BASES DE DATOS SEGURAS, LA CLAVE ESTÁ EN LA GESTIÓN

LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE BASES DE DATOS SE CONVIERTE EN UN PROBLEMA DE PRIMER ORDEN CUANDO LOS DATOS CRÍTICOS DE LA EMPRESA SE EXPONEN A LAS POSIBLES VULNERABILIDADES TECNOLÓGICAS.

VICTOR SANTOS ESCOLANO. INGENIERÍA DE CLIENTES DE ACENS, THE HOSTING COMPANY.
GUSTAVO SAN FELIPE LOBO. RESPONSABLE DE SEGURIDAD DE ACENS, THE HOSTING COMPANY.

A lo largo de este artículo se aporta una visión general de cómo se debe realizar adecuadamente la gestión de la seguridad en sistemas de bases de datos, evitando en la medida de lo posible los detalles técnicos concretos que puedan perder valor en el tiempo. Desde el punto de vista de la seguridad se buscará respuesta a preguntas tales como: ¿qué implica que una base de datos sea transaccional? ¿qué cuestiones hay que tener en cuenta en el clustering? ¿para qué sirven los roles y grupos de usuarios? ¿de qué manera afectan y ayudan a la seguridad de las aplicaciones existentes sobre bases de datos? ¿cómo es viable gestionar la combinación de todo lo anterior sin permanecer en un estado de alerta permanente?

Los conceptos de seguridad en bases de datos son los mismos que se plantean en cualquier otro sector de tecnologías de la información, pero en su aplicación práctica poseen muchas particularidades. Cada dato tiene unas consideraciones distintas. Dentro de una misma tabla, no es lo mismo conocer el campo "apellido" que el campo "salario", y dentro de este mismo, no es lo mismo conocer el del registro "bedel" que el del registro "consejero delegado".

¿DE QUÉ SEGURIDAD HABLAMOS?

La situación ideal es aquella en la que se logra gestionar el estado y garantizar un nivel adecuado de los tres aspectos fundamentales de la seguridad de la información: integridad, confidencialidad y disponibilidad. Aplicado al entorno de las bases de datos se trata de garantizar que los datos almacenados son veraces y no están corruptos, que sólo accede a cada dato aquél al que le corresponde acceder, y que la información está disponible cuando se requiere su uso. Este aspecto es fundamental en aplicaciones que no conocen de horarios, o en aquellas en las que es imprescindible contar con los datos en ciertas franjas horarias independientemente del número de accesos simultáneos que se estén realizando.

Para lograr dichas premisas y contemplar la seguridad en todos sus aspectos hay que tener en cuenta tres áreas diferenciadas:

- **Seguridad física:** sistemas *hardware*, soportes, dependencias, etc. La seguridad física siempre es importante, aunque este artículo se va a centrar en las particularidades de las bases de datos.
- **Seguridad lógica:** aplicaciones, protocolos, procesos informáticos, elementos de protección de red, etc.
- **Seguridad político-corporativa:** legislación aplicable, la política general, normas, procedimientos, convenciones internas, etc.

LA COOPERACIÓN, EL 'BUSINESS TO BUSINESS' Y LA CONFEDERACIÓN OBLIGAN A UN ACCESO INTEGRADO A BASES DE DATOS HETEROGÉNEAS E INDEPENDIENTES

Dichas áreas están interrelacionadas, y para garantizar el nivel de protección óptimo frente a las posibles amenazas en cada área se implementarán principalmente y de forma coherente, medidas de seguridad de tres tipos:

- **Activas o preventivas.** El ejemplo para seguridad lógica sería el cortafuegos (*firewall*), la valla en seguridad física y las normas en seguridad político-corporativa.
- **Pasivas, como auditoría, detección y/o alarma.** Por ejemplo, las cámaras de

SEGURIDAD REFORZADA

La seguridad en el acceso a la información puede reforzarse considerablemente si en la aplicación que consulta a la base de datos se emplean mecanismos de autenticación fuerte, como pueden ser:

- *Tokens* de autenticación.
- Certificados digitales almacenados en tarjetas inteligentes.
- Dispositivos de autenticación biométrica.
- Etc.

CCTV, los sistemas IDS y los planes de auditoría.

- **De recuperación, como por ejemplo el Disaster Recovery Plan**, las copias de seguridad o Backup, y la SAI y/o grupo electrógeno.

QUIÉN ACCEDE A QUÉ Y DESDE DÓNDE

La cooperación, el *business to business* y la confederación obligan a un acceso integrado a bases de datos heterogéneas e independientes, que normalmente emplean distintos sistemas y tecnologías. La aplicación que solicita los datos no entiende ni le interesa lo que hay por debajo, y el usuario final, es decir, la persona que utiliza dicha aplicación, normalmente tampoco.

