M1.870 - Fundamentos de ciberseguridad.

José Enrique Rodríguez González.

PEC1: Riesgos, vulnerabilidades y amenazas.

Actividad 1 (50% puntuación).

En esta actividad vamos a realizar un análisis de riesgos en una situación ficticia. Suponed que sois analistas de riesgos o auditores contratados por una PYME para analizar sus riesgos. La empresa, una pequeña compañía conocida como "Pepe Gotera y Otilio" es una empresa de reformas y reparaciones conocida en el mercado.
En una primera entrevista, la directora Ofelia, os ha explicado que personalmente controla la parte de contabilidad, temas legales y de contratación de personal con su portátil. Para otros temas, dispone de un ayudante en la oficina para gestionar correos y llamadas, así como para realizar acciones comerciales que buscan nuevos clientes. La empresa tiene un técnico de sistemas, el señor Bacterio, que gestiona/administra todos los sistemas informáticos y pone parches. Finalmente, hay dos trabajadores de campo, Pepe y Otilio, que disponen de smartphones para estar en contacto y poder disponer de información de los clientes (dirección, acciones a realizar…).
Ofelia, su ayudante y Bacterio trabajan en una oficina, donde todos disponen de equipos portátiles con Windows 10, antivirus y herramientas ofimáticas (Microsoft Office), y los puestos de trabajo cableados con línea a internet con una Fibra a 600 MB.
En la misma oficina, para montar el negocio, han puesto en una habitación separada un rack (armario) con dos servidores Windows 2019 Server, (uno solo para el correo/dns y el otro con el portal http/https y una base de datos MySQL). Para securizarlo un poco, han puesto dos Firewalls, uno de protección al exterior y otro a la red interna.
No entraremos a bajo nivel, por lo que no vamos a ver detalles de la marca de FW o el antivirus.

Preguntas.

1. Identifica todos los activos que observas en la PYME y agrúpalos en una columna utilizando los tipos que indica MAGERIT en sus buenas prácticas.
2. Identifica para cada activo las Amenazas que pueden tener.

3. Haz una valoración subjetiva del valor del activo, y de la probabilidad que se materialice una amenaza, así como su impacto en caso de que se haga efectiva la amenaza.
   Para unificar criterios utilizad la siguiente tabla:

----	**Rango económico**	**Frecuencia**	**Impacto**	**Valor**
Muy alto	Activo > 15.000 €	1 vez al día	> 80 %	3,5
Alto	5.000 € < activo < 15.000 €	1 vez cada dos semanas	50% < x < 80 %	2,5
Normal	1.000 € < activo < 5.000 €	1 vez cada dos meses	20 % < x < 50 %	1,5
Bajo	300 € < activo < 1.000 €	1 vez cada 6 meses	5 % < x < 20 %	1
Muy bajo	activo < 300 €	1 vez al año	x < 5 %	0

4. Calcula el riesgo intrínseco y explica cómo lo has calculado.
5. Identifica/enumera qué salvaguardas observas y valora su impacto.
6. Calcula el riesgo residual y explica cómo lo has calculado.
    1. Aconsejamos utilizar una hoja de cálculo y recoger los campos:
        - Tipo.
        - Activo.
        - Amenaza.
        - Valor activo.
        - Frecuencia.
        - Impacto.
        - Riesgo intrínseco.
        - Salvaguarda.
        - Riesgo residual.
7. Si Ofelia preguntara qué puede hacer para mejorar la seguridad de la oficina, dado el informe que has elaborado, haz una propuesta de tres salvaguardas y justifícalas.

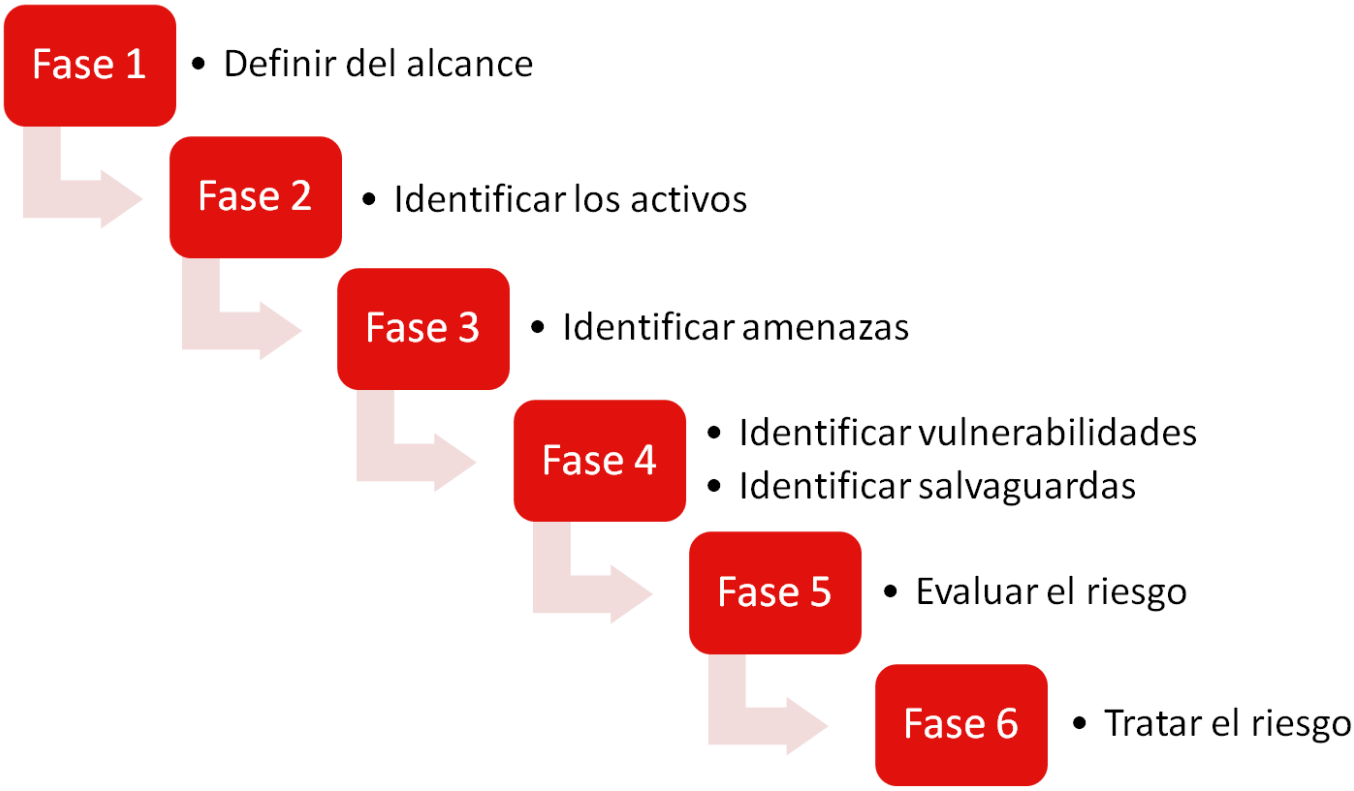
Respuestas.

Introducción

Como se puede observar en el ejercicio propuesto y, concretamente, el orden de las preguntas, vemos claramente que seguir las preguntas es seguir el Método de análisis de riesgos que ofrece la web del incibe en el siguiente entrada de blog titulado ¡Fácil y sencillo! Análisis de riesgos en 6 pasos, esta web será la que usaremos principalmente de **fuente** para la realización del análisis de riesgos por las siguientes razones:

- El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.
    - Entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.
    - La misión de INCIBE: reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información.
- Cabe destacar que el CNI-CCN tiene su scope enfocado a los siguientes sectores:
    - Sector público,
    - Sistemas información clasificada
    - Empresas de interés estratégico, estas se definen según la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y se resumen en:
        - Servicios de salud como Hospitales, ambulatorios... ya sean de la de entidades publicas o privadas.
        - Entidades financieras y bancarias.
        - Proveedores de servicios digitales.
        - Empresas encargadas de Servicios de Abastecimiento de aguas y saneamiento de aguas residuales.
        - Empresas de Transporte.
        - Infraestructuras digitales.
        - Energía.
- El ejercicio se identifica con una PYME la cual no tiene Interés Estratégico.
- Por todo lo anterior, se coliga que la referencia a utilizar es INCIBE.

Destacar también que en la siguiente imagen, declara orden por orden la realización de la realización de un análisis de riesgos, siendo la fase 1 (Alcance del sistema) el enunciado del problema.



> Imagen explicativa de las fases del análisis de riesgos de la web del citado blog incibe.

1. Identifica todos los activos que observas en la PYME y agrúpalos en una columna utilizando los tipos que indica MAGERIT en sus buenas prácticas.

