Proyecto de SGSI: Análisis de Riesgos PharmaDistribución S.L.

Elaborado por:
Gonzalo Sánchez Maroto
Francisco Iván San Segundo Álvarez
Daniel García Salinas
Fecha: 19 de diciembre de 2024

Resumen: Este documento contiene un análisis estructurado de las características, riesgos y controles de seguridad IT en PharmaDistribución S.L.

Índice general

Capítulo 1

Características de la empresa

1.1. Panorámica IT de la empresa

PharmaDistribucion S.L. es una pequeña empresa del sector logístico y distribución de productos farmaceuticos. Esta cuenta con un total de 30 trabajadores que se encargan de garantizar una entrega eficiente y segura de medicamentos a los clientes.

Al ser completamente dependientes de la tecnología, ya que la totalidad de la cadena de suministros depende de ella (necesidad de automatización, seguridad, accesibilidad y conexión), se debe proteger correctamente los recursos, tales como:

- Sus servidores físicos para el guardado de la información de entregas y productos.
- Su software de pedidos.
- Sus servicios de red que permitan que la información sobre los pedidos llegue correctamente a la empresa final.

En definitiva, el area IT debe enfrentar el reto de proteger a los recursos informáticos de ciberataques, manteniendo la eficiencia de los mismos y sin crear un sistema excesivamente complejo para los usuarios finales.

1.2. Departamento y ubicaciones

PharmaDistribución S.L. cuenta con una oficina central que alberga los distintos departamentos que conforman la empresa:
1. Administrativo: Facturación y contratos
2. Comercial: Relación con los clientes
3. General: Toma decisiones estratégicas
4. IT: Gestión de infraestructuras y seguridad
5. Atención al cliente: Soporte y gestión de pedidos
6. Logística: Gestión de almacenes

Además, dispone de un almacén logístico donde se gestionan las operaciones de inventario y distribución.

El departamento IT está compuesto por un pequeño equipo responsable de la infraestructura tecnológica y la seguridad de la información. Este equipo se comunicará con el resto de departamentos, para asegurarse de que se cumplan las exigencias de cada uno.

1.3. Infraestructura IT

La infraestructura tecnológica de PharmaDistribución S.L. se compone de los siguientes elementos:

- Servidores físicos(2) y en la nube(1) para el almacenamiento de datos y el funcionamiento de las aplicaciones.
- Estaciones de trabajo(20) distribuidas entre los departamentos de la empresa.
- Dispositivos móviles para los empleados(10-20), que permitan llevar a cabo funciones logísticas y de soporte
- Redes internas con diversos dispositivos (routers, switches,...) protegidas por un firewall físico y conexiones VPN seguras.
- Software de gestión y acceso a los productos como ERP, CRM, Plataforma Web, App móvil y un sistema de correos corporativo.

La infraestructura física debe soportar correctamente la utilización de los servicios detallados en el apartado 1.4

1.4. Servicios necesarios en la organización

Para que la empresa este definida correctamente, debemos establecer una serie de servicios necesarios para su funcionamiento:

- **ERP**: Servicio que ayude a la organización a optimizar sus procesos de negocio. Debe incluir un servicio de gestión de inventarios y pedidos para los empleados.
- **CRM**: Servicio para la facturación y la contabilidad, para facilitar las transacciones con los clientes.
- **Plataforma Web**: Servicio que permite a los usuarios realizar pedidos gracias a catálogos actualizados, integración de medidas de pago, acceder a el envío de sus pedidos ya realizados y modificar las características de sus pedidos a través de Internet.
- **App Móvil**: Servicio que funciona de forma similar a la plataforma web(ofrece las mismas características), pero de forma más interactiva para usuarios recurrentes
- **Sistema de correo Microsoft 365**: Servicio que permitirá la correcta comunicación entre departamentos para llevar a cabo así tareas conjuntas, así como comunicación con vendedores y clientes.
- **AWS**: Servicio que permite almacenar los datos de los productos y su distribución en la nube, consiguiendo así más fiabilidad a la hora de guardar estos.
- **Defensa Perimetral**: Servicio externo de una empresa que ofrece soluciones sobre seguridad, prevención de ataques y protección en el perímetro de la red (IDS,IPS).
- **VPN**: Servicio que permite la conexión remota de los trabajadores a la red de la empresa para así facilitar el trabajo externo y el acceso a los datos 24/7.

1.5. Requerimientos de acceso interno y externo

Para garantizar un acceso seguro y funcional a los recursos de la organización, los requerimientos de acceso interno y externo se dividen en los siguientes puntos clave:

Acceso Interno

- **Autenticación robusta**: Uso de credenciales únicas para cada empleado, con autenticación de dos factores (2FA) en sistemas críticos.
- **Control de accesos por rol**: Implementar políticas de acceso basadas en roles para limitar el acceso a información sensible según el puesto de trabajo.
- **Acceso dispositivos a la red interna**: Solo permitido a dispositivos registrados y autorizados, mediante políticas de gestión de dispositivos.
- **Conexión segura**: Todo el tráfico interno debe estar cifrado utilizando protocolos seguros(AES).
- **Auditoría de accesos**: Registro de los archivos de log y monitoreo de estos por parte del departamento de IT para asegurarse que no ha habido ningún intruso.