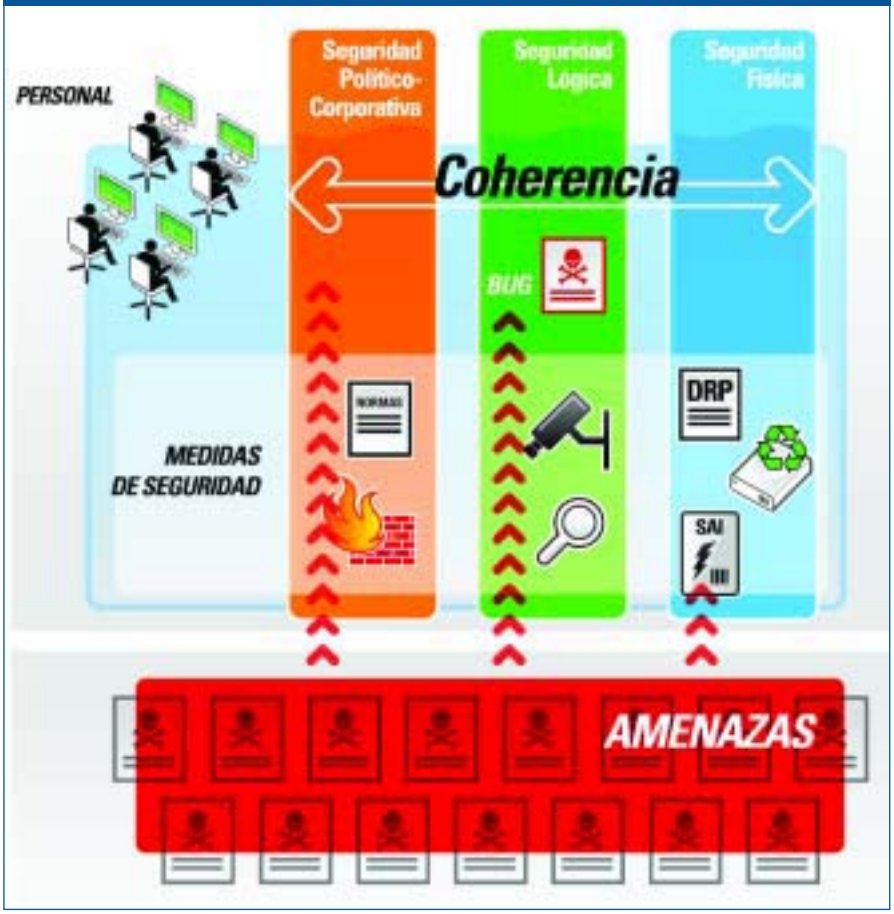
En esta jungla de sistemas dispares, motores de distintos fabricantes, accesos ubicuos y aplicaciones preexistentes, se trata de acomodar la seguridad. No es sencillo. Hay que poner de acuerdo a ingenieros en la fase de diseño, desarrolladores en la fase de construcción y administradores en la fase de operación, para ver quién se va a encargar de qué. Posteriormente, ajustar las interdependencias y un largo etcétera de pormenores para alcanzar el objetivo. Y todo con un único fin: que el acceso a unos datos concretos se produzca por quien debe y desde donde debe. Y que ese alguien no tenga permiso ni derecho a acceder o modificar lo que no le corresponde.

Para ello, habrá que poner de acuerdo a los sistemas operativos, bases de datos, elementos de red y sistemas de almacenamiento. Entre ellos se acomodan para funcionar con unos o con otros por motivos técnicos, económicos o políticos, pero aún así, las combinaciones son muchas.

En un primer nivel de control de acceso lógico es necesario implementar tecnología *firewall* (cortafuegos) como primer filtro en el que se establecen qué redes de confianza pueden acceder a las bases de datos. Posteriormente, es importante analizar la seguridad de las aplicaciones que acceden a la propia base de datos, ya que normalmente el usuario no se introduce directamente a la base de datos, sino que utiliza un cliente o una aplicación *web* que es realmente quien se identifica y accede al motor de la base de datos. La seguridad del código es necesaria para evitar ataques del tipo SQL-Injection, originados por la falta de validación de los datos de entrada en la aplicación que "ataca" (y nunca mejor dicho) a la base de datos.

A continuación se analizan las herramientas y funcionalidades de la propia base de datos para afinar el acceso en el ámbito de tablas, registros e incluso campos concretos en el ámbito del usuario.

