Leonis Manuel Diaz Pacheco

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

Leonis Manuel Diaz Pacheco

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
Activos críticos	Cámaras IP, seguridad de la empresa, transmisiones.
Amenaza	Acceso no autorizado a cámaras.
Vulnerabilidades	Contraseñas por defecto, firmware desactualizado, sin HTTPS.
Impacto	Alto: violación de privacidad y reputación.
Probabilidad	Alta: configuración insegura.
Nivel de riesgo	Crítico.
Aceptable	No.
Tratamiento	Cambiar contraseñas, actualizar firmware, usar HTTPS y autenticación.
Responsables	Proveedor de seguridad, área de TI.
Tiempo estimado	2 semanas.
Monitoreo	Logs de acceso, alertas automáticas.
Recomendación	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
Activos críticos	Bases de datos con información personal.
Amenaza	Uso indebido de datos por contratista.
Vulnerabilidades	Sin registros de acceso, sin política de privilegios, sin acuerdos legales.
Impacto	Muy alto: violación de privacidad, sanciones legales.
Probabilidad	Media-Alta: sin controles internos.
Nivel de riesgo	Alto.
Aceptable	No.
Tratamiento	Implementar control de accesos, clasificar datos, firmar acuerdos.
Responsables	Dirección TIC, jurídica y recursos humanos.
Tiempo estimado	1 mes.
Monitoreo	Auditorías internas y monitoreo de accesos.
Recomendación	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
Activos críticos	Sitio web institucional.

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