Ataques Informáticos Basados en la Integridad de la Información

Iván Gallardo-Bernal[a]

Resumen

Asegurar la integridad de la información es una de las tareas más complejas de cualquier organización ya sea pública, privada o del tercer sector, no obstante es también uno de los aspectos más vulnerables debido a que estas entidades priorizan la automatización de sus procesos con el objetivo de agilizar las tareas administrativas y optimizar la recolección y sistematización de datos, sin establecer parámetros o procedimientos que permitan verificar que toda la información fue almacenada correctamente en la base de datos y lo más importante que ésta sea precisa y coherente.
Este documento ampliará el análisis de los conceptos de integridad de la información con la perspectiva de distintos profesionales de las tecnologías de la información y describirá un posible ataque a sistemas de información en producción, tomando como referente el Sistema Integral Contra la Obesidad que almacena al menos 55 mil datos de pacientes reales de distintas ubicaciones geográficas del estado de Guerrero. Se seleccionó esta plataforma debido a que desde su análisis, desarrollo, implementación y puesta en punto se permitió el acceso para el análisis y la interpretación de la información.

Palabras clave: integridad de la información, TIC´S, seguridad de la información.

Abstract

To ensure Information Integrity is one of the most complex tasks of any organization whether public, private or from third sector. Nevertheless it is also one of the most vulnerable aspects, because these entities prioritize the automation of its processes aiming to streamline administrative tasks and optimize the collection and systematization of data without setting parameters or procedures to monitor that all information is loaded correctly on the database, and most importantly, make it consistent and accurate.
This document will expand the analysis of the concepts of Information Integrity with the perspective of various professionals in the Information Technologies and will describe a possible attack to information systems in production; taking as reference the Integral System against Obesity, that stores at least 55 thousand patient records from different geographical locations in the state of Guerrero. This platform was chosen due to the fact that since its analysis, development and start up, we were allowed access to analyze and interpret information.

Keywords: information integrity, information security.

Introducción

Analizar y definir el concepto de integridad de la información es una situación compleja, su definición puede tener distintas interpretaciones. Por lo anterior, el campo de la integridad de la información se muestra como un terreno fértil para los problemas de comunicación o malos entendidos, y corre el riesgo de que alguna actividad no se lleve a cabo satisfactoriamente, por el desconocimiento de las responsabilidades por parte de los personajes involucrados en los procesos automatizados de cualquier organización.

El que se generen problemas de integridad de la información materializa una fuerte amenaza debido a que exhibe y extiende cualquier vulnerabilidad dentro de la organización, lo que afecta a distintos activos vitales de la misma y genera problemas severos que se agudizan gradualmente.

[a] Universidad Autónoma de Guerrero, Unidad Académica de Comunicación y Mercadotecnia, Av. Bachilleres esquina Osa Mayor, Fracc. Villas Caminos Sur; C.P. 39097. Chilpancingo, Guerrero.

Correspondencia: Iván Gallardo Bernal
Universidad Autónoma de Guerrero UAGRO
Correo electrónico: mtigallardo@gmail.com

En el ámbito organizacional contar con información sensible y pública es un riesgo necesario, la integración de sistemas de información genera nuevos problemas de seguridad que deben ser atendidos con una alta prioridad.

Si pensamos como un hacker sabremos que los servidores de bases de datos de cada empresa están ubicados jerárquicamente en el nivel más alto dentro de todos los servidores en el ambiente, pues estos incluyen datos y por lo tanto, información detallada sobre estados financieros, recursos humanos, clientes y proveedores; la cual mantiene a la compañía dentro del negocio, y por ende, se convierte en el activo más importante. Lo anterior muestra a la organización, la necesidad de asegurar tal información (Rodríguez, 2012).

