INFORME DE EVALUACIÓN DE SEGURIDAD

Autor: Emanuel Gómez Palacios – División de Ciberseguridad

Fecha: 07/09/2024

Confidencialidad: Uso interno – Información Sensible

# 1. Resumen

Este informe detalla los resultados de una simulación de intrusión controlada sobre la infraestructura de Empresa 049 con el objetivo de evaluar la efectividad de los informes de seguridad previos y su impacto en la gestión de riesgos, incluyendo revisiones post implementación.  
  
*El ejercicio se desarrolló bajo autorización formal, abarcando validación de hallazgos reportados como corregidos, detección de nuevas brechas y análisis de utilidad de los informes previos.*

# 2. Métricas Generales

|  |  |
| --- | --- |
| Indicador | Resultado |
| Vulnerabilidades críticas detectadas en informe previo | 10 |
| Vulnerabilidades críticas corregidas | 7 |
| Vulnerabilidades críticas persistentes | 3 |
| Nuevas vulnerabilidades críticas detectadas | 4 |
| Reducción de riesgo global post-implementación | 45% |
| Tiempo promedio de corrección de hallazgos (días) | 32 |
| Porcentaje de recomendaciones aplicadas | 70% |
| Cumplimiento con políticas internas | 80% |

# 3. Tabla de Riesgos Persistentes y Nuevos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Tipo de Riesgo | Descripción | CVSS v3 | Impacto Negocio | Estado |
| R1 | Persistente | Inyección SQL en módulo de reportes internos | 9.1 (Crítico) | Acceso a datos sensibles | No corregido |
| R2 | Persistente | Credenciales expuestas en repositorio Git | 8.2 (Alto) | Compromiso de cuentas internas | No corregido |
| R3 | Persistente | Configuración insegura en firewall | 7.5 (Alto) | Acceso no autorizado a red interna | Parcialmente corregido |
| R4 | Nuevo | API interna expuesta sin autenticación | 9.0 (Crítico) | Acceso completo a backend | No corregido |
| R5 | Nuevo | Política de contraseñas debilitada en AD | 8.5 (Alto) | Incremento de riesgo de fuerza bruta | No corregido |
| R6 | Nuevo | Servicio SSH abierto en segmento público | 7.8 (Alto) | Posible intrusión remota | No corregido |
| R7 | Nuevo | Falta de validación de entrada en formulario web | 7.3 (Alto) | Riesgo de XSS persistente | No corregido |

# 4. Efectividad de los Informes Previos

|  |  |  |
| --- | --- | --- |
| Criterio Evaluado | Puntaje (1-5) | Observación |
| Claridad técnica | 4 | Detallan bien vulnerabilidades, pero lenguaje muy técnico. |
| Priorización por criticidad | 3 | Basada solo en impacto técnico, no en impacto de negocio. |
| Trazabilidad de hallazgos | 4 | Incluye referencias, pero no métricas de verificación. |
| Seguimiento post-implementación | 2 | No se aplicaron controles recurrentes. |
| Utilidad para gerencia | 3 | Requiere interpretación técnica previa. |

# 5. Análisis de Impacto en la Gestión de Riesgos

**- Positivo:**  
 - Reducción significativa de brechas conocidas.  
 - Mayor conciencia en áreas técnicas.

**- Negativo:**  
 - Persistencia de vulnerabilidades críticas.  
 - Ausencia de métricas post-implementación.  
 - Nuevos riesgos introducidos por cambios de infraestructura sin evaluación previa.

# 6. Recomendaciones

1. Implementar ciclo de gestión de riesgos continuo con pruebas trimestrales de Ethical Hacking.  
2. Incorporar matriz de priorización combinando impacto técnico y de negocio.  
3. Usar métricas claras: tiempo de cierre, % de riesgo mitigado, % de hallazgos reincidentes.  
4. Estandarizar informes en formato mixto técnico-gerencial con resúmenes ejecutivos claros.  
5. Integrar validación de seguridad en procesos de cambio y despliegue (DevSecOps).

# 7. Conclusión

El análisis evidencia que la efectividad de los informes de seguridad previos fue moderada: hubo avances importantes en reducción de riesgo, pero sin un ciclo de verificación estructurado se mantienen vulnerabilidades críticas y surgen nuevos riesgos no previstos.  
  
Se recomienda a la dirección de seguridad implementar un plan de validación continua que garantice que las medidas aplicadas sean efectivas y sostenibles en el tiempo.