Disponibilidad del dato

Tipos y ciclo de vida del dato

CONTENIDO

Objetivos

- Conocer las oportunidades de acceso a los datos.
- Dimensionar la utilidad de los datos.
- Establecer las bases de la seguridad de los datos.

Acceso

La accesibilidad hace referencia a la autorización o no que se tiene para consultar o manipular el dato, para ello se verán cuáles son los tipos de acceso más comunes.

Las páginas ASP con acceso a datos permiten interactuar con la información de una base de datos, ya sea para obtener información y mostrarla al usuario o bien para actualizar su contenido.

Al tratarse de información en continua actualización la presencia de una base de datos y su consulta dinámica se hacen indispensables.

Para conectarse a una base de datos, las páginas ASP utilizan la tecnología *activex data objects* (ADO) y pueden accederse a sistemas de gestión de bases de datos compatibles con ODBC (SQL Server, Access, Informix o Oracle, entre otras).

Conexión

Pueden utilizarse dos sistemas de conexión a base de datos:

Mediante DSN

Este sistema consiste en definir un identificador de la conexión mediante el driver ODBC accesible desde el panel de control. Posteriormente, desde las páginas ASP, se practica el acceso mediante un *string* de conexión, que incluye el identificador antes mencionado. Para crear un DSN en Windows, se debe realizar el siguiente proceso:

- Hacer clic en el botón Inicio.
- Seleccionar la opción panel de control del menú configuración.
- En la ventana del panel de control seleccionar fuentes de datos ODBC.
- Acceder a la pestaña DSN de sistema.
- Seleccionar la base de datos que quieres añadir.
- Definir un nombre a la conexión y la localización física de la base de datos.

Sin DSN

Este sistema requiere almacenar directamente el archivo de la BD en un directorio del servidor. De este modo, en la conexión se utilizará un *string* un poco más complejo, ya que deben identificarse tanto el driver como el directorio físico completo de la base de datos.

Estos son los 3 pasos para realizar la conexión:

- Crear el objeto para conectarse a la base de datos mediante la instrucción.
- Definir la conexión (con/sin DNS).
- Abrir la conexión.

Mediante el lenguaje Structured Query Language (SQL)

Puede interactuarse con los motores de base de datos relacionales para obtener y modificar la información almacenada en la base de datos.

La mayoría de este acceso, además de solicitar los canales exactos, suelen solicitar que esté logueado, es decir, que tenga un usuario y contraseña para acceder a ellas, adicionalmente suelen establecerse perfiles de usuario, por lo que no todos los usuarios podrán realizar todas las acciones, tendrán permisos para actuar dentro del entorno de los datos que les permitirá realizar algunas acciones y otras no, lo mismo ocurrirá eventualmente con la visualización.

Repositorios de datos abiertos o públicos

Es el caso de los datos manejados por las oficinas estadales de estadística, cuya información suele estar a disposición de los usuarios para su descarga, esta información no cuenta por supuestos con datos de identificación sensible de los ciudadanos, atendiendo a las normativas que prohíben la divulgación de este tipo de información. También se encuentran este tipo de repositorios de datos alrededor de la comunidad científica, de estudios ya publicados por sus autores.

Utilidad

Una base de datos es un contenedor informático en el que guardar y consultar datos relacionados con un mismo tema o actividad, para la manipulación eficiente de esta colección de informaciones se precisan programas especializados.

La utilidad de la información para conocer y estudiar cualquier fenómeno o evento es indiscutible, considerando que el origen de esta información siempre son los datos estos se vuelven la base inequívoca de esta utilidad.

La utilidad de un recurso cualquiera es para qué sirve, mientras que la usabilidad es la oportunidad de uso, ambos conceptos son importantes en el contexto que actualmente pretendemos desarrollar, los datos son útiles, pero a la a la vez deben ser altamente usables.

En el mundo actual los datos se encuentran alojados en multitud de formas y depósitos que permiten su actualización sistemática, haciendo que estos estén en condición de permitir consultas en tiempo real para conocer la situación o estatus de un proceso en marcha, así mismo permite acceder a bancos de datos generalizados que darán respuesta a infinidad de interrogantes de la vida actual tanto en la ciencia como en la vida.

En el caso particular de las empresas los datos son un valor indiscutible, las empresas suelen captar sus datos a través de sus diferentes sistemas de CRM o ERP que documentan su operación, inicialmente con la intención de poder realizar las gestiones administrativas asociadas a esta tales como compras, ventas, facturación, control de inventario, control logístico, entre otros, todos estos registros permitirán dibujar de forma íntegra el cómo opera la organización y en algunos casos y dependiendo de la naturaleza de los datos recolectados y de su manejo permitirán realizar modelos o inferencias que nos aproximen a información futura, es decir a la aplicación de métodos inferenciales que nos permitan realizar estimaciones o proyecciones sobre el comportamiento del negocio para períodos posteriores.