Acceso Externo

- **Autenticación segura para usuarios externos**: Clientes y socios comerciales deben autenticarse utilizando credenciales únicas y limitaciones en el número de intentos de sesión.
- **VPN para empleados remotos**: Acceso remoto seguro a la red interna mediante conexiones VPN con cifrado de alta seguridad (IPsec).
- **Plataforma web segura**: Debe incluir medidas como autenticación, cifrado HTTPS, y protección frente a ataques comunes como inyecciones o XSS (cross-site scripting).
- **App móvil protegida**: Integración de medidas como autenticación biométrica, cifrado de datos locales.
- **Limitación por IP**: Gracias al firewall, ACLs, listas blancas de acceso IP...
- **Auditoría de accesos**: Monitoreo de los registros de actividad de los usuarios para asegurarnos de que se cumplen las políticas de seguridad.

En ambos casos, los sistemas deben ser capaces de escalar y adaptarse según las necesidades de la organización, manteniendo la seguridad como prioridad.

1.6. Política de seguridad

Para asegurarnos de que los servicios funcionen correctamente, se aplicarán unas políticas de seguridad acordes a estos, que aparecen listadas a continuación:

- Garantizar la confidencialidad, integridad y disponibilidad de la información.
- Implementar medidas de seguridad en todos los sistemas críticos.
- Proteger los datos personales y financieros de los clientes y proveedores.
- Realizar auditorías regulares para identificar vulnerabilidades

1.7. Agentes implicados

Los agentes que interactúan con PharmaDistribución S.L. incluyen los siguientes:

- **Proveedores de servicios tecnológicos**: AWS para el almacenamiento de información en la nube y Microsoft 365 para la comunicación empleado-cliente.
- **Clientes**: Usuarios que realizan pedidos y consultas a través de la plataforma web o la aplicación móvil.
- **Socios comerciales**: Empresas colaboradoras que gestionan el transporte, distribución y logística de los productos.
- **Empleados**: Trabajadores que se encargan del correcto funcionamiento de la empresa y de tramitar los pedidos de los clientes.
- **Proveedores de infraestructura**: Compañías encargadas de garantizar la disponibilidad de la infraestructura en la nube y las conexiones de red perimetrales (coneción con ISP).
- **Auditores externos**: Organismos que realizan auditorías periódicas sobre la seguridad y el cumplimiento de normativas en la periferia de la red.

Estos agentes deben cumplir con las políticas de seguridad establecidas por la organización y garantizar la integridad de los datos compartidos o gestionados.

Capítulo 2

Análisis de Riesgos

2.1. Catálogo de activos, requerimientos de seguridad y activos valiosos

El catálogo de activos es una lista de los recursos, información y servicios que una organización considera valiosos, y cuya protección es crítica para su funcionamiento. En este contexto, se incluyen los siguientes activos:

Inventario de activos

A continuación se presenta el inventario de activos organizados en categorías:

- **Servicios:**
  - Servicios de soporte técnico y atención al cliente.
  - Plataformas de servicio en la nube, ya sean IaaS, PaaS, SaaS...
  - Servicios internos de mantenimiento y gestión de infraestructura llevados a cabo por el departamento IT.
- **Datos e información:**
  - Bases de datos de clientes, proveedores y empleados.
  - Bases de datos con información financiera y contable.
  - Bases de datos con información sobre los productos, stock y pedidos.
  - Bases de datos con otros tipos de documentación tanto interna como externa (datos comerciales, gubernamentales, legislativos,...).
- **Aplicaciones Software:**
  - Software de gestión empresarial (ERP).
  - Herramientas de comunicación: correo electrónico proporcionado por Microsoft 365.
  - Plataformas de gestión de relaciones con el cliente (CRM).
  - Aplicación web y móvil.
- **Equipos informáticos:**
  - 20 estaciones de trabajo entre computadoras de escritorio y portátiles de empleados.
- **Personal:**

    - Empleados divididos en los departamentos anteriormente mencionados. 1.2
    - Dirección de la empresa que tomará las decisiones de mayor peso.

- **Redes de comunicaciones:**
    - Infraestructura de red interna (routers, switches, firewalls).
    - Conexiones externas y enlaces de comunicación con otras organizaciones que proveeran a nuestra organización de ciertos servicios.
    - VPNs para comunicaciones seguras.

- **Soportes de información:**
    - Dispositivos de almacenamiento de backup para guardar correctamente la información para prevenir su perdida en caso de fallo.
    - 2 Servidores físicos y uno en la nube, que alojan servicios y datos críticos.

- **Equipos auxiliares:**
    - Dispositivos de comunicación (teléfonos, videoconferencias).
    - Equipos periféricos (impresoras, escáneres, proyectores).

- **Instalaciones:**
    - Infraestructura física como oficinas, salas de servidores y centros de datos.
    - Equipos para mantener en correcto funcionamiento los servidores: sistemas de refrigeración, UPS (sistemas de alimentación ininterrumpida) y otros sistemas de soporte.