De tal modo que sería interesante dejar de pensar en lo perfecto que puede ser nuestro esquema de seguridad y sugerir que éste en todo momento puede ser perfectible. Este documento surge de la necesidad de identificar los ámbitos a partir de los cuales podrían suscitarse problemas de integridad de la información, debido a que estos ataques en muchas ocasiones emergen desde el interior de la misma organización.

La información es un activo valioso y hay que protegerlo, pero las compañías no saben cómo hacerlo (Sánchez, 2013). La investigación que aquí se presenta tiene como objeto de estudio al Sistema Integral contra la Obesidad (SIOB), que es una herramienta tecnológica que permite la concentración, regionalización, diagnóstico y establecimiento de estrategias que permitan identificar los agentes determinantes de la obesidad en las distintas regiones del estado de Guerrero, así como la creación de un censo de pacientes dentro de las demarcaciones de su territorio. El análisis realizado por SIOB fortalece el desarrollo de estrategias de erradicación de esta enfermedad.

En la siguiente sección de este artículo se encontrará definiciones de integridad descritas por diversos profesionales de las Tecnologías de la Información y Comunicación (TIC´s). Más adelante en el apartado sistema SIOB se describe el sistema y sus características arquitectónicas, así como las métricas de seguridad implementadas, el uso y manejo de bitácoras electrónicas en el sistema, así como algunos posibles escenarios de ataque a la integridad de la información. Finalmente se presentan las conclusiones y algunas recomendaciones para fortalecer la seguridad de los sistemas de información dentro de cualquier organización.

La integridad de la información

Es posible ilustrar un problema de integridad en una situación cotidiana, por ejemplo, si una persona está hospitalizada y el médico prescribe una dosis contabilizada por hora de unos 5 miligramos (mg) de un medicamento, y por diversas situaciones de manera accidental o intencional, se modifica su expediente electrónico y se establece una dosis de 200 mg, ello podría traer consecuencias mortales para el paciente.

La perspectiva de integridad de la información es una apreciación que es adaptable al interés de los profesionales del área de las nuevas TIC's. Para el responsable de la seguridad en determinada organización, la "integridad de los datos" puede definirse como la imposibilidad de que cualquier persona modifique información sin ser descubierto, esta situación no sólo apunta a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurados [SDLC], revisión de códigos fuente por expertos o software específico de comprobación de códigos, pruebas exhaustivas, etc.), sino también a la integridad personal (responsabilidad, confianza, honestidad, fiabilidad, compromiso organizacional, etc.) (Gelbstein, 2011).

Para el administrador de las redes y servidores de los Servicios Estatales de Salud, la integridad de la información no se limita al aseguramiento físico de los servidores de aplicaciones, muros de fuego y revisión de la infraestructura del cableado estructurado, sino también a la revisión minuciosa de los canales por los cuales se transporta la información ya que es una brecha muy grande por donde se puede ejecutar un ataque (Arellano, 2014).

Para el Administrador de Bases de Datos (DBA) de una organización; la integridad dependerá en gran medida de que la información cargada a una base de datos sea precisa, válida y coherente. Es muy probable que los DBA también analicen la integridad referencial, de las entidades y de los dominios.

Para el propietario de los datos (Denominado en algunas ocasiones Sponsor), la "integridad de los datos" puede ser un parámetro importante de calidad, ya que demuestra que las relaciones entre las entidades están regidas por reglas de negocio adecuadas, que incluyen mecanismos de validación, como la realización de pruebas para identificar registros que no cuentan con relaciones precisas (Gelbstein, 2011).

Existen entonces distintas definiciones que producen cierta confusión semántica, uno de los principales motivos por los que las bases de datos son los objetos menos protegidos de la infraestructura de tecnologías de la Información.

Por otro lado, fenómenos como la descentralización de los sistemas de información en las organizaciones, el problema recurrente de sistemas heredados y la disponibilidad de entornos de programación cada vez más complejos, no evalúan muchas veces la calidad e integridad de datos, lo que origina problemas a la seguridad de información y al software en sí; dado que la mayoría de los sistemas descifran problemas momentáneos y no están sujetos a un proceso de gestión del ciclo de vida y tampoco están preocupados por evaluar el aprendizaje adquirido a través de la experiencia, para fortalecer la inteligencia de negocios de la organización.