En el caso de la ciencia también ofrece la oportunidad de hacer cálculos muy finos basados en las observaciones ya existentes de fenómenos específicos.

Y desde el punto de vista demográfico los datos permiten diseñar y dimensionar todas las capacidades y condiciones que un estado debe tener y debería tener a futuro para atender integralmente las necesidades de una población en los diferentes ámbitos de obligación (salud, educación, infraestructura, vivienda, entre otros).

La utilidad de los datos no es dimensionable, ya que su valor podría indicarse como infinito, pueden ocurrir muchísimas maneras distintas de aprovechar un mismo dato, según la necesidad del investigador o el interesado, por lo que la utilidad de los datos se podría considerar como absoluta, aunque en un momento determinado un dato o una porción de los datos puede resultar irrelevante para el estudio un evento en particular, pero esta relevancia no los invalida ni los desprecia de forma general solo atiende a su pertinencia particular dentro de un estudio.

Seguridad

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos, sitios *web*, etc. La seguridad de datos también protege los datos de una posible intrusión.

Comprender el riesgo de los datos sensibles es clave. El análisis de riesgo de datos incluye descubrir, identificar y clasificarlo, por lo que los administradores de datos pueden tomar medidas tácticas y estratégicas para asegurar que los datos sean seguros.

Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización.

Mecanismos utilizados para generar seguridad en el manejo de datos

Tendencias recientes han demostrado que los ataques de *ransomware* están aumentando en frecuencia y en gravedad. Se ha convertido en un negocio en auge para ladrones cibernéticos y *hackers*, que acceden a la red, secuestran datos y sistemas.

Entonces, ¿qué conceptos deberían conocerse que puedan ayudar a proteger la red y prevenir esta nueva ola de ataques cibernéticos modernos?

Ingeniería de la seguridad de datos

La ingeniería de seguridad cubre mucho terreno e incluye muchas medidas, desde pruebas de seguridad y revisiones de código regulares hasta la creación de arquitecturas de seguridad y modelos de amenazas para mantener una red bloqueada y segura desde un punto de vista holístico.

Encriptación

La encriptación protege los datos y archivos reales almacenados en ellos o que viajan entre ellos a través de Internet. En el caso de que los datos sean interceptados, la encriptación dificulta que los *hackers* hagan algo con ellos. Esto se debe a que los datos encriptados son ilegibles para usuarios no autorizados sin la clave de encriptación.

Detección de intrusión y respuesta ante una brecha de seguridad

Los sistemas de detección de intrusos de red (NIDS) supervisan de forma continua y pasiva el tráfico de la red en busca de un comportamiento que parezca ilícito o anómalo y lo marcan para su revisión. Los NIDS no solo bloquean ese tráfico, sino que también recopilan información sobre él y alertan a los administradores de red.

Firewall (corta fuegos)

Es un *software* o *hardware* diseñado con un conjunto de reglas para bloquear el acceso a la red de usuarios no autorizados. Son excelentes líneas de defensa para evitar la interceptación de datos y bloquear el *malware* que intenta entrar en la red, y también evitan que la información importante salga, como contraseñas o datos confidenciales.

Análisis de vulnerabilidades

El software de análisis de seguridad se utiliza para aprovechar cualquier vulnerabilidad de un ordenador, red o infraestructura de comunicaciones, priorizando y abordando cada uno de ellos con planes de seguridad de datos que protegen, detectan y reaccionan.

Pruebas de intrusión

Las pruebas de intrusión implican la ejecución de procesos manuales o automatizados que interrumpen los servidores, las aplicaciones, las redes e incluso los dispositivos de los usuarios finales para ver si la intrusión es posible y dónde se produjo esa ruptura.

Información de seguridad y gestión de eventos

Es lo que se conoce como Información de Seguridad y Gestión de Eventos (SIEM). SIEM es un enfoque integral que monitoriza y reúne cualquier detalle sobre la actividad relacionada con la seguridad de TI que pueda ocurrir en cualquier lugar de la red, ya sea en servidores, dispositivos de usuario o *software* de seguridad como NIDS y *firewalls*. Los sistemas SIEM luego compilan y hacen que esa información esté centralizada y disponible para que se pueda administrar y analizar los registros en tiempo real, e identificar de esta forma los patrones que destacan.

Ciberseguridad: HTTPS, SSL y TLS

Todos los usuarios de Internet deben protegerse de la posibilidad de compartir información privada en todo Internet, existen diferentes estándares y protocolos de cómo se envía la información a través de esta red. Las conexiones cifradas y las páginas seguras con protocolos HTTPS pueden ocultar y proteger los datos enviados y recibidos en los navegadores. Para crear canales de comunicación seguros, los profesionales de seguridad de Internet pueden implementar protocolos TCP/IP (con medidas de criptografía entretejidas) y métodos de encriptación como *secure sockets layer* (SSL) o *transport layer security* (TLS).

