La integridad de los datos: el aspecto más relegado de la seguridad de la información

El **Dr. Ed Gelbstein** se ha desempeñado en el campo de la TI durante más de 40 años y dirigió el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (ONU), entidad que se ocupa de la prestación de servicios de TI a la mayoría de las organizaciones que integran el sistema de la ONU en todo el mundo. Desde que abandonó su cargo en la ONU, Gelbstein se ha desempeñado como asesor en materia de TI para la Junta de Auditores de la ONU y el Tribunal Nacional de Cuentas de Francia (Cour des Comptes), además de integrar el cuerpo docente de la Universidad Webster de Ginebra, Suiza. El Dr. Gelbstein participa asiduamente como orador en conferencias internacionales, donde suele abordar temas relacionados con auditorías, riesgos, gobierno y seguridad de la información, y es autor de diversas publicaciones. Actualmente vive en Francia y se lo puede contactar a través de la siguiente dirección de correo electrónico: ed.gelbstein@gmail.com.

El tema de la seguridad de la información ha cobrado visibilidad en distintos ámbitos: en el trabajo, en el hogar y durante el traslado de un lugar a otro. Se trata, principalmente, de prevenir los ataques destinados a restringir la disponibilidad (por ejemplo, la denegación del servicio) y a introducir software malintencionado (malware) que permita a un tercero manipular datos e información sin autorización (por ejemplo, para robar, divulgar, modificar o destruir datos).

El gusano informático Stuxnet, que fue descubierto en el año 2010, alteró el funcionamiento de un proceso industrial, ya que fue diseñado con la finalidad de dañar equipos físicos y modificar las indicaciones de los operadores a cargo de la supervisión, para impedir, de este modo, que se identificara cualquier anomalía en los equipos.[1] Si esta modalidad de ataque a la integridad de los datos (denominado también "ataque semántico") se hubiera replicado en otros sistemas, podría haber causado problemas graves en infraestructuras informáticas de importancia crítica, como las de servicios públicos, servicios de urgencia, control de tráfico aéreo y cualquier otro sistema que dependa en gran medida de la TI y resulte indispensable para la sociedad. El gobierno de la información es un factor esencial para la consolidación de la integridad de los datos.

Un artículo publicado recientemente en *ISACA Journal* presenta una infraestructura de gobierno de datos desarrollada por Microsoft para garantizar la privacidad, la confidencialidad y el cumplimiento normativo. El artículo analiza las funciones que desempeñan las personas, los procesos y la tecnología; el ciclo de vida de los datos; y los principios de privacidad y confidencialidad de la información. También incluye enlaces a trabajos más pormenorizados sobre la informática de confianza (o trustworthy computing).[2]

En el presente trabajo se ampliará el análisis de estos temas, enfocándose en la integridad de los datos, las normas y los procedimientos recomendados a los que esta debe ajustarse, y la función del gobierno de datos. Este artículo también presenta un marco para el gobierno de datos sin control exclusivo.

De los tres principales dominios de la seguridad de la información, el de la disponibilidad es el que se encuentra más estrechamente ligado a la tecnología y es posible su medición. El tiempo improductivo (downtime) es visible y puede expresarse como valor absoluto (por ejemplo, en minutos por incidente) o como porcentaje, y no se requiere demasiado esfuerzo para entender que una disponibilidad de "cinco nueves" (99,999 por ciento) representa en total unos cinco minutos de tiempo improductivo acumulado en un año. Los operadores de los centros de datos saben lo que se necesita para alcanzar este valor.

La confidencialidad es un concepto que se puede explicar fácilmente, pero solo tiene alguna utilidad cuando los datos y documentos han sido clasificados en categorías —como "público", "restringido a", "embargado hasta" y "reservado"— que reflejan la necesidad que tiene una empresa de protegerlos.

No es conveniente que los técnicos que se encargan de la infraestructura y servicios de TI se ocupen de realizar esta clasificación, ya que probablemente no tengan un conocimiento cabal del negocio y, en caso de emplearse la modalidad de externalización (outsourcing) o un sistema de computación en la nube (cloud computing), es posible que además no pertenezcan a la empresa. Por lo tanto, el control y el proceso de clasificación de datos debe quedar en manos del personal del negocio, mientras que los proveedores de servicios y soluciones de TI deben ocuparse de proporcionar las herramientas y los procesos necesarios, como son los controles para la gestión de accesos e identidades (Identity Access Management o IAM) y la encriptación.

