Tarea 1.5: Blindar a "CiberLibros", una librería online en expansión (Fase 2)

Trabajo realizado por:
Samuel Romero de los Reyes

Curso de especialización en:
CETI

Índice

1. Resumen ejecutivo

El análisis identifica varios riesgos críticos para CiberLibros: Los riesgos pueden provocar pérdida de ventas, interrupción del servicio, fuga de datos y daños reputacionales.

Para reducirlos, se propone implementar medidas esenciales como protección para ataques, autentificar al iniciar sesión, formación en informática, dividir las redes y hacer copias de seguridad automáticas y hacer un ciberseguro.

La hoja de ruta establece acciones inmediatas en seguridad básica (0-3 meses), mejoras técnicas y organizativas en el medio plazo (3-9 meses) y una estrategia de seguridad continua en el largo plazo. Estas medidas permitirán a CiberLibros mejorar su resiliencia y proteger tanto sus datos como la continuidad del negocio.

2. Top 5 Riesgos Prioritarios

2.1. Denegación de servicio del servidor web

Naturaleza del riesgo:
Ataques que saturan el servidor web, aprovechando su poca capacidad de mitigación en hosting compartido.

Impacto en el negocio:
Pérdida de ventas, caída total de la web, mala imagen ante los clientes y posibles incumplimientos legales si se afecta el servicio de pagos.

2.2. Ingeniería social en las estaciones de trabajo

Naturaleza del riesgo:
Empleados engañados mediante correos o mensajes falsos debido a falta de formación y uso de dispositivos personales.

Impacto en el negocio:
Infecciones, robo de credenciales, interrupción del trabajo y riesgo elevado de fuga de datos personales.

2.3. Denegación de servicio al router

Naturaleza del riesgo:
Ataques que bloquean el router, aprovechando configuraciones débiles o firmware desactualizado.

Impacto en el negocio:
Toda la oficina se queda sin Internet, paralizando ventas, logística y atención al cliente, afectando reputación y operativa.

2.4. Errores de los usuarios en la copia de seguridad

Naturaleza del riesgo:
Borrado accidental, mala configuración o fallos al realizar copias debido a procesos no formalizados.

Impacto en el negocio:
Pérdida de datos críticos, retrasos operativos, errores en pedidos y posibles incidentes legales por pérdida de información personal.

2.5. Ingeniería social al desarrollador web

Naturaleza del riesgo:
Intentos de engaño al desarrollador, que tiene privilegios altos y pocos controles de seguridad.

Impacto en el negocio:
Modificación o secuestro de la web, robo de datos, interrupción del servicio y graves consecuencias legales y reputacionales.

3. Plan de Tratamientos de Riesgos

3.1. Denegación de servicio del servidor web

Tratamiento: Mitigar + Transferir
Acciones clave:

- Activar protección anti-DDoS y WAF.
- Mejorar hosting o activar monitorización de disponibilidad.
- Contratar ciberseguro para cubrir interrupción del negocio.

Justificación:
La web es el canal principal de ventas; su caída implica pérdidas directas.

3.2. Ingeniería social en las estaciones de trabajo

Tratamiento: Mitigar
Acciones clave:

- Formación en phishing.
- Activar 2FA en accesos críticos.
- Formalizar política BYOD.
- Filtrado avanzado de correo.

Justificación:
Los empleados son la puerta de entrada más frecuente a ataques.

3.3. Denegación de servicio al router / Wi-Fi

Tratamiento: Mitigar
Acciones clave:

- Actualizar firmware.
- Separar red de invitados y corporativa.
- Usar router empresarial con capacidades de seguridad.
- Monitorizar tráfico anómalo.

Justificación:
Sin router no hay Internet: toda la operación se detiene.

3.4. Errores de usuarios en las copias de seguridad

Tratamiento: Mitigar + Aceptar parcialmente
Acciones clave:

- Automatizar backups y protegerlos contra borrado.
- Aplicar regla 3-2-1.
- Probar restauraciones periódicamente.

Justificación:
Los errores humanos son comunes, pero mitigables, parte del riesgo es aceptable por coste/beneficio.

3.5. Ingeniería social al desarrollador web

Tratamiento: Mitigar + Transferir
Acciones clave:

- Activar 2FA en todos los accesos técnicos.

- Usar gestor seguro de contraseñas.
- Limitar accesos por VPN o IP.
- Formar al desarrollador en ataques dirigidos.

Justificación:
Es un perfil con privilegios técnicos; si lo comprometen, se compromete el sistema entero.