Primeramente, se procederá a identificar todos los activos de la empresa, los cuales se clasificarán por tipo según lo solicitado en el enunciado, posteriormente, se procederá a la elaboración de una tabla, siguiendo la guía de elaboración de análisis de riesgos publicado en el portal web de incibe, a continuación de una tabla tal y como se especifica en la siguiente imagen:

De acuerdo el enunciado, se ha identificado los siguientes activos en la PYME "Pepe Gotera y Otilio", estos activos han sido agrupado según los tipos que indica MAGERIT en sus buenas prácticas:

1. Información:
    - Datos de clientes (direcciones, acciones a realizar, etc.).
    - Contabilidad y temas legales.
    - Datos de contratación de personal.
2. Personal:
    - Directora Ofelia.
    - Ayudante de oficina.
    - Técnico de sistemas Sr. Bacterio.
    - Trabajadores de campo: Pepe y Otilio.
3. Equipos y sistemas:
    - Portátil de la Directora Ofelia.
    - Portátil del ayudante de oficina.
    - Portátil del técnico de sistemas Sr. Bacterio.
    - Smartphones de Pepe y Otilio.
4. Infraestructura tecnológica:

- 2 servidores Windows 2019 Server (uno para correo/DNS y otro para portal HTTP/HTTPS y base de datos MySQL).
- 2 Firewalls (uno de protección al exterior y otro a la red interna).
- Rack (armario) para servidores.
- Conexión a Internet de fibra óptica a 600 MB.
- Puestos de trabajo cableados.

5. Software:
   - Sistema operativo Windows 10 en portátiles
   - Herramientas ofimáticas Microsoft Office
   - Antivirus
   - Sistema operativo Windows 2019 Server en servidores
   - Base de datos MySQL

A continuación, se procede a realizar una tabla identificando cada uno de los activos según la imagen anterior.

ID activo	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico (Si/no)
1	Datos de clientes	Información de clientes (direcciones, acciones a realizar, etc.)	Ofelia	Información	Base de datos MySQL	Sí
2	Contabilidad y temas legales	Documentos e información relacionados con contabilidad y asuntos legales	Ofelia	Información	Portátil de Ofelia	Sí
3	Datos de contratación de personal	Información sobre contrataciones y empleados	Ofelia	Información	Portátil de Ofelia	Sí
4	Directora Ofelia	Encargada de la dirección, contabilidad, contratación y temas legales	N/A	Personal	Oficina	Sí

ID activo	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico (Si/no)
5	Ayudante de oficina	Asistente para la gestión de correos, llamadas y acciones comerciales	Ofelia	Personal	Oficina	Sí
6	Técnico de sistemas Sr. Bacterio	Responsable de la administración de sistemas informáticos y parches	Ofelia	Personal	Oficina	Sí
7	Trabajador de campo Pepe	Trabajador de campo realizando reformas y reparaciones	Ofelia	Personal	Trabajo de campo	Sí
8	Trabajador de campo Otilio	Trabajador de campo realizando reformas y reparaciones	Ofelia	Personal	Trabajo de campo	Sí
9	Portátil Ofelia	Portátil utilizado por Ofelia para gestionar la empresa	Ofelia	Equipos y sistemas	Oficina	Sí
10	Portátil ayudante	Portátil utilizado por el ayudante de oficina para gestionar correos y llamadas	Ayudante de oficina	Equipos y sistemas	Oficina	No

ID activo	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico (Si/no)
11	Portátil Sr. Bacterio	Portátil utilizado por el técnico de sistemas para administrar sistemas informáticos	Sr. Bacterio	Equipos y sistemas	Oficina	Sí
12	Smartphone Pepe	Smartphone utilizado por Pepe para comunicación y acceso a información de clientes	Sr. Bacterio	Equipos y sistemas	Trabajo de campo	Si
13	Smartphone Otilio	Smartphone utilizado por Otilio para comunicación y acceso a información de clientes	Sr. Bacterio	Equipos y sistemas	Trabajo de campo	Si
14	Servidor correo/DNS	Servidor Windows 2019 para correo y DNS	Sr. Bacterio	Infraestructura tecnológica	Rack en oficina	Sí
15	Servidor portal/MySQL	Servidor Windows 2019 para portal HTTP/HTTPS y base de datos MySQL	Sr. Bacterio	Infraestructura tecnológica	Rack en oficina	Sí
16	Firewalls	Dispositivos para proteger la red interna y externa	Sr. Bacterio	Infraestructura tecnológica	Rack en oficina	Sí
17	Rack	Armario para alojar servidores y firewalls	Sr. Bacterio	Infraestructura tecnológica	Oficina	No

ID activo	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico (Si/no)
18	Conexión a Internet	Fibra óptica a 600 MB para conexión a Internet	Sr. Bacterio	Infraestructura tecnológica	Oficina	Sí
19	Puestos de trabajo cableados	Conexiones cableadas de red para conectar los portátiles de Ofelia, el ayudante y Sr. Bacterio	Sr. Bacterio	Infraestructura tecnológica	Oficina	No
20	Sistema operativo Windows 10	Sistema operativo en portátiles de Ofelia, ayudante y Sr. Bacterio	Sr. Bacterio	Software	Portátiles	No
21	Microsoft Office	Herramientas ofimáticas utilizadas en los portátiles	Sr. Bacterio	Software	Portátiles	No
22	Antivirus	Software de protección contra malware y virus en portátiles	Sr. Bacterio	Software	Portátiles	Sí
23	Sistema operativo Windows 2019 Server	Sistema operativo en servidores de correo/DNS y portal/MySQL	Sr. Bacterio	Software	Servidores	Sí
24	Base de datos MySQL	Sistema de gestión de base de datos en servidor portal/MySQL	Sr. Bacterio	Software	Servidor portal/MySQL	Sí

2. Identifica para cada activo las Amenazas que pueden tener.

Identificar las amenazad es un proceso posterior a la identificación de los activos, para que estas amenazas tengan consistencia, tienen que tener una relación con los activos ya que si no tiene relación esta amenaza con los activos, estas amenazas no tendrían cabida en este análisis de riesgos, tampoco un riesgo no es un riesgo en sí si no afecta como mínimo a un o de los pilares de la ciberseguridad estudiados en este MASTER en otras asignaturas, Integridad, Confidencialidad, Disponibilidad, Trazabilidad y No repudio.

Por todo lo anteriormente expuesto en el párrafo anterior se procede, para cada activo y para que sea mas fácilmente entendible, a realizar una tabla con las siguientes columnas:

- ID de la amenaza.
    - Será un identificador que relaciona el activo con la amenaza.
- Nombre del activo que sufre la amenaza.
- Tipo de activo.
- Nombre de la amenaza.
- Descripción de la amenaza.
- Pilares de la ciberseguridad que afecta.
    - Integridad, Confidencialidad, Disponibilidad, Trazabilidad, No repudio.

