LABORATORIO 3

Plan de Respuesta a Incidentes de Seguridad (IRP)

# 1. Información General

Nombre del documento: Plan de Respuesta a Incidentes de Seguridad  
Responsable: Jorge Humberto Rodriguez Baquero  
Fecha de revisión: 28/05/2025  
Versión: 1.0

# 2. Objetivo

Establecer los pasos a seguir ante un incidente de seguridad informática para reducir su impacto, restaurar operaciones normales y prevenir futuras ocurrencias.

# 3. Equipo de Respuesta a Incidentes (CSIRT)

|  |  |  |
| --- | --- | --- |
| Nombre | Rol | Contacto |
| Ana Pérez | Coordinadora de CSIRT | ana@empresa.com |
| Carlos Gómez | Analista de Seguridad | carlos@empresa.com |
| Soporte TI | Técnico de sistemas | soporte@empresa.com |

# 4. Clasificación de Incidentes

|  |  |  |
| --- | --- | --- |
| Tipo de Incidente | Descripción | Ejemplo |
| Acceso no autorizado | Usuario o atacante accede sin permiso | Hacker accede al correo interno |
| Malware | Código malicioso que afecta sistemas | Ransomware, troyano |
| Denegación de servicio (DoS) | Ataque que impide el uso de servicios | Web caída por sobrecarga |
| Phishing | Engaño para obtener datos | Correo falso solicitando contraseña |

# 5. Pasos de Respuesta

## a. Detección y Análisis

- Monitorear sistemas con SIEM y antivirus.  
- Verificar logs de accesos, firewalls y actividad sospechosa.  
- Confirmar la existencia del incidente.

## b. Contención

- Aislar sistemas comprometidos (red, usuarios, dispositivos).  
- Cambiar contraseñas o revocar accesos.  
- Aplicar políticas de seguridad temporales.

## c. Erradicación

- Eliminar malware o cuentas maliciosas.  
- Corregir configuraciones vulnerables.  
- Aplicar parches y actualizaciones.

## d. Recuperación

- Restaurar desde backups seguros.  
- Verificar la integridad del sistema.  
- Monitorear comportamiento post-incidente.

## e. Lecciones Aprendidas

- Reunión de análisis con el equipo.  
- Elaboración de informe final.  
- Ajustar políticas y entrenar al personal.

# 6. Informe de Incidente (Plantilla básica)

Fecha del incidente:   
Sistema afectado:   
Tipo de incidente:   
Descripción breve:   
Acciones tomadas:   
Resultado:   
Recomendaciones:

# 7. Medidas Preventivas

- Capacitación en ciberseguridad.  
- Simulacros de respuesta.  
- Actualización constante de sistemas.

**Conceptos Clave sobre Manejo de Incidentes en Cisco Networking Academy**

1. **Definición de incidente de seguridad**
   * Un incidente de seguridad es cualquier evento que compromete la **confidencialidad**, **integridad** o **disponibilidad** de la información o los sistemas.
2. **Ciclo de vida del manejo de incidentes**  
   Cisco enseña un enfoque estructurado que típicamente sigue este ciclo:
   * **Preparación**
     + Desarrollo de políticas, procedimientos, equipos y herramientas para responder a incidentes.
     + Capacitación del personal y simulacros.
   * **Detección y análisis**
     + Identificación de eventos anómalos.
     + Clasificación y priorización de incidentes.
     + Herramientas como IDS/IPS, SIEM, y logs.
   * **Contención**
     + Acciones para limitar el alcance del ataque y evitar su propagación.
     + Puede ser contención a corto y largo plazo.
   * **Erradicación**
     + Eliminación del malware o accesos no autorizados.
     + Aplicación de parches o reconfiguración de sistemas.
   * **Recuperación**
     + Restauración de sistemas afectados a un estado operativo normal.
     + Monitoreo para asegurar que no haya más amenazas activas.
   * **Lecciones aprendidas (post-mortem)**
     + Documentación y análisis del incidente.
     + Recomendaciones para mejorar políticas y defensa.

**Otros conceptos importantes relacionados**

* **Equipo de respuesta a incidentes (CSIRT)**  
  Conjunto de profesionales encargados de manejar los incidentes de seguridad.
* **Clasificación de incidentes**  
  Según su severidad, tipo de ataque, sistemas afectados, etc.
* **Indicadores de compromiso (IoCs)**  
  Evidencia que sugiere que una brecha o ataque ha ocurrido.
* **Plan de respuesta a incidentes (IRP)**  
  Documento formal que describe cómo la organización debe responder ante incidentes.