- **Imagen y reputación de la empresa:**
    - Marca corporativa y presencia en redes sociales.
    - Relación con clientes y proveedores.
    - Opinión pública sobre la empresa y sus productos/servicios.

Inventario de Activos

Clasificación de activos

Clase de activo	Descripción
[D] Datos / Información	Información generada o manejada por el centro almacenada en diferentes soportes de información.
[S] Servicios	Servicios o funciones prestados por la organización para cubrir una necesidad de los usuarios.
[SW] Software	Aplicaciones informáticas tanto de desarrollo propio como aplicaciones externas que permiten realizar tareas específicas.
[HW] Hardware	Equipos informáticos que actúan como soportes de datos o que albergan servicios informáticos.
[P] Personal	Empleados, incluyendo directivos y personal técnico.
[N] Redes de Comunicaciones	Infraestructura de red interna y conexiones externas seguras, como VPNs.
[SI] Soportes de Información	Dispositivos de almacenamiento y servidores físicos y en la nube.
[EA] Equipos Auxiliares	Periféricos, teléfonos, videoconferencias y equipos adicionales.
[I] Instalaciones	Infraestructura física como oficinas y centros de datos.
[IR] Imagen y Reputación	Marca corporativa, presencia en redes y relación con clientes/proveedores.

Cuadro 2.1: Clasificación de activos y descripción.

Valor	Descripción
Muy Alto	Daño crítico para el centro.
Alto	Daño grave para el centro.
Medio	Daño importante para el centro.
Bajo	Daño menor para el centro.

Cuadro 2.2: Descripción de los valores de impacto.

Inventario de Activos Detallado

Cód.	Nombre	Descripción	Dependencia y Justificación
S.1	Soporte técnico	Atención y resolución de incidencias.	P.2: Atiende requerimientos (departamento atención al cliente).
Conf.: Medio, Integ.: Alto, Disp.: Muy Alto, Trazab.: Medio			

Cód.	Nombre	Descripción	Dependencia y Justificación
S.2	Plataformas en la nube	Servicios IaaS, PaaS, SaaS externos.	SI.2: almacenan los datos; D: datos a almacenar.
Conf.: Muy Alto, Integ.: Alto, Disp.: Muy Alto, Trazab.: Alto			
S.3	Gestión infraestructura	Mantenimiento de sistemas IT.	P.2: llevan a cabo el mantenimiento (departamento TI).
Conf.: Alto, Integ.: Alto, Disp.: Alto, Trazab.: Medio			
D.1	BBDD clientes	Datos de clientes, pedidos y relaciones.	S.2: Servicio contratado para alojar datos; SW.1/.2/.4: modifica datos; SI: almacena datos
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Medio, Trazab.: Alto			
D.2	Información financiera	Registros financieros críticos.	SW.1/.4: modificación de información financiera; SI: almacenamiento de información financiera.
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Alto, Trazab.: Alto			
D.3	Gestión inventario y pedidos	Control de stock y operaciones.	SW.1/.4: modificación de información logística; SI: almacenamiento de información logística.
Conf.: Alto, Integ.: Alto, Disp.: Alto, Trazab.: Medio			
D.4	Documentación interna	Información legal y comercial.	SI: almacenamiento de información.
Conf.: Alto, Integ.: Medio, Disp.: Medio, Trazab.: Medio			
SW.1	ERP empresarial	Gestión de finanzas, stock y RRHH.	D.1/.2/.3: datos almacenados para el ERP; SI: dispositivos almacenamiento
Conf.: Alto, Integ.: Muy Alto, Disp.: Alto, Trazab.: Alto			
SW.2	CRM	Herramienta de gestión de clientes.	D.1/.3: datos almacenados para el CRM; SI: dispositivos almacenamiento
Conf.: Alto, Integ.: Alto, Disp.: Medio, Trazab.: Medio			
SW.3	Herramientas de comunicación	Correo electrónico y Teams.	HW.1 y EA.1: Dispositivos de comunicación, N.1/.2: Transmite comunicaciones
Conf.: Medio, Integ.: Medio, Disp.: Alto, Trazab.: Bajo			
SW.4	Aplicación web/móvil	Plataforma accesible para usuarios.	SI: almacenar datos; D.1/.2/.3: datos clientes
Conf.: Alto, Integ.: Alto, Disp.: Alto, Trazab.: Medio			
N.1	Infraestructura interna	Routers, switches y firewalls.	HW.1: equipos de conexion; SI, EA.1/.2: conectados entre si.
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Alto, Trazab.: Alto			
N.2	VPNs seguras	Conexiones cifradas externas.	N.1; depende de seguridad interna también; P.2: departamento IT que gestiona seguridad
Conf.: Muy Alto, Integ.: Alto, Disp.: Alto, Trazab.: Alto			