ID de Amenaza	**Activo**	**Tipo de Activo**	**Nombre de la amenaza**	**Descripción de la amenaza**	**Pilares de la ciberseguridad que afecta**
1_1	Datos de clientes	Información	Acceso no autorizado	Acceso a información de clientes por personal no autorizado o atacantes externos	Confidencialidad
1_2	Datos de clientes	Información	Manipulación de datos	Alteración de la información de clientes de manera intencional o accidental	Integridad
1_3	Datos de clientes	Información	Pérdida de datos	Pérdida de información de clientes debido a fallos del sistema, errores humanos o ataques maliciosos	Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
1_4	Datos de clientes	Información	Divulgación involuntaria	Divulgación de información de clientes a terceros no autorizados debido a errores humanos o fallas en la seguridad	Confidencialidad
2_1	Contabilidad y temas legales	Información	Acceso no autorizado	Acceso a información de contabilidad y temas legales por personal no autorizado o atacantes externos	Confidencialidad
2_2	Contabilidad y temas legales	Información	Manipulación de datos	Alteración de la información de contabilidad y temas legales de manera intencional o accidental	Integridad
2_3	Contabilidad y temas legales	Información	Pérdida de datos	Pérdida de información de contabilidad y temas legales debido a fallos del sistema, errores humanos o ataques maliciosos	Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
2_4	Contabilidad y temas legales	Información	Divulgación involuntaria	Divulgación de información de contabilidad y temas legales a terceros no autorizados debido a errores humanos o fallas en la seguridad	Confidencialidad
3_1	Datos de contratación de personal	Información	Acceso no autorizado	Acceso a información de contratación de personal por personal no autorizado o atacantes externos	Confidencialidad
3_2	Datos de contratación de personal	Información	Manipulación de datos	Alteración de la información de contratación de personal de manera intencional o accidental	Integridad
3_3	Datos de contratación de personal	Información	Pérdida de datos	Pérdida de información de contratación de personal debido a fallos del sistema, errores humanos o ataques maliciosos	Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
3_4	Datos de contratación de personal	Información	Divulgación involuntaria	Divulgación de información de contratación de personal a terceros no autorizados debido a errores humanos o fallas en la seguridad	Confidencialidad
4_1	Directora Ofelia	Personal	Amenaza interna	Acciones malintencionadas o negligentes de la directora que pueden comprometer la seguridad de la información	Confidencialidad, Integridad, Disponibilidad
4_2	Directora Ofelia	Personal	Ingeniería social	Manipulación por parte de atacantes externos para obtener información confidencial	Confidencialidad, Trazabilidad, No repudio
4_3	Directora Ofelia	Personal	Errores humanos	Equivocaciones o descuidos al manejar información sensible	Confidencialidad, Integridad, Disponibilidad
5_1	Ayudante de oficina	Personal	Amenaza interna	Acciones malintencionadas o negligentes del ayudante que pueden comprometer la seguridad de la información	Confidencialidad, Integridad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
5_2	Ayudante de oficina	Personal	Ingeniería social	Manipulación por parte de atacantes externos para obtener información confidencial	Confidencialidad, Trazabilidad, No repudio
5_3	Ayudante de oficina	Personal	Errores humanos	Equivocaciones o descuidos al manejar información sensible	Confidencialidad, Integridad, Disponibilidad
6_1	Técnico de sistemas Sr. Bacterio	Personal	Amenaza interna	Acciones malintencionadas o negligentes del técnico que pueden comprometer la seguridad de los sistemas	Confidencialidad, Integridad, Disponibilidad
6_2	Técnico de sistemas Sr. Bacterio	Personal	Ingeniería social	Manipulación por parte de atacantes externos para obtener acceso a sistemas y recursos	Confidencialidad, Trazabilidad, No repudio
6_3	Técnico de sistemas Sr. Bacterio	Personal	Errores humanos	Equivocaciones o descuidos al administrar sistemas y aplicar parches de seguridad	Confidencialidad, Integridad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
6_4	Técnico de sistemas Sr. Bacterio	Personal	Vulnerabilidades no parcheadas	Incapacidad para identificar o aplicar parches de seguridad a tiempo, dejando los sistemas expuestos a amenazas	Confidencialidad, Integridad, Disponibilidad
7_1	Trabajador de campo Pepe	Personal	Robo o pérdida del smartphone	Pérdida o robo del dispositivo de Pepe mientras trabaja en el campo	Confidencialidad, Disponibilidad
7_2	Trabajador de campo Pepe	Personal	Acceso no autorizado al smartphone	Acceso por parte de terceros no autorizados a la información almacenada en el smartphone	Confidencialidad, Integridad, Trazabilidad
7_3	Trabajador de campo Pepe	Personal	Infección por malware o virus	Infección del smartphone de Pepe por malware o virus	Integridad, Disponibilidad, Trazabilidad
8_1	Trabajador de campo Otilio	Personal	Robo o pérdida del smartphone	Pérdida o robo del dispositivo de Otilio mientras trabaja en el campo	Confidencialidad, Disponibilidad
8_2	Trabajador de campo Otilio	Personal	Acceso no autorizado al smartphone	Acceso por parte de terceros no autorizados a la información almacenada en el smartphone	Confidencialidad, Integridad, Trazabilidad
8_3	Trabajador de campo Otilio	Personal	Infección por malware o virus	Infección del smartphone de Otilio por malware o virus	Integridad, Disponibilidad, Trazabilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
9_1	Portátil Ofelia	Equipos y sistemas	Robo o pérdida del portátil	Pérdida o robo del portátil de Ofelia, que contiene información crítica de la empresa	Confidencialidad, Disponibilidad
9_2	Portátil Ofelia	Equipos y sistemas	Acceso no autorizado al portátil	Acceso por parte de terceros no autorizados a la información almacenada en el portátil	Confidencialidad, Integridad, Trazabilidad, No repudio
9_3	Portátil Ofelia	Equipos y sistemas	Infección por malware o virus	Infección del portátil de Ofelia por malware o virus	Integridad, Disponibilidad, Trazabilidad
9_4	Portátil Ofelia	Equipos y sistemas	Ataque de phishing	Ataque de phishing dirigido a Ofelia a través de su correo electrónico	Confidencialidad, Integridad, Trazabilidad, No repudio
9_5	Portátil Ofelia	Equipos y sistemas	Ataque DDoS	Ataque DDoS que impide el acceso a recursos y servicios en el portátil de Ofelia	Disponibilidad
9_6	Portátil Ofelia	Equipos y sistemas	Ataque de fuerza bruta	Ataque de fuerza bruta para obtener acceso no autorizado al portátil de Ofelia	Confidencialidad, Integridad, Trazabilidad, No repudio

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
10_1	Portátil ayudante	Equipos y sistemas	Robo o pérdida del portátil	El portátil del ayudante puede ser robado o extraviado, resultando en la exposición de información confidencial	Confidencialidad, Disponibilidad
10_2	Portátil ayudante	Equipos y sistemas	Ataque de malware	El portátil del ayudante puede ser infectado con malware, lo que podría resultar en la corrupción de datos o el acceso no autorizado a información	Integridad, Confidencialidad
10_3	Portátil ayudante	Equipos y sistemas	Acceso no autorizado	Alguien sin permiso puede obtener acceso al portátil del ayudante, lo que podría llevar a la exposición o alteración de datos	Integridad, Confidencialidad, Trazabilidad
11_1	Portátil Sr. Bacterio	Equipos y sistemas	Robo o pérdida del portátil	El portátil del Sr. Bacterio puede ser robado o extraviado, lo que podría resultar en la exposición de información confidencial y comprometer la seguridad de la red	Confidencialidad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
11_2	Portátil Sr. Bacterio	Equipos y sistemas	Ataque de malware	El portátil del Sr. Bacterio puede ser infectado con malware, lo que podría resultar en la corrupción de datos, acceso no autorizado a información o comprometer la seguridad de la red	Integridad, Confidencialidad
11_3	Portátil Sr. Bacterio	Equipos y sistemas	Acceso no autorizado	Alguien sin permiso puede obtener acceso al portátil del Sr. Bacterio, lo que podría llevar a la exposición o alteración de datos, así como comprometer la seguridad de la red	Integridad, Confidencialidad, Trazabilidad
12_1	Smartphone Pepe	Equipos y sistemas	Robo o pérdida del smartphone	El smartphone de Pepe puede ser robado o extraviado, lo que podría resultar en la exposición de información confidencial	Confidencialidad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
12_2	Smartphone Pepe	Equipos y sistemas	Ataque de malware	El smartphone de Pepe puede ser infectado con malware, lo que podría resultar en la corrupción de datos o el acceso no autorizado a información	Integridad, Confidencialidad
12_3	Smartphone Pepe	Equipos y sistemas	Acceso no autorizado	Alguien sin permiso puede obtener acceso al smartphone de Pepe, lo que podría llevar a la exposición o alteración de datos	Integridad, Confidencialidad, Trazabilidad
12_4	Smartphone Pepe	Equipos y sistemas	Pérdida de conexión	El smartphone de Pepe puede experimentar problemas de conectividad, lo que podría afectar su capacidad para comunicarse y acceder a la información de los clientes	Disponibilidad
13_1	Smartphone Otilio	Equipos y sistemas	Pérdida o robo del dispositivo	El smartphone de Otilio puede ser perdido o robado, exponiendo información confidencial y comprometiendo la seguridad de la empresa	Confidencialidad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
13_2	Smartphone Otilio	Equipos y sistemas	Infección por malware	El smartphone de Otilio puede ser infectado por malware, lo que puede resultar en la exposición de datos, interrupción del servicio o daños en el dispositivo	Integridad, Confidencialidad, Disponibilidad
13_3	Smartphone Otilio	Equipos y sistemas	Acceso no autorizado	Un atacante puede obtener acceso no autorizado al smartphone de Otilio y acceder a la información y sistemas de la empresa	Confidencialidad, Integridad
14_1	Servidor correo/DNS	Infraestructura tecnológica	Ataque DDoS	El servidor de correo/DNS puede ser objetivo de un ataque DDoS, lo que puede causar interrupciones en los servicios de correo y DNS	Disponibilidad
14_2	Servidor correo/DNS	Infraestructura tecnológica	Vulnerabilidades no parcheadas	El servidor de correo/DNS puede tener vulnerabilidades no parcheadas que permitan a un atacante acceder a la información y comprometer la seguridad de la empresa	Confidencialidad, Integridad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
14_3	Servidor correo/DNS	Infraestructura tecnológica	Phishing y suplantación de identidad	El servidor de correo/DNS puede ser utilizado para realizar ataques de phishing y suplantación de identidad, comprometiendo la seguridad de la empresa y sus clientes	Confidencialidad, Integridad, Trazabilidad, No repudio
15_1	Servidor portal/MySQL	Infraestructura tecnológica	Inyección SQL	El servidor portal/MySQL puede ser vulnerable a ataques de inyección SQL, permitiendo a un atacante acceder a la base de datos y comprometer la seguridad de la información	Confidencialidad, Integridad, Disponibilidad
15_2	Servidor portal/MySQL	Infraestructura tecnológica	Vulnerabilidades no parcheadas	El servidor portal/MySQL puede tener vulnerabilidades no parcheadas que permitan a un atacante acceder a la información y comprometer la seguridad de la empresa	Confidencialidad, Integridad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
15_3	Servidor portal/MySQL	Infraestructura tecnológica	Acceso no autorizado	Un atacante puede obtener acceso no autorizado al servidor portal/MySQL y acceder a la información y sistemas de la empresa	Confidencialidad, Integridad, Disponibilidad
16_1	Firewalls	Infraestructura tecnológica	Ataque externo	Intento de acceso no autorizado a la red de la empresa por parte de un atacante externo	Confidencialidad, Integridad, Disponibilidad
16_2	Firewalls	Infraestructura tecnológica	Vulnerabilidades de software	Fallo en el software del firewall que puede ser explotado por un atacante para comprometer la red	Confidencialidad, Integridad, Disponibilidad
16_3	Firewalls	Infraestructura tecnológica	Configuración incorrecta	Errores en la configuración del firewall que pueden permitir el acceso no autorizado o filtraciones de información	Confidencialidad, Integridad, Disponibilidad
16_4	Firewalls	Infraestructura tecnológica	Fallo de hardware	Un fallo en el hardware del firewall puede provocar una interrupción en la protección de la red	Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
17_1	Rack	Infraestructura tecnológica	Acceso físico no autorizado	Acceso no autorizado al rack que aloja servidores y firewalls, permitiendo la manipulación o robo de equipos	Confidencialidad, Integridad, Disponibilidad
17_2	Rack	Infraestructura tecnológica	Daños ambientales	Daños causados por desastres naturales, incendios, inundaciones o problemas eléctricos que afectan al rack y sus componentes	Disponibilidad
18_1	Conexión a Internet	Infraestructura tecnológica	Interrupción del servicio	Pérdida de la conexión a Internet debido a problemas con el proveedor de servicios de Internet, daños en la infraestructura o ataques DDoS	Disponibilidad
18_2	Conexión a Internet	Infraestructura tecnológica	Intercepción de datos	Captura y monitoreo no autorizado de datos transmitidos a través de la conexión a Internet	Confidencialidad, Trazabilidad, No repudio

