

Tarea 1.5: Blindar a "CiberLibros", una librería online en expansión (Fase 1)



Trabajo realizado por:
Samuel Romero de los Reyes

Curso de especialización en:
CETI

Índice

1. Contexto y Alcance.....	3
1.1 Contexto Organizativo.....	3
1.2. Infraestructura Tecnológica.....	3
1.3. Alcance del Análisis de Riesgos.....	3
1.4. Activos Identificados.....	4
1.4.1 Activos de Hardware.....	4
1.4.2 Activos de Software.....	4
1.4.3 Activos de Información.....	4
1.4.4 Activos de Personal.....	4
1.4.5 Activos Intangibles.....	4
2. Análisis de Riesgos.....	5

1. Contexto y Alcance

1.1 Contexto Organizativo

CiberLibros es una PyME fundada hace tres años que se dedica a la venta de libros técnicos y de nicho. Opera principalmente en el sector del comercio electrónico (retail) bajo un modelo de negocio B2C, comercializando sus productos a través de una plataforma web y una aplicación móvil recientemente lanzada. Su crecimiento acelerado ha sido impulsado por el éxito de su tienda online y su actividad constante en redes sociales.

La empresa cuenta con una plantilla de 20 empleados distribuidos entre atención al cliente, marketing, logística y un desarrollador web a tiempo parcial. Actualmente, no dispone de personal especializado en TI o ciberseguridad, lo que plantea retos adicionales en la gestión de riesgos tecnológicos.

1.2. Infraestructura Tecnológica

La infraestructura tecnológica de CiberLibros presenta los siguientes elementos principales:

- Servidor web alojado en un proveedor de hosting compartido.
- Base de datos de clientes, que incluye información personal (nombre, dirección, historial de compras) y datos de pago cifrados.
- Red interna de oficina compuesta por 15 estaciones de trabajo (Windows y macOS) y una red Wi-Fi que da servicio a empleados e invitados.
- Software en la nube, incluyendo un sistema de gestión de inventario y un CRM.
- Uso de dispositivos personales por parte de los empleados para acceder al correo corporativo y gestionar redes sociales, dentro de una política BYOD.

El director general ha expresado preocupaciones recientes relacionadas con ataques de ransomware y phishing, especialmente por su impacto potencial sobre los datos de clientes y la continuidad operativa.

1.3. Alcance del Análisis de Riesgos

El análisis de riesgos abarcará todos los elementos tecnológicos, humanos y organizativos que participan en las operaciones de CiberLibros. Su objetivo es identificar amenazas, vulnerabilidades y posibles impactos sobre la confidencialidad, integridad y disponibilidad de la información y los servicios.

El alcance incluye:

- Activos tecnológicos clave (hardware y software).
- Activos de información vinculados a la operación del negocio.
- Personal con roles críticos en la gestión o uso de sistemas de información.
- Activos intangibles para la continuidad del negocio y la confianza del cliente.

No se considerarán activos ajenos a la infraestructura tecnológica o humana de CiberLibros, ni elementos externos.

1.4. Activos Identificados

1.4.1 Activos de Hardware

1. Servidor web (HW1)
2. Estaciones de trabajo de empleados (HW2)
3. Router y red Wi-Fi corporativa (HW3)

1.4.2 Activos de Software

1. Plataforma web de comercio electrónico (SW1)
2. Aplicación móvil (SW2)
3. CRM en la nube (SW3)

1.4.3 Activos de Información

1. Base de datos de clientes (Media1)
2. Historial de ventas y transacciones (Media2)
3. Copias de seguridad locales de inventario y pedidos (Media3)