El método más sencillo para medir la confidencialidad tiene una lógica binaria: el carácter confidencial de la información puede haberse preservado (si la información no se ha divulgado) o no (si se ha divulgado). Lamentablemente, este método no resulta demasiado útil, ya que no refleja los efectos de la divulgación de los datos, que abarcan desde situaciones bochornosas hasta atentados contra la seguridad nacional.

Si analizamos la noción de integridad, la situación se torna más compleja, porque se trata de un concepto que puede tener distintas interpretaciones. Este es un terreno fértil para los problemas de comunicación y los malentendidos, con el consiguiente riesgo de que una actividad no se lleve a cabo satisfactoriamente por las confusiones en torno a las responsabilidades pertinentes.

¿QUÉ DEBEMOS ENTENDER POR "INTEGRIDAD"?

La importancia de la integridad de los datos se puede ilustrar con un sencillo ejemplo: Una persona necesita un tratamiento hospitalario que incluye la administración diaria de un medicamento en dosis de 10 miligramos (mg). Accidental o intencionalmente, se produce una modificación en el registro electrónico del tratamiento y las dosis quedan establecidas en 100 mg, con consecuencias mortales. Para tomar otro ejemplo, podríamos imaginar una situación propia de una obra de ficción que antecediera al ataque del virus

Stuxnet en 2010 y preguntarnos qué ocurriría si alguien interfiriera los sistemas de control de una central nuclear para que simularan condiciones de funcionamiento normal cuando, en realidad, se ha provocado una reacción en cadena.[3] ¿Podemos afirmar que los profesionales reconocen las múltiples definiciones de la "integridad de los datos"? Veamos:

- **Para un encargado de seguridad**, la "integridad de los datos" puede definirse como la imposibilidad de que alguien modifique datos sin ser descubierto. Desde la perspectiva de la seguridad de datos y redes, la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria. Si examinamos el concepto de "integridad", podríamos concluir que no solo alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurados [SDLC], revisión de códigos fuente por expertos, pruebas exhaustivas, etc.), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etc.).
- **Para un administrador de bases de datos**, la "integridad de los datos" puede depender de que los datos introducidos en una base de datos sean precisos, válidos y coherentes. Es muy probable que los administradores de bases de datos también analicen la integridad de las entidades, la integridad de los dominios y la integridad referencial —conceptos que podría desconocer un experto en infraestructuras instruido en normas ISO 27000 o en la serie 800 de publicaciones especiales (SP 800) del Instituto Nacional de Normas y Tecnología (NIST, National Institute of Standards and Technology) de los EE. UU.
- **Para un arquitecto o modelador de datos**, la "integridad de los datos" puede estar relacionada con el mantenimiento de entidades primarias únicas y no nulas. La unicidad de las entidades que integran un conjunto de datos se define por la ausencia de duplicados en el conjunto de datos y por la presencia de una clave que permite acceder de forma exclusiva a cada una de las entidades del conjunto.
- **Para el propietario de los datos (es decir, para el experto en la materia)**, la "integridad de los datos" puede ser un parámetro de la 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 huérfanos.
- **Para un proveedor**, la "integridad de los datos" es:

> *La exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro de datos. La integridad de los datos se establece en la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores.*[4]

- **En un diccionario disponible en línea**, se define la "integridad de los datos" de este modo:

> *Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. La integridad de los datos es uno de los seis componentes fundamentales de la seguridad de la información.*[5]

Sin duda, podemos encontrar muchas otras definiciones. Pero todas contienen superposiciones, aluden a temas de distinta índole y 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 TI.

El planteo del problema no termina aquí. La descentralización de los sistemas de información y la disponibilidad de entornos de programación eficaces para los usuarios finales, como las hojas de cálculo, han creado vulnerabilidades potencialmente descontroladas en la integridad de los datos, ya que esas hojas de cálculo se utilizan como fundamento de decisiones ejecutivas, sin evaluar, muchas veces, la calidad e integridad de los datos. ¿Cómo deberíamos abordar este problema? En primer lugar, podríamos considerar que se trata de un problema que atañe:

- A la seguridad de la información, dado que no se puede garantizar la integridad de los datos.
- A la calidad del software, dado que la mayoría de las hojas de cálculo no está sujeta a un proceso de gestión del ciclo de vida.
- A la inteligencia de negocios, dado 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").

