***Universidad tecnológica de santa Catarina***

***Nombre  
Carlos alexis rodriguez garcia***

***Matricula  
22051***

***Fecha  
06/10/2025***

**Lista de Controles y Medidas de Seguridad para el Sistema**

**1. Cifrado de Contraseñas:**

Para qué sirve: Protege las contraseñas de los usuarios para que, incluso si alguien accede a la base de datos, no pueda leerlas.

Cómo funciona: Las contraseñas se transforman mediante un algoritmo (como bcrypt o Argon2) en una cadena de caracteres irreconocible (hash) antes de guardarse. Cuando un usuario inicia sesión, la contraseña que ingresa se cifra de nuevo y se compara con el hash almacenado.

**2. Validación de Entrada:**

Para qué sirve: Previene ataques como inyección SQL o Cross-Site Scripting (XSS), asegurando que los datos ingresados por los usuarios no sean maliciosos.

Cómo funciona: El sistema revisa y limpia toda la información que recibe, rechazando o sanitizando cualquier dato que no cumpla con los formatos esperados (por ejemplo, bloquear caracteres especiales peligrosos en un formulario).

**3. Control de Acceso Basado en Roles (RBAC):**

Para qué sirve: Garantiza que cada usuario solo pueda acceder a las funciones y datos acordes a su perfil (ej: administrador, empleado, invitado).

Cómo funciona: Se asignan roles a los usuarios y cada rol tiene permisos específicos. El sistema verifica estos permisos antes de permitir cualquier acción.

**4. Copias de Seguridad (Backups):**

Para qué sirve: Minimiza la pérdida de información en caso de fallos del sistema, ataques o desastres.

Cómo funciona: Se realizan respaldos automáticos y periódicos de la base de datos y archivos críticos, almacenándolos en una ubicación segura y separada del servidor principal.

**5. Conexión Segura (HTTPS/SSL):**

Para qué sirve: Protege la integridad y confidencialidad de los datos que se transmiten entre el usuario y el servidor.

Cómo funciona: Utiliza un certificado SSL/TLS para cifrar la comunicación, evitando que terceros intercepten o modifiquen la información durante la transmisión.

**6. Autenticación de Dos Factores (2FA):**

Para qué sirve: Añade una capa extra de seguridad al proceso de inicio de sesión, más allá de la contraseña.

Cómo funciona: Tras ingresar su contraseña, el usuario debe proporcionar un segundo factor de verificación, como un código temporal enviado a su teléfono o generado por una app.

**7. Registro y Monitoreo de Actividad (Logging):**

Para qué sirve: Permite detectar y investigar actividades sospechosas o incidentes de seguridad.

Cómo funciona: El sistema registra (logs) eventos importantes como inicios de sesión, accesos a datos sensibles y cambios críticos. Estos logs se monitorizan en busca de anomalías.

**8. Actualizaciones y Parches de Seguridad:**

Para qué sirve: Corrige vulnerabilidades conocidas en el software del sistema.

Cómo funciona: Se mantiene actualizado el sistema operativo, frameworks, librerías y aplicaciones, aplicando los parches de seguridad más recientes proporcionados por los desarrolladores.

**9. Políticas de Contraseñas Robustas:**

Para qué sirve: Dificulta que las contraseñas sean adivinadas o crackeadas.

Cómo funciona: El sistema obliga a los usuarios a crear contraseñas que cumplan ciertos criterios (longitud mínima, uso de mayúsculas, minúsculas, números y símbolos).

**10. Firewall de Aplicación Web (WAF):**  
- Para qué sirve: Filtra y bloquea el tráfico malicioso dirigido a la aplicación.  
- Cómo funciona: Se sitúa entre la aplicación web e Internet, analizando las peticiones HTTP para identificar y bloquear patrones de ataque comunes.

**11. Manejo Seguro de Sesiones:**  
- Para qué sirve: Previene que un atacante secuestre la sesión de un usuario legítimo.  
- Cómo funciona: Las sesiones se gestionan con identificadores únicos y aleatorios, se invalidan después del cierre de sesión y tienen un tiempo de expiración.

**12. Principio de Mínimo Privilegio:**  
- Para qué sirve: Limita el daño potencial que puede causar un usuario o proceso si es comprometido.  
- Cómo funciona: Se conceden a los usuarios y sistemas solo los permisos estrictamente necesarios para realizar sus tareas.