Debido a esto se tiene que la introducción de datos erróneos produce resultados erróneos algo que en inglés se conoce como "GIGO" "Garbage In, Garbage Out", lo que significa que si "entra basura, sale basura" (Bininda, 2004).

Los ataques a la integridad de los datos consisten en la modificación intencional de los mismos, sin autorización alguna, en algún momento de su ciclo de vida, este ciclo comprende las siguientes etapas:

- Introducción, creación o adquisición de datos.
- Procesamiento o derivación de datos.
- Almacenamiento, replicación y distribución de datos.
- Archivado y recuperación de datos.
- Realización de copias de respaldo y restablecimiento de datos.
- Borrado, eliminación y destrucción de datos.

El Sistema SIOB

El Sistema Integral contra la obesidad (SIOB) es un sistema de información que emerge en el contexto de la estrategia nacional contra la obesidad impulsada por el Gobierno Federal de México. Debido a esto cada estado de la república sugiere e instrumenta el desarrollo de estrategias propias para colaborar en la prevención, erradicación o disminución de este padecimiento.

El sistema SIOB, tiene como objetivo general obtener una radiografía real, que exponga el porcentaje de cobertura del padecimiento en todas las regiones de su aplicación, esta información servirá para identificar en qué ubicación geográfica existe una mayor concentración de la enfermedad y se analicen los factores determinantes que predominan en la propagación de este padecimiento.

Por otro lado, SIOB está sujeto a las normas de la Organización Mundial de la Salud (OMS), para el cálculo del Índice de Masa Corporal (IMC) y clasifica los resultados de la muestra por rangos de edades y género. Esta norma sugiere la obtención del Índice de Masa Corporal (IMC) de acuerdo a la edad y el género de cada paciente (OMS,2014).

SIOB contempla un área de reportes que permite la explotación estadística de la información, lo que genera estrategias específicas para cada sector de la población. Los datos que alberga SIOB son de alta confidencialidad ya que manejan información privada de los pacientes, por lo cual los mecanismos de seguridad deberán ser avanzados y respetar las normas de salud federales para salvaguardar la información. En la Figura 1 se muestra la interfaz del usuario administrador.

Arquitectura del Sistema

El sistema está construido en Java y satisface la arquitectura del Modelo Vista Controlador (MVC) y cuenta con los siguientes detalles técnicos:

- Entorno de programación Netbeans
- Framework Java Server Faces
- Base de datos Mysql 5
- Servidor de aplicaciones Apache Tomcat 6.0

Figura 1. Interfaz de usuario Bitácora Intermedia
Fuente: Secretaría de Salud del Estado de Guerrero.

La infraestructura del sistema se ubica sobre un servidor central en el Centro de Datos de los Servicios Estatales de Salud, en la capital del estado de Guerrero, Chilpancingo, y de manera simultánea la aplicación está replicada en un servidor virtual hospedado en TRIARA, centro de datos nivel 5 en territorio nacional. Las bases de datos respetan la normalización sugerida por Boyce Codd (Codd, 1970).

El sistema de información almacena los datos poblacionales reales de al menos 41,000 pacientes que han tenido contacto con servicios de salud en el estado de Guerrero ya sean centros de salud, hospitales generales o establecimientos de apoyo (UNEME, CAPACITS, entre otros). En la Figura 2 se muestra la máscara de captura de los datos generales del paciente.

