**No monitorear incidentes de seguridad**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Gestión de seguridad / Detección de incidentes / Respuesta a incidentes

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | No monitorear incidentes de seguridad |
| Categoría | Seguridad / Operación / Monitoreo |
| Causas probables | Falta de sistemas de monitoreo, ausencia de personal capacitado, falta de alertas, mala configuración de herramientas. |
| Consecuencias | Incidentes no detectados, ataques prolongados, daño a la infraestructura, pérdida de datos, incumplimiento normativo. |
| Fuente | Auditorías, reportes de incidentes, análisis post-mortem. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (común en organizaciones sin sistemas de monitoreo) |
| Impacto potencial | Crítico (puede llevar a brechas graves y prolongadas) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Falta de alertas, ausencia de logs relevantes, tiempos de respuesta largos. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar sistemas de monitoreo y detección de intrusos (IDS/IPS) | Seguridad / DevOps | SIEM, Splunk, OSSIM, Wazuh |
| Configurar alertas automáticas y notificaciones | Seguridad | Integración con sistemas de comunicación |
| Capacitar al personal en análisis y respuesta rápida | Recursos Humanos | Talleres, simulacros |
| Revisar y actualizar políticas de monitoreo | Seguridad / PM | Manuales y procedimientos |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Analizar y responder rápidamente a alertas | Seguridad | Playbooks, equipo SOC |
| Contener y aislar sistemas afectados | Seguridad / DevOps | Segmentación, firewalls |
| Comunicación interna y externa clara | Gestión / Seguridad | Protocolos de comunicación |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Realizar análisis post-mortem de incidentes | Seguridad / PM | Informes y lecciones aprendidas |
| Mejorar y ajustar sistemas y procedimientos | Seguridad | Actualizaciones de herramientas |
| Capacitación continua y simulacros | Recursos Humanos | Cursos, talleres |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Ataques prolongados sin detección | Pérdida de datos, daño a infraestructura | $60,000 MXN |
| Incapacidad de respuesta rápida | Incremento de daños y costos | $45,000 MXN |
| Sanciones por incumplimiento normativo | Multas y auditorías legales | $30,000 MXN |
| Daño reputacional y pérdida de confianza | Clientes y socios | $25,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$160,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de sistemas IDS/IPS y SIEM | $8,000 MXN |
| Configuración de alertas y notificaciones | $3,000 MXN |
| Capacitación de personal | $4,000 MXN |
| Actualización de políticas y procedimientos | $2,000 MXN |
| Total medidas preventivas: | → $17,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Análisis y respuesta a incidentes | $5,000 MXN |
| Contención y aislamiento de sistemas | $4,000 MXN |
| Comunicación y coordinación | $3,000 MXN |
| Total medidas de mitigación: | → $12,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Análisis post-mortem y mejora de sistemas | $5,000 MXN |
| Capacitación y simulacros continuos | $3,500 MXN |
| Total medidas correctivas: | → $8,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $17,000 MXN |
| 🚨 Mitigación | $12,000 MXN |
| 🔄 Recuperación | $8,500 MXN |
| 💥 Costo de no hacer nada | $160,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $17,000 + $12,000 + $8,500 = **$37,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $160,000 – $37,500 = **$122,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **327% de ROI**