



**INSTITUTO TECNOLÓGICO[®]
de Pabellón de Arteaga**

TEC

DOCUMENTO

Actividad

Nombre del Alumno

Sara del Carmen Sanches de la Rosa

Materia

Seguridad de Base de Datos

Docente

Oscar Lenin Espinoza Alvares

Fecha

29/01/2024

Instrucciones: Investigar un ejemplo de un sistema de información.

-Definición

-Datos sensibles.

-Políticas de seguridad

Ejemplo de un Sistema de Información: Sistema de Gestión de Salud Electrónica

Definición:

Un Sistema de Gestión de Salud Electrónica (EHR) es un sistema de información digitalizado que almacena, gestiona y proporciona acceso a la información médica de los pacientes. Este sistema integra datos de diversos proveedores de atención médica y facilita la colaboración entre profesionales de la salud. El EHR incluye información médica clave, como historias clínicas, resultados de pruebas, recetas médicas, informes de procedimientos, entre otros.

Datos Sensibles:

Los datos almacenados en un EHR son extremadamente sensibles, ya que contienen información médica detallada sobre los pacientes. Algunos de los datos sensibles incluyen:

Información de Identificación Personal (PII): Nombre completo, fecha de nacimiento, dirección, número de seguro social, etc.

Historia Clínica: Diagnósticos médicos, tratamientos anteriores, historial de enfermedades, alergias, etc.

Resultados de Pruebas: Información detallada de pruebas de laboratorio, radiografías, imágenes médicas, etc.

Prescripciones y Medicamentos: Detalles de medicamentos recetados, dosis, frecuencia, etc.

Información Financiera: Datos relacionados con facturación médica, seguros de salud, etc.

Políticas de Seguridad:

Debido a la naturaleza sensible de la información manejada por un EHR, se implementan políticas de seguridad rigurosas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Algunas de las políticas de seguridad típicas incluyen:

Acceso Controlado: Se implementan sistemas de autenticación y autorización para garantizar que solo el personal autorizado tenga acceso a información específica. Esto incluye roles y permisos definidos.



Cifrado de Datos: La información almacenada y transmitida en el EHR se cifra para protegerla contra accesos no autorizados. Esto se aplica tanto a nivel de almacenamiento como a las comunicaciones.

Auditoría y Monitorización: Se establecen sistemas de registro y seguimiento para supervisar las actividades relacionadas con los datos. Esto ayuda a identificar posibles brechas de seguridad o uso indebido.

Respaldo y Recuperación: Se implementan procedimientos robustos de respaldo y recuperación para garantizar la disponibilidad de datos en caso de desastres, errores o ataques cibernéticos.

Entrenamiento del Personal: El personal que maneja el EHR recibe capacitación regular sobre las mejores prácticas de seguridad y la importancia de proteger la información confidencial del paciente.

Actualizaciones y Parches: Se mantienen actualizados los sistemas y se aplican parches de seguridad para mitigar vulnerabilidades conocidas y reducir el riesgo de intrusiones.