Quizás podríamos concluir que abarca los tres aspectos; en tal caso, el siguiente paso consistiría en determinar quién debería abordar el problema (el propietario de los datos, el usuario final que diseñó la hoja de cálculo, el departamento o proveedor de servicios de TI o todos juntos).

DISPARADORES DE LA PÉRDIDA DE INTEGRIDAD DE LOS DATOS

En la sección anterior se analizó, a modo de ejemplo, el uso de hojas de cálculo diseñadas por los usuarios sin someterlas a pruebas ni incluir documentación (hecho que se ve agravado por la introducción manual de datos, particularmente cuando no se validan los valores ingresados), pero existen otros disparadores de problemas que podrían resultar aún más graves:

- Modificación de los permisos y privilegios de acceso.
- Imposibilidad de rastrear el uso de contraseñas privilegiadas, en especial cuando es compartido.
- Errores del usuario final que afectan los datos de producción.
- Aplicaciones vulnerables a la introducción de códigos ocultos (como los "backdoors").
- Procesos de control de cambios y acreditación deficientes o no desarrollados plenamente.
- Fallas en la configuración de software y dispositivos de seguridad.
- Aplicación de parches en forma incorrecta o incompleta.
- Conexión de dispositivos no autorizados a la red corporativa.
- Uso de aplicaciones no autorizadas en dispositivos conectados a la red corporativa.
- Segregación de funciones (SoD) inadecuada o no aplicada.

> "La función de auditoría de TI podría carecer de la masa crítica necesaria para efectuar auditorías que contemplen todos los aspectos."

Por si esto fuera poco, la función de auditoría de TI podría carecer de la masa crítica necesaria para efectuar auditorías que contemplen todos estos aspectos.

ATAQUES A LA INTEGRIDAD DE LOS DATOS

Los ataques a la integridad de los datos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida. En el contexto del presente artículo, el ciclo de vida de los datos comprende las siguientes etapas:

- Introducción, creación y/o adquisición de datos.
- Procesamiento y/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 fraude —el más antiguo de los métodos destinados a atacar la integridad de los datos— tiene múltiples variantes, las cuales no analizaremos en el presente artículo, excepto para mencionar un caso que, en el año 2008, apareció en la primera plana de los periódicos de todo el mundo: Un empleado de Societe Generale de Francia incurrió en delitos de "abuso de confianza, falsificación y uso no autorizado de los sistemas informáticos del banco", que produjeron pérdidas estimadas en €4900 millones.[6] A juzgar por la cantidad de publicaciones y conferencias internacionales que abordan el tema del fraude, es probable que este caso siga estando vigente durante algún tiempo.

Hace años que las organizaciones que operan tanto en el sector público como en el privado sufren alteraciones en sus sitios web, pero, más allá del eventual perjuicio a la reputación de una empresa, ninguno de los daños ocasionados puede considerarse "catastrófico".

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 en una hoja de cálculo) o la encriptación de datos y posterior exigencia de un "rescate" para revelar la clave de desencriptación. En los últimos años se han producido numerosos ataques de características similares a las mencionadas, que afectan principalmente los discos duros de las computadoras personales. Debería esperarse que tarde o temprano se produzcan ataques de este tipo destinados a los servidores.

La modificación no autorizada de sistemas operativos (servidores y redes) y/o de software de aplicaciones (como los "backdoors" o códigos no documentados), tablas de bases de datos, datos de producción y configuración de infraestructura también se consideran ataques a la integridad de los datos. Es lógico suponer que los hallazgos de las auditorías de TI incluyen con regularidad las fallas producidas en procesos clave, particularmente en la gestión del acceso privilegiado, la gestión de cambios, la segregación de funciones y la supervisión de registros. Estas fallas posibilitan la introducción de modificaciones no autorizadas y dificultan su detección (hasta que se produce algún incidente).