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
18_3	Conexión a Internet	Infraestructura tecnológica	Manipulación del tráfico	Un atacante altera o redirige el tráfico de Internet de la empresa para acceder a datos confidenciales o interrumpir las comunicaciones	Confidencialidad, Integridad, Disponibilidad, Trazabilidad, No repudio
19_1	Puestos de trabajo cableados	Infraestructura tecnológica	Acceso no autorizado	Personas no autorizadas pueden acceder a la red interna a través de los puestos de trabajo cableados	Confidencialidad, Integridad
19_2	Puestos de trabajo cableados	Infraestructura tecnológica	Manipulación física	Ataques físicos a los cables de red, como cortar o dañar los cables, pueden afectar la conexión	Disponibilidad
19_3	Puestos de trabajo cableados	Infraestructura tecnológica	Intercepción de tráfico	Interceptar el tráfico de red en los puestos de trabajo cableados a través de técnicas como el sniffing	Confidencialidad, Trazabilidad
20_1	Sistema operativo Windows 10	Software	Vulnerabilidades del sistema operativo	Explotación de vulnerabilidades no parcheadas en el sistema operativo Windows 10	Confidencialidad, Integridad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
20_2	Sistema operativo Windows 10	Software	Malware	Infección por malware como virus, troyanos o ransomware en los portátiles con Windows 10	Confidencialidad, Integridad, Disponibilidad
20_3	Sistema operativo Windows 10	Software	Ataques de fuerza bruta	Ataques de fuerza bruta para obtener acceso a las cuentas de usuario en los portátiles con Windows 10	Confidencialidad, Integridad
21_1	Microsoft Office	Software	Vulnerabilidades de Microsoft Office	Explotación de vulnerabilidades en las herramientas de Microsoft Office	Confidencialidad, Integridad, Disponibilidad
21_2	Microsoft Office	Software	Phishing y malware a través de documentos de Office	Envío de documentos maliciosos que explotan vulnerabilidades o engañan al usuario para obtener información confidencial	Confidencialidad, Integridad
21_3	Microsoft Office	Software	Pérdida de datos	Pérdida o corrupción de datos almacenados en documentos de Microsoft Office debido a errores humanos o de software	Integridad, Disponibilidad, Trazabilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
22_1	Antivirus	Software	Ataque de malware	Infección del software antivirus por malware específico diseñado para desactivarlo o eludirlo	Integridad, Confidencialidad, Disponibilidad
22_2	Antivirus	Software	Vulnerabilidades no parcheadas	Explotación de vulnerabilidades del antivirus que no han sido parcheadas por el fabricante	Integridad, Confidencialidad, Disponibilidad
22_3	Antivirus	Software	Desactualización	Uso de una versión desactualizada del software antivirus que no detecta las últimas amenazas	Integridad, Confidencialidad, Disponibilidad
23_1	Sistema operativo Windows 2019 Server	Software	Ataques de fuerza bruta	Intento de acceso no autorizado a través de ataques de fuerza bruta en cuentas de usuario	Confidencialidad, Disponibilidad, Trazabilidad
23_2	Sistema operativo Windows 2019 Server	Software	Vulnerabilidades del sistema operativo	Explotación de vulnerabilidades conocidas o desconocidas en el sistema operativo	Integridad, Confidencialidad, Disponibilidad

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	Descripción de la amenaza	Pilares de la ciberseguridad que afecta
23_3	Sistema operativo Windows 2019 Server	Software	Configuración insegura	Configuraciones incorrectas o inseguras que permiten el acceso no autorizado	Integridad, Confidencialidad, Disponibilidad, Trazabilidad
24_1	Base de datos MySQL	Software	Inyección SQL	Explotación de vulnerabilidades en la base de datos mediante inyecciones SQL para extraer o modificar información	Integridad, Confidencialidad, Trazabilidad, No repudio
24_2	Base de datos MySQL	Software	Acceso no autorizado	Acceso indebido a la base de datos por parte de usuarios internos o externos	Confidencialidad, Integridad, Disponibilidad, Trazabilidad
24_3	Base de datos MySQL	Software	Ataque DDoS	Ataque de denegación de servicio que impide el acceso a la base de datos	Disponibilidad
24_4	Base de datos MySQL	Software	Fuga de información	Fuga de datos sensible almacenados en la base de datos debido a fallos de seguridad o malas prácticas	Confidencialidad, Integridad, Trazabilidad, No repudio

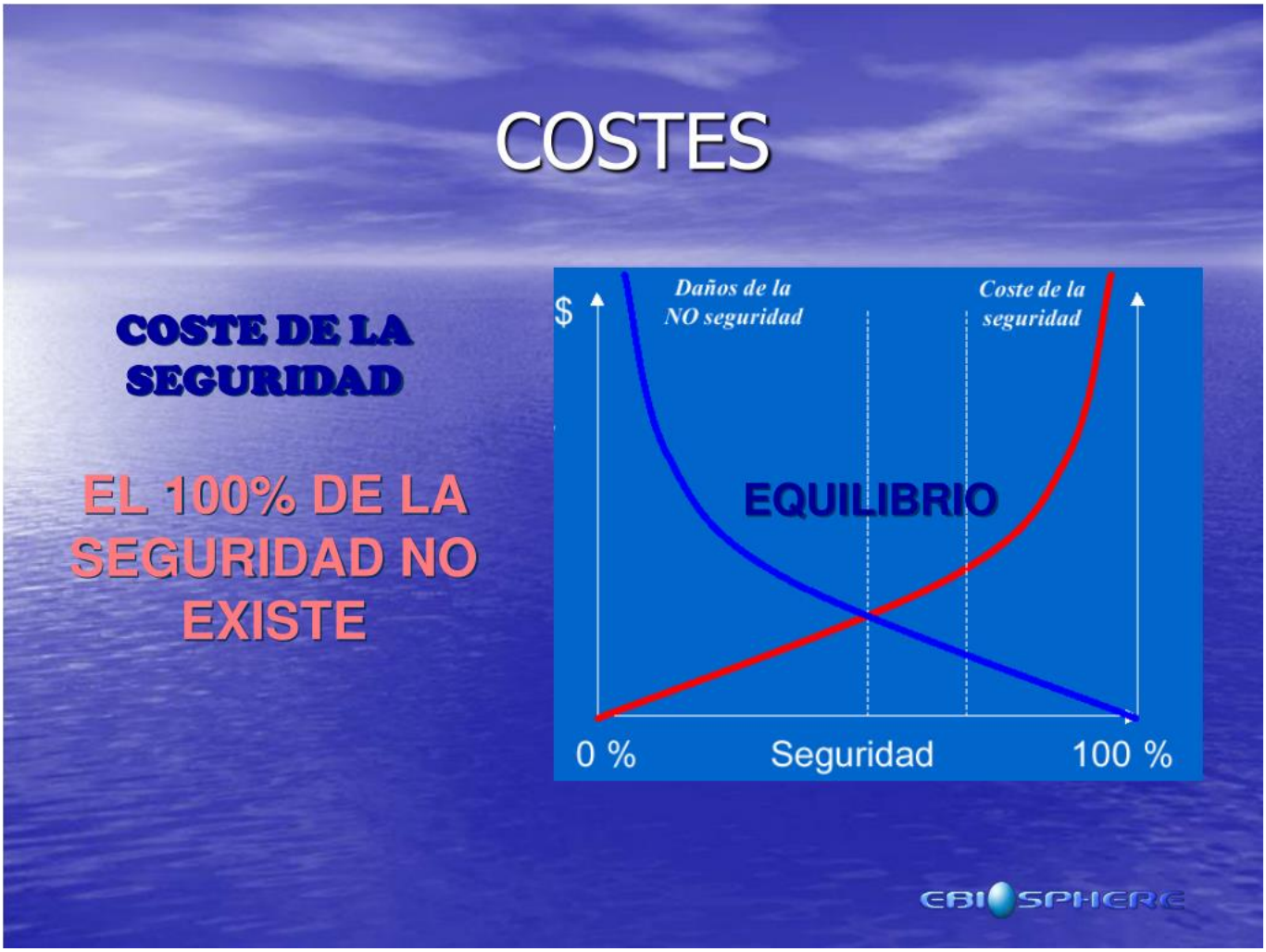
CONCLUSIONES A LAS TABLAS DE LAS AMENAZAS:

