**Mal manejo de datos sensibles en logs**

* **Tipo de riesgo:** Técnico / Seguridad / Cumplimiento
* **Categoría:** Registro de actividad / Gestión de información / Protección de datos

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Mal manejo de datos sensibles en logs |
| Categoría | Seguridad / Desarrollo / Legal |
| Causas probables | Falta de configuración adecuada de logs, impresión directa de respuestas del servidor, ausencia de filtros, desconocimiento de los datos sensibles. |
| Consecuencias | Exposición de contraseñas, tokens, correos o datos personales en archivos accesibles, incumplimiento normativo, acceso no autorizado a información crítica. |
| Fuente | Análisis de logs, revisiones de código, herramientas de escaneo de seguridad, auditorías legales. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (común en entornos sin revisión estricta de logs) |
| Impacto potencial | Alto (puede comprometer datos personales y contraseñas) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Logs que contienen tokens, contraseñas, JSON completos con información sensible, mensajes sin sanitización. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Configurar herramientas de logging para excluir campos sensibles | Dev / QA | Winston, Log4j, Pino, Morgan |
| Usar filtros y máscaras de datos al registrar objetos | Backend / Seguridad | Regex, filtros personalizados |
| Clasificar qué datos se consideran sensibles en el sistema | Legal / Seguridad | Política de datos, lineamientos DLP |
| Revisar manualmente los logs críticos antes de liberar versiones | QA / Arquitecto | Pull requests, checklist de revisión |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Eliminar o anonimizar los logs expuestos | DevOps / Seguridad | Scripts, herramientas de búsqueda |
| Reemplazar logs sensibles por versiones sanitizadas | Backend / QA | Sanitizadores, filtros por entorno |
| Limitar el acceso a archivos de log | DevOps / Seguridad | Permisos, cifrado, IAM roles |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría completa del sistema de logging | QA / Seguridad | Splunk, ELK, Graylog |
| Regenerar claves, tokens o credenciales expuestos en los logs | Seguridad / DevOps | Vault, rotación de tokens |
| Establecer política de revisión y control de logs por cada release | PMO / QA | Políticas internas, checklist CI/CD |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Filtración de contraseñas o tokens por logs | Acceso no autorizado a cuentas | $20,000 MXN |
| Incumplimiento normativo por datos personales | Multas o auditorías regulatorias | $30,000 MXN |
| Tiempo de remediación y rotación de credenciales | Trabajo técnico urgente | $10,000 MXN |
| Impacto reputacional y pérdida de usuarios | Desconfianza por exposición indirecta | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$75,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Configuración segura de herramientas de logging | $3,000 MXN |
| Desarrollo de filtros de datos sensibles | $2,000 MXN |
| Definición de política de privacidad de logs | $2,000 MXN |
| Revisión QA previa al despliegue con foco en logging | $2,000 MXN |
| Total medidas preventivas: | → $9,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Búsqueda y eliminación de logs expuestos | $2,500 MXN |
| Sanitización en caliente de archivos de log | $1,500 MXN |
| Restricción de acceso y control de permisos | $1,000 MXN |
| Total medidas de mitigación: | → $5,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría completa del sistema de logging | $3,000 MXN |
| Rotación de claves y credenciales expuestas | $3,000 MXN |
| Establecimiento de políticas estrictas de control de logs | $2,500 MXN |
| Total medidas correctivas: | → $8,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $9,000 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $8,500 MXN |
| 💥 Costo de no hacer nada | $75,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $9,000 + $5,000 + $8,500 = **$22,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $75,000 – $22,500 = **$52,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **233% de ROI**