Otro método de ataque a la integridad de los datos es la interferencia en los sistemas de control de supervisión y adquisición de datos (SCADA, Supervisory Control and Data Acquisition), como los que se utilizan en infraestructuras críticas (suministro de agua, electricidad, etc.) y procesos industriales. A menudo, la función de TI no interviene en la instalación, el funcionamiento ni la gestión de estos sistemas. El ataque dirigido a plantas de enriquecimiento de uranio en Irán durante el año 2010 había sido planeado con la finalidad de alterar el comportamiento de los sistemas de centrifugación sin que los tableros de control indicaran ninguna anomalía.[7]

Cabe destacar que muchos de estos sistemas de control no están conectados a Internet y que, en el caso de la inyección del software Stuxnet, debió realizarse una intervención manual,[8] hecho que confirma la teoría de que el "hombre" sigue siendo el eslabón más débil de la cadena de aseguramiento/seguridad de la información.

ALINEAMIENTO CON NORMAS Y MEJORES PRÁCTICAS PARA GESTIÓN DE RIESGOS Y CUMPLIMIENTO

Para las empresas que aún no han comenzado a preparar estrategias de defensa, un buen punto de partida es la adopción de los procedimientos recomendados, como el de *Security Requirements for Data Management* (Requerimientos de seguridad para la gestión de datos), descrito en la sección de Entrega y soporte (DS, Deliver and Support) 11.6 de COBIT (Objetivos de control para la TI y tecnologías afines), junto con los procedimientos indicados en la correspondiente sección de la guía de aseguramiento *IT Assurance Guide: Using COBIT®*.[9] Estas publicaciones resumen el objetivo de

control y los factores determinantes de valor y de riesgo, e incluyen una lista de pruebas recomendadas para el diseño del control.

ISACA también publicó una serie de documentos que establecen correspondencias entre las normas sobre seguridad de la información y COBIT 4.1, y que resultan sumamente valiosos para profesionales y auditores. Además, se ha publicado recientemente en *COBIT Focus* un excelente artículo que establece una correspondencia entre la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS, Payment Card Industry Data Security Standard) v2.0 y COBIT 4.1.[10]

La Asociación Internacional de Gestión de Datos (Data Management Association International, DAMA) ofrece un recurso adicional: *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK); se recomiendan especialmente los capítulos tres ("Data Governance"), siete ("Data Security Management") y doce ("Data Quality Management").[11]

Desde la perspectiva del cumplimiento normativo, existe un marco legislativo cada vez más amplio que asigna a las organizaciones la responsabilidad de garantizar la integridad de los datos y del aseguramiento de la información (information assurance o IA). En los EE. UU. se han aprobado las siguientes leyes, que imponen severas sanciones en caso de incumplimiento: Data Quality Act (Ley de Calidad de los Datos), Sarbanes-Oxley Act (Ley Sarbanes-Oxley), Gramm-Leach-Bliley Act (Ley Gramm-Leach-Bliley), Health Insurance Portability and Accountability Act (Ley de Transferibilidad y Responsabilidad de los Seguros de Salud) y Fair Credit Reporting Act (Ley de Garantía de Equidad Crediticia). También existe la Federal Information Security Management Act (Ley Federal de Gestión de Seguridad de la Información), que establece sanciones económicas en caso de incumplimiento de las disposiciones vigentes. (El análisis de las leyes vigentes fuera de los EE. UU. excede el alcance del presente artículo; sin embargo, cabe destacar dos excelentes ejemplos de legislación comparada, como la directiva de la Unión Europea [UE] para la protección de los datos ["Directive on Data Protection"] y la 8.ª directiva de la UE sobre derechos de sociedades ["8th Company Law Directive"] en relación con las auditorías legales[12, 13]).

¿CÓMO GARANTIZAR UNA MAYOR INTEGRIDAD DE LOS DATOS?

La adopción de mejores prácticas debe complementarse con la formalización de las responsabilidades correspondientes a los procesos de negocio y TI que soportan y mejoran la seguridad de los datos.

Delimitación de responsabilidades en la Empresa

En todo programa de aseguramiento de la integridad de los datos deben estar definidas las responsabilidades de "detección y detención" ("Detect, Deter" o 2D); de "prevención y preparación" ("Prevent, Prepare" o 2P); y de "respuesta y recuperación" ("Respond, Recover" o 2R).[14] Como propietarias de los datos, las áreas de negocio deben tomar la iniciativa, mientras que el proveedor de servicios de TI —se trate de personal interno o contratado mediante la modalidad de externalización de servicios— debe ocuparse de la implementación.