Cuadro 1. Áreas de la seguridad



EN UN PRIMER NIVEL DE CONTROL DE ACCESO LÓGICO ES NECESARIO IMPLEMENTAR TECNOLOGÍA 'FIREWALL' COMO PRIMER FILTRO

¿ES TODO ES TAN COMPLEJO? ¿NADIE NOS AYUDA?

Lo cierto y por fortuna es que en la última década los fabricantes han realizado un auténtico esfuerzo por facilitarles las cosas a administradores y gestores. La seguridad ha sido siempre una pieza clave en este campo, y en cada nueva versión hemos tenido avances cualitativos importantes.

A continuación se enumeran algunos de los "inventos" más notables de los últimos años, tratando de no particularizar sobre fabricantes. Por otro lado, unos aprenden de los otros y al cabo de un tiempo, todos aplican los descubrimientos de los demás.

LAS VISTAS. Las vistas son una excelente forma de dar al usuario la información que necesita y sólo ésa. Son simples consultas a través de las cuales el usuario final únicamente ve determinadas columnas, filas o campos que cumplan un criterio. Se crea así un esquema conceptual a partir de lo que el usuario solicita. Esto evitará tener información redundante. Se han desarrollado bastante y mejorado el tipo de vistas, lo que supone la creación de vistas materializadas, vistas multinivel, vistas fragmentadas, subvistas, etc.

PERMISOS DE USUARIO. Con los permisos de usuario se trata de definir qué puede hacer un usuario concreto, o qué tipo de operaciones no le están permitidas. En los

permisos se suele distinguir entre autorizar, no decir nada, o denegar explícitamente.
A diferencia de la vida real, donde uno le puede dar las llaves de su casa a quien desee, los usuarios pueden no ser propietarios de sus objetos, y no tener permiso para delegar nada. Aquí se definen permisos sobre tablas, vistas, procedimientos, y casi todo lo que se nos pueda ocurrir. La complejidad puede ser casi infinita, con un sinfín de jerarquías que se pueden contradecir, pues no sólo es a qué se da permiso, sino también quién lo da, y que ocurre si simultáneamente se otorga un permiso por un usuario y otro lo deniega explícitamente. Con idea de simplificar esto se idearon los roles.

ROLES. Los roles son simplemente conjuntos permisos que se unen para mayor comodidad. Los sistemas suelen traer algunos predefinidos, "administrador" o "usuario" son dos de ellos, pero realmente los roles están destinados a ser personalizados. Dentro de un rol se puede incluir, por ejemplo, el acceso tres vistas, la ejecución de seis procedimientos concretos, y la escritura en una tabla. De esta forma se acota el alcance de un usuario concreto, y por tanto el daño que puede llegar a hacer. Existen roles específicos para la función de asignación de roles, siendo estos los que deben controlarse de forma más estricta.

GRUPOS DE CONSUMIDORES. Una cuestión que gana peso día a día en materia de seguridad es el control en el consumo de recursos. Determinados usuarios utilizan de forma intensiva o incluso abusan de ellos, a pesar de que son limitados. Si no se controla esto, podría suceder que se produjera un retraso en las nóminas de una empresa, porque el departamento de desarrollo está probando una herramienta, y ésta es defectuosa. Con este objeto, los grupos de consumidores controlan las consultas, transacciones, tiempo de CPU, etc., que pueden consumir o llegar a consumir los agentes. Esto se hace, ni más ni menos, que para garantizar la calidad de servicio de la base de datos.

AUDITORIA. Los fabricantes han hecho hincapié en la auditoría, los *logs*, las trazas de error y los distintos mecanismos que facilitan el control y análisis de lo que hacen los usuarios. Mejor dicho, de aquellos elementos susceptibles de ser controlados. Se pueden así, establecer eventos que hay que monitorizar. No se vigila, por tanto, todo el sistema, igual que las cámaras de circuito cerrado de televisión, sólo se graban los lugares conflictivos o los que pueden serlo.

LA MÁQUINA DEL TIEMPO. En las bases de datos transaccionales avanzadas se ha conseguido el efecto de rebobinar hasta el lugar donde se produjo el error o se perdieron los datos. Estos sistemas son caros en cuanto a tecnología y recursos, pero eliminan el mayor peligro que tienen los sistemas de información: el factor humano. Con estos mecanismos se puede observar el contenido de una tabla hace media hora, hace dos u ocho. Esto no se puede mantener durante mucho tiempo en bases con alta carga de transacciones, pues los volúmenes de datos serían inmanejables.