4. Hoja de Ruta de Implementación

4.1. Corto Plazo (0-3 meses)

Acciones rápidas, de bajo coste y alto impacto.

1. Proteger servidor web y router (riesgo alto)
   - Activar protección anti-DDoS del hosting.
   - Activar o instalar WAF básico (Cloudflare gratuito es viable).
   - Cambiar contraseña del router y actualizar firmware.
   - Separar Wi-Fi corporativa y Wi-Fi invitados.
2. Mitigar ingeniería social en estaciones y desarrollador
   - Implementar 2FA en correo, CRM y accesos técnicos.
   - Configurar filtros anti-phishing en el correo corporativo.
   - Lanzar formación básica en phishing para todos los empleados.
3. Asegurar las copias de seguridad
   - Configurar copias automáticas de sistemas críticos.
   - Verificar que las copias están protegidas contra borrado accidental.
   - Prueba inicial de restauración para garantizar que funcionan.
4. Documentación mínima
   - Crear procedimiento rápido para reporting de incidentes.
   - Definir responsable de coordinar backups y actualizaciones.

4.2. Medio Plazo (3-9 meses)

Acciones que requieren más esfuerzo pero reducen riesgos estructurales.

1. Profesionalizar la seguridad técnica

- Migrar la web a un hosting más robusto si el actual no ofrece seguridad adecuada.
- Implementar VPN para accesos del desarrollador.
- Endurecer la configuración del router o adquirir un router empresarial.

2. Reducción de errores humanos

- Impartir formación recurrente en ciberseguridad cada trimestre.
- Establecer política BYOD formalizada (antivirus, contraseñas, actualizaciones).
- Revisar permisos y privilegios de usuarios (mínimo privilegio).

3. Seguridad en copias de seguridad

- Aplicar la regla 3-2-1 completa:
    - 3 copias
    - 2 soportes distintos
    - 1 externa (nube o almacenamiento fuera del edificio)
- Realizar pruebas de restauración mensuales.

4. Ciberseguro

- Evaluar y contratar un ciberseguro que cubra interrupciones del negocio y fuga de datos.

4.3. Largo Plazo (9-18 meses)

Acciones que fortalecen la madurez de la empresa en seguridad.

1. Gestión continua de seguridad

- Implantar un plan de gestión de parches para estaciones y aplicaciones.
- Crear un inventario de activos actualizado.
- Implementar un sistema de monitorización centralizada (logs, accesos, alertas).

2. Mejora de la resiliencia

- Migración progresiva a infraestructura más segura, como hosting dedicado con WAF avanzado.
- Evaluación anual de riesgos y actualización del plan.

3. Cultura de seguridad

- Integrar la seguridad en los procesos de trabajo (por ejemplo, checklist de seguridad para nuevas contrataciones o cambios de infraestructura).
- Establecer simulaciones periódicas de phishing.

5. Conclusión

El análisis realizado demuestra que CiberLibros enfrenta riesgos significativos que afectan directamente a la continuidad del negocio, la protección de los datos y la confianza de los clientes. Los cinco riesgos prioritarios identificados, denegación de servicio del servidor web, ingeniería social en las estaciones de trabajo, denegación de servicio al router, errores en las copias de seguridad e ingeniería social dirigida al desarrollador web, representan amenazas críticas tanto por su alta probabilidad como por el impacto operativo, financiero y reputacional que pueden generar.

El Plan de Tratamiento propone medidas realistas y adaptadas a una PyME sin personal técnico dedicado, combinando controles técnicos (protección anti-DDoS, WAF, 2FA, segmentación de redes), organizativos (política BYOD, gestión de privilegios, procedimientos de incidentes) y formativos (concienciación en phishing y buenas prácticas). Además, la complementariedad entre mitigar y transferir ciertos riesgos, como la interrupción del negocio o el compromiso de cuentas privilegiadas, permite reducir de manera efectiva el riesgo residual.

La hoja de ruta establece un enfoque escalonado: acciones inmediatas de corto plazo, mejoras estructurales de medio plazo y el desarrollo de una cultura de seguridad y resiliencia a largo plazo. Este planteamiento garantiza que CiberLibros pueda reforzar su postura de seguridad de forma progresiva, optimizando recursos y priorizando los riesgos más críticos.

En conjunto, las medidas propuestas permiten a la organización avanzar hacia un modelo de seguridad más sólido, reducir de manera significativa las vulnerabilidades actuales y asegurar la continuidad del negocio en un entorno digital cada vez más amenazante.