Las buenas prácticas a adoptar son:

- **Tomar posesión de los datos y asumir la responsabilidad de garantizar su integridad.** Solo el personal de la unidad de negocio correspondiente puede ocuparse de esta tarea. Cuando se aplica la modalidad de externalización de servicios y operaciones de TI, este requisito resulta obvio, pero cuando esos servicios y operaciones se suministran a nivel interno, se suele caer en el error de considerar que los datos pertenecen al área de TI y que esta área es la responsable de preservar la confidencialidad e integridad de la información.

  Para tomar el control de la información, se debe realizar una evaluación de valores que permita calcular el costo potencial de la pérdida de la integridad de los datos y contemple las pérdidas económicas directas (por ejemplo, en caso de fraude o problemas operativos graves), los gastos judiciales y el perjuicio causado a la reputación de la empresa.
- **Controlar los derechos y privilegios de acceso**. Los principios de necesidad de conocer (need to know, NtK) y mínimos privilegios (least privilege, LP) constituyen prácticas eficaces y no son, en teoría, difíciles de aplicar. El crecimiento de las redes sociales y la noción de que todos somos productores de información exigen mayor amplitud y voluntad de intercambio. Las redes sociales se están transformando en una fuerza que resiste y desafía la aplicación de los principios de NtK y LP.

  Es necesario formalizar, documentar, revisar y auditar regularmente los procesos de solicitud, modificación y eliminación de derechos de acceso. La acumulación de privilegios —cuando una persona mantiene privilegios históricos al cambiar de responsabilidades— supone un grave riesgo para la empresa y podría afectar la segregación correcta de funciones.

  Es común en las organizaciones, no llevar un inventario completo y actualizado sobre quién accede a qué, ni se posee una lista completa de los privilegios de usuario. Varios proveedores ofrecen productos capaces de obtener automáticamente toda la información relacionada con esos privilegios.

  Una vez que se han aplicado los principios de NtK y LP a partir de un proceso exhaustivo de gestión de accesos e identidades, el acceso privilegiado sigue siendo un tema delicado que es indispensable analizar y controlar, ya que permite acceder libremente a los datos de producción y códigos fuente. Cuando un usuario está en condiciones de omitir los procedimientos de control de cambios, existe el riesgo de que se produzcan daños serios.

  Las unidades de negocio que cuenten con administradores y/o programadores de bases de datos a cargo de la gestión de las aplicaciones deberían, al menos, mantener un registro que consigne quiénes tienen acceso a qué datos, además de asegurarse de que se mantengan y revisen los registros de cambios. Cuando el tipo de tecnología empleada admita el uso compartido de

contraseñas privilegiadas, se debería evaluar la posibilidad de utilizar herramientas que identifiquen claramente a toda persona que acceda a las instalaciones, registren la fecha y hora de acceso, y señalen los cambios realizados.

- **Segregación de funciones (SoD)**. Este es un concepto de probada eficacia práctica, en el que seguramente harán hincapié las auditorías internas cuando se revisen sistemas y transacciones de carácter confidencial. Este concepto se enfrenta con la presión permanente para reducir costos y personal en las organizaciones, que puede suponer un riesgo para el negocio.

Responsabilidades de los equipos de apoyo de TI y usuarios finales

Quien se ocupe de suministrar sistemas informáticos y servicios tecnológicos (una unidad de negocio, el departamento de TI de la empresa, el proveedor de servicios de externalización, etc.) deberá demostrar que se están tomando las medidas adecuadas —como las que se definen en los procedimientos de *Manage data* (Gestión de datos) de la sección DS11 de COBIT— para alcanzar un grado de desarrollo apropiado, y que se está realizando una correcta medición y supervisión de rendimiento y riesgos, con la consiguiente elaboración de los informes pertinentes.

Los equipos de apoyo de usuarios finales (tanto los que integran el área de TI como los que operan de forma independiente) suelen ser los responsables de la creación de cuentas y credenciales de acceso a los sistemas y datos. Estas cuentas y credenciales deben estar plenamente documentadas y solo deberán ser utilizadas cuando se hayan concedido formalmente las autorizaciones pertinentes.

Responsabilidades de la Auditoría Interna

Los auditores se ocupan de realizar evaluaciones independientes y objetivas para determinar en qué medida se han definido y respetado las responsabilidades de las unidades de negocioy del equipo de TI respecto de la preservación de la integridad de los datos.

