Carlos Alberto Rasgo Solano

Identifique **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.

Identificación en caso 1:

Activos	Datos de las notas y Datos de los usuarios de la plataforma
Amenazas	**Ataque Phishing**
Vulnerabilidades	No hay factor de autenticación, no hay informes de seguridad sobre ingresos sospechosos y no hay registro u notificaciones sobre modificaciones de datos masivos.
Impactos	• Manipulación de registros académicos → daño a integridad de datos • Pérdida de confianza y posibles acciones disciplinarias/legales • Costos de investigación, restauración y comunicación
Probabilidad	**Alta**
Niveles de Riesgo	Alto
Medidas de Tratamiento	• Implementar 2FA para todas las cuentas del sistema académico • Desplegar filtros antiphishing en correo (spam, sandbox de enlaces)

Carlos Alberto Rasgo Solano

	• Programas regulares de capacitación y simulacros de phishing • Políticas de cambio y fortaleza de contraseñas • Monitoreo de accesos y alertas de actividad inusual • Página de login con validación de dominio y TLS, más banner de seguridad

🧩 **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.

Identificación en caso 2:

Activos	• Historias clínicas digitales • Archivos administrativos/financieros • Servidores y estaciones de trabajo • Software de gestión odontológica • Reputación y confianza de pacientes
Amenazas	**• Ransomware distribuido por correo malicioso** **• Propagación lateral interna**
Vulnerabilidades	• Antivirus caducado • Ausencia de copias de seguridad automáticas

Carlos Alberto Rasgo Solano

	• Falta de segmentación de red • Falta de concienciación del personal ante phishing
Impactos	• Pérdida de acceso a datos clínicos → interrupción de la atención • Daño reputacional y posible pérdida de pacientes • Sanciones regulatorias (protección de datos de salud) • Costos de rescate, restauración y downtime
Probabilidad	**Alta**
Niveles de Riesgo	Critico
Medidas de Tratamiento	• Implantar copias de seguridad automáticas offline / inmutables • Actualizar y centralizar antivirus/EDR en todos los equipos • Segmentar la red (VLAN clínica vs. administración, DMZ correo) • Filtrado de correo con sandbox y bloqueo de adjuntos ejecutables • Programa continuo de formación anti-phishing al personal • Plan de respuesta a incidentes y pruebas de restauración periódicas • Política de principio de mínimo privilegio y MFA

Carlos Alberto Rasgo Solano

🧩 **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.

Identificación en caso 3:

Activos	• Cámaras IP y su firmware • Flujo de video en vivo (datos sensibles) • Red corporativa y servidores NVR • Privacidad de clientes/empleados • Reputación y contratos de la empresa de seguridad
Amenazas	**• Intruso externo que explota interfaz web abierta** **• Bot nets que buscan cámaras vulnerables**
Vulnerabilidades	• HTTP sin TLS ni autenticación fuerte • Contraseñas por defecto "admin/admin" • Firmware desactualizado con CVE conocidos • Falta de registros y alertas de acceso
Impactos	• Exposición de imágenes privadas → riesgos legales (protección de datos, privacidad) • Uso de cámaras como punto de entrada a la red interna • Daño reputacional y pérdida de clientes • Posibles sanciones regulatorias
Probabilidad	**Alta**
Niveles de Riesgo	Alto
Medidas de Tratamiento	

Carlos Alberto Rasgo Solano

	• Cambiar contraseñas por defecto e implementar políticas de contraseñas robustas • Actualizar firmware inmediatamente y establecer proceso de parches continuo • Deshabilitar acceso HTTP; habilitar HTTPS con certificados válidos y MFA • Limitar acceso remoto mediante VPN o lista blanca de direcciones IP • Activar y supervisar logs y alertas de acceso inusual • Segmentar la red de video del resto de la infraestructura • Auditorías de seguridad periódicas y hardening de dispositivos

🧩 **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.

Identificación en caso 4:

Activos	• Bases de datos con información personal de ciudadanos (P II) • Servidores y sistemas de gestión de bases de datos • Confidencialidad/privacidad de los ciudadanos • Cumplimiento normativo (protección de datos, Ley Habeas Data)

Carlos Alberto Rasgo Solano

	• Reputación y confianza pública de la alcaldía
Amenazas	**• Empleado/contratista interno que filtra o vende datos** **• Robo de información por actores externos si hay fuga inicial**
Vulnerabilidades	• Sin registros de logs ni auditoría • Acceso a BD sin controles de privilegios/roles • Falta de clasificación de la información • Ausencia de acuerdos de confidencialidad con contratistas
Impactos	• Divulgación masiva de datos personales y sanciones legales. • Pérdida de confianza ciudadana y daño reputacional • Posibles demandas colectivas • Costos de notificación y remediación
Probabilidad	Media
Niveles de Riesgo	**Alto**
Medidas de Tratamiento	• Establecer roles y privilegios mínimos (principio de mínimo privilegio) • Implementar logging, monitoreo y auditorías periódicas de acceso a BD • Clasificar la información y aplicar controles según criticidad • Firmar NDA y realizar due-diligence a contratistas • Implementar DLP y cifrado en reposo y tránsito • Capacitación sobre protección de datos y ética • Plan de respuesta a incidentes y notificación a afectados

Carlos Alberto Rasgo Solano

🧩 **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.

Identificación en caso 5:

Activos	• Sitio web institucional de la universidad (front-end y back-end) • Servidor y ancho de banda de hosting • Base de datos de inscripciones (indirectamente afectada) • Continuidad de proceso de admisiones • Imagen y confianza de la universidad
Amenazas	• **Ataque de denegación de servicio desde múltiples IP**
Vulnerabilidades	• Sin WAF ni servicios anti-DDoS • Servidor sobrecargado, sin arquitectura de alta disponibilidad • Falta de monitoreo en tiempo real • Comunicación tardía al equipo de sistemas (3 h)
Impactos	• Caída de la web 8 h, retraso/fracaso en inscripciones • Pérdida financiera por matrículas no procesadas a tiempo • Daño reputacional y quejas de estudiantes • Posible incumplimiento de SLA y contratos de hosting
Probabilidad	Media
Niveles de Riesgo	**Alto**

Carlos Alberto Rasgo Solano

Medidas de Tratamiento	• Implementar WAF/servicio anti-DDoS en la capa de borde o CDN • Diseñar arquitectura escalable • Configurar alertas y monitoreo 24/7 (tráfico y tiempo de respuesta) • Plan de respuesta a incidentes con notificación inmediata a TI • Pruebas de estrés periódicas y simulacros de DDoS • Revisión de capacidad y contratos de hosting para burst traffic