La operación del sistema contempla el siguiente proceso:

- Registro de capturista según el esquema de roles de usuario (médico, enfermera, activador físico, nutriólogo, responsable regional, responsable estatal, administrador general, súper usuario)
- Captura de los datos generales y características personales del paciente.
- Diagnóstico automatizado por la herramienta según criterios de la OMS (nivel de desnutrición o grado de obesidad)
- Almacenamiento de información en el centro de datos.
- Replicación en la base de datos en el centro de datos virtual.
- Explotación de la información a través de reportes dinámicos

Mecanismos de Seguridad

La seguridad se denomina como la prevención de cualquier acceso no autorizado, supresión no autorizada o modificación de la información. Las principales dimensiones de seguridad que se deben tener en cuenta para proporcionar la satisfacción del usuario son la disponibilidad, confidencialidad e integridad (Thakur, Gopta y Gopta, 2014).

Los usuarios del sistema SIOB manejan un nombre de usuario y contraseña que se valida del lado del servidor. Estas contraseñas instrumentan el algoritmo encrypt 64 en un mecanismo de sesiones, guardando entonces la información en la base de datos de manera cifrada. Los usuarios tienen la capacidad de cambiar sus contraseñas en cualquier momento blindando de esta manera la posibilidad de usurpar la identidad. La información viaja cifrada en todo momento al ser ingresada en el sistema.

Las sesiones están controladas desde el servidor de aplicaciones, por lo cual el tiempo de vida de

Figura 2. Formulario de registro de pacientes.
Fuente: Elaboración propia.

una sesión se controla por inactividad por un lapso de 30 minutos. El código fuente de la aplicación es verificado por diversas instancias por lo cual sigue un proceso de lectura de código y artefactos para evaluar que efectivamente cada transacción del sistema cumpla con el análisis de requerimientos.