DESEQUILIBRIOS EN LAS RESPONSABILIDADES DE ASEGURAMIENTO Y PRESERVACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El aseguramiento de la información (IA) consiste en la gestión de riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos, y con los sistemas y procesos empleados en la realización de esas actividades. El IA se desarrolló a partir de la implementación de la seguridad de la información, que, a su vez, surgió como resultado de las prácticas y los procedimientos vinculados a la seguridad informática.

Los proveedores de servicios (como las organizaciones de TI y las empresas dedicadas a la externalización de servicios) tienen una clara responsabilidad respecto del control de las tecnologías y su funcionamiento, y deben aplicar las medidas necesarias para preservar la confidencialidad, integridad y disponibilidad (confidentiality, integrity, availability o CIA) de la información en un entorno operativo. En cuanto a la protección de los datos, los servicios proporcionados abarcan la realización de copias de respaldo y la implementación de procesos de recuperación ante desastres con objetivos claramente definidos para la recuperación a un momento dado (identificación de la cantidad de datos perdidos en un incidente) y documentados en acuerdos de nivel de servicio (service level agreements, SLA). Por otro lado, los proveedores de servicios no son responsables del gobierno de datos ni de las diversas actividades relacionadas con este proceso.

Los SLA definen claramente las responsabilidades de los proveedores de servicios de TI, pero no se ocupan de las que deben asumir los propietarios de los sistemas. Esto produce cierta confusión respecto de las distintas responsabilidades e impide verificar si los datos están clasificados correctamente, y si las funciones y responsabilidades de los usuarios de datos y, en particular, de los usuarios con acceso privilegiado se adecuan a la función crítica que cada uno desempeña. Por consiguiente, la integridad de los datos sigue siendo el aspecto más relegado de la seguridad y el aseguramiento de la información.

MEDICIÓN DE LA INTEGRIDAD DE LOS DATOS

Existen muy pocas publicaciones sobre mediciones clave, rendimiento e indicadores clave de riesgo aplicados a la integridad de los datos en un contexto relacionado con la seguridad de la información. A continuación se mencionan algunos puntos que pueden resultar útiles para comenzar:

- Un inventario de los derechos de acceso privilegiado, que indique ¿quién tiene acceso a qué información? , ¿quién tiene autorización para hacer qué? , ¿y en qué fecha se revisó y actualizó por última vez un documento?.
- Un inventario de los datos que es posible extraer, transformar y cargar en otro sistema.
- El número de usuarios que han mantenido derechos y privilegios de acceso históricos.
- El número de cuentas huérfanas o inactivas.

> "La integridad de los datos sigue siendo el aspecto más relegado de la seguridad y el aseguramiento de la información."

- El número de sistemas de aplicación que contienen derechos de acceso mediante codificación rígida o códigos ocultos ("backdoors").
- El número de veces que fue necesario acceder a los datos de producción para realizar modificaciones o correcciones.
- El número o porcentaje de accesos y/o cambios no autorizados a los datos de producción, que se hubieren identificado.
- El número de problemas de seguridad relacionados con los datos (en un año/un mes).
- El número de sistemas que la solución IAM corporativa principal no cubre.
- Un índice de datos incorrectos o incoherentes.
- El porcentaje del modelo de datos de la empresa (o aplicación crítica) que se ha cubierto con medidas destinadas a preservar la integridad.
- El número de medidas incluidas en bases de datos y aplicaciones para detectar discrepancias en los datos.

- El número de medidas aplicadas para detectar el acceso no autorizado a los datos de producción.
- El número de medidas aplicadas para detectar el acceso no autorizado a los SO.
- El número de medidas aplicadas para detectar las modificaciones que no han estado sujetas a ningún procedimiento de control de cambios.
- El valor anual de las pérdidas económicas ocasionadas por operaciones de fraude a través de sistemas informáticos.
- La cantidad de ataques destinados a destruir la integridad de los datos en los sistemas de SCADA.
- La cantidad de comunicados de prensa generados a partir de los problemas que afectaron la integridad de los datos.