SALVAGUARDA Y 'BACKUP'. Aquí las bases de datos han crecido y mejorado. Los años en los que se paraba el sistema por la noche para realizar su copia han pasado a la historia. Ahora se necesita que el *backup* sea mucho más granular, continuo y rápido para que no se tenga que parar de ninguna forma la base de datos. En este punto es conveniente verificar que el mecanismo de *backup* que se está empleando es el adecuado para la tecnología concreta. El principal problema es que no se puede realizar una copia de ficheros "tal cual", es necesario disponer de un agente que "hable" con la base de datos, o en el peor de los casos programar un volcado y hacer backup de dicho fichero.

REPLICACIÓN Y SINCRONÍA. A colación del punto anterior, una buena forma de tener una copia de la base de datos consiste en disponer de una réplica en un emplaza-

NORMAS DE OBLIGADO CUMPLIMIENTO

La Ley Orgánica de Tratamiento de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre, LOPD) refleja las cuestiones que se tienen que tener en cuenta en la recogida y tratamiento de los datos personales almacenados en bases de datos (denominados "ficheros" en la propia ley) y su incumplimiento puede dar lugar a sanciones que van desde los 600 euros para las infracciones leves hasta los 600.000 euros para las infracciones muy graves.

miento remoto. Normalmente, esta solución, más cara y compleja, suele utilizarse por motivos de rendimiento y no de seguridad, pero llegado el caso, cumple ambos cometidos. Las bases de datos esclavas se utilizan normalmente como lugar de consulta, y en ellas no se realizan transacciones (inserciones, borrados o modificaciones), pues si así fuera podríamos tener problemas de consistencia.

Las soluciones de réplica múltiple se han empezado a desarrollar con contenidos estáticos como páginas o vídeos (no deja de ser una paradoja llamar a un vídeo "contenido estático") y en el siguiente punto veremos como vencemos el límite físico del almacenamiento local. Todo se orienta a una deslocalización de los ficheros. En un futuro no muy lejano, puede que dentro de una misma aplicación, unos datos estén ubicados en un emplazamiento, y otros (dentro de la misma página de consulta) a 1.000 kilómetros de distancia, con todo lo que ello implica.

LA GUERRA DE LA COMPLEJIDAD

Como se ha comentado con anterioridad, conforme crece de forma notable la complejidad entre sistemas, garantizar su seguridad se convierte en algo vital. La rapidez y la sencillez de manejo suele oponerse a la seguridad. En este juego, en ocasiones de suma cero, debe primar lo segundo sobre lo primero. Más vale ir despacio que no llegar.

La seguridad en el acceso a la información puede reforzarse considerablemente si en la aplicación que consulta a la base de datos se emplean mecanismos de autenticación fuerte, como pueden ser:

- *Tokens* de autenticación.
- Certificados digitales almacenados en tarjetas inteligentes.
- Dispositivos de autenticación biométrica.
- Etc.

De esta forma conseguimos que para autorizar el acceso no baste el conocimiento de un identificador de usuario y contraseña, sino en una combinación de: "lo que sabes" más "lo que tienes" más "lo que eres". Asimismo, para aumentar el nivel de seguridad en el propio almacenamiento se puede recurrir al cifrado de datos, ya sea empleando las utilidades y funciones que pueda proporcionar la propia base de datos o utilizando herramientas de terceros para cifrar los datos utilizando material criptográfico del usuario antes de proporcionárselos al motor de la base de datos.

Por otro lado, las bases de datos han ido evolucionando en cuanto a tamaño y capacidad según se han desarrollado las diferentes tecnologías de almacenamiento.

La seguridad en los datos dentro del *scale out process* dependerá de cómo se entiendan comunicaciones, almacenamiento y bases de datos. Todo un reto. La deslocalización de los datos, tendrá consecuencias en el acceso y la seguridad que hoy de momento no se plantean.

SEGURIDAD "DE LEY"

En lo referente al cumplimiento de la legislación vigente, y en el muy probable caso de que las bases de datos vayan a almacenar algún tipo de dato referente a personas, el principal aspecto a tener en cuenta es el relativo a la Ley Orgánica de Tratamiento de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre, LOPD).

Esta ley, por cuyo cumplimiento vela la Agencia Española de Protección de Datos, refleja las cuestiones que se tienen que tener en cuenta en la recogida y tratamiento de los datos personales almacenados en bases de datos (denominados "ficheros" en la propia ley) y su incumplimiento puede dar lugar a sanciones que van desde los 600 euros para las infracciones leves hasta los 600.000 euros para las infracciones muy graves.