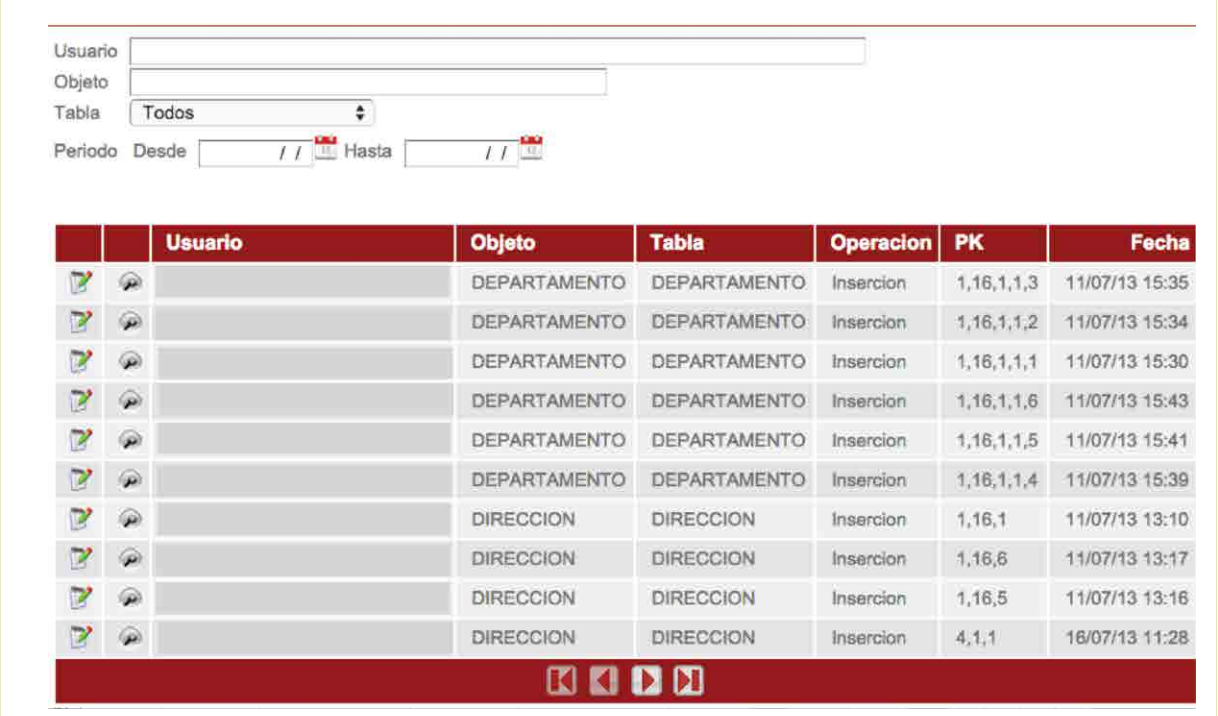
Bitácoras Electrónicas

El sistema SIOB maneja como mecanismo adicional de seguridad la instrumentación de bitácoras electrónicas a diversos niveles que obedecen el siguiente proceso. Al ingresar el usuario, el sistema registra una bitácora automática con los siguientes atributos: nombre de usuario, dirección IP, dirección MAC, operación realizada, fecha/hora, objeto modificado, tabla modificada. Al guardar este registro, la bitácora se almacena en el centro de datos de la organización y en el centro de datos remoto. La bitácora denominada inicial, no podrá modificarse por sistema y los datos serán entregados a un reporte al administrador regional.

Existe otro tipo de bitácora, a nivel de servidor de bases de datos, y se inicializa cuando algún usuario ingresa a la base de datos, se activa un web services que reserva los datos (los mismos de la bitácora inicial) para el administrador de las bases de datos, quien tendrá la posibilidad de verificar los accesos al servidor central y el servidor remoto comparando con el log de operaciones del servidor de bases de datos, en el archivo de transacciones log, se almacenan las operaciones hechas por las transacciones antes de ser escritos en las bases de datos (Doucet, 2002). El log mantiene los datos consistentes, garantizando la escritura de todos los cambios o la cancelación de estos.

Esta bitácora tampoco puede ser modificada por el administrador de las bases de datos y es denominada bitácora intermedia (Figura 3).

Por último existe un registro final que almacena el control de las dos bitácoras anteriores a través de una aplicación alternativa denominada "control de mando", que permite visualizar la bitácora inicial, administrar la bitácora intermedia y gene-



		Usuario	Objeto	Tabla	Operacion	PK	Fecha
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,3	11/07/13 15:35
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,2	11/07/13 15:34
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,1	11/07/13 15:30
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,6	11/07/13 15:43
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,5	11/07/13 15:41
			DEPARTAMENTO	DEPARTAMENTO	Insercion	1,16,1,1,4	11/07/13 15:39
			DIRECCION	DIRECCION	Insercion	1,16,1	11/07/13 13:10
			DIRECCION	DIRECCION	Insercion	1,16,6	11/07/13 13:17
			DIRECCION	DIRECCION	Insercion	1,16,5	11/07/13 13:16
			DIRECCION	DIRECCION	Insercion	4,1,1	16/07/13 11:28

Figura 3. Bitácora Intermedia.
Fuente: Elaboración propia.

rar una nueva bitácora de consulta de información que verifica los accesos a las bitácoras por parte del administrador general de bases de datos, por lo cual es una bitácora final operada a nivel ejecutivo.

Posibles ataques al sistema SIOB

Los ataques a la integridad, se podrían presentar de la siguiente manera:

Las bombas lógicas, el software no autorizado que se introduce en un sistema por acción de las personas encargadas de programarlo/mantenerlo, los troyanos y demás virus similares también pueden afectar la integridad de los datos a través de la introducción de modificaciones (por ejemplo, al definir una fórmula incorrecta para calcular el IMC) o la encriptación de datos y posterior exigencia de un "rescate" para revelar la clave de encriptación.

Algunas bombas lógicas pueden ser detectadas y eliminadas antes de que exploten con el periódico "escaneo" de todos los programas, incluyendo los archivos comprimidos, con un adecuado programa antivirus que debe ser ejecutado siempre que el usuario conecte su máquina a la red de Internet.