LA IMPORTANCIA DEL GOBIERNO DE DATOS

El gobierno de datos se centra específicamente en los recursos de información que se procesan y difunden. Los elementos clave del gobierno de datos pueden clasificarse en seis categorías básicas: accesibilidad, disponibilidad, calidad, coherencia, seguridad y verificabilidad (mediante auditorías) de los datos. La DAMA ha publicado la guía DMBOK[15], que presenta un marco integral para la gestión y el gobierno de datos, incluidas las tareas que deben realizarse, y las entradas, las salidas, los procesos y los controles.

CONCLUSIÓN

La regla GIGO (que afirma que la introducción de datos erróneos genera resultados erróneos) tiene la misma vigencia hoy que cuando fue formulada, hace 60 años La diferencia entre aquella época y la actual radica en el crecimiento exponencial del volumen de los datos digitales, pero este crecimiento no ha ido acompañado del desarrollo y la consolidación de las disciplinas vinculadas al gobierno de datos. Las características básicas de la CIA (los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad) no han variado, y la disponibilidad sigue siendo el único componente que se puede medir mediante parámetros claramente definidos y ampliamente aceptados.

> "El volumen de los datos digitales ha crecido de manera exponencial, pero este crecimiento no ha ido acompañado del desarrollo y la consolidación de las disciplinas vinculadas al gobierno de datos."

La no aplicación de métricas sobre la integridad de los datos debería considerarse un obstáculo, porque sin ella una empresa no está en condiciones de reconocer cuánto han "mejorado" o "empeorado" la confidencialidad o la integridad desde la introducción de los procedimientos o procesos para administrarlas.

En la medida en que el gobierno de datos no reciba el mismo grado de atención que el gobierno de TI (y este siga siendo el eslabón más débil de la cadena del gobierno corporativo), las organizaciones estarán expuestas a graves riesgos que podrían afectar sus operaciones, su economía, su capacidad de cumplimiento y su reputación.

NOTA DE LA REDACCIÓN

Si desea leer otros textos relacionados con este tema, ubique el libro *Managing Enterprise Information Integrity: Security, Control and Audit Issues* en la Librería de ISACA (ISACA Bookstore). Para obtener información, puede consultar el Apéndice sobre la Librería de ISACA en esta edición del *Journal*, visitar la página *www.isaca.org/bookstore*, enviar un mensaje por correo electrónico a *bookstore@isaca.org* o llamar al +1.847.660.5650.

REFERENCIAS

1 Farwell, James P.; Rafal Rohozinski; "Stuxnet and the Future of Cyber War", *Survival*, vol. 53, número 1, 2011

2 Salido, Javier; "Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach", *ISACA Journal*, vol. 6, 2010

3 Dobbs, Michael; *The Edge of Madness*, Simon & Shuster UK Ltd., RU, 2008

4 IBM, *Top 3 Keys to Higher ROI From Data Mining*, artículo técnico de IBM SPSS

5 *YourDictionary.com, http://computer.yourdictionary.com/data-integrity*

6 Véase Kerviel, Jerome; *L'engranage, Memoires d'un Trader*, Flammarion, Francia, 2010, y Societe Generale, *www.societegenerale.com/en/search/node/kerviel.*

7 *Op. cit.*, Farwell

8 Broad, William J.; John Markoff; David E. Sanger; "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, 15 de enero de 2011, *www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all*

9 IT Governance Institute, *IT Assurance Guide: Using COBIT®*, EE. UU., 2007, pág. 212

10 Bankar, Pritam; Sharad Verma; "Mapping PCI DSS v2.0 With COBIT 4.1", *COBIT Focus*, vol. 2, 2011, *www.isaca.org/cobitnewsletter*

11 Data Management Association International (DAMA), *The DAMA Guide to the Data Management Body of Knowledge*, Technics Publications LLC, EE. UU., 2009, *www.dama.org/i4a/pages/index.cfm?pageid=3345*

12 Unión Europea (UE), Directiva 95/46/CE, emitida por el Parlamento Europeo y el Consejo el 24 de octubre de 1995, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

13 UE, Directiva 2006/43/CE, emitida por el Parlamento Europeo y el Consejo el 17 de mayo de 2006, sobre la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas del Consejo 78/660/CEE y 83/349/CEE y se deroga la Directiva del Consejo 84/253/CEE.

14 Adaptado de US Chiefs of Staff Joint Publication 3-28, "Civil Support", EE. UU., 14 de septiembre de 2007

15 *Op. cit.*, DAMA