**Plan de Seguridad Informática para la Aplicación EduShare.js**

**1. Introducción**

El presente documento establece el Plan de Seguridad Informática para EduShare.js, una plataforma de cursos educativos. El objetivo es garantizar la protección de los sistemas, la integridad de los datos, y la privacidad de los usuarios mediante controles y medidas alineadas a estándares de seguridad informática.

**2. Objetivos del Plan de Seguridad Informática**

Proteger la confidencialidad, integridad y disponibilidad de la información.

Prevenir accesos no autorizados y ataques informáticos.

Establecer protocolos de detección y respuesta a incidentes de seguridad.

Asegurar el cumplimiento de normativas legales y estándares de seguridad.

|  |  |  |
| --- | --- | --- |
| Riesgo | Impacto | Mitigación |
| Acceso no autorizado a cuentas | Robo de datos personales. | Implementación de autenticación multifactor (MFA). |
| Ataques DDoS | Caída del servicio, impidiendo el acceso a los usuarios. | Implementar sistemas de mitigación de DDoS en la nube. |
| Inyección SQL | Robo y modificación de datos en la base de datos. | Validación de entradas y consultas parametrizadas. |
| Vulnerabilidad en APIs | Exposición de datos sensibles. | Auditorías periódicas y pruebas de seguridad. |
| Robo de credenciales | Acceso no autorizado a la plataforma. | Uso de hash y sal en las contraseñas (bcrypt). |
| Malware y ransomware | Bloqueo de sistemas y secuestro de datos. | Monitoreo constante y antivirus en servidores. |
| Fuga de datos en dispositivos móviles | Exposición de información crítica. | Cifrado de datos en tránsito y en reposo. |

4. Políticas de Seguridad

4.1 Autenticación y Control de Acceso

Implementar MFA para todos los usuarios y administradores.

Control de roles y permisos para restringir el acceso según la función.

Política de cierre de sesión automático tras un período de inactividad.

4.2 Gestión de Datos y Privacidad

Uso de cifrado AES-256 para el almacenamiento de información.

Cifrado SSL/TLS en la comunicación entre cliente y servidor.

Anonimización de datos sensibles para pruebas y desarrollo.

4.3 Respaldo y Recuperación de Datos

Respaldo diario de bases de datos en servidores externos.

Pruebas periódicas de restauración de datos para verificar la integridad de los respaldos.

4.4 Gestión de Actualizaciones

Aplicación de parches de seguridad de manera inmediata.

Actualización continua de librerías y dependencias utilizadas en EduShare.js.

4.5 Seguridad en APIs

Implementación de OAuth 2.0 para autenticación en APIs.

Auditoría continua de APIs y uso de herramientas para pruebas de penetración.

5. Plan de Monitoreo y Detección de Amenazas

Implementación de un SIEM (Sistema de Gestión de Eventos de Seguridad) para monitorear

correlacionar eventos sospechosos.

Análisis de logs en tiempo real para detectar accesos no autorizados.

Uso de sistemas de detección y prevención de intrusiones (IDS/IPS).

**6. Plan de Respuesta a Incidentes**

|  |  |
| --- | --- |
| Fase | Acción |
| Detección | Identificación de anomalías mediante alertas automatizadas. |
| Contención | Bloqueo de cuentas afectadas y aislamiento de los sistemas comprometidos. |
| Erradicación | Eliminación de la vulnerabilidad y restauración de datos desde respaldos. |
| Recuperación | Verificación del sistema y reactivación del servicio. |
| Análisis | Informe detallado del incidente y medidas preventivas futuras. |

**8. Cumplimiento Normativo y Estándares**

ISO/IEC 27001: Estándar de gestión de la seguridad de la información.

GDPR: Regulación de protección de datos personales para usuarios europeos.

Ley de Protección de Datos Personales: Cumplir con normativas locales aplicables.

**9. Indicadores de Seguridad (KPIs)**

|  |  |  |
| --- | --- | --- |
| **Indicador** | **Objetivo** | **Frecuencia de Medición** |
| Incidentes detectados | Máximo 1 por trimestre | Trimestral |
| Tiempo de respuesta a incidentes | Menos de 1 hora | Mensual |
| Tasa de intentos de acceso fallido | 0% en cuentas críticas | Mensual |
| Aplicación de parches de seguridad | Menos de 24 horas tras la notificación | Continuo |

**10. Roles y Responsabilidades**

|  |  |
| --- | --- |
| **Rol** | **Responsabilidad** |
| Responsable de Seguridad Informática | Supervisar y ejecutar el plan de seguridad. |
| Equipo de Desarrollo | Implementar medidas de seguridad en el ciclo de desarrollo. |
| Equipo de Operaciones | Monitorear sistemas y gestionar actualizaciones. |
| Usuarios | Cumplir con las políticas de seguridad y reportar actividades sospechosas. |

11. Conclusión

El Plan de Seguridad Informática de EduShare.js garantiza la protección integral de la plataforma, resguardando la información de los usuarios y asegurando la continuidad del servicio. La combinación de controles preventivos, monitoreo constante y una respuesta efectiva a incidentes permitirá mantener la seguridad de la aplicación y fomentar la confianza de sus usuarios. Este plan será revisado periódicamente para ajustarse a nuevas amenazas y regulaciones, alineando las operaciones con los más altos estándares de seguridad informática.