- Como es de esperar, a cada uno de los activos, pueden tener varias amenazas, resultando lógico que resulte una multiplicación del tipo de primer grado.
    - es decir 0 ≤ (Nº de amenazas) ≤ (Nº de activos)^2.
    - En este caso, de 24 activos, han resultado un total de 81 amenazas posibles, siendo resultado una relación (Nº de amenazas) = 3.375 x (Nº de activos) y cumpliéndose la formula del apartado anterior. como 3.375 ≤ (Nº de activos), se cumple la condición anterior.
    - Relativo a este punto, cabe destacar que este modelo de validación es valido cuando la entidad de activos es lo suficientemente grande, ya que el enunciado se pueden abstraer un numero amplio de activos, 24, y hacer al menos 2 o 3 amenazas por activo.
- Como se puede observar, se pueden clasificar muchas amenazas por tipo de información, ya que el caso de los activos de información, cada uno de ellos tienen los mismo tipos de amenaza.
- A colación de lo anterior, en el apartado personal, podemos diferenciar de usuario de oficina con una serie de amenazas que son idénticas, exceptuando una particular del Sr. Bacterio (`Vulnerabilidades no parcheadas`). Por otro lado, Los trabajadores de campo, también tienen unas vulnerabilidades distintas por ser trabajadores de campo y usar dispositivos móviles.
- Relativo a equipos y sistemas, pasa lo mismo que en el primer apartado, tienen una serie de amenazas propias del tipo de dispositivo (`Robo o pérdida`, `Acceso no autorizado`,`Infección por malware o virus`) y otras mas especificas como puede ser `ataque de phishing` al portátil de Ofelia o también conocido como phishing al CEO.
- Mismo caso para los activos de Infraestructura tecnológica, pero es de lógica que no vas a hacer una injection SQL al servidor DNS, le harías un ataque DDoS, también como el caso de los firewall que pueden estar mal configurados. Por otro lado relativo al Rack, lugar donde se instalan los servidores, son mas ataques del tipo físico ya que es ina infraestructura en sí y no tiene parte de información del mismo, pero si sus amenazas pueden afectar en el sistema. Relativo a Conexión de Internet y a la red cableada de la oficina, como al fin y al cabo la red cableada depende del router y su funcionamiento, ya que es este dispositivo quien enruta a un equipo u otro conectado o permite su acceso al exterior. Las amenazas son las mismas.
- Por ultimo relativo a las amenazas de tipo software, cabe destacar la importancia de los parches de actualizaciones de los mismos, y después los ataques que se cada uno de los tipos de ataques que se pueden hacer a cada uno de los distintos software.
- Como ya he indicado anteriormente, para la definición de una amenaza o no, es necesario indicar que pilar de la ciberseguridad vulnera, para asi tener claro a que esta afectando, asi poder después definir mejor las salvaguardas.
- Cabe destacar por ultimo, que en activos como los trabajadores Pepe y Otilio tienen amenazas relativas a `Infección por malware o virus`, en estos caso hago mas referencia a que puedan utilizar el móvil para uso personal, el cual no se indica expresamente ni tampoco lo indica el enunciado, pero es de interés que por parte del personal pueda ser instalado aplicaciones no deseadas ya que puedan ser del **tipo BYOD (Bring Your Own Device)** o del **tipo COPE (Corporate owned, personally enabled)**, siendo este segundo tipo una manera mas segura del manejo de la información ya que los modos personal y trabajo son totalmente estancos e independientes en el dispositivo.

---

3. Haz una valoración subjetiva del valor del activo, y de la probabilidad que se materialice una amenaza, así como su impacto en caso de que se haga efectiva la amenaza.

En correspondencia de la web de utilizada como fuente, este utiliza unos valores distintos, no incluyendo la dimension de valor del activo, que indicando como reflexión personal, esta dimension afecta a los costes de la empresa y, teniendo en cuenta lo indicado en el siguiente gráfico. Considero necesario para una empresa de cualquier índole añadir el valor económico.



> En esta imagen se detalla cuando los valores de seguridad son eficientes frente a los costes de exposición, indicando que hay que tomar una solución de compromiso entre el coste de exposición (daños de la no seguridad) y el coste de la seguridad implementada, teniendo en cuenta que la seguridad al 100% no existe.

En relación con el párrafo anterior, el valor del activo se debe de añadir al coste de exposición como una dimensión mas. cosa que nuestra fuente de referencia, **INCIBE** en el blog dedicado a un análisis de riesgos, no implementa.

A continuación, se muestra una tabla con todas las amenazas anteriores indicando de manera subjetiva el valor del activo, la probabilidad de materialización de la amenaza y el impacto del mismo.

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto
1_1	Datos de clientes	Acceso no autorizado	Alto	Normal	Alto
1_2	Datos de clientes	Manipulación de datos	Alto	Bajo	Alto
1_3	Datos de clientes	Pérdida de datos	Alto	Bajo	Muy alto
1_4	Datos de clientes	Divulgación involuntaria	Alto	Bajo	Alto
2_1	Contabilidad y temas legales	Acceso no autorizado	Alto	Normal	Alto
2_2	Contabilidad y temas legales	Manipulación de datos	Alto	Bajo	Alto
2_3	Contabilidad y temas legales	Pérdida de datos	Alto	Bajo	Muy alto
2_4	Contabilidad y temas legales	Divulgación involuntaria	Alto	Bajo	Alto
3_1	Datos de contratación de personal	Acceso no autorizado	Normal	Bajo	Alto
3_2	Datos de contratación de personal	Manipulación de datos	Normal	Bajo	Normal
3_3	Datos de contratación de personal	Pérdida de datos	Normal	Bajo	Alto
3_4	Datos de contratación de personal	Divulgación involuntaria	Normal	Bajo	Normal
4_1	Directora Ofelia	Amenaza interna	Muy alto	Bajo	Muy alto
4_2	Directora Ofelia	Ingeniería social	Muy alto	Bajo	Alto
4_3	Directora Ofelia	Errores humanos	Muy alto	Normal	Normal
5_1	Ayudante de oficina	Amenaza interna	Normal	Bajo	Normal

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto
5_2	Ayudante de oficina	Ingeniería social	Normal	Normal	Normal
5_3	Ayudante de oficina	Errores humanos	Normal	Normal	Normal
6_1	Técnico de sistemas Sr. Bacterio	Amenaza interna	Alto	Bajo	Normal
6_2	Técnico de sistemas Sr. Bacterio	Ingeniería social	Alto	Normal	Normal
6_3	Técnico de sistemas Sr. Bacterio	Errores humanos	Alto	Normal	Normal
6_4	Técnico de sistemas Sr. Bacterio	Vulnerabilidades no parcheadas	Alto	Normal	Alto
7_1	Trabajador de campo Pepe	Robo o pérdida del smartphone	Normal	Bajo	Bajo
7_2	Trabajador de campo Pepe	Acceso no autorizado al smartphone	Normal	Bajo	Bajo
7_3	Trabajador de campo Pepe	Infección por malware o virus	Normal	Normal	Bajo
8_1	Trabajador de campo Otilio	Robo o pérdida del smartphone	Normal	Bajo	Bajo
8_2	Trabajador de campo Otilio	Acceso no autorizado al smartphone	Normal	Bajo	Bajo
8_3	Trabajador de campo Otilio	Infección por malware o virus	Normal	Normal	Bajo
9_1	Portátil Ofelia	Robo o pérdida del portátil	Normal	Bajo	Bajo
9_2	Portátil Ofelia	Acceso no autorizado al portátil	Normal	Bajo	Normal
9_3	Portátil Ofelia	Infección por malware o virus	Normal	Normal	Normal
9_4	Portátil Ofelia	Ataque de phishing	Normal	Normal	Normal