Las bombas lógicas son muy fáciles de programar pero su debilidad es que no se replican a sí mismas, razón por la cual no pueden esparcirse hacia víctimas no deseadas y en esta medida, son menos dañinas para el sistema que otros tipos de ataques.

Las bombas lógicas, si bien se han utilizado en la mayoría de los casos para defraudar el patrimonio económico, también han sido utilizadas para atacar los aparatos de control informático de servicios públicos, lo que genera procesos no deseados y actividades cibernéticas no contempladas en los programas afectados, con el consiguiente peligro para la comunidad (Amado, 2007).

Una vez consumado un ataque de este tipo, la intrusión permitiría modificar cualquier rol de usuario, alterando cualquier información sobre los pacientes registrados en el sistema, lo que se denomina usurpación de identidad. Para fortalecer la vigilancia en este ámbito podrían realizarse auditorías para conocer en qué momento se registran cambios a nivel de aplicación tomando en

cuenta que los logs de operaciones del manejador de bases de datos pueden también ser sujetos a auditoria.

Parece complicado mantener vigilados todos los aspectos antes mencionados, pero es necesario entonces establecer algunas estrategias que puedan fortalecer la integridad de la información:

- Delimitación de responsabilidades en la organización. Tomar posesión de los datos y generar accesos controlados (¿Quién hace qué?).
- Controlar derechos y privilegios de acceso para usuarios internos y externos de las aplicaciones de la organización.
- Segregación de funciones.
- Contabilización y auditoría del número de usuarios que han mantenido derechos y privilegios de acceso histórico.
- Controlar y contabilizar el número de veces que fue necesario acceder a los datos de producción para realizar modificaciones o correcciones.
- Realizar el índice de datos incorrectos e incoherentes.
- Supervisar el número de cuentas inactivas en las aplicación.

Como mecanismo adicional de seguridad es posible emplear técnicas como IAM ó IDM, (identidad y control de acceso ó identidad y gestión de accesos), que ayudan a proteger la información personal del acceso no autorizado al tiempo que facilitan su disponibilidad para los usuarios legítimos. Estas tecnologías incluyen mecanismos de autenticación, control de los datos y los controles de acceso de recursos, sistemas de aprovisionamiento y administración de cuentas de usuario. Desde una perspectiva de cumplimiento, las capacidades de IAM permiten a una organización realizar un seguimiento preciso y hacer cumplir los permisos de usuario en toda la empresa (Salido, 2010).

Conclusiones

Con la finalidad de proteger la información en las organizaciones y tomando en cuenta que actualmente la información es considerada uno de los activos más valiosos, es posible contar con distintos niveles de seguridad desarrollando un blindaje de alto nivel en los sistemas de información, adquiriendo hardware de seguridad, estableciendo políticas de privacidad, generando bitácoras electrónicas de movimientos, realizando auditorías periódicas por las distintas áreas por donde viaja la información, contratando personal experto en el área de la seguridad y diversas medidas adicionales, no obstante, para que todas estas herramientas permeen el aseguramiento de la información y promuevan la integridad de la información, deberán ser complementadas con un plan estratégico que establezca un sentido de pertenencia para los todos los colaboradores de la institución, teniendo en cuenta que son los personajes más cercanos a la información y en cualquier momento podrían tomar una decisión errónea que provoque un serio problema para la misma.

Aunado a lo anterior resulta imprescindible la creación de estrategias que fortalezcan el gobierno de los datos ya que en la actualidad esta actividad ha llegado a ser sumamente importante dentro de las organizaciones de todos los tamaños, debido a que cada vez es más evidente que los problemas en el manejo de la información afectan directamente a la toma de decisiones, pero no existen procesos ni políticas que permitan garantizar la confiabilidad de los datos.

