PROYECTO INTEGRADOR

Plan de Políticas de Seguridad Informátican y

de Base de Datos

Jhoan Alvarez, Lenin Carcelen y Luis Valarezo

04/02/2026

Pontificia Universidad Católica del Ecuador

Contenido

Plan de Políticas de Seguridad Informática y de Base de Datos

1. Contexto General

- **Sistema Operativo:** Windows 10/11 (desarrollo y despliegue)

- **Infraestructura:** On-premise (servidor local)

- **Motor de Base de Datos:** MongoDB (NoSQL) y/o SQL Server.

2. Directrices Generales de Seguridad

2.1. Controles de Acceso

- Implementar autenticación robusta (JWT) para usuarios y administradores.

- Definir roles y permisos mínimos necesarios (principio de menor privilegio).

- Restringir el acceso a la base de datos solo a servicios y usuarios autorizados.

- Utilizar listas blancas de IP para acceso administrativo.

2.2. Encriptación

- Encriptar las contraseñas de usuarios en la base de datos usando algoritmos seguros (bcrypt, Argon2).

- Usar HTTPS para todas las comunicaciones entre frontend, backend y base de datos.

- Encriptar datos sensibles en tránsito y en reposo (TLS/SSL para conexiones a la base de datos).

2.3. Respaldos (Backups)

- Realizar respaldos automáticos diarios de la base de datos.
- Almacenar los respaldos en ubicaciones seguras y, de ser posible, fuera del servidor principal.
- Probar periódicamente la restauración de respaldos para asegurar su integridad.

2.4. Monitoreo y Auditoría

- Implementar registros (logs) de acceso y operaciones críticas en la aplicación y la base de datos.
- Monitorear intentos de acceso no autorizados y alertar sobre actividades sospechosas.
- Revisar periódicamente los logs y establecer alertas automáticas.

2.5. Gestión de Vulnerabilidades

- Mantener actualizado el sistema operativo, el motor de base de datos y las dependencias del proyecto.
- Aplicar parches de seguridad tan pronto como estén disponibles.
- Realizar análisis de vulnerabilidades periódicos (herramientas como OWASP ZAP, dependabot, etc.).
- Limitar la exposición de puertos y servicios solo a los estrictamente necesarios.

2.6. Buenas Prácticas Adicionales

- Deshabilitar cuentas y servicios innecesarios en el sistema operativo y la base de datos.
- Configurar firewalls y reglas de red para restringir el tráfico.
- Utilizar variables de entorno para credenciales y configuraciones sensibles.
- Capacitar a los usuarios y administradores sobre buenas prácticas de seguridad.

3. Esquema de Roles y Permisos

- **Administrador:** Acceso total a la gestión de usuarios, alertas y configuraciones.

- **Usuario estándar:** Acceso solo a funcionalidades propias de su rol.

- **Limpieza:** Acceso restringido a módulos de limpieza y alertas relacionadas.

4. Procedimientos de Respuesta ante Incidentes

- Definir un protocolo de respuesta ante incidentes de seguridad (bloqueo de cuentas, restauración de respaldos, notificación a responsables).

- Documentar y reportar todos los incidentes para análisis posterior.

5. Referencias y Normativas

- OWASP Top 10

- NIST SP 800-53

- ISO/IEC 27001