**No proteger endpoints administrativos**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Seguridad de aplicaciones / Autenticación / Control de acceso

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | No proteger endpoints administrativos |
| Categoría | Seguridad / Control de acceso / Desarrollo |
| Causas probables | Falta de autenticación fuerte, ausencia de restricciones IP, configuración incorrecta, falta de monitoreo. |
| Consecuencias | Accesos no autorizados, modificación o destrucción de datos, pérdida de control del sistema. |
| Fuente | Auditorías de seguridad, análisis de vulnerabilidades, reportes de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (vulnerabilidad común en sistemas mal configurados) |
| Impacto potencial | Crítico (puede comprometer toda la aplicación y datos) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Endpoints sin autenticación, accesos desde IPs no autorizadas, reportes de intrusión. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar autenticación fuerte (MFA/2FA) | Desarrollo / Seguridad | Authenticator apps, tokens hardware |
| Restringir acceso a endpoints por IP o VPN | DevOps / Seguridad | Firewalls, listas blancas IP |
| Configurar reglas de acceso y autorización estrictas | Seguridad / Dev | Frameworks de autorización |
| Realizar revisiones y pruebas de seguridad periódicas | QA / Seguridad | Pentesting, escaneo de vulnerabilidades |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar y bloquear accesos sospechosos | Seguridad / DevOps | Sistemas IDS/IPS, firewalls |
| Aplicar parches y configuraciones urgentes | DevOps | Gestión de configuración |
| Auditar actividad y responder a incidentes | Seguridad | SIEM, análisis forense |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisar y fortalecer políticas de acceso | PM / Seguridad | Manuales, políticas internas |
| Capacitación y sensibilización del equipo | Recursos Humanos | Talleres, cursos |
| Implementar monitoreo continuo y alertas | Seguridad / DevOps | SIEM, herramientas de monitoreo |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Acceso no autorizado y control total del sistema | Robo, manipulación o destrucción de datos | $60,000 MXN |
| Pérdida de datos críticos y reputación | Daños operativos y desconfianza de clientes | $40,000 MXN |
| Costos legales y regulatorios | Multas y asesoría legal | $30,000 MXN |
| Investigación y recuperación | Horas-hombre, consultoría técnica | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$150,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de MFA/2FA | $5,000 MXN |
| Configuración de restricciones IP/VPN | $3,000 MXN |
| Pruebas y auditorías de seguridad | $3,500 MXN |
| Capacitación del equipo | $2,500 MXN |
| Total medidas preventivas: | → $14,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Detección y bloqueo de accesos sospechosos | $4,000 MXN |
| Aplicación de parches y ajustes urgentes | $3,000 MXN |
| Auditoría y respuesta a incidentes | $3,000 MXN |
| Total medidas de mitigación: | → $10,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Actualización de políticas y capacitación continua | $4,000 MXN |
| Implementación de monitoreo y alertas | $3,000 MXN |
| Total medidas correctivas: | → $7,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $14,000 MXN |
| 🚨 Mitigación | $10,000 MXN |
| 🔄 Recuperación | $7,000 MXN |
| 💥 Costo de no hacer nada | $150,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $14,000 + $10,000 + $7,000 = **$31,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $150,000 – $31,000 = **$119,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **384% de ROI**