Las organizaciones deben contemplar dentro de su plan de desarrollo, manuales operativos que contribuyan a garantizar la confiabilidad, integridad de los datos y el gobierno de los datos, sin estos planes no es posible conocer cuánto se ha avanzado, lo que constituye un retroceso en el ámbito de la seguridad y representa un obstáculo importante para el resguardo correcto de la información.

El gobierno de los datos es una disciplina encargada de la orquestación de personas, procesos y tecnología que permite a una organización posicionar la información como un recurso de valor empresarial y al mismo tiempo es la encargada de mantener a los usuarios, auditores y reguladores satisfechos, usando la mejora de la calidad de los datos para retener clientes, constituyendo y guiando a nuevos nichos de oportunidad en el mercado.

Para conquistar el gobierno de los datos es necesario contemplar los siguientes pasos:

Establecer metas. Sentencias principales que guían la operación y desarrollo de la cadena de suministro de información.

Definir métricas. Conjunto de medidas usadas para evaluar la efectividad del programa y los procesos de gobierno asociados.

Tomar decisiones. La estructura organizacional y el modelo de cambio ideológico para analizar y crear políticas de decisión.

Comunicar políticas. Herramientas, habilidades y técnicas usadas para comunicar decisiones políticas a la organización.

Medir resultados. Comparar resultados de las políticas con las metas, entradas, modelos de decisión y comunicación para proveer constante retroalimentación sobre la efectividad de la política.

Auditar. Herramienta usada para comprobar todo.

Estos procesos deberán ser revisados, ajustados y readaptados en diversos momentos, ya que el riesgo más fuerte en los ataques a la integridad de los datos son *los mismos integrantes de la organización*, o personas que de manera directa o indirecta tienen contacto con los datos sensibles de la organización por lo cual es necesario el involucramiento de todos los miembros de la organización para lograr las metas y cumplir con los objetivos con un sentido de responsabilidad y pertenencia a un plan estratégico articulado a los objetivos globales de las organizaciones.

Referencias

Amado, I. (2007). Ciberterrorismo. Una aproximación a su tipificación como conducta delictiva. Derecho penal y criminología. Revista del Instituto de Ciencias Penales y Criminológicas.

Arellano, H. (2014). Comentarios de integridad referencial. Dirección de redes e infraestructura Salud Guerrero.

Bininda, EOR., Jones, K.E., Price, S.A., Cardillo, M., Grenyer, R.& Purvis, A. (2004). Garbage in, garbage out. In Phylogenetic supertrees (267- 280). Springer Netherlands.

Codd, F.E. (1970). Relational model of data for large shared data banks. Communications of the ACM.Disponible en: http://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf

Doucet, A., Gançarski, S., León, C.& Rukoz, M. (2002). Estrategias para verificar restricciones de integridad globales en multibase de datos con transacciones anidadas. Disponible en http://www.revista.unam.mx/vol.3/num4art38/

Gelbstein, E.D. (2011). La integridad de los datos: el aspecto más relegado de la seguridad de la información. Journal ISACA, 6.

OMS (2014). Nota descriptiva 311, tablas de índice de masa corporal. Disponible en http://www.who.int/mediacentre/factsheets/fs311/es/.

Rodríguez, H. (2012). Asegurar la información, pensar como hacker. Developerworks. Disponible en http:// www.ibm.com/developerworks/ssa/local/im/pensar-como-hacker/

Salido, J. (2010). Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach, JournalISACA, vol. 6.

Sánchez, C.L. (2013). La información es el activo más valioso para muchas empresas, Sin embargo, no la tienen asegurada. Disponible en: http://bts.inese.es/

Thakur, A.S., Gupta, P.K. & Gupta, P. (2015). Handling Data Integrity Issue in SaaS Cloud. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications(FICTA) 2014 (127-134). Springer International Publishing.

Recibido: 12 de marzo de 2015
Corregido: 15 de mayo de 2015
Aceptado: 22 de mayo de 2015

Conflicto de interés: No existe conflicto de interés