases [17]

E. Optim . [6]

Software de IBM para la gestión del cliclo de vida útil de los datos, a través de la cual se pueden manejar aspectos como: data archiving, gestión de ciclo de vida de los datos en ambientes de Big Data, nube y virtual.

VIII. ¿Cuándo exponemos los datos personales?

Cada vez que se ingresan datos como: nombre completo, número de teléfono, dirección, documentos, fotos, audios, videos, notas y otros, a sitios web. Estos datos son susceptibles de ser consultados por personas no autorizadas o para fines no legítimos.

Cuando se entrega información en el diligenciamiento de formatos de mercadeo, en centros comerciales, supermercados y otros sitios públicos sin cuestionar la finalidad de su recopilación o las prácticas aplicadas en el tratamiento de ésta información.

Cuando se envía o recibe a través de los diferentes medios de comunicación, información sensible propia de cada quien, sin las medidas de seguridad apropiadas, con el riesgo de ser interceptada, accedida o modificada con fines desconocidos y no autorizados.

Cuando se atienden ofertas de mercadeo y promociones que ofrecen incentivos a cambio de información personal.

IX. ¿Bases de datos ilegales?

La Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, ha venido atendiendo los reclamos de los ciudadanos frente al manejo de su información personal, lo que le ha permitido a la Superintendencia, identificar e investigar organizaciones que ofrecen bases de datos de información personal sin aplicar las medidas de seguridad pertinentes. [8]

La problemática de la comercialización no autorizada, de bases de datos que incluyen información personal, es común a diferentes países, debido a que estas bases de datos pueden ser obtenidas de modo ilegal de operadores de telefonía móvil, empresas de servicios masivos, entidades bancarias, call center, entre otros. [4]

Las debilidades de seguridad para custodiar estas bases de datos, sumado a las herramientas disponibles para accederlas sin ser identificado, permite que se incremente la comercialización de bases de datos. [5]

A continuación se presentan algunas noticias que involucran el uso o acceso indebido de información personal:


14 agosto 2012

"Datos reservados de 31 millones de colombianos fueron extraídos ilegalmente por la Dijín"

DENUNCIA Según una denuncia del director del Censo Electoral, Anthony Cotrino Sossa, datos biográficos y minucias dactiloscópicas de más de 31 millones de ciudadanos fueron extraídos de la Registraduría por dos agentes de la Dijin sin orden judicial.

El pasado viernes, en horas de la madrugada, y en una diligencia judicial, dos agentes de la Dijin de Bogotá aprovecharon para copiar "de forma ilegal" una de las bases de datos más custodiadas y reservadas de la Registraduría: el Censo Electoral.

Figura 1 Noticias sobre extracción de datos personales sin autorización [7]

SIC investiga ventas ilegales de bases de datos

Bogotá D.C., 17 de abril de 2012.-La Superintendencia de Industria y Comercio ha abierto en el último mes investigaciones contra empresas dedicas a la comercialización de bases de datos con información financiera y crediticia al advertir el presunto incumplimiento de la Ley 1266 de Habeas Data. En los reclamos presentados ante la Superintendencia por ciudadanos que se quejan del mal manejo de su información personal, se ha advertido la posible operación ilegal de empresas firmas que podrían estar comercializando información crediticia y comercial de los colombianos a empresas inescrupulosas o engañando a las fuentes de información y a los ciudadanos. Las quejas de los afectados han puesto en evidencia que estas compañías informales, que al parecer no cumplen con los requerimientos mínimos de funcionamiento, ofrecen sus bases de datos a diferentes compañías financieras y del sector real, sin contar con las autorizaciones que por ley deben obtener de los ciudadanos y sin cumplir con las condiciones de seguridad de la información requeridas para estas operaciones de transferencia.

Figura 2 Venta Ilegal de Bases de Datos [8]

"Copia ilegal de la base de datos del censo pone en riesgo la reserva de cerca de 31 millones de colombianos": director del Censo Electoral. [9]

"Investigan ventas ilegales de bases de datos con información financiera y crediticia de ciudadanos" [10]

I. Países que regulan la protección de datos personales

A continuación se presenta una lista de países que regulan la protección de datos personales, haciendo claridad de que pueden existir otros. [2]

México *Ley LFPDPPP*
(Ley Federal de Protección de Datos Personales en Posesión de Particulares)
Argentina *Ley 25326*
Uruguay *Ley 18331*
Nicaragua *Ley 787*
Unión Europea *Directiva 95/46/CE*
Protección de datos personales de los Estados miembros de la Unión
Unión Europea *Convenio 108 del concejo de 1981*
España *LOPD*
(Ley Orgánica de Protección de Datos de carácter personal)

II. Conclusiones

Con la creciente relevancia que ha tomado la información personal a lo largo del tiempo, las naciones han tomado conciencia de la necesidad de su protección y han aunado esfuerzos traducidos en regulaciones legales de obligatorio cumplimiento o acuerdos entre estados, sin embargo, el proceso de sensibilización y concienciación entre los individuos no ha sido tan apresurada como debiera, originando vulnerabilidades en la seguridad de los datos personales, o, vacíos al momento de protegerlos por medio de la ley.

