Actividad: Evaluación de Seguridad en Sistemas para inicio de sesión (login).

Objetivo:

Los estudiantes evaluarán la seguridad de su sistema de login utilizando una matriz de riesgos basada en la norma ISO/IEC 27001. Además, investigarán en qué consiste esta norma y profundizarán en la definición de los riesgos identificados.

Instrucciones:

- Cada equipo debe tener listo su sistema de login desarrollado como parte de su desarrollo web.
- La matriz de riesgos (como la que diseñamos anteriormente), es la siguiente:

Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Medidas de Mitigación
Fuga de Información				
Comunicación No Cifrada				
Inyección SQL				
Ataques de Fuerza Bruta				
XSS (Cross-Site Scripting)				

CSRF (Cross-Site Request Forgery)				
Almacenamiento Inseguro de Contraseñas				

¿Qué es la norma ISO/IEC 27001 y cuál es su objetivo?

¿Qué es un Sistema de Gestión de Seguridad de la Información (SGSI)?

¿Cómo se aplica la norma en el desarrollo de software?

Recursos sugeridos:

- Sitio oficial de ISO
- Artículos y guías sobre ISO/IEC 27001.

Recursos sugeridos:

- OWASP (Open Web Application Security Project): owasp.org
- Artículos técnicos sobre vulnerabilidades comunes (ya investigaron algo al respecto).

Evaluación del Sistema de Login (pueden modificarla o mejorarla)

Paso 1: Identificación de Riesgos

- Revisar su sistema de login y comparar su implementación con las medidas de seguridad sugeridas en la matriz de riesgos.
- Ejemplo:

  ¿Usan consultas parametrizadas para prevenir inyección SQL?

  ¿Han implementado autenticación de dos factores (2FA)?

  ¿Cómo almacenan las contraseñas (hashing, salting)?

Paso 2: Aplicación de la Matriz de Riesgos

Completar la matriz de riesgos para su sistema de login, evaluando:

- **Impacto:** ¿Qué tan grave sería el riesgo si se materializa?
- **Probabilidad:** ¿Qué tan probable es que ocurra?
- **Nivel de Riesgo:** Combinación de Impacto y Probabilidad.
- **Medidas de Mitigación:** ¿Qué acciones pueden tomar para reducir el riesgo?

Paso 3: Documentación

El documento a entregar debe de contener sus hallazgos en un informe que incluya:

1. Descripción de su sistema de login.
2. Matriz de riesgos completada.
3. Explicación de los riesgos identificados y su investigación.
4. Recomendaciones para mejorar la seguridad.