Cód.	Nombre	Descripción	Dependencia y Justificación
SI.1	Copias de seguridad	Dispositivos de almacenamiento de backup.	D.1/.2/.3: datos a guardar; S.2: servicio que almacena
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Medio, Trazab.: Alto			
SI.2	Servidores físicos y nube	Equipos que alojan datos críticos.	D.1/.2/.3: datos a guardar; S.2: servicio que almacena
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Alto, Trazab.: Alto			
HW.1	Equipos de trabajo	PCs y portátiles empleados.	D: datos a recoger; P.2; usaran los equipos; EA: ayudan a la comunicación
Conf.: Medio, Integ.: Alto, Disp.: Alto, Trazab.: Medio			
EA.1	Comunicación	Teléfonos y videollamadas.	N.1: redes internas transportan comunicación
Conf.: Medio, Integ.: Medio, Disp.: Alto, Trazab.: Bajo			
EA.2	Periféricos	Impresoras, escáneres y proyectores.	HW.1: hardware al que se conectan
Conf.: Bajo, Integ.: Medio, Disp.: Medio, Trazab.: Bajo			
P.1	Dirección	Alta gerencia de la empresa.	D.4: dependen legalidad para decisiones
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Bajo, Trazab.: Alto			
P.2	Empleados	Personal operativo dividido en áreas.	P.1: Depeden de las ordenes de la directiva; HW.1: dependen de los recursos que sean ofrecidos
Conf.: Alto, Integ.: Alto, Disp.: Medio, Trazab.: Medio			
I.1	Infraestructura física	Oficinas y salas de servidores.	
Conf.: Alto, Integ.: Alto, Disp.: Medio, Trazab.: Medio			
I.2	Sistemas de soporte	Refrigeración, UPS.	SI.2
Conf.: Alto, Integ.: Alto, Disp.: Alto, Trazab.: Medio			
IR.1	Marca corporativa	Identidad visual y presencia pública.	P : directiva y atención al cliente
Conf.: Muy Alto, Integ.: Muy Alto, Disp.: Medio, Trazab.: Alto			
IR.2	Opinión pública	Reputación con clientes y proveedores.	P
Conf.: Alto, Integ.: Alto, Disp.: Medio, Trazab.: Medio			
IR.3	Redes sociales	Presencia en plataformas digitales.	
Conf.: Alto, Integ.: Medio, Disp.: Medio, Trazab.: Medio			

2.2. Listado de amenazas

2.2.1. NATURALES

1. Inundación

Descripción: Daños causados por inundaciones que afectan servidores y oficinas, comprometiendo la infraestructura física y disponibilidad de datos críticos.
Probabilidad: Baja

Activos afectados	C	I	D	A	T
N.1 - Infraestructura interna fugas	-	-	MA	-	-
I.1 - Infraestructura física	-	-	B	-	-
SI.2 - Servidores físicos	-	-	A	-	-
SI.1 - Copias de seguridad	-	-	A	-	-
HW.1 - Hardware	-	-	A	-	-
EA - Destrucción de periféricos en general	-	-	A	-	-

2. Terremoto

Descripción: Movimiento sísmico que daña directamente la estructura física
Probabilidad: Baja

Activos afectados	C	I	D	A	T
N.1 - Infraestructura interna	-	-	MA	-	-
I.1 - Infraestructura física	-	-	B	-	-
SI.2 - Servidores físicos	-	-	A	-	-
SI.1 - Copias de seguridad	-	-	A	-	-

2.2.2. DE ORIGEN INDUSTRIAL

1. Cortes involuntarios y prolongados de energía

Descripción: Cortes eléctrico causados por problemas por parte de la compañía eléctrica contratada (cortes involuntarios, no por caus planificada)
Probabilidad: Baja

Activos afectados	C	I	D	A	T
D - Pérdida de datos en general	-	-	MA	-	-
SW - Caída de software en general	-	-	A	-	-

2. Incendio en la delegación

Descripción: Incendio causado por un mal funcionamiento de ciertos dispositivos o errores humanos a la hora de relizar tareas de gestión.
Probabilidad: Baja

Activos afectados	C	I	D	A	T
D - de los datos en general	-	-	MA	-	-
SW - Caída del software por pérdida de datos	-	A	A	-	-
S.1 - Indisponibilidad del servicio por pérdida de datos	-	A	A	-	-
N.1 - Infraestructura interna	-	-	A	-	-
SI.2 - Servidores físicos	-	-	A	-	-
SI.1 - Copias de seguridad	-	-	A	-	-

3. Fugas de refrigerante o problemas en los sistemas de ventilación

Descripción: Por errores de fábrica, estos sistemas pueden fallar o romperse.
Probabilidad: Baja

Activos afectados	C	I	D	A	T
N.1 - Infraestructura interna	-	-	B	-	-
SI.2 - Servidores físicos	-	-	M	-	-
SI.1 - Copias de seguridad	-	-	M	-	-
S - Caída de los servicios por pérdida de datos	-	A	M	-	-
D - Datos en general	-	-	MA	-	-

2.2.3. ERRORES Y FALLOS NO INTENCIONADOS

1. Modificación/Eliminación initencionada de la BBDD o de alguno de sus elementos

Descripción: Ciertos comandos/errores humanos pueden provocar pérdida de datos de las bases de datos en los servidores físicos
Probabilidad: Media

Activos afectados	C	I	D	A	T
D - Eliminación de los datos en general	M	A	A	M	-

2. Error en el establecimiento de permisos

Descripción: Error a la hora de establecer los permisos de usuario a nuevos usuarios o usuarios ya existentes.
Probabilidad: Media