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto
9_5	Portátil Ofelia	Ataque DDoS	Normal	Bajo	Muy Bajo
9_6	Portátil Ofelia	Ataque de fuerza bruta	Normal	Bajo	Normal
10_1	Portátil ayudante	Robo o pérdida del portátil	Normal	Bajo	Bajo
10_2	Portátil ayudante	Ataque de malware	Normal	Normal	Normal
10_3	Portátil ayudante	Acceso no autorizado	Normal	Bajo	Bajo
11_1	Portátil Sr. Bacterio	Robo o pérdida del portátil	Normal	Bajo	Bajo
11_2	Portátil Sr. Bacterio	Ataque de malware	Normal	Normal	Normal
11_3	Portátil Sr. Bacterio	Acceso no autorizado	Normal	Bajo	Bajo
12_1	Smartphone Pepe	Robo o pérdida del smartphone	Bajo	Bajo	Bajo
12_2	Smartphone Pepe	Ataque de malware	Bajo	Bajo	Bajo
12_3	Smartphone Pepe	Acceso no autorizado	Bajo	Bajo	Bajo
12_4	Smartphone Pepe	Pérdida de conexión	Bajo	Muy bajo	Bajo
13_1	Smartphone Otilio	Pérdida o robo del dispositivo	Bajo	Bajo	Bajo
13_2	Smartphone Otilio	Infección por malware	Bajo	Bajo	Bajo
13_3	Smartphone Otilio	Acceso no autorizado	Bajo	Bajo	Bajo
14_1	Servidor correo/DNS	Ataque DDoS	Alto	Normal	Alto
14_2	Servidor correo/DNS	Vulnerabilidades no parcheadas	Alto	Normal	Normal
14_3	Servidor correo/DNS	Phishing y suplantación de identidad	Alto	Bajo	Normal
15_1	Servidor portal/MySQL	Inyección SQL	Alto	Normal	Alto

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto
15_2	Servidor portal/MySQL	Vulnerabilidades no parcheadas	Alto	Normal	Normal
15_3	Servidor portal/MySQL	Acceso no autorizado	Alto	Bajo	Normal
16_1	Firewalls	Ataque externo	Alto	Bajo	Normal
16_2	Firewalls	Vulnerabilidades de software	Alto	Normal	Normal
16_3	Firewalls	Configuración incorrecta	Alto	Bajo	Bajo
16_4	Firewalls	Fallo de hardware	Alto	Muy bajo	Bajo
17_1	Rack	Acceso físico no autorizado	Normal	Bajo	Normal
17_2	Rack	Daños ambientales	Normal	Muy bajo	Normal
18_1	Conexión a Internet	Interrupción del servicio	Normal	Bajo	Normal
18_2	Conexión a Internet	Intercepción de datos	Normal	Bajo	Normal
18_3	Conexión a Internet	Manipulación del tráfico	Normal	Bajo	Normal
19_1	Puestos de trabajo cableados	Acceso no autorizado	Normal	Bajo	Normal
19_2	Puestos de trabajo cableados	Manipulación física	Normal	Muy bajo	Bajo
19_3	Puestos de trabajo cableados	Intercepción de tráfico	Normal	Bajo	Normal
20_1	Sistema operativo Windows 10	Vulnerabilidades del sistema operativo	Normal	Normal	Normal
20_2	Sistema operativo Windows 10	Malware	Normal	Normal	Normal
20_3	Sistema operativo Windows 10	Ataques de fuerza bruta	Normal	Bajo	Normal
21_1	Microsoft Office	Vulnerabilidades de Microsoft Office	Normal	Normal	Normal

ID de Amenaza	Activo	Nombre de la amenaza	Valor del activo	Probabilidad que se materialice la amenaza	Impacto
21_2	Microsoft Office	Phishing y malware a través de documentos de Office	Normal	Normal	Normal
21_3	Microsoft Office	Pérdida de datos	Normal	Bajo	Normal
22_1	Antivirus	Ataque de malware	Normal	Normal	Normal
22_2	Antivirus	Vulnerabilidades no parcheadas	Normal	Normal	Normal
22_3	Antivirus	Desactualización	Normal	Bajo	Normal
23_1	Sistema operativo Windows 2019 Server	Ataques de fuerza bruta	Alto	Bajo	Normal
23_2	Sistema operativo Windows 2019 Server	Vulnerabilidades del sistema operativo	Alto	Normal	Normal
23_3	Sistema operativo Windows 2019 Server	Configuración insegura	Alto	Bajo	Normal
24_1	Base de datos MySQL	Inyección SQL	Alto	Normal	Alto
24_2	Base de datos MySQL	Acceso no autorizado	Alto	Bajo	Normal
24_3	Base de datos MySQL	Ataque DDoS	Alto	Bajo	Normal
24_4	Base de datos MySQL	Fuga de información	Alto	Bajo	Normal

CONCLUSIONES RELATIVAS A LA VALORACIÓN DE LAS AMENAZAS

- Se han realizado la valoración de las amenazas anteriormente encontradas, en el siguiente apartado al calcular su riesgo intrínseco, se procederá a valorar que amenazas se pueden descartar como tal ya que su riesgo intrínseco es muy bajo.

---

4. Calcula el riesgo intrínseco y explica cómo lo has calculado.

Para calcular el riesgo intrínseco de cada amenaza, se usará la siguiente fórmula:

RIESGO INTRÍNSECO = VALOR DEL ACTIVO x PROBABILIDAD DE QUE SE MATERIALICE LA AMENAZA x IMPACTO

Cabe destacar que en la web de **INCIBE** donde nos explican los pasos a realizar para elaborar un análisis de riesgos, nos indica que:

`A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto: RIESGO = PROBABILIDAD x IMPACTO.`

En este caso que ocupa la web solo trata el riego en las dimensiones de probabilidad e impacto, y en nuestro caso, estamos aplicando una nueva dimension.

Por otro lado, haciendo uso de los apuntes de cuando cursé la asignatura de Sistemas de Gestión de la Seguridad de la Información (M1.809) indica lo siguiente:

- `Para este estudio, únicamente es necesario realizar una multiplicación de los valores que hemos indicado hasta ahora:`
  `Riesgo = Valor del activo × Vulnerabilidad × Impacto`
  `Para MAGERIT, el estudio de la situación actual es el análisis de riesgos intrínseco, es decir, el análisis de la situación en la que se encuentra la organización en el momento del estudio aunque ya posea medidas de seguridad implanta-das.Recordemos que definimos los riesgos intrínsecos como aquellos a los que estamos expuestos sin tener en cuenta las medidas de seguridad que podamos implantar. En el caso de MAGERIT, se entiende como intrínseca la situación en la que nos encontramos teniendo en consideración todos los elementos que posee la organización`
  - Por todo lo anteriormente Expuesto, se considera valido el uso de la formula indicada en el inicio del presente apartado 4.

Para quedar de una manera mas visual, he procedido a adaptar la tabla del apartado anterior sustituyendo las columnas de `Valor del activo`, `Probabilidad que se materialice la amenaza` e `Impacto` por la columna de `Riesgo intrínseco`, en donde se realizará la operación de calculo e indicando en **negrita** el resultado cuantitativo.

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
1_1	Datos de clientes	Acceso no autorizado	2.5 x 1.5 x 2.5 = **9.375**
1_2	Datos de clientes	Manipulación de datos	2.5 x 1 x 2.5 = **6.25**
1_3	Datos de clientes	Pérdida de datos	2.5 x 1 x 3.5 = **8.75**

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
1_4	Datos de clientes	Divulgación involuntaria	2.5 x 1 x 2.5 = **6.25**
2_1	Contabilidad y temas legales	Acceso no autorizado	2.5 x 1.5 x 2.5 = **9.375**
2_2	Contabilidad y temas legales	Manipulación de datos	2.5 x 1 x 2.5 = **6.25**
2_3	Contabilidad y temas legales	Pérdida de datos	2.5 x 1 x 3.5 = **8.75**
2_4	Contabilidad y temas legales	Divulgación involuntaria	2.5 x 1 x 2.5 = **6.25**
3_1	Datos de contratación de personal	Acceso no autorizado	1.5 x 1 x 2.5 = **3.75**
3_2	Datos de contratación de personal	Manipulación de datos	1.5 x 1 x 1.5 = **2.25**
3_3	Datos de contratación de personal	Pérdida de datos	1.5 x 1 x 2.5 = **3.75**
3_4	Datos de contratación de personal	Divulgación involuntaria	1.5 x 1 x 1.5 = **2.25**
4_1	Directora Ofelia	Amenaza interna	3.5 x 1 x 3.5 = **12.25**
4_2	Directora Ofelia	Ingeniería social	3.5 x 1 x 2.5 = **8.75**
4_3	Directora Ofelia	Errores humanos	3.5 x 1.5 x 1.5 = **6.75**
5_1	Ayudante de oficina	Amenaza interna	1.5 x 1 x 1.5 = **2.25**
5_2	Ayudante de oficina	Ingeniería social	1.5 x 1.5 x 1.5 = **3.375**
5_3	Ayudante de oficina	Errores humanos	1.5 x 1.5 x 1.5 = **3.375**
6_1	Técnico de sistemas Sr. Bacterio	Amenaza interna	2.5 x 1 x 1.5 = **3.75**
6_2	Técnico de sistemas Sr. Bacterio	Ingeniería social	2.5 x 1.5 x 1.5 = **5.625**

