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

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
```

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.

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;
```

Plan de Seguridad NoSQL

Objetivo General:
Garantizar la seguridad, integridad y disponibilidad de los datos de devoluciones de productos en la base de datos de MongoDB para la farmacia.

Objetivos Específicos:

- Proteger los datos de devoluciones contra accesos no autorizados, asegurando que solo los usuarios autorizados puedan acceder y modificar esta información.
- Mantener la integridad de los datos de devoluciones, evitando modificaciones no autorizadas y garantizando la precisión de la información registrada.
- Garantizar la disponibilidad de los datos de devoluciones en todo momento para los usuarios autorizados, minimizando el riesgo de pérdida de datos.
- Cumplir con las regulaciones de privacidad y protección de datos aplicables, asegurando el manejo adecuado y seguro de la información sensible de los clientes y productos.

Roles y Usuarios:

Administrador del Sistema: Responsable de la configuración y gestión de la base de datos MongoDB.
Usuarios: Administrador del sistema
Privilegios: Acceso completo a todas las operaciones en la base de datos.

Farmacéutico Principal: Responsable de gestionar las devoluciones de productos.
Usuarios: Farmacéutico principal
Privilegios: Lectura y escritura en la colección de devoluciones.

Asistente de Farmacia: Asistente encargado de registrar devoluciones y gestionar inventario.
Usuarios: Asistente de farmacia
Privilegios: Lectura y escritura limitada en la colección de devoluciones.
Privilegios:
Lectura: Permite a los usuarios ver los datos de devoluciones.
Escritura: Permite a los usuarios agregar, actualizar o eliminar registros de devoluciones.

Calendarización de Respaldo:

- Realizar copias de seguridad diarias de la base de datos completa de MongoDB, incluida la colección de devoluciones.
- Almacenar las copias de seguridad en un almacenamiento seguro y fuera del sitio para proteger contra desastres físicos.
- Probar regularmente la restauración de los respaldos para garantizar su integridad y disponibilidad en caso de necesidad.

Creación de Usuarios y Roles:
Iniciar Sesión en MongoDB: Utiliza el cliente de MongoDB (como mongo shell) y conéctate a tu instancia de MongoDB.
Crear una Base de Datos y una Colección para la Gestión de Usuarios y Roles: Puedes utilizar una base de datos específica (por ejemplo, "admin") para almacenar esta información.
Crear Usuarios:

```
use admin
db.createUser({
    user: "nombre_usuario",
    pwd: "contraseña",
    roles: ["rol"]
})
```

Reemplaza "**nombre_usuario**" y "**contraseña**" con los valores deseados. Además, especifica el rol apropiado para el usuario.
Crear Roles Personalizados (Opcional): Si necesitas roles personalizados, puedes definirlos utilizando el comando **db.createRole().**

Asignación de Privilegios:
Roles Predeterminados: MongoDB proporciona roles predefinidos como **read, readWrite, dbOwner,** etc. Puedes asignar estos roles a los usuarios utilizando el comando **db.grantRolesToUser().**

Roles Personalizados: Si has creado roles personalizados, puedes asignarlos a los usuarios utilizando el mismo comando **db.grantRolesToUser().**

Creación de Respaldos:
Utilizando **mongodump:** MongoDB proporciona la herramienta mongodump para realizar copias de seguridad de una base de datos o una colección.

```
mongodump --db nombre_base_datos --out ruta_destino
```

Reemplaza **"nombre_base_datos"** con el nombre de tu base de datos y **"ruta_destino**" con la ubicación donde deseas almacenar el respaldo.

Respaldo
Ejecutar **mongodump:** Una vez en el directorio adecuado, ejecuta el comando mongodump. Por ejemplo:

```
mongodump --db nombre_de_la_base_de_datos --out ruta_del_destino
```

Reemplaza **"nombre_de_la_base_de_datos"** con el nombre de la base de datos que deseas respaldar.
Reemplaza **"ruta_del_destino"** con la ubicación donde deseas almacenar el respaldo. Si no especificas una ruta, el respaldo se guardará en un directorio llamado dump en el directorio actual.
Verificar el Respaldo: Una vez que **mongodump** haya terminado de ejecutarse, puedes verificar el respaldo