III. Referencias

[1] M. D. Buchain, «Revista Contaduría Pública,» 04 abril 2012. [En línea]. Disponible en: http://contaduriapublica.org.mx/?p=3053. [Último acceso: 06 abril 2013].

[2] E. Bru Cuadrada, «IDP- REVISTA DE INTERNET, DERECHO Y POLITICA,» Septiembre 2007. [En línea]. Disponible en: http://idp.uoc.edu. [Último acceso: 07 abril 2013].

[3] S. Gauthronet y D. Étienne, *Comisión de las Comunidades Europeas - Comunicaciones Comerciales no solilcitadas y protección de datos,* , 2001.

[4] elmostrador.com, «elmostrador,» 06 marzo 2013. [En línea]. Disponible en: http://www.elmostrador.cl/noticias/pais/2013/03/06/harboe-ppd-denuncia-venta-ilegal-de-base-de-datos-de-companias-de-telefonia-movil/. [Último acceso: 01 abril 2013].

[5] S. López, «Se duplica venta ilegal de bases de datos personales,» b:secure, 07 enero 2013. [En línea]. Disponible en: http://www.bsecure.com.mx/featured/aumenta-venta-ilegal-de-bases-de-datos-personales/. [Último acceso: 03 abril 2013].

[6] IBM, «InfoSphere Optim Data Lifecycle Management Solutions,» [En línea]. Disponible en: http://www-01.ibm.com/software/data/optim/. [Último acceso: 04 abril 2013].

[7] SEMANA, «"Datos reservados de 31 millones de colombianos fueron extraídos ilegalmente por la Dijín",» 12 agosto 2012. [En línea]. Disponible en: http://www.semana.com/nacion/articulo/datos-reservados-31-millones-colombianos-fueron-extraidos-ilegalmente-dijin/262917-3. [Último acceso: 04 abril 2013].

[8] Superintendencia de Industria y Comercio, «SIC investiga ventas ilegales de Bases de Datos,» 17 abril 2012. [En línea]. Disponible en: http://www.sic.gov.co/sic-investiga-ventas-ilegales-de-bases-de-datos. [Último acceso: 02 abril 2013].

[9] Registraduria Nacional del Estado Civil, «Comunicado de Prensa No. 391 de 2012,» 14 agosto 2012. [En línea]. Disponible en: http://www.registraduria.gov.co/Copia-ilegal-de-la-base-de-datos.html. [Último acceso: 10 04 2013].

[10] LEGIS, «ambitojuridico.com LEGIS,» 19 abril 2012. [En línea]. Disponible en: http://www.ambitojuridico.com/BancoConocimiento/N/noti-120419-10(investigan_ventas_ilegales_de_bases_de_datos_con_informacion_financiera_y_creditici)/noti-120419-10(investigan_ventas_ilegales_de_bases_de_datos_con_informacion_financiera_y_creditici).asp. [Último acceso: 09 abril 2013].

[12] Congreso de Colombia, (17, octubre, 2012). "Ley Estatutaria 1581 de 2012".[Online] Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[13] Díaz, Sergio - Granados Guida. (2013). "Proyecto de decreto Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012" [online]. Disponible en: https://www.mincomercio.gov.co/descargar.php?id=65683

[14] Cano, Jeimy J., "Introducción a la Informática Forense", Cap. 2 Páginas 64 – 73, [Online] , disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[15] Oracle, (12, December, 2012). "Oracle Announces Oracle Audit Vault and Database Firewall", [Online]. Disponible en: http://www.oracle.com/us/corporate/press/1885421?ssSourceSiteId=ocomes

[16] IBM Corporation, (Mayo, 2012). "Asegure la información de la empresa y garantice el cumplimiento". [Online]. Disponible en: ftp://ftp.software.ibm.com/software/pdf/mx/0_Asegure_la_informacion_de_la_empresa_y_garantice_el_cumplimiento.pdf

[17] INFORMATICA, (2012). "Enmascaramiento de Datos". [Online]. Disponible en: http://www.informatica.com/la/products/data-masking/

[18] McAfee An Intel Company, (17, octubre, 2012). "Seguridad de Bases de Datos de McAfee".[Online] Disponible en: http://www.mcafee.com/mx/resources/solution-briefs/sb-database-security.pdf

[19] IEEE, Preparación de Artículos para TRANSACCIONES y PERIÓDICOS del IEEE, (2002) versión en español.

Autores

Gustavo Francisco España Paz
Ingeniero de Sistemas de la Universidad Antonio Nariño - 2000.
Experiencia de 10 años como DBA Oracle
Conocimientos en Sistemas Operativos Linux, AIX, Windows Server, TSM, RHEV

Yenny Leguízamo Avila
Ingeniera de Sistemas de la Universidad Católica de Colombia – 2007.
Auditora Senior de IRMeA desde hace aproximadamente 5 años.
Cobit 4.1, ISO 27001:2005, ISO 9001:2000
2013