**¿Qué es la seguridad de las bases de datos?**

La seguridad de las bases de datos son los procesos, herramientas y controles que aseguran y protegen las bases de datos contra amenazas accidentales e intencionadas. El objetivo de la seguridad de las bases de datos es proteger los datos confidenciales y mantener la confidencialidad, disponibilidad e integridad de la base de datos. Además de proteger los datos dentro de la base de datos, la seguridad de la base de datos protege el sistema de gestión de la base de datos y las aplicaciones asociadas, los sistemas, los servidores físicos y virtuales y la infraestructura de red.

## Tipos de seguridad de bases de datos

### Seguridad de las redes

* Los**Firewalls** son la primera línea de defensa en la seguridad de bases de datos DiD. Lógicamente, un firewall es un separador o limitador del tráfico de red, que puede configurarse para aplicar la directiva de seguridad de datos de su organización. Si utiliza un firewall, aumentará la seguridad del sistema operativo, ya que proporciona un cuello de botella en el que pueden concentrarse las medidas de seguridad.

### Administración de acceso

* **Autenticación** es el proceso de demostrar que el usuario es quien dice ser introduciendo el ID de usuario y la contraseña correctos. Algunas soluciones de seguridad permiten a los administradores administrar de forma centralizada las identidades y permisos de los usuarios de la base de datos. Esto incluye la minimización de almacenamiento de contraseñas y permite directivas centralizadas de rotación de contraseñas.
* **Autorización** permite a cada usuario acceder a determinados objetos de datos y realizar ciertas operaciones en la base de datos como leer pero no modificar datos, modificar pero no borrar datos, o borrar datos.
* **Control de acceso** es realizado por el administrador del sistema, que asigna permisos a un usuario dentro de una base de datos. Los permisos se administran idealmente agregando cuentas de usuario a [roles de base de datos](https://go.microsoft.com/fwlink/?linkid=2240627) y asignando permisos a nivel de base de datos a dichos roles. Por ejemplo, [de seguridad de nivel de fila](https://go.microsoft.com/fwlink/?linkid=2240550) (RLS) permite a los administradores de bases de datos restringir el acceso de lectura y escritura a filas de datos en función de la identidad, la pertenencia a roles o el contexto de ejecución de consultas de un usuario. RLS centraliza la lógica de acceso en la propia base de datos, lo que simplifica el código de la aplicación y reduce el riesgo de revelación accidental de datos.

### Protección contra amenazas

* **Auditoría** realiza un seguimiento de las actividades de la base de datos y ayuda a mantener el cumplimiento de las normas de seguridad registrando los eventos de la base de datos en un registro de auditoría. Esto le permite supervisar las actividades en curso de la base de datos, así como analizar e investigar la actividad histórica para identificar posibles amenazas o sospechas de abuso y violaciones de la seguridad.
* **Detección de amenazas** descubre las actividades anómalas de la base de datos que indican una posible amenaza para la seguridad de la base de datos y puede mostrar información sobre eventos sospechosos directamente al administrador.

### Protección de la información

* **Cifrado de datos** protege los datos confidenciales convirtiéndolos a un formato alternativo, de modo que solo las partes interesadas puedan descifrarlos y devolverlos a su forma original y acceder a ellos. Aunque el cifrado no resuelve los problemas de control de acceso, mejora la seguridad al limitar la pérdida de datos cuando se eluden los controles de acceso. Por ejemplo, si el equipo anfitrión de la base de datos está mal configurado y un usuario malintencionado obtiene datos sensibles, como números de tarjetas de crédito, esa información robada podría ser inútil si está encriptada.
* **Copia de seguridad y recuperación de la base de datos** es fundamental para proteger la información. Este proceso implica hacer copias de seguridad de la base de datos y de los archivos de registro de forma periódica y almacenar las copias en un lugar seguro. La copia de seguridad y el archivo están disponibles para restaurar la base de datos en caso de fallo o infracción de la seguridad.
* **Seguridad física**limita estrictamente el acceso al servidor físico y a los componentes de hardware. Muchas organizaciones con bases de datos locales usan salas cerradas con acceso restringido para el hardware del servidor de base de datos y los dispositivos de red. También es importante limitar el acceso a los soportes de copia de seguridad almacenándolos en un lugar seguro fuera de las instalaciones.
* **Seguridad de hardware**tiene que ver con todos los dispositivos físicos que pueden contener o por los que pueden transitar los datos, por ejemplo, firewalls o cortafuegos de hardware, servidores proxy, módulos de seguridad para claves encriptadas, sistemas de autenticación, entre otros.
* **Seguridad de software**en este caso se enfoca a la parte virtual, es decir, a los programas, plataformas, software y aplicaciones enfocados a la protección de la información. El ejemplo más conocido en este caso son los **antivirus**.
* **Seguridad de red** este tipo de seguridad se enfoca en el camino por donde se transmiten datos, como es el caso de la nube, con el fin de garantizar el acceso a los datos sin hacerlos vulnerables a un posible robo. Aquí se concentra todo tipo de defensa contra espionaje cibernético, hackeos, troyanos, intercepción de comunicaciones y demás.
* **Respaldos de base de datos** un tipo de seguridad específico es el respaldo de las bases de datos, los cuales pueden ser completos cuando se copian todos los datos; diferenciales cuando solamente se almacenan datos que han sido modificados o actualizados, o backups incrementales cuando se guarda información añadida.
* **Encriptación** con esta se protegen los datos que además de estar almacenados hacen algún tipo de recorrido por la red. Si hubiera un robo de datos, lo que hace este tipo de seguridad es dificultar al ciberdelincuente la interpretación y uso de los mismos.
* **Detección de intrusos**este tipo de seguridad se activa cuando el sistema detecta que alguien está queriendo entrar a un acceso denegado o hay una actividad sospechosa alrededor de los datos. Se trata de sistemas de detección de intrusos de red (NIDS) que están monitoreando de forma continua el tránsito de datos.
* **Gestión de incidentes** los sistemas de información de seguridad y gestión de eventos (SIEM) visualizan la seguridad de bases de datos de una forma integral, ya que a través del monitoreo hacen un análisis de incidencias para generar informes que ayudan a la gestión de la información segura.
* **Protocolos de internet** toda acción en internet supone un riesgo cibernético porque te haces visible y estás en el camino de todos, por lo tanto, este tipo de seguridad busca proteger a los usuarios en internet a través de sistemas de ciberseguridad HTTPS, SSL y TLS, que se aplican para que los sitios web sean seguros y los usuarios puedan compartir información o interactuar en estos espacios.
* **Prevención de pérdida de datos (DLP)** este tipo de seguridad aplica acciones que garanticen que ciertos datos no sean enviados desde la red, de tal forma que supervisa y asegura a las personas autorizadas que no se están copiando o compartiendo datos confidenciales.
* **Defensa a profundidad** este tipo de seguridad trata de abarcar todas las rutas, entornos y procesos por los que circulan o se almacenan los datos de una empresa, por lo que implicará tecnologías o sistemas para cifrar, enmascarar datos, aplicar controles de acceso, monitorear constantemente y generar informes.