**Seguridad y Protección de Datos**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tipo** | **Riesgo** | **Probabilidad** | | | | | **Impacto** | | | | | **Medidas de Mitigación** |
| 1 | Fugas de datos personales de usuarios | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Cifrado en tránsito y en reposo, control de acceso |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 2 | Ataques por inyección SQL | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Uso de ORM y validación de entradas |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 3 | Almacenamiento inseguro de contraseñas | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Hash con bcrypt o Argon2 + salting |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 4 | APIs expuestas sin autenticación | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | |  | | --- | | Autenticación con tokens y verificación JWT |  |  | | --- | |  | |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 5 | Sesiones vulnerables a secuestro (session hijacking) | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | |  | | --- | |  |  |  | | --- | | Cookies HttpOnly, expiración de sesiones, token rotation | |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 6 | No cumplir con regulaciones (ej. LFPDPPP, GDPR) | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Auditorías legales y política de privacidad |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 7 | Mal manejo de datos sensibles en logs | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Configuración de logs para excluir información privada |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 8 | Fallos de seguridad en almacenamiento en la nube | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Configuración segura en S3/GCS con políticas adecuadas |
| Cuantitativo |  |  |  |  |  |  |  |  |  |  |
| 9 | Ataques DDoS | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | CDN, firewall de aplicaciones (WAF) y límites de tasa (rate limiting) |
| Cuantitativo |  |  |  |  |  |  |  |  |  |  |
| 10 | Vulnerabilidades por librerías desactualizadas | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Actualizaciones regulares y escaneo de dependencias |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 11 | Aplicación sin mecanismos de respaldo | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Backup automático cifrado y recuperación probada |
| Cuantitativo |  |  |  |  |  |  |  |  |  |  |
| 12 | Accesos no autorizados al backend | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Segmentación de red y firewalls |
| Cuantitativo |  |  |  |  |  |  |  |  |  |  |
| 13 | Exposición de claves en repositorios públicos | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Uso de git-secrets y revisión automatizada |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 14 | No revocar accesos de personal que deja el proyecto | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Gestión centralizada de accesos (IAM) |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 15 | Fallos en la gestión de permisos por roles | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Control RBAC y pruebas de autorización |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 16 | No validar archivos subidos por el usuario | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Escaneo de archivos, restricción de tipos y tamaño |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 17 | No proteger endpoints administrativos | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | |  | | --- | |  |  |  | | --- | | Autenticación fuerte y restricciones IP | |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 18 | Faltas en el cifrado de tokens o cookies | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Uso de AES-256, HMAC y protocolos seguros (TLS 1.2+) |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 19 | No monitorear incidentes de seguridad | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Sistema de detección de intrusos (IDS) y alertas |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 20 | No auditar accesos y modificaciones de datos | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Logging de auditoría con revisiones periódicas |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 21 | Fallas en la política de privacidad o aviso legal | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Revisión legal y actualizaciones periódicas |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 22 | Inyección de scripts maliciosos (XSS) | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Escapado adecuado y CSP (Content Security Policy) |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 23 | Fallas en la verificación de identidad del usuario | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Verificación en dos pasos (2FA) |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |
| 24 | API sin límites de acceso por IP o usuario | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Rate limiting y uso de API Gateway |
| Cuantitativo |  |  |  |  |  |  |  |  |  |  |
| 25 | Pruebas de seguridad no automatizadas | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | Integración de herramientas como OWASP ZAP o Snyk |
| Cualitativo |  |  |  |  |  |  |  |  |  |  |