LABORATORIO 14

Laboratorio 14: Técnicas de Mitigación de Riesgos - Análisis de Casos Reales de Incidentes de Seguridad

1. Introducción

Conceptos clave:

Riesgo: Posibilidad de pérdida o daño debido a amenazas que afectan a activos valiosos.

Controles de mitigación:

Preventivos: Evitan que ocurra un incidente (ej: firewall, antivirus).

Detectivos: Identifican un incidente en el momento (ej: IDS).

Correctivos: Minimizan el impacto tras el incidente (ej: backups).

2. División en Grupos

Grupos definidos:

Seguridad de la Información

Continuidad del Negocio

Cumplimiento Normativo

Capacitación del Personal

Grupo asignado: Seguridad de la Información.

3. Escenario de Riesgo

Ataque de ransomware que cifra bases de datos financieras. Los atacantes exigen $50,000 USD en criptomonedas.

Análisis del escenario:

Activos vulnerables: Bases de datos, servidores, acceso a red.

Amenazas: Phishing, vulnerabilidades en el software, controles obsoletos.

4. Selección de Controles

Controles propuestos:

Firewall avanzado

Costo: $12,000,000 COP/año

Eficacia: Alta

Backups incrementales en la nube

Costo: $18,000,000 COP/año

Eficacia: Alta

Capacitación en seguridad para empleados

Costo: $3,500,000 COP/año

Eficacia: Alta

Antivirus con protección contra ransomware

Costo: $9,000,000 COP/año

Eficacia: Alta

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control | Plazo | |  |  | | --- | --- | |  | **Responsable** | |
| Firewall avanzado | 3 semanas | Equipo de TI |
| Backups en la nube | 1 mes | Infraestructura |
| Capacitación | 2 semanas | |  |  | | --- | --- | |  | RRHH | |
| Antivirus | 10 días | TI |

**Recursos necesarios:**

* Personal técnico especializado
* Proveedor de capacitación externa
* Presupuesto total estimado: $42,500,000 COP

**6. Monitoreo y Mejora**

**KPIs propuestos:**

* Número de ataques bloqueados por el firewall
* Éxito en pruebas de restauración de backups
* Correos phishing detectados
* Frecuencia de detección de malware

**Revisión periódica:**

* Firewall y antivirus: trimestral
* Backups: mensual
* Capacitación: anual con actualizaciones semestrales

**Mejoras propuestas:**

* Evaluar implementación de un SOC si los incidentes persisten
* **Escenario:** Ataque de ransomware a bases de datos financieras
* **Controles seleccionados:** Firewall, backups, capacitación, antivirus
* **Implementación:** Dentro de 1 mes
* **Monitoreo:** KPIs previamente definidos