UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO

MATERIA: AUDITORÍA DE SISTEMAS

ALUMNO:

ROBERTO DANIEL SAAVEDRA CABALLERO

PERIODO: 2025B

Políticas de Seguridad y Control

En el desarrollo del sistema de control escolar, se han implementado diversas políticas y medidas para garantizar la seguridad y protección de la información de los usuarios y los datos académicos almacenados. Estas políticas buscan minimizar riesgos, prevenir accesos no autorizados y asegurar la integridad y disponibilidad de la información. A continuación, se detallan los aspectos principales:

**Control de Accesos**

El sistema cuenta con un control de accesos riguroso, basado en perfiles de usuario. Únicamente los administradores tienen acceso completo al sistema, incluyendo la gestión de alumnos, materias, inscripciones y calificaciones. Los permisos se dividen de la siguiente manera:

* **Administradores:** Pueden crear, editar y eliminar registros de alumnos y materias, asignar inscripciones, registrar calificaciones y gestionar otros administradores.
* **Alumnos (si se implementa módulo de usuario alumno):** Solo pueden consultar sus datos personales y calificaciones, sin posibilidad de modificar información crítica del sistema.

Cada usuario debe autenticarse con un nombre de usuario y contraseña únicos. Además, se aplican medidas para evitar el acceso simultáneo desde múltiples dispositivos con la misma cuenta, reduciendo el riesgo de uso indebido de credenciales.

**Protección de Datos**

Para proteger la información sensible del sistema, se implementan las siguientes medidas:

* **Cifrado de contraseñas:** Todas las contraseñas de usuarios se almacenan utilizando algoritmos de hashing seguros (por ejemplo, password\_hash en PHP), evitando que las contraseñas se guarden en texto plano en la base de datos.
* **Validación de formularios:** Todos los datos ingresados por los usuarios son validados y sanitizados para prevenir ataques de inyección SQL y otras vulnerabilidades de seguridad web.
* **Conexiones seguras:** Se recomienda implementar conexiones HTTPS en el servidor para proteger la transmisión de datos entre el cliente y el servidor, evitando la interceptación de información sensible.
* **Roles y permisos:** Cada acción dentro del sistema está restringida según el rol del usuario, garantizando que no se pueda acceder a funcionalidades no autorizadas.

**Respaldos de Información**

Para asegurar la disponibilidad y recuperación de la información en caso de fallos, se implementa un plan de respaldos periódicos de la base de datos:

* **Frecuencia:** Se programan respaldos completos de la base de datos al menos una vez por semana, y respaldos incrementales diarios si se realizan cambios frecuentes.
* **Almacenamiento seguro:** Los archivos de respaldo se almacenan en un lugar seguro y fuera del servidor principal, ya sea en un almacenamiento en la nube o en dispositivos de almacenamiento externos.
* **Restauración de datos:** El procedimiento de restauración se prueba periódicamente para garantizar que los respaldos puedan recuperarse correctamente en caso de pérdida de información.

Estas políticas combinadas aseguran que los datos del sistema se mantengan seguros, protegidos de accesos no autorizados y recuperables en situaciones de emergencia, garantizando la confiabilidad y continuidad del sistema de control escolar.