Activos afectados	C	I	D	A	T
S.3 - Gestión infraestructura	MA	MA	M	MA	-
SW.1 - Modificación ERP	MA	MA	MA	MA	-
SW.3 - Modificación herramientas de comunicación	MA	-	-	MA	-

3. Desactivación accidental de sistemas de soporte

Descripción: Error a la hora modificar los sistemas de soporte, provocando la caída temporal de estos.
Probabilidad: Media

Activos afectados	C	I	D	A	T
I.2 - Sistemas de soporte	-	-	MA	-	-
N.1 - Infraestructura interna	-	-	MA	-	-
SI.2 - Servidores físicos y nube	-	-	MA	-	-
EA.1 - Elementos de comunicación	-	-	MA	-	-
S.2 - Plataformas en la nube	-	-	MA	-	-

2.2.4. ATAQUES INTENCIONADOS

1. Ataque de Ransomware

Descripción: Inyección de ransomware que impida la utilización de equipos.
Probabilidad: Alta

Activos afectados	C	I	D	A	T
N.1 - Infraestructura interna	-	-	MA	-	-
SI.2 - Servidores físicos y nube	-	-	MA	-	-
EA.2 - Elementos de comunicación	-	-	MA	-	-
HW.1 - Equipos de trabajo	-	-	MA	-	-

2. Ataque de Man In The Middle

Descripción: Interceptación del tráfico entre 2 partes.
Probabilidad: Alta

Activos afectados	C	I	D	A	T
N.1 - Infraestructura interna	MA	MA	M	MA	-
N.2 - VPNs seguras	MA	MA	B	MA	-
SW.3 - Herramientas de comunicación	MA	MA	B	MA	-
SW.4 - Aplicación web/móvil	MA	MA	B	MA	-
D.1 - Bases de datos de clientes	MA	MA	B	MA	-
SI.2 - Servidores físicos y nube	MA	MA	B	MA	-

3. Ataque de Phishing

Descripción: Engaño mediante correos electrónicos, sitios web o comunicaciones falsas para robar credenciales o información confidencial.
Probabilidad: Alta

Activos afectados	C	I	D	A	T
SW.3 - Herramientas de comunicación	MA	M	-	MA	-
SW.2 - CRM	MA	M	-	MA	-
D.1 - Bases de datos de clientes	MA	M	-	-	-
HW.1 - Equipos de trabajo	MA	-	-	-	-
IR.2 - Opinión pública	MA	-	-	-	-

4. Ataque de Inyección SQL

Descripción: Inserción de código SQL malicioso en entradas no validadas, permitiendo manipular bases de datos.
Probabilidad: Media-Alta

Activos afectados	C	I	D	A	T
D.1 - Bases de datos de clientes	MA	MA	M	-	-
D.2 - Información financiera	MA	MA	M	-	-
SW.1 - ERP empresarial	MA	MA	M	-	-
SW.4 - Aplicación web/móvil	MA	MA	M	-	-
SI.2 - Servidores físicos y nube	MA	MA	M	-	-

2.3. Listado de riesgos

Los riesgos se definen como la probabilidad de que una amenaza ocurra y cause daño a los activos valiosos. A continuación, se detallan algunos de los riesgos identificados:

2.3.1. Activo: S.1 - Soporte Técnico

Descripción: Atención y resolución de incidencias.

S1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Incendio delegación	-	A	A	-	M	A	-	M	M	-	B	M
Fugas refrigerante/problemas ventilación	-	A	A	-	M	M	-	M	M	-	B	B

2.3.2. Activo: S.2 - Plataformas en la Nube

Descripción: Servicios IaaS, PaaS y SaaS externos.

S2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Fugas refrigerante/problemas ventilación	-	A	A	-	M	M	-	M	M	-	B	B
Desactivación accidental de sistemas	-	-	MA	-	-	A	-	-	A	-	-	A

2.3.3. Activo: S.3 - Gestión Infraestructura

Descripción: Mantenimiento de sistemas IT.

S3												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Fugas refrigerante/problemas ventilación	-	A	M	-	A	M	-	M	M	-	M	M
Error establecimiento de permisos	MA	MA	M	A	A	M	A	A	M	A	A	M

2.3.4. Activo: D.1 - BBDD Clientes

Descripción: Datos de clientes, pedidos y relaciones.

D1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energia	-	-	MA	-	-	A	-	-	A	-	-	M
Incendio delegación	-	-	MA	-	-	A	-	-	A	-	-	M
Fugas refrigerante/problemas ventilación	-	-	MA	-	-	A	-	-	A	-	-	M
Modificación y eliminación inintencionada base de datos	M	A	A	M	M	M	M	A	A	M	M	M
Man in the Middle	MA	MA	B	A	A	B	MA	MA	M	A	A	B
Phising	MA	M	-	A	M	-	MA	M	-	A	M	-
Inyección SQL	MA	MA	M	A	A	M	MA	MA	M	A	A	M

2.3.5. Activo: D.2 - Información Financiera

Descripción: Registros financieros críticos.