Las obligaciones recogidas en la LOPD contemplan aspectos tales como la obligatoriedad de registrar los "ficheros" que almacenen datos de carácter personal, la calidad de datos y la proporcionalidad, el deber de información en la recogida, aspectos a tener en cuenta en el tratamiento y la posible cesión a terceros, las transferencias internaciones de datos, y los derechos de los afectados (acceso, rectificación y cancelación, oposición).

Centrándonos en las medidas de seguridad específicas, la LOPD se complementa con el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos personales. Este reglamento, cuya nueva versión se ha retrasado y está anunciada para el segundo semestre del 2007, establece que medidas de seguridad se deben establecer en función del tipo de datos almacenados en el fichero. Estas medidas incluyen la realización de un documento de seguridad y pueden llegar hasta la obligatoriedad de auditoría bianual e incluso la transmi-

sión cifrada de datos. Existe un cuadro resumen en la siguiente ubicación web: *https://www.agpd.es/upload/Informa%20AEPD/cuadro_reglamento1.pdf*
Para más información se recomienda consultar la página web de la Agencia de Protección de Datos (*http://www.agpd.es*), en la que se puede consultar y buscar desde la legislación aplicable y documentos de interés, hasta los ficheros inscritos en el registro y las resoluciones (con sanción o no) emitidas por dicha agencia.

GESTIÓN Y CONTROL INTERNO

A lo largo del presente artículo se han mencionado las directrices generales cuya aplicación en la práctica puede destrozar un diseño perfecto, por ejemplo, fallos en el *software* (de funcionamiento o específicos de seguridad), incompatibilidades entre las diferentes aplicaciones, la incorrecta dimensión de los recursos de hardware y comunicaciones, los malos hábitos de las personas (sobre todo cuando no son conscientes del porqué de los controles o no se les ha transmitido la importancia de mantener la seguridad en la información que manejan).
Si nuestro sistema de base de datos tiene conexión directa o indirecta (por ejemplo, vía *web*) con redes públicas, como Internet, será necesario tener en cuenta el elevado número de potenciales atacantes que existen y que están deseosos de utilizar los recursos de la empresa y, en el peor de los casos, interesados en la información que alberga la base de datos.

Del mismo modo, a la hora de garantizar la seguridad lógica del propio motor de base de datos es importante aplicar una correcta política de parcheado. Este mantenimiento no es obvio, pues los efectos de aplicar los parches de forma precipitada pueden ser incluso peores que los derivados de no aplicarlo. Los fabricantes de herramientas comerciales de bases de datos suelen agrupar varios parches y programar su anuncio para facilitar esta tarea. La elección de aplicar un parche o conjunto de parches en un momento concreto tendrá que venir determinada por varios factores:

1. ¿Necesito la funcionalidad extra proporcionada por el parche?
2. ¿Es un parche crítico para la seguridad del sistema?
3. ¿Permite sacar provecho de la vulnerabilidad de forma remota?

El elemento fundamental para garantizar que las medidas anteriormente mencionadas están siendo aplicadas con la lógica que corresponde es el control interno ("que tu mano izquierda vea lo que hace la derecha"). Todo lo que no está documentado no existe. No se puede depender del conocimiento concreto de un buen equipo de técnicos, puesto que tenemos que contar con las circunstancias que afectan a las personas (vacaciones, bajas, rotación de personal, etc.).
Por otro lado, con el paso del tiempo todo sistema de información se degrada; por ejemplo, un proyecto puede quedar correctamente establecido en su inicio, pero si no se establece un correcto plan de auditoría nunca se tendrá una visión real en el tiempo del estado de la seguridad del sistema de bases de datos. Los resultados de dichas auditorías deben contribuir a la mejora de la seguridad, constituyendo el típico ciclo PDCA (*Plan-Do-Check-Act*) que se inicia durante el diseño del proyecto y se repite durante la vida útil del mismo.
La gestión y el control interno son fundamentales para garantizar el éxito. Es más importante tener identificadas las vulnerabilidades y poder trazar el seguimiento de su gestión que invertir de forma puntual en tecnología de protección que introduzca más elementos de complejidad a un escenario ya de por sí complejo.

SE NECESITA QUE EL 'BACKUP' SEA MUCHO MÁS GRANULAR, CONTINUO Y RÁPIDO PARA QUE NO SE TENGA QUE PARAR DE NINGUNA FORMA LA BASE DE DATOS

«Bases de datos seguras, la clave está en la gestión». © Ediciones Deusto.

Si desea más información relacionada con este tema, introduzca el código 16101 en www.e-deusto.com/buscadorempresarial