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
6_3	Técnico de sistemas Sr. Bacterio	Errores humanos	2.5 x 1.5 x 1.5 = **5.625**
6_4	Técnico de sistemas Sr. Bacterio	Vulnerabilidades no parcheadas	2.5 x 1.5 x 2.5 = **9.375**
7_1	Trabajador de campo Pepe	Robo o pérdida del smartphone	1.5 x 1 x 1 = **1.5**
7_2	Trabajador de campo Pepe	Acceso no autorizado al smartphone	1.5 x 1 x 1 = **1.5**
7_3	Trabajador de campo Pepe	Infección por malware o virus	1.5 x 1.5 x 1 = **2.25**
8_1	Trabajador de campo Otilio	Robo o pérdida del smartphone	1.5 x 1 x 1 = **1.5**
8_2	Trabajador de campo Otilio	Acceso no autorizado al smartphone	1.5 x 1 x 1 = **1.5**
8_3	Trabajador de campo Otilio	Infección por malware o virus	1.5 x 1.5 x 1 = **2.25**
9_1	Portátil Ofelia	Robo o pérdida del portátil	1.5 x 1 x 1 = **1.5**
9_2	Portátil Ofelia	Acceso no autorizado al portátil	1.5 x 1 x 1.5 = **2.25**
9_3	Portátil Ofelia	Infección por malware o virus	1.5 x 1.5 x 1.5 = **3.375**
9_4	Portátil Ofelia	Ataque de phishing	1.5 x 1.5 x 1.5 = **3.375**
9_5	Portátil Ofelia	Ataque DDoS	1.5 x 1 x 0 = **0**
9_6	Portátil Ofelia	Ataque de fuerza bruta	1.5 x 1 x 1.5 = **2.25**
10_1	Portátil ayudante	Robo o pérdida del portátil	1.5 x 1 x 1 = **1.5**
10_2	Portátil ayudante	Ataque de malware	1.5 x 1.5 x 1.5 = **3.375**
10_3	Portátil ayudante	Acceso no autorizado	1.5 x 1 x 1 = **1.5**
11_1	Portátil Sr. Bacterio	Robo o pérdida del portátil	1.5 x 1 x 1 = **1.5**
11_2	Portátil Sr. Bacterio	Ataque de malware	1.5 x 1.5 x 1.5 = **3.375**
11_3	Portátil Sr. Bacterio	Acceso no autorizado	1.5 x 1 x 1 = **1.5**
2_1	Smartphone Pepe	Robo o pérdida del smartphone	1 x 1 x 1 = **1**
12_2	Smartphone Pepe	Ataque de malware	1 x 1 x 1 = **1**

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
12_3	Smartphone Pepe	Acceso no autorizado	1 x 1 x 1 = **1**
12_4	Smartphone Pepe	Pérdida de conexión	1 x 0 x 1 = **0**
13_1	Smartphone Otilio	Pérdida o robo del dispositivo	1 x 1 x 1 = **1**
13_2	Smartphone Otilio	Infección por malware	1 x 1 x 1 = **1**
13_3	Smartphone Otilio	Acceso no autorizado	1 x 1 x 1 = **1**
14_1	Servidor correo/DNS	Ataque DDoS	2.5 x 1.5 x 2.5 = **6.375**
14_2	Servidor correo/DNS	Vulnerabilidades no parcheadas	2.5 x 1.5 x 1.5 = **4.125**
14_3	Servidor correo/DNS	Phishing y suplantación de identidad	2.5 x 1 x 1.5 = **3.75**
15_1	Servidor portal/MySQL	Inyección SQL	2.5 x 1.5 x 2.5 = **6.375**
15_2	Servidor portal/MySQL	Vulnerabilidades no parcheadas	2.5 x 1.5 x 1.5 = **4.125**
15_3	Servidor portal/MySQL	Acceso no autorizado	2.5 x 1 x 1.5 = **3.75**
16_1	Firewalls	Ataque externo	2.5 x 1 x 1.5 = **3.75**
16_2	Firewalls	Vulnerabilidades de software	2.5 x 1.5 x 1.5 = **4.125**
16_3	Firewalls	Configuración incorrecta	2.5 x 1 x 1 = **2.5**
16_4	Firewalls	Fallo de hardware	2.5 x 0 x 1 = **0**
17_1	Rack	Acceso físico no autorizado	1.5 x 1 x 1.5 = **2.25**
17_2	Rack	Daños ambientales	1.5 x 0 x 1.5 = **0**
18_1	Conexión a Internet	Interrupción del servicio	1.5 x 1 x 1.5 = **2.25**
18_2	Conexión a Internet	Intercepción de datos	1.5 x 1 x 1.5 = **2.25**
18_3	Conexión a Internet	Manipulación del tráfico	1.5 x 1 x 1.5 = **2.25**

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
19_1	Puestos de trabajo cableados	Acceso no autorizado	1.5 x 1 x 1.5 = **2.25**
19_2	Puestos de trabajo cableados	Manipulación física	1.5 x 0 x 1 = **0**
19_3	Puestos de trabajo cableados	Intercepción de tráfico	1.5 x 1 x 1.5 = **2.25**
20_1	Sistema operativo Windows 10	Vulnerabilidades del sistema operativo	1.5 x 1.5 x 1.5 = **4.5**
20_2	Sistema operativo Windows 10	Malware	1.5 x 1.5 x 1.5 = **4.5**
20_3	Sistema operativo Windows 10	Ataques de fuerza bruta	1.5 x 1 x 1.5 = **2.25**
21_1	Microsoft Office	Vulnerabilidades de Microsoft Office	1.5 x 1.5 x 1.5 = **4.5**
21_2	Microsoft Office	Phishing y malware a través de documentos de Office	1.5 x 1.5 x 1.5 = **4.5**
21_3	Microsoft Office	Pérdida de datos	1.5 x 1 x 1.5 = **2.25**
22_1	Antivirus	Ataque de malware	1.5 x 1.5 x 1.5 = **4.5**
22_2	Antivirus	Vulnerabilidades no parcheadas	1.5 x 1.5 x 1.5 = **4.5**
22_3	Antivirus	Desactualización	1.5 x 1 x 1.5 = **2.25**
23_1	Sistema operativo Windows 2019 Server	Ataques de fuerza bruta	2.5 x 1 x 1.5 = **3.75**
23_2	Sistema operativo Windows 2019 Server	Vulnerabilidades del sistema operativo	2.5 x 1.5 x 1.5 = **6.375**
23_3	Sistema operativo Windows 2019 Server	Configuración insegura	2.5 x 1 x 1.5 = **3.75**
24_1	Base de datos MySQL	Inyección SQL	2.5 x 1.5 x 2.5 = **9.375**
24_2	Base de datos MySQL	Acceso no autorizado	2.5 x 1 x 1.5 = **3.75**

ID de Amenaza	Activo	Nombre de la amenaza	Riesgo intrínseco
24_3	Base de datos MySQL	Ataque DDoS	2.5 x 1 x 1.5 = **3.75**
24_4	Base de datos MySQL	Fuga de información	2.5 x 1 x 1.5 = **3.75**

CONCLUSIONES RELATIVAS AL RIESGO INTRÍNSECO

- Relativo a las amenazas de riesgo intrínseco son 0 cabe destacar lo siguiente:
    - El Realizar un ataque DDoS a la directora Ofelia, cabe destacar que el impacto es 0 ya que ella es la jefa del equipo, que sus trabajadores deben de estar lo suficientemente "empoderados" para tomas soluciones sin necesidad de que la Jefa, cuando este ausente de su puesto y no disponible para este ataque, sus trabajadores puedan llevar su trabajo adelante sin necesidad de autorización directa de ella, en caso de necesidad, siempre las directrices se pueden dar de manera telefónica.
    - La pérdida de conexión de red del Smartphone de Pepe es 0 debido a que la probabilidad es muy baja, cuando sea necesario adquirir información de trabajos pendientes. Por tanto, para que esta amenaza sea efectiva tiene que cumplirse a la vez los varias condiciones a la vez (AND).
    - Pepe no tiene trabajos en cola almacenados en su dispositivo.
    - Pepe necesita ver si tiene trabajos en cola.
    - Se considera no tener conexión a internet al menos durante 1 hora en las 3 infraestructuras de red móvil (suponiendo que el smartphone es 4G, ya que la 5G no esta totalmente implantada), se considera con una probabilidad inexistencial ya que hoy dia ni las lineas se saturan como pasaba en año nuevo, de hecho una forma para evitar esta deficiencia era dejar de usar la red mas rápida (pasarse de 3G a 2G) y de esta manera sigues teniendo conexión.
    - Cuando realice el enumeración de riesgos, lo valoré para ambos, pero al saber que después se iba a desechar por esta razón, no lo indiqué para el smartphone de Otilio.
    - Relativo a fallos en el hardware de un firewall, cabe destacar que pasa lo mismo que con el smartphone de los trabajadores de campo, su probabilidad de que ocurra la amenaza es muy baja

---

5. Identifica/enumera qué salvaguardas observas y valora su impacto.

En el enunciado del presente ejercicio, de manera implícita se observan las siguientes salvaguardas:

1. Control de acceso basado en roles (SV1):

- La directora Ofelia controla personalmente la parte de contabilidad, temas legales y de contratación de personal.
- Esto sugiere que existe cierto grado de control de acceso a la información en la empresa.

