**Almacenamiento inseguro de contraseñas**

* **Tipo de riesgo:** Técnico / Seguridad / Legal
* **Categoría:** Gestión de credenciales / Desarrollo seguro / Protección de datos

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Almacenamiento inseguro de contraseñas |
| Categoría | Seguridad / Infraestructura / Desarrollo |
| Causas probables | Uso de almacenamiento en texto plano, cifrado reversible, falta de hashing, ausencia de salting, errores en configuración de base de datos. |
| Consecuencias | Robo de cuentas, escalamiento de privilegios, acceso no autorizado, daño reputacional, incumplimiento legal. |
| Fuente | Auditoría de seguridad, análisis de bases de datos, revisión de código, reportes de usuarios o análisis forense. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (común por malas prácticas en fases tempranas) |
| Impacto potencial | Alto (puede comprometer la seguridad de múltiples cuentas) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Contraseñas visibles o recuperables, ausencia de hash, logs con credenciales, falta de controles de acceso a base de datos. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

**A. Medidas Preventivas (Antes del riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar almacenamiento de contraseñas con hashing seguro (bcrypt/Argon2) | Backend / Dev | bcrypt, Argon2, PBKDF2 |
| Agregar salting único por usuario | Backend | Librerías de seguridad, random salts |
| Aplicar validación de contraseñas fuertes | Frontend / Backend | OWASP Password Policy, zxcvbn |
| Asegurar bases de datos con controles de acceso estrictos | DevOps / DBA | IAM, roles, encriptación de volúmenes |
| Establecer políticas de cambio periódico de contraseñas | Seguridad / Legal | Políticas internas, avisos automatizados |

**B. Medidas de Mitigación (Durante el riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Invalidar contraseñas comprometidas y forzar reinicio de sesión | Backend / Soporte | Notificaciones, reinicio obligatorio |
| Notificar a los usuarios afectados | Comunicación | Correo, SMS, protocolo de alerta |
| Aislar y reforzar la seguridad de la base de datos afectada | DBA / DevOps | Copia de respaldo, cifrado, firewall |

**C. Medidas Correctivas (Después del riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Migrar todas las contraseñas a hash seguro con salting | Backend / QA | Scripts de migración, bcrypt, Argon2 |
| Realizar auditoría completa de accesos y configuraciones | Seguridad TI | SIEM, revisión manual, checklists |
| Documentar incidente y reforzar normativas internas | QA / PMO | Políticas de seguridad, RCA, postmortem |

**4. ESTIMACIÓN DE PÉRDIDAS ECONÓMICAS POR RIESGO NO CONTROLADO**

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Robo de contraseñas y accesos no autorizados | Vulneración de cuentas, daño a usuarios | $40,000 MXN |
| Daño reputacional por exposición en medios / usuarios | Pérdida de confianza, fuga de usuarios | $20,000 MXN |
| Migración forzada de credenciales | Tiempo de desarrollo y validación | $12,000 MXN |
| Soporte técnico para restablecimientos masivos | Carga operativa adicional | $8,000 MXN |
| Posibles sanciones legales por falta de protección | Multas por LFPDPPP u otras normativas | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$95,000 MXN** |

**5. COSTO DE IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTROL**

**A. Costos de Medidas Preventivas (Antes del riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de hashing con bcrypt/Argon2 | $3,000 MXN |
| Aplicación de políticas de contraseñas seguras | $1,500 MXN |
| Aseguramiento de la base de datos | $2,500 MXN |
| Capacitación del equipo en gestión segura de contraseñas | $2,000 MXN |
| Total medidas preventivas: | → $9,000 MXN |

**B. Costos de Medidas de Mitigación (Durante el riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Notificación y restablecimiento de contraseñas | $2,500 MXN |
| Refuerzo de seguridad en bases de datos | $2,000 MXN |
| Aislamiento de sistemas y protocolos de respuesta | $1,500 MXN |
| Total medidas de mitigación: | → $6,000 MXN |

**C. Costos de Medidas Correctivas (Después del riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Migración de contraseñas a sistema seguro | $5,000 MXN |
| Auditoría de accesos y logs | $3,000 MXN |
| Documentación y actualización de políticas | $2,000 MXN |
| Total medidas correctivas: | → $10,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $9,000 MXN |
| 🚨 Mitigación | $6,000 MXN |
| 🔄 Recuperación | $10,000 MXN |
| 💥 Costo de no hacer nada | $95,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $9,000 + $6,000 + $10,000 = **$25,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $95,000 – $25,000 = **$70,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **280% de ROI**