D2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	MA	-	-	A	-	-	A	-	-	M
Incendio delegación	-	-	MA	-	-	A	-	-	A	-	-	M
Fugas refrigerante/problemas ventilación	-	-	MA	-	-	A	-	-	A	-	-	M
Modificación y eliminación inintencionada base de datos	M	A	A	M	M	M	M	A	A	M	M	M
Man in the Middle	MA	MA	B	A	A	B	MA	MA	M	A	A	B
Phising	MA	M	-	A	M	-	MA	M	-	A	M	-
Inyección SQL	MA	MA	M	A	A	M	MA	MA	M	A	A	M

2.3.6. Activo: D.3 - Gestión Inventario y Pedidos

Descripción: Control de stock y operaciones logísticas.

D3												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	MA	-	-	A	-	-	A	-	-	M
Incendio delegación	-	-	MA	-	-	A	-	-	A	-	-	M
Fugas refrigerante/problemas ventilación	-	-	MA	-	-	A	-	-	A	-	-	M
Modificación y eliminación inintencionada base de datos	M	A	A	M	M	M	M	A	A	M	M	M

2.3.7. Activo: D.4 - Documentación Interna

Descripción: Información legal y comercial interna.

D4												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	MA	-	-	A	-	-	A	-	-	M
Incendio delegación	-	-	MA	-	-	A	-	-	A	-	-	M
Fugas refrigerante/problemas ventilación	-	-	MA	-	-	A	-	-	A	-	-	M
Modificación y eliminación inintencionada base de datos	M	A	A	M	M	M	M	A	A	M	M	M

2.3.8. Activo: SW.1 - ERP Empresarial

Descripción: Sistema de gestión de finanzas, stock y RRHH.

SW1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	A	-	-	A	-	-	A	-	-	M
Incendio delegación	-	A	A	-	M	M	-	M	M	-	B	B
Error establecimiento de permisos	MA	MA	MA	A	A	A	A	A	A	A	A	A
Inyección SQL	MA	MA	M	A	A	A	A	A	A	A	A	A

2.3.9. Activo: SW.2 - CRM

Descripción: Herramienta de gestión de relaciones con clientes.

SW2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	A	-	-	A	-	-	A	-	-	M
Incendio delegación	-	A	A	-	M	M	-	M	M	-	B	B
Phising	MA	M	-	A	M	-	MA	A	-	A	M	-

2.3.10. Activo: SW.3 - Herramientas de Comunicación

Descripción: Correo electrónico y herramientas de mensajería (Teams).

SW3												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	A	-	-	A	-	-	A	-	-	M
Incendio delegación	-	A	A	-	M	M	-	M	M	-	B	B
Phising	MA	M	-	A	M	-	MA	A	-	A	M	-
Man in the Middle	MA	MA	B	A	A	MB	MA	MA	B	MA	MA	B
Establecimiento de permisos	MA	-	-	A	-	-	MA	-	-	A	-	-

2.3.11. Activo: SW.4 - Aplicación Web/Móvil

Descripción: Plataforma accesible para usuarios internos y externos.

SW4												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Cortes involuntarios y prolongados de energía	-	-	A	-	-	A	-	-	A	-	-	M
Incendio delegación	-	A	A	-	M	M	-	M	M	-	B	B
Inyección SQL	MA	MA	M	A	A	M	MA	MA	M	A	A	M
Man in the Middle	MA	MA	B	A	A	MB	MA	MA	B	MA	MA	B

2.3.12. Activo: N.1 - Infraestructura Interna

Descripción: Routers, switches y firewalls críticos para la red interna.

N1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	MA	-	-	A	-	-	M	-	-	M
Terremoto	-	-	MA	-	-	A	-	-	M	-	-	M
Incendio			A			A			M			M
Fuga refrigerante y problemas de ventilación	-	-	B	-	-	MB	-	-	B	-	-	MB
Desactivación accidental de sistemas de soporte	-	-	MA	-	-	A	-	-	A	-	-	M
Ransomware	-	-	MA	-	-	A	-	-	MA	-	-	A
Man in the Middle	MA	MA	M	A	A	M	MA	MA	M	A	A	M

2.3.13. Activo: N.2 - VPNs Seguras

Descripción: Conexiones cifradas para acceso externo seguro.

N2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Man in the Middle	MA	MA	B	A	A	B	MA	MA	M	A	A	B

2.3.14. Activo: SI.1 - Copias de Seguridad

Descripción: Dispositivos para almacenamiento de backup.

SI.1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	A	-	-	M	-	-	M	-	-	M
Terremoto	-	-	A	-	-	M	-	-	M	-	-	M
Incendio delegación	-	-	A	-	-	A	-	-	A	-	-	A
Fugas de refrigerante/problemas de ventilación	-	-	B	-	-	B	-	-	B	-	-	B

2.3.15. Activo: SI.2 - Servidores Físicos y Nube

Descripción: Equipos que alojan datos críticos y servicios en la nube.

