

Universidad Tecnológica de Xicotepec de Juárez

Ingeniería en Desarrollo y Gestión de Software

CMD

Integrantes:

Cristian Eduardo Ojeda Gayosso M-210180

Myriam Valderrabano Cortes M-210467

Daniela Aguilar Torres M-200051

Plan de Seguridad

Materia: Administración de Base de Datos

Profesor: M.T.I. Marco A. Ramírez Hernández

Cuatrimestre:8 Grupo: A

Periodo Enero-abril 2024



Seguridad de datos farmacia intrahospitalaria

Objetivo General:

Garantizar la integridad, confidencialidad y disponibilidad de los datos y recursos en el área de farmacia, protegiendo la información confidencial del paciente y asegurando el cumplimiento de regulaciones y estándares de seguridad.

Objetivos Específicos:

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI):

Desarrollar e implementar, procedimientos y controles de seguridad de la información específicos en el área de farmacia.

Establecer roles y responsabilidades claros para la gestión de la seguridad de la información en el área de farmacia.

Proteger la Confidencialidad de los Datos del Paciente:

Implementar mecanismos de acceso seguro para proteger los datos médicos confidenciales de los pacientes.

Garantizar que solo el personal autorizado tenga acceso a la información del paciente y que este acceso esté basado en roles y privilegios definidos.

Asegurar la Integridad de los Datos del Inventario:

Implementar controles de integridad de datos para garantizar que el inventario de medicamentos y las prescripciones médicas no sean modificadas.

Establecer un proceso de verificación de cambios en el inventario y en las prescripciones para detectar y prevenir alteraciones indebidas.

Usuarios y Privilegios

Los usuarios son las personas que interactúan con el sistema, y los privilegios determinan qué acciones pueden realizar dentro del sistema.

Se crean cuentas de usuario para cada empleado y se asignan privilegios específicos según su función en la farmacia.

Administrador del sistema: Acceso total a la base de datos y capacidad para asignar privilegios a otros usuarios.

Farmacéutico principal: Acceso completo a la base de datos de medicamentos y pacientes.

Asistentes de farmacia: Acceso limitado para dispensación de medicamentos y actualización de inventario.

Personal médico: Acceso limitado a la información de pacientes y prescripción de medicamentos.

```
-- Crear un nuevo usuario  
CREATE USER 'nombre_usuario'@'localhost' IDENTIFIED BY 'contraseña';
```

Roles de Usuario

Los roles de usuario definen las responsabilidades y el acceso a los datos dentro del sistema.

Los roles de usuario garantizan que cada empleado tenga acceso solo a la información necesaria para realizar sus tareas, lo que ayuda a prevenir el acceso no autorizado a datos sensibles.

Administrador del Sistema: Este rol tiene acceso total al sistema y tiene la capacidad de administrar usuarios, configuraciones y privilegios.

Privilegios: Acceso completo a todas las funcionalidades del sistema, incluyendo la base de datos de medicamentos, pacientes y empleados.

- Capacidad para crear, modificar y eliminar cuentas de usuario.
- Capacidad para asignar y revocar privilegios a otros usuarios.

Farmacéutico Principal: Este rol está destinado al farmacéutico principal encargado de la gestión de medicamentos y pacientes en la farmacia.

Privilegios: Acceso completo a la base de datos de medicamentos, incluyendo la capacidad de agregar, actualizar y eliminar registros de medicamentos.

- Acceso completo a la base de datos de pacientes, permitiendo la visualización de historiales médicos y la creación de nuevas entradas para pacientes.
- Capacidad para generar informes y estadísticas relacionadas con el inventario de medicamentos y las transacciones de dispensación.

Asistente de Farmacia: Este rol está destinado a los asistentes de farmacia que realizan tareas operativas en la farmacia, como la dispensación de medicamentos y la actualización del inventario.

Privilegios: Acceso limitado a la base de datos de medicamentos, permitiendo la búsqueda y visualización de información sobre medicamentos disponibles.

- Capacidad para realizar dispensación de medicamentos, registrando las ventas y actualizando el inventario.
- Acceso limitado a la base de datos de pacientes, permitiendo la búsqueda y visualización de información básica sobre pacientes.

```
-- Crear un nuevo rol
CREATE ROLE 'nombre_rol';

-- Asignar privilegios al rol
GRANT SELECT, INSERT, UPDATE, DELETE ON base_de_datos.tabla TO 'nombre_rol';

-- Asignar rol al usuario
GRANT 'nombre_rol' TO 'nombre_usuario'@'localhost';
```

Seguridad de Datos

La seguridad de datos se refiere a las medidas tomadas para proteger la confidencialidad, integridad y disponibilidad de la información.

Se implementan medidas de seguridad como autenticación de usuarios, control de acceso basado en roles, encriptación de datos.

- Autenticación de usuarios mediante contraseñas robustas y cifradas.
- Control de acceso basado en roles para garantizar que cada usuario tenga acceso solo a la información relevante para su función.
- Encriptación de datos sensibles, como la información médica del paciente y los detalles de la prescripción.

La seguridad de datos ayuda a proteger la información sensible de la farmacia contra accesos no autorizados, manipulación maliciosa y pérdida de datos.

Respaldo de Datos

El respaldo de datos implica hacer copias de seguridad de la información para protegerla contra la pérdida o el daño.

RespalDOS diarios: La información de pacientes y el inventario de medicamentos que cambian con frecuencia. Esto garantiza que se capturen todas las actualizaciones y cambios recientes en los datos.

Para realizar un respaldo de una base de datos MySQL utilizamos el comando ``mysqldump`` en la línea de comandos

1. Ejecutar el comando `mysqldump`: Una vez que estés dentro de la base de datos que deseas respaldar, ejecuta el comando ``mysqldump`` para generar el respaldo. Utiliza el siguiente comando:

```
mysqldump -u root -p mi_base_de_datos > respaldo_mi_base_de_datos.sql
```

5. Proporcionar la contraseña: Después de ejecutar el comando, se te solicitará que ingreses la contraseña de tu usuario MySQL. Ingresa la contraseña y presiona Enter.

6. Verificar el archivo de respaldo: Una vez que el comando haya terminado de ejecutarse, verifica que se haya creado el archivo de respaldo en el directorio especificado.

También podemos realizar los respaldos automáticamente:

Crear un evento para el respaldo automático:

```
CREATE EVENT backup_event
ON SCHEDULE EVERY 1 DAY
STARTS CURRENT_TIMESTAMP
DO
BEGIN
    -- Nombre del archivo de respaldo (incluye la fecha actual)
    SET @backup_file = CONCAT('/ruta/del/directorio/de/respaldo/backup_', DATE_FORMAT(NOW(), '%Y%m%d'), '.sql');

    -- Comando para realizar el respaldo utilizando mysqldump
    SET @backup_query = CONCAT('mysqldump -u usuario -pcontraseña nombre_base_de_datos > ', @backup_file);

    -- Ejecutar el comando de respaldo
    PREPARE stmt FROM @backup_query;
    EXECUTE stmt;
    DEALLOCATE PREPARE stmt;
END;
```