2. Firewalls de protección (SV2):

- La empresa cuenta con dos firewalls, uno de protección al exterior y otro a la red interna.
- Estas medidas de seguridad ayudan a proteger los sistemas de la empresa de accesos no autorizados y ataques externos.

3. Antivirus (SV3):

- Los equipos portátiles cuentan con Windows 10 y antivirus.
- El uso de antivirus ayuda a proteger los dispositivos de malware y otras amenazas de seguridad.

4. Herramientas ofimáticas seguras(SV4):

- La empresa utiliza Microsoft Office.
- Microsoft Office es una suite ofimática que incluye medidas de seguridad y protección de la información.

5. Técnico de sistemas (SV5):

- La empresa cuenta con el señor Bacterio, un técnico de sistemas que administra los sistemas informáticos y aplica parches.
- a presencia de un profesional dedicado a mantener y proteger los sistemas informáticos es en sí misma una salvaguarda.

Una vez identificado las salvaguardas, se proceden a asociarlas a las amenazas y a calcular el impacto del mismo sobre la salvaguarda de manera individual.

ID de Amenaza	**Activo**	**Tipo de Activo**	**Nombre de la amenaza**	**salvaguarda para la amenaza**	**Impacto de la salvaguarda**
1_1	Datos de clientes	Información	Acceso no autorizado	SV1, SV2	Alta
1_2	Datos de clientes	Información	Manipulación de datos	SV1, SV4	Normal
1_3	Datos de clientes	Información	Pérdida de datos	SV3, SV5	Baja
1_4	Datos de clientes	Información	Divulgación involuntaria	SV1	Normal

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
2_1	Contabilidad y temas legales	Información	Acceso no autorizado	SV1, SV2	Alta
2_2	Contabilidad y temas legales	Información	Manipulación de datos	SV1, SV4	Normal
2_3	Contabilidad y temas legales	Información	Pérdida de datos	SV3, SV5	Baja
2_4	Contabilidad y temas legales	Información	Divulgación involuntaria	SV1	Normal
3_1	Datos de contratación de personal	Información	Acceso no autorizado	SV1, SV2	Alta
3_2	Datos de contratación de personal	Información	Manipulación de datos	SV1, SV4	Normal
3_3	Datos de contratación de personal	Información	Pérdida de datos	SV3, SV5	Baja
3_4	Datos de contratación de personal	Información	Divulgación involuntaria	SV1	Normal
4_1	Directora Ofelia	Personal	Amenaza interna	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
4_2	Directora Ofelia	Personal	Ingeniería social	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
4_3	Directora Ofelia	Personal	Errores humanos	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
5_1	Ayudante de oficina	Personal	Amenaza interna	No Detectada en el enunciado	No hay salvaguarda asociada al impacto

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
5_2	Ayudante de oficina	Personal	Ingeniería social	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
5_3	Ayudante de oficina	Personal	Errores humanos	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
6_1	Técnico de sistemas Sr. Bacterio	Personal	Amenaza interna	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
6_2	Técnico de sistemas Sr. Bacterio	Personal	Ingeniería social	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
6_3	Técnico de sistemas Sr. Bacterio	Personal	Errores humanos	SV5	Baja
6_4	Técnico de sistemas Sr. Bacterio	Personal	Vulnerabilidades no parcheadas	SV5	Normal
7_1	Trabajador de campo Pepe	Personal	Robo o pérdida del smartphone	SV3	Baja
7_2	Trabajador de campo Pepe	Personal	Acceso no autorizado al smartphone	SV1	Normal
7_3	Trabajador de campo Pepe	Personal	Infección por malware o virus	SV3	Normal
8_1	Trabajador de campo Otilio	Personal	Robo o pérdida del smartphone	SV3	Baja
8_2	Trabajador de campo Otilio	Personal	Acceso no autorizado al smartphone	SV1	Normal
8_3	Trabajador de campo Otilio	Personal	Infección por malware o virus	SV3	Normal

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
9_1	Portátil Ofelia	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
9_2	Portátil Ofelia	Equipos y sistemas	Acceso no autorizado al portátil	SV1, SV2	Alta
9_3	Portátil Ofelia	Equipos y sistemas	Infección por malware o virus	SV3	Normal
9_4	Portátil Ofelia	Equipos y sistemas	Ataque de phishing	SV4, SV5	Normal
9_5	Portátil Ofelia	Equipos y sistemas	Ataque DDoS	SV2	Alta
9_6	Portátil Ofelia	Equipos y sistemas	Ataque de fuerza bruta	SV2	Alta
10_1	Portátil ayudante	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
10_2	Portátil ayudante	Equipos y sistemas	Ataque de malware	SV3	Normal
10_3	Portátil ayudante	Equipos y sistemas	Acceso no autorizado	SV1, SV2	Alta
11_1	Portátil Sr. Bacterio	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
11_2	Portátil Sr. Bacterio	Equipos y sistemas	Ataque de malware	SV3, SV5	Normal
11_3	Portátil Sr. Bacterio	Equipos y sistemas	Acceso no autorizado	SV1, SV2, SV5	Alta
12_1	Smartphone Pepe	Equipos y sistemas	Robo o pérdida del smartphone	SV3	Baja
12_2	Smartphone Pepe	Equipos y sistemas	Ataque de malware	SV3	Normal

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
12_3	Smartphone Pepe	Equipos y sistemas	Acceso no autorizado	SV1	Normal
12_4	Smartphone Pepe	Equipos y sistemas	Pérdida de conexión	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
13_1	Smartphone Otilio	Equipos y sistemas	Pérdida o robo del dispositivo	SV3	Baja
13_2	Smartphone Otilio	Equipos y sistemas	Infección por malware	SV3	Baja
13_3	Smartphone Otilio	Equipos y sistemas	Acceso no autorizado	SV1	Normal
14_1	Servidor correo/DNS	Infraestructura tecnológica	Ataque DDoS	SV2	Alta
14_2	Servidor correo/DNS	Infraestructura tecnológica	Vulnerabilidades no parcheadas	SV5	Alta
14_3	Servidor correo/DNS	Infraestructura tecnológica	Phishing y suplantación de identidad	SV5	Normal
15_1	Servidor portal/MySQL	Infraestructura tecnológica	Inyección SQL	SV5	Alta
15_2	Servidor portal/MySQL	Infraestructura tecnológica	Vulnerabilidades no parcheadas	SV5	Alta
15_3	Servidor portal/MySQL	Infraestructura tecnológica	Acceso no autorizado	SV1	Normal
16_1	Firewalls	Infraestructura tecnológica	Ataque externo	SV2	Muy alta
16_2	Firewalls	Infraestructura tecnológica	Vulnerabilidades de software	SV5	Alta
16_3	Firewalls	Infraestructura tecnológica	Configuración incorrecta	SV5	Alta
16_4	Firewalls	Infraestructura tecnológica	Fallo de hardware	No Detectada en el enunciado	No hay salvaguarda asociada al impacto

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
17_1	Rack	Infraestructura tecnológica	Acceso físico no autorizado	SV1	Alta
17_2	Rack	Infraestructura tecnológica	Daños ambientales	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
18_1	Conexión a Internet	Infraestructura tecnológica	Interrupción del servicio	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
18_2	Conexión a Internet	Infraestructura tecnológica	Intercepción de datos	SV2	Normal
18_3	Conexión a Internet	Infraestructura tecnológica	Manipulación del tráfico	SV2	Normal
19_1	Puestos de trabajo cableados	Infraestructura tecnológica	Acceso no autorizado	SV1	Normal
19_2	Puestos de trabajo cableados	Infraestructura tecnológica	Manipulación física	No Detectada en el enunciado	No hay salvaguarda asociada al impacto
19_3	Puestos de trabajo cableados	Infraestructura tecnológica	Intercepción de tráfico	SV2	Baja
20_1	Sistema operativo Windows 10	Software	Vulnerabilidades del sistema operativo	SV5	Alta
20_2	Sistema operativo Windows 10	Software	Malware	SV3	Alta
20_3	Sistema operativo Windows 10	Software	Ataques de fuerza bruta	SV1	Normal
21_1	Microsoft Office	Software	Vulnerabilidades de Microsoft Office	SV4	Baja

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
21_2	Microsoft Office	Software	Phishing y malware a través de documentos de Office	SV3	Normal
21_3	Microsoft Office	Software	Pérdida de datos	SV4	Normal
22_1	Antivirus	Software	Ataque de malware	SV