Estudiate:

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

Elemento	Análisis
Activos Críticos	Sistema académico, credenciales de acceso, base de datos de notas, correo institucional
Amenazas y Vulnerabilidades	Phishing, sin 2FA, sin filtros antispam, usuarios no capacitados
Impacto / Probabilidad	Alto / Alta
Nivel de Riesgo	Crítico
¿Riesgo Aceptable?	No
Plan de Tratamiento	Activar 2FA, implementar filtros antiphishing, capacitar a usuarios, definir protocolo de respuesta
Responsables / Tiempo Estimado	Área TI / 2 semanas para medidas técnicas, 1 mes para capacitación
Mecanismos de Monitoreo	Auditoría de accesos, reportes de phishing, logs del sistema
Conclusiones y Recomendaciones	Fortalecer controles técnicos y humanos, establecer protocolos de incidentes

CASO 2: Ransomware en una clínica odontológica

Elemento	Análisis
Activos Críticos	Archivos clínicos, administrativos y financieros
Amenazas y Vulnerabilidades	Ransomware, antivirus caducado, sin backups, red no segmentada
Impacto / Probabilidad	Muy Alto / Alta
Nivel de Riesgo	Crítico
¿Riesgo Aceptable?	No
Plan de Tratamiento	Renovar antivirus, establecer backups automáticos, segmentar red, formación en ciberseguridad
Responsables / Tiempo Estimado	Área TI / 1 mes
Mecanismos de Monitoreo	Verificación de backups, registros de actividad, monitoreo de red
Conclusiones y Recomendaciones	Implementar controles preventivos y políticas de recuperación de datos

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

Elemento	Análisis
Activos Críticos	Cámaras IP, privacidad de transmisiones, red de vigilancia
Amenazas y Vulnerabilidades	Acceso remoto inseguro, firmware desactualizado, contraseñas por defecto
Impacto / Probabilidad	Alto / Media
Nivel de Riesgo	Alto
¿Riesgo Aceptable?	No
Plan de Tratamiento	Actualizar firmware, cambiar credenciales, activar autenticación segura y HTTPS
Responsables / Tiempo Estimado	Técnico de red / 2 semanas
Mecanismos de Monitoreo	Logs de acceso, alertas de IPs externas, escaneo de vulnerabilidades
Conclusiones y Recomendaciones	Urgente reforzar seguridad básica de dispositivos IoT y limitar accesos

CASO 4: Uso indebido de información personal en una alcaldía

Elemento	Análisis
Activos Críticos	Bases de datos de ciudadanos, información personal
Amenazas y Vulnerabilidades	Acceso indebido, sin registros de logs, sin acuerdos de confidencialidad, sin clasificación de información
Impacto / Probabilidad	Alto / Media
Nivel de Riesgo	Alto
¿Riesgo Aceptable?	No
Plan de Tratamiento	Definir políticas de acceso, registrar logs, firmar acuerdos de confidencialidad, clasificar la información
Responsables / Tiempo Estimado	Jurídica y TI / 3 semanas
Mecanismos de Monitoreo	Auditoría de accesos, revisiones legales periódicas
Conclusiones y Recomendaciones	Necesario implementar controles organizativos y técnicos sobre datos personales

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

Elemento	Análisis
Activos Críticos	Sitio web institucional, disponibilidad del servicio de inscripciones
Amenazas y Vulnerabilidades	Ataque DoS, sin mitigación, sin alta disponibilidad, sin monitoreo
Impacto / Probabilidad	Medio / Alta
Nivel de Riesgo	Medio-Alto
¿Riesgo Aceptable?	No
Plan de Tratamiento	Implementar WAF, activar balanceo de carga, establecer monitoreo en tiempo real
Responsables / Tiempo Estimado	Área TI / 1 mes
Mecanismos de Monitoreo	Logs de red, alertas de tráfico anómalo, análisis de disponibilidad
Conclusiones y Recomendaciones	Fortalecer infraestructura web con medidas preventivas y capacidad de respuesta