SI.2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	A	-	-	M	-	-	M	-	-	M
Terremoto	-	-	A	-	-	M	-	-	M	-	-	M
Incendio delegación	-	-	A	-	-	A	-	-	A	-	-	A
Fugas de refrigerante/problemas de ventilación	-	-	B	-	-	B	-	-	B	-	-	B
Desactivación accidental de sistemas	-	-	MA	-	-	A	-	-	A	-	-	M
Ransomware	-	-	MA	-	-	A	-	-	MA	-	-	A
Man in the Middle	MA	MA	B	A		A	MA	MA	M	A	A	M
Inyección SQL	MA	MA	M	A	A	M	MA	MA	M	A	A	M

2.3.16. Activo: HW.1 - Equipos de Trabajo

Descripción: PCs y portátiles utilizados por el personal operativo.

HW.1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	A	-	-	M	-	-	M	-	-	M
Ransomware	-	-	MA	-		A	-	-	MA	-	-	A
Phising	MA	-	-	A	-	-	MA	-	-	A	-	-

2.3.17. Activo: EA.1 - Comunicación

Descripción: Teléfonos y dispositivos utilizados para comunicación.

EA.1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	A	-	-	M	-	-	M	-	-	M
Desactivación accidental de sistemas	-	-	MA	-	-	A	-	-	A	-	-	M

2.3.18. Activo: EA.2 - Periféricos

Descripción: Dispositivos como impresoras, escáneres y proyectores.

EA.2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-		A	-	-	M	-	-	M	-	-	M
Ransomware	-	-	MA	-	-	A	-	-	MA	-	-	A

2.3.19. Activo: IR.2 - Opinión Pública

Descripción: Reputación y percepción de la organización por clientes y proveedores.

IR.2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Phising	MA	-	-	A	-	-	MA	-	-	A	-	-

2.3.20. Activo: I.1 - Infraestructura Física

Descripción: Oficinas y salas de servidores.

I.1												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Inundación	-	-	B	-	-	B	-	-	MB	-	-	MB
Terremoto	-	-	B	-	-	B	-	-	MB	-	-	MB

2.3.21. Activo: I.2 - Sistemas de Soporte

Descripción: Refrigeración, sistemas de energía y UPS.

I.2												
AMENAZAS	**IMPACTO POTENCIAL**			**IMPACTO ACUMULADO**			**RIESGO POTENCIAL**			**RIESGO ACUMULADO**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
Desactivación accidental de sistemas de soporte	-	-	MA	-	-	A	-	-	A	-	-	A

2.4. Priorización de riesgos

La priorización de riesgos se realiza considerando tanto la probabilidad de que ocurra un evento como el impacto que tendría sobre la organización. Para ello, se utiliza una matriz de riesgo que clasifica los riesgos en diferentes niveles de prioridad:

AMENAZA	IMPACTO	PROBABILIDAD	RIESGO
INUNDACIÓN	3	1	3
TERREMOTO	3	1	3
CORTE ENERGÍA	3	1	3
INCENDIO	3	1	3
FUGA VENTILACIÓN	2	1	2
MODIFICACIÓN/ELIMINACIÓN BASE DE DATOS	3	2	6
ERROR ESTABLECIMIENTO PERMISOS	3	2	6
DESACTIVACIÓN ACCIDENTAL S.S.	3	2	6
RANSOMWARE	3	3	9
MAN IN THE MIDDLE	2	3	6
PHISING	3	3	9
SQL INJECTION	3	3	9

Los riesgos con mayor prioridad son aquellos que tienen alta probabilidad de ocurrir y un impacto significativo en los activos de la organización. En este caso, los ciberataques serían nuestro mayor riesgo. Aun así no deberíamos descuidar otros aspectos al tener estos un nivel de riesgo también elevado.

Capítulo 3

Salvaguardas (Contramedidas de seguridad)

3.1. Por objetivo de seguridad

OBJ 1: PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

- PR.1: Implementar sistemas de drenaje y protección contra inundaciones.
- PR.2: Elevar servidores y equipos críticos por encima del nivel del suelo.
- PR.3, RC.1: Contar con copias de seguridad externas o en la nube.
- PR.4: Instalar racks y soportes antisísmicos para servidores.
- PR.5: Asegurar el edificio con medidas estructurales antisísmicas.
- CR.1: Tener planes de recuperación ante desastres.
- PR.6, IM.1: Implementar generadores de respaldo para energía continua.
- PR.7: Garantizar redundancia en sistemas críticos.
- PR.8: Implementar sistemas de detección y extinción de incendios.
- PR.9: Asegurar el mantenimiento preventivo de equipos eléctricos.
- IM.2, AD.1: Tener planes de evacuación y contingencia.
- PR.10: Realizar mantenimiento periódico de sistemas de refrigeración.
- MN.1, DC.1: Implementar monitoreo continuo de temperatura en servidores.
- PR.11: Contar con ventilación y refrigeración redundante.
- PR.12, EL.1: Implementar sistemas antivirus y antimalware actualizados.
- AW.1: Capacitar al personal en detección y prevención de ransomware.

OBJ 2: AUTENTICACIÓN

- PR.13: Implementar cifrado de extremo a extremo (TLS/SSL).
- PR.14, IM.3: Utilizar VPNs seguras para comunicaciones remotas.