Detección de amenazas en punto final

Se pueden prevenir ataques de *ransomware* siguiendo buenas prácticas de seguridad, como tener *software* antivirus, el último sistema operativo y copias de seguridad de datos en la nube y en un dispositivo local. Sin embargo, esto es diferente para organizaciones que tienen múltiple personal, sistemas e instalaciones que son susceptibles a ataques.

Prevención de pérdida de datos (DLP)

Dentro de la seguridad de punto final hay otra estrategia de seguridad de datos importante: la prevención de pérdida de datos (DLP). Esencialmente, esto abarca las medidas que se toman para asegurar que no se envían datos confidenciales desde la red, ya sea a propósito, o por accidente. Puede implementarse software DLP para supervisar la red y asegurarse de que los usuarios finales autorizados no estén copiando o compartiendo información privada o datos que no deberían.

Seguridad de datos *in house versus* en la nube

El uso del *cloud* o nube está claramente en auge, pero no todas las organizaciones están dispuestas a dar el salto que representa tener los datos en casa y pasarlo a la nube, un lugar en el que cuesta materializar o concretar la percepción de donde se encuentra realmente el dato, generando por tanto un temor asociado a la seguridad del dato y otro a la eventual desaparición de este. Un proveedor en la nube de ofrecer a sus clientes opciones de monitorización continua de la aplicación y cumplimiento de los mecanismos de seguridad.

Auditoría continua

Si un proveedor de la nube es serio acerca de la seguridad de datos, esa seriedad se extiende a la auditoría continua, monitorización y pruebas de seguridad de todos los aspectos operacionales de la infraestructura. Además de garantizar una mayor fiabilidad de las soluciones, la auditoría continua garantiza que todo el *software* se actualiza a la última versión, se identifican y resuelven todas las anomalías en el rendimiento del sistema y se cumplen todos los requisitos de cumplimiento de seguridad. La monitorización constante asegura que cualquier comportamiento irregular sea inmediatamente identificado e investigado.

Automatización y repetibilidad

La infraestructura de la nube se desarrolla pensando en automatización: menos intervención manual en funciones de rutina y menos oportunidades para que se cometan errores. Los servicios en la nube realizan un número limitado de tareas por diseño. Estas tareas están estandarizadas, al igual que la mayoría del *hardware*, equipos de red, aplicaciones y sistemas operativos utilizados para realizar esas tareas. Esta estandarización facilita la seguridad de las infraestructuras *cloud*.

Controles de acceso más estrictos

Una preocupación importante es la pérdida de control de datos para las empresas si los datos se encuentran fuera de su *firewall*. Este control se extiende a la creencia de que algunos empleados del proveedor de la nube tienen acceso general a sus datos confidenciales. Un proveedor de *cloud* gestionado adecuadamente tendrá varios roles compartiendo responsabilidades para toda la solución *cloud* sin que ninguna persona tenga acceso total a todos los componentes de la solución. En otras palabras, ninguna persona tiene el nivel de acceso necesario para amenazar la seguridad o confidencialidad de los datos de un cliente.

Comparativa de seguridad en las instalaciones *vs* en la nube

La idea de que las infraestructuras locales son más seguras que las infraestructuras en la nube es un mito. El acceso físico no autorizado a los centros de datos en la nube es extremadamente raro. Las peores infracciones ocurren detrás de los *firewalls* de las empresas y de sus propios empleados. Los datos en una nube pueden residir en cualquier número de servidores en cualquier número de ubicaciones, en lugar de un servidor dedicado dentro de la red local.

Un servicio *cloud* posee una gran cantidad de recursos técnicas para monitorizar la situación de protección de la red 20/7/365, cuando se trabaja en local en general no se cuenta con este despliegue de recursos.

Riesgo de cumplimiento

Las implicaciones y los costes de las brechas de seguridad de datos son noticia de primera plana y abarcan todo, desde la pérdida de puestos de trabajo hasta la pérdida de ingresos e imagen. A medida que el volumen y la proliferación de datos continúan creciendo, los enfoques de seguridad tradicionales ya no ofrecen la seguridad de datos necesaria.

Bibliografía

[1] Power Data, "Seguridad de datos: en qué consiste y qué es importante en tu empresa, 2021 [En línea]. Disponible en: https://www.powerdata.es/seguridad-de-datos. [accedido 08-nov-2021]

[2] Programación.net, "Conceptos básicos de acceso a bases de datos", [En línea]. Disponible en: https://programacion.net/articulo/conceptos_basicos_de_acceso_a_bases_de_datos_45. [accedido 08-nov-2021]

[3] "Principios y recomendaciones básicas en ciberseguridad – informe buenas prácticas", CCN-CERT, España, 2021 [En línea]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html. [accedido 08-nov-2021]

[4] "Incibe-cert.es", 2021 [En línea] Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf. [accedido 08-nov-2021]