

Laboratorio 13

Escenarios donde los estudiantes identifiquen activos, amenazas, vulnerabilidades, impactos, probabilidad, niveles de riesgo y medidas de tratamiento siguiendo la norma ISO 31000 en el contexto de ciberseguridad.

CASO 1: Robo de credenciales por phishing en una entidad educativa

Escenario:

Un estudiante recibe un correo aparentemente institucional con un enlace a una supuesta plataforma de calificaciones. Al ingresar sus credenciales, estas son capturadas por un tercero. Al día siguiente, se detecta que alguien accedió con esas credenciales a los registros de notas y los modificó.

Detalles clave:

- Plataforma afectada: sistema académico web.
- No existe segundo factor de autenticación (2FA).
- No hay filtros de spam o análisis de enlaces en los correos entrantes.
- Usuarios no han recibido capacitación en ciberseguridad.

Elemento	Descripción
Activos críticos	Sistema académico, credenciales, registros de notas.
Amenaza	Phishing (robo de credenciales).
Vulnerabilidades	Sin 2FA, sin filtros de spam, sin análisis de enlaces, sin capacitación.
Impacto	Alto: alteración de notas, pérdida de confianza.
Probabilidad	Alta: sin medidas de protección ni formación.
Nivel de riesgo	Crítico.
Aceptable	No.
Tratamiento	Activar 2FA, filtros de spam, capacitación.
Responsables	Área de sistemas, bienestar, directivos.
Tiempo estimado	1 mes para 2FA, 2 semanas filtros, 2 semanas capacitación.
Monitoreo	Alertas de acceso, logs, encuestas.
Recomendación	Invertir en medidas preventivas y educativas inmediatas.

CASO 2: Ransomware en una clínica odontológica

**Escenario:**

Un empleado abre un archivo adjunto en un correo que aparenta ser una factura. Inmediatamente, el sistema muestra un mensaje de que todos los archivos han sido cifrados. Piden un rescate en criptomonedas. La clínica no cuenta con respaldos automáticos actualizados.

**Detalles clave:**

- Archivos clínicos, administrativos y financieros cifrados.
- Software antivirus caducado.
- Sin políticas de copia de seguridad.
- Sin segmentación de red.
- El ransomware se propaga a todas las estaciones de trabajo.

Elemento	Descripción
Activos críticos	Archivos clínicos, administrativos y financieros.
Amenaza	Ransomware.
Vulnerabilidades	Antivirus caducado, sin backups, sin segmentación de red.
Impacto	Muy alto: pérdida de datos vitales y operatividad.
Probabilidad	Alta: sin defensas básicas.
Nivel de riesgo	Crítico.
Aceptable	No.
Tratamiento	Actualizar antivirus, crear políticas de respaldo, segmentar red.
Responsables	Departamento TI, administración.
Tiempo estimado	1 mes para implementación de políticas y respaldos.
Monitoreo	Monitoreo de red, verificación de respaldos periódicos.
Recomendación	Priorizar protección de datos y continuidad operativa.

**CASO 3: Acceso no autorizado a cámara IP de una empresa**

**Escenario:**

Una empresa de seguridad privada instala cámaras IP para monitoreo remoto. Sin embargo, no cambian las contraseñas por defecto ni actualizan el firmware. Un atacante logra visualizar transmisiones en vivo desde una interfaz web abierta al público.

**Detalles clave:**

- 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.

Elemento	Descripción
<b>Activos críticos</b>	Cámaras IP, seguridad de la empresa, transmisiones.
<b>Amenaza</b>	Acceso no autorizado a cámaras.
<b>Vulnerabilidades</b>	Contraseñas por defecto, firmware desactualizado, sin HTTPS.
<b>Impacto</b>	Alto: violación de privacidad y reputación.
<b>Probabilidad</b>	Alta: configuración insegura.
<b>Nivel de riesgo</b>	Crítico.
<b>Aceptable</b>	No.
<b>Tratamiento</b>	Cambiar contraseñas, actualizar firmware, usar HTTPS y autenticación.
<b>Responsables</b>	Proveedor de seguridad, área de TI.
<b>Tiempo estimado</b>	2 semanas.
<b>Monitoreo</b>	Logs de acceso, alertas automáticas.
<b>Recomendación</b>	Nunca usar configuraciones por defecto, políticas claras de instalación.

**CASO 4: Uso indebido de información personal en una alcaldía**

**Escenario:**

Un contratista accede a bases de datos con información personal de ciudadanos para “validar datos”. Después se descubre que vendía esta información a una empresa de marketing. La alcaldía no tenía controles para registrar el acceso a datos sensibles.

**Detalles clave:**

- No existen registros de logs ni auditoría.
- 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.

Elemento	Descripción
<b>Activos críticos</b>	Bases de datos con información personal.
<b>Amenaza</b>	Uso indebido de datos por contratista.
<b>Vulnerabilidades</b>	Sin registros de acceso, sin política de privilegios, sin acuerdos legales.
<b>Impacto</b>	Muy alto: violación de privacidad, sanciones legales.
<b>Probabilidad</b>	Media-Alta: sin controles internos.
<b>Nivel de riesgo</b>	Alto.
<b>Aceptable</b>	No.
<b>Tratamiento</b>	Implementar control de accesos, clasificar datos, firmar acuerdos.
<b>Responsables</b>	Dirección TIC, jurídica y recursos humanos.
<b>Tiempo estimado</b>	1 mes.
<b>Monitoreo</b>	Auditorías internas y monitoreo de accesos.
<b>Recomendación</b>	Proteger datos sensibles con políticas estrictas y registro detallado.

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

Escenario:

El sitio web de una universidad sufre una caída durante el proceso de inscripciones. El análisis revela un ataque de denegación de servicio (DoS) lanzado desde múltiples IPs, provocando la caída del servidor durante 8 horas.

Detalles clave:

- 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.

Elemento	Descripción
<b>Activos críticos</b>	Sitio web institucional.
<b>Amenaza</b>	Ataque DoS (Denegación de Servicio).
<b>Vulnerabilidades</b>	Sin WAF, sin monitoreo, sin alta disponibilidad.
<b>Impacto</b>	Alto: caída del servicio durante inscripciones.
<b>Probabilidad</b>	Alta: sin preparación técnica.
<b>Nivel de riesgo</b>	Crítico.
<b>Aceptable</b>	No.
<b>Tratamiento</b>	Implementar WAF, balanceadores de carga, monitoreo 24/7.
<b>Responsables</b>	Área de TI, infraestructura digital.
<b>Tiempo estimado</b>	1 mes.
<b>Monitoreo</b>	Monitoreo en tiempo real y alertas.
<b>Recomendación</b>	Prepararse ante incidentes críticos en momentos clave del año.