OBJ 3: AUTORIZACIÓN

- AD.2, PR.15: Implementar políticas estrictas de control de acceso y permisos.
- PR.16, RC.2: Realizar copias de seguridad periódicas de la configuración de los sistemas.
- MN.2, DC.2: Monitorear y auditar accesos a los sistemas críticos.
- AW.2: Capacitar a administradores en gestión de permisos.
- AD.3, DC.3: Revisar y auditar regularmente la asignación de permisos.
- PR.17, AD.4: Automatizar procesos de gestión de permisos.

OBJ 4: INTEGRIDAD DE LA INFORMACIÓN

- PR.18: Validar y sanitizar entradas de usuario en aplicaciones.
- PR.19: Implementar consultas parametrizadas en bases de datos.

OBJ 5: AUDITORÍA DE ACTIVIDADES DE SEGURIDAD

- DC.4, MN.3: Implementar sistemas de alerta para operaciones críticas.
- MN.4: Monitorear y registrar acciones realizadas en sistemas de soporte.
- DC.5, MN.5: Monitorear redes para detectar actividad sospechosa.
- DC.6: Realizar pruebas de penetración para detectar vulnerabilidades.
- AW.3: Capacitar a los empleados en identificación de correos fraudulentos.
- PR.20, DC.7: Implementar filtros antispam y autenticación de correos (DMARC).
- AW.4, DC.8: Realizar simulaciones de ataques phishing periódicamente.

3.2. Por tipo de activo

Clase de Activo	**Amenazas**	**Salvaguardas**
[**D**]	Modificación/ Eliminación de Base de Datos	PR.3, RC.1; PR.12, EL.1; PR.16, RC.3; PR.17; PR.19
[**S**]	Desactivación Accidental de Sistemas de Soporte	CR.1; IM.3; PR.13; PR.14, IM.3
[**SW**]	SQL Injection	PR.12, EL.1; PR.18; PR.19; DC.6; PR.20, DC.7
[**HW**]	Inundación, Terremoto, Corte de Energía	PR.2; PR.4; PR.6, IM.1; PR.7; PR.10; MN.1, DC.1; PR.11
[**P**]	Error en Establecimiento de Permisos, Phishing	AW.1; AW.2; AW.3; AW.4; AW.5, DC.8
[**N**]	Man in the Middle, Phishing	PR.14, IM.3; DC.5, MN.5; DC.4, MN.3; DC.6
[**SI**]	Inundación, Terremoto	PR.1; PR.2; PR.3, RC.1; PR.4
[**EA**]	Incendio	PR.8; PR.9; IM.2, AD.1
[**I**]	Inundación, Terremoto, Incendio, Corte de Energía	PR.1; PR.5; PR.6, IM.1; IM.2, AD.1
[**IR**]	Ransomware, Phishing	AW.4; AW.5, DC.8; PR.20, DC.7

Cuadro 3.1: Clasificación de salvaguardas y amenazas por tipo de activo.

Capítulo 4

Controles del SGSI

4.1. Controles organizacionales

- Realización de auditorías externas e internas
- Realización de cursos/exámenes a los empleados para comprobar sus facultades

4.2. Controles técnicos

- Usar técnicas de pentesting para comprobar los permisos de usuario para acceder a bases de datos
- Realizar movimientos fraudulentos para observar los archivos de log
- Comprobar los planes de restauración de las copias de seguridad

4.3. Controles físicos

- Revisiones de sistemas antiincendios/inundaciones/fallos eléctricos
- Comprobar el mantenimiento de los sistemas de soporte

4.4. Controles de comunicación

- Asegurarse de que los firewalls filtran correctamente todo el tráfico
- Realizar envíos de correos con carácter fraudulento, publicitario y de dudoso origen para comprobar los sistemas de autenticación del correo electrónico

4.5. Controles legales

- Mantener un equipo que este al tanto de las novedades en la legalidad
- Asegurarse de que los proveedores de servicios están cumpliendo con su trabajo

Capítulo 5

Bibliografía y material de apoyo

- Presentaciones de la asignatura (en su mayor parte las diapositivas pertenecientes a: TEMA 3: Materiales de clase (Transparencias). Su uso ha sido principalmente para el análisis de activos, riesgos y amenazas
- Manual de Usuario de Pilar: Salvaguardas: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2841-ccn-stic-470i1-pilar-manual-de-usuario-v7-1/file?format=html
- Excels proporcionados por el profesor: De aqui hemos obtenido posibles activos y riesgos y fijarnos en el cálculo de los riesgos
- Magerit: Facilitó el catálogo de activos y establecer los origenes de las amenazas
- CHATGPT: Ayuda con la realización de tablas en latex debido a nuestra poca experiencia y como fuente inicial de información que fue debidamente contrastada más tarde con el resto de fuentes.

Capítulo 6

Reparto del trabajo

Todos los miembros del grupo han participado en igual medida en la realización de esta tarea, ya sea mediante la realización del texto, el planteamiento de ideas o el análisis de los diversos elementos del documento. Al entregar este documento con nuestros nombres, todos manifestamos estar de acuerdo con que se nos gradúe con la misma nota.