1.4.4 Activos de Personal

1. Personal de atención al cliente (P1)
2. Desarrollador web a tiempo parcial (P2)

1.4.5 Activos Intangibles

1. Reputación corporativa (I1)
2. Confianza del cliente en la plataforma (I2)

2. Análisis de Riesgos

ANÁLISIS DE RIESGOS				
Activo	Amenaza	Probabilidad	Impacto	Riesgo
Servidor Web	Errores de los usuarios	Medio (2)	Medio (2)	4
Servidor Web	Denegación de servicio	Alto (3)	Alto (3)	9
Servidor Web	Robo	Bajo (1)	Alto (3)	3
Servidor Web	Ingeniería social	Alto (3)	Alto (3)	9
Estaciones de trabajo	Errores de los usuarios	Alto (3)	Medio (2)	6
Estaciones de trabajo	Denegación de servicio	Bajo (1)	Alto (3)	3
Estaciones de trabajo	Robo	Medio (2)	Alto (3)	6
Estaciones de trabajo	Ingeniería social	Alto (3)	Alto (3)	9
Router	Errores de los usuarios	Medio (2)	Alto (3)	6
Router	Denegación de servicio	Alto (3)	Alto (3)	9
Router	Robo	Bajo (1)	Alto (3)	3
Router	Ingeniería social	Medio (2)	Alto (3)	6
Plataforma web	Errores de los usuarios	Medio (2)	Alto (3)	6
Plataforma web	Denegación de servicio	Alto (3)	Alto (3)	9
Plataforma web	Robo	Bajo (1)	Alto (3)	3
Plataforma web	Ingeniería social	Alto (3)	Alto (3)	9
Aplicación móvil	Errores de los usuarios	Medio (2)	Medio (2)	4
Aplicación móvil	Denegación de servicio	Medio (2)	Alto (3)	6
Aplicación móvil	Robo	Bajo (1)	Alto (3)	3
Aplicación móvil	Ingeniería social	Alto (3)	Alto (3)	9
CRM	Errores de los usuarios	Medio (2)	Alto (3)	6
CRM	Denegación de servicio	Alto (3)	Alto (3)	9
CRM	Robo	Bajo (1)	Alto (3)	3
CRM	Ingeniería social	Alto (3)	Alto (3)	9
Base de datos clientes	Errores de los usuarios	Medio (2)	Alto (3)	6
Base de datos clientes	Denegación de servicio	Alto (3)	Alto (3)	9
Base de datos clientes	Robo	Bajo (1)	Alto (3)	3
Base de datos clientes	Ingeniería social	Alto (3)	Alto (3)	9
Historial de ventas	Errores de los usuarios	Bajo (1)	Medio (2)	2
Historial de ventas	Denegación de servicio	Medio (2)	Alto (3)	6
Historial de ventas	Robo	Bajo (1)	Alto (3)	3
Historial de ventas	Ingeniería social	Bajo (1)	Alto (3)	3
Copias de seguridad	Errores de los usuarios	Alto (3)	Alto (3)	9
Copias de seguridad	Denegación de servicio	Medio (2)	Alto (3)	6
Copias de seguridad	Robo	Medio (2)	Alto (3)	6
Copias de seguridad	Ingeniería social	Alto (3)	Alto (3)	9
Personal de atención al cliente	Errores de los usuarios	Alto (3)	Alto (3)	9
Personal de atención al cliente	Denegación de servicio	Bajo (1)	Bajo (1)	1
Personal de atención al cliente	Robo	Bajo (1)	Medio (2)	2

Personal de atención al cliente	Ingeniería social	Alto (3)	Alto (3)	9
Desarrollador web	Errores de los usuarios	Alto (3)	Alto (3)	9
Desarrollador web	Denegación de servicio	Bajo (1)	Alto (3)	3
Desarrollador web	Robo	Bajo (1)	Alto (3)	3
Desarrollador web	Ingeniería social	Alto (3)	Alto (3)	9
Reputación corporativa	Errores de los usuarios	Alto (3)	Alto (3)	9
Reputación corporativa	Denegación de servicio	Bajo (1)	Bajo (1)	1
Reputación corporativa	Robo	Bajo (1)	Alto (3)	3
Reputación corporativa	Ingeniería social	Bajo (1)	Alto (3)	3
Confianza del cliente	Errores de los usuarios	Alto (3)	Alto (3)	9
Confianza del cliente	Denegación de servicio	Bajo (1)	Bajo (1)	1
Confianza del cliente	Robo	Bajo (1)	Alto (3)	3
Confianza del cliente	Ingeniería social	Bajo (1)	Alto (3)	3