Laboratorio 13 – Rigoberto Márquez

Escenario 1: Ataque de phishing a institución educativa

Activos clave en riesgo: Sistema académico, accesos de usuario, historial de calificaciones.

Peligro y puntos débiles:

- **Peligro:** Phishing (engaño para obtener datos).
- **Debilidades:** Autenticación de un solo factor, ausencia de control de correo no deseado, falta de educación en seguridad para usuarios.

Consecuencias y posibilidad:

- **Consecuencias:** Graves (alteración de calificaciones).
- **Posibilidad:** Elevada (usuarios vulnerables al phishing).

Riesgo total: Significativo.
¿Se puede tolerar?: No.

Acciones para reducir el riesgo:

- Implementar doble factor de autenticación.
- Activar protección contra spam y revisión de enlaces.
- Educar a los usuarios en ciberseguridad.

Responsables y plazos:

- Departamento de TI: 2 semanas (filtros y 2FA).
- Administración académica: 1 mes (capacitación).

Seguimiento:

- Análisis de registros de acceso.
- Pruebas simuladas de phishing.

Resumen y sugerencias:
Es crucial fortalecer la seguridad técnica y la concientización para evitar el robo de accesos.

Caso 2: Ransomware en una clínica odontológica

1. **Activos críticos:** Archivos clínicos, administrativos y financieros.
2. **Amenazas y vulnerabilidades:**
    - **Amenaza:** Ransomware.

    - **Vulnerabilidades:** Antivirus caducado, sin respaldos, sin segmentación de red.
3. **Impacto y probabilidad:**
    - **Impacto:** Crítico (pérdida de información vital).
    - **Probabilidad:** Alta (correo con malware).
4. **Nivel de riesgo:** Crítico.
5. **¿Riesgo aceptable?:** No.
6. **Plan de tratamiento:**
    - Implementar respaldos automáticos y actualizados.
    - Renovar el antivirus y aplicar políticas de segmentación.
    - Capacitación sobre correos maliciosos.
7. **Responsables y tiempo estimado:**
    - Área de TI: 1 mes para toda la implementación.
8. **Mecanismos de monitoreo:**
    - Supervisión diaria de respaldos y antivirus.
    - Pruebas de restauración de datos.
9. **Conclusiones y recomendaciones:**
   La prevención es clave. Las políticas de respaldo y seguridad deben estar activas.

Caso 3: Acceso no autorizado a cámara IP de una empresa

1. **Activos críticos:** Grabaciones, privacidad del cliente.
2. **Amenazas y vulnerabilidades:**
    - **Amenaza:** Acceso externo no autorizado.
    - **Vulnerabilidades:** Acceso remoto habilitado vía HTTP sin autenticación segura, firmware desactualizado con vulnerabilidades conocidas, contraseñas por defecto ("admin/admin"), el sistema no genera alertas ni logs de acceso.
3. **Impacto y probabilidad:**
    - **Impacto:** Crítico (violación a la privacidad).
    - **Probabilidad:** Alta (configuraciones por defecto).
4. **Nivel de riesgo:** Fatal.
5. **¿Riesgo aceptable?:** No.
6. **Plan de tratamiento:**
    - Cambiar las contraseñas por defecto.
    - Actualizar el firmware.
    - Generar alertas para accesos no autorizados.
7. **Responsables y tiempo estimado:**
    - Equipo técnico: 1 semana.
8. **Mecanismos de monitoreo:**
    - Alertas de acceso.
    - Revisión de registros de actividad.
9. **Conclusiones y recomendaciones:**
   No se debe subestimar la configuración inicial de los dispositivos de red.

Caso 4: Uso indebido de información personal en una alcaldía

1. **Activos críticos:** Base de datos con información personal.
2. **Amenazas y vulnerabilidades:**
    - **Amenaza:** Personal interno con malas prácticas.
    - **Vulnerabilidades:** No existen registros de logs ni auditorías, acceso a bases de datos sin niveles de privilegio, sin política de clasificación de la información, no se realizaron acuerdos de confidencialidad con el contratista.
3. **Impacto y probabilidad:**
    - **Impacto:** Crítico (violación a la confidencialidad).
    - **Probabilidad:** Alta (no se establecen buenas políticas de seguridad).
4. **Nivel de riesgo:** Crítico.
5. **¿Riesgo aceptable?:** No.
6. **Plan de tratamiento:**
    - Implementar registros de logs y auditorías.
    - Configurar niveles de privilegio.
    - Firmar acuerdos de confidencialidad con contratistas.
7. **Responsables y tiempo estimado:**
    - Área de TI: 15 días para toda la implementación.
8. **Mecanismos de monitoreo:**
    - Supervisión diaria de logs.
    - Alertas para accesos no autorizados.
9. **Conclusiones y recomendaciones:**
   El control del acceso a datos sensibles es esencial en el sector público.

Caso 5: Corte de servicio por ataque DoS a sitio web institucional

1. **Activos críticos:** Sitio web institucional, servidor de inscripciones.
2. **Amenazas y vulnerabilidades:**
    - **Amenaza:** Ataque de denegación de servicio (DoS).
    - **Vulnerabilidades:** No existían medidas de mitigación como WAF o protección DoS, el servidor web estaba sobrecargado y sin alta disponibilidad, no había monitoreo en tiempo real, no se informó al área de sistemas hasta pasadas 3 horas.
3. **Impacto y probabilidad:**
    - **Impacto:** Crítico (indisponibilidad del servicio en un momento clave).
    - **Probabilidad:** Alta (riesgo de ataques reiterados, como los lanzados por botnets).
4. **Nivel de riesgo:** Crítico.
5. **¿Riesgo aceptable?:** No.
6. **Plan de tratamiento:**
    - Implementar WAF y balanceo de carga.
    - Activar monitoreo 24/7.
    - Definir un plan de respuesta ante incidentes.
7. **Responsables y tiempo estimado:**
    - Departamento de sistemas: 10 días.
8. **Mecanismos de monitoreo:**
    - Sistemas de detección de intrusos.
    - Monitoreo en tiempo real.

9. **Conclusiones y recomendaciones:**
   Las plataformas críticas deben tener alta disponibilidad y mecanismos de defensa activos.

Apuntes:

La gestión de riesgos es un proceso sistemático que permite a las organizaciones identificar, evaluar y tratar los riesgos que podrían afectar sus objetivos (ISO, 2018)

Sistema de gestión de la seguridad: iso 270001

Evaluación y análisis de los riesgos: 31000

Alcance: limitar que proceso, que área vamos a cubrir. Ejm: Procesos TI del área de infraestructura.

Liderazgo y compromiso: Requiere inversión, necesita ser aprobado desde la gerencia…

Identificación de activos y riesgos: activos: hardware, software y analizar los riegos.

Proceso de evaluación de riesgos

Identificación de Riesgos

En esta primera fase, el objetivo es identificar todos los posibles riesgos que podrían ocurrir. Esto implica hacer un inventario exhaustivo de los activos, amenazas y vulnerabilidades presentes (ISO, 2018; NIST, 2012).

- **Activos:** Son los recursos que la organización quiere proteger, ya sean físicos (edificios, equipos), lógicos (datos, sistemas) o intangibles (reputación, marca).
- **Amenazas:** Son eventos o condiciones externas o internas que podrían causar daño a los activos. Pueden ser naturales (desastres naturales), humanas (errores, sabotaje) o tecnológicas (ciberataques).
- **Vulnerabilidades:** Son debilidades en los sistemas, procesos o personas que podrían ser explotadas por las amenazas.

Análisis de Riesgos

Una vez identificados los riesgos, se procede a analizarlos para comprender mejor su naturaleza y alcance (ISO, 2018; NIST, 2012).

- **Probabilidad:** Es la estimación de la frecuencia con la que un riesgo podría ocurrir.
- **Impacto:** Son las consecuencias negativas que podría tener la materialización de un riesgo.

Evaluación de Riesgos

La evaluación de riesgos consiste en determinar la importancia relativa de cada riesgo identificado. Esto implica comparar los riesgos entre sí y establecer prioridades para su tratamiento (ISO, 2018; NIST, 2012).

- **Criterios de evaluación:** Se establecen criterios específicos para evaluar los riesgos, como la probabilidad, el impacto, la urgencia, etc.
- **Tolerancia al riesgo:** Se define el nivel de riesgo que la organización está dispuesta a aceptar.
- **Priorización de riesgos:** Los riesgos se ordenan según su importancia, lo que permite enfocar los esfuerzos en aquellos que representan una mayor amenaza.

Comunicación y consulta en la gestión de riesgos (ISO, 2018; NIST, 2012).

¿Por qué es tan importante la comunicación efectiva en la gestión de riesgos?

- Transparencia
- Colaboración
- Toma de decisiones informada
- Aumento de la conciencia
- Mejora de la confianza
- Cumplimiento normativo

Monitoreo y revisión de riesgos
Actualización continua de la evaluación de riesgos

La gestión de riesgos no es un proceso estático, sino dinámico y evolutivo. Los riesgos están en constante cambio debido a factores internos y externos a la organización (ISO, 2018; NIST, 2012). Por esta razón, es fundamental implementar un sistema de monitoreo y revisión que permita mantener actualizada la evaluación de riesgos.

¿Por qué es importante el monitoreo y revisión de riesgos?

- Detección temprana de cambios
- Evaluación de la efectividad de las medidas de mitigación
- Adaptación a cambios en el entorno
- Mejora continua
- Cumplimiento normativo

Monitoreo y revisión de riesgos

¿Cómo se realiza el monitoreo y revisión de riesgos?
Existen diversas herramientas y técnicas para monitorear y revisar los riesgos, entre ellas (ISO, 2018; NIST, 2012):

- Informes periódicos
- Reuniones de revisión
- Auditorías
- Indicadores clave de rendimiento (KPI)
- Software especializado

Actualización continua de la evaluación de riesgos

La actualización continua de la evaluación de riesgos es un proceso iterativo que implica (ISO, 2018; NIST, 2012):

1. Identificar los cambios
2. Evaluar el impacto de los cambios
3. Actualizar la evaluación de riesgos
4. Revisar las medidas de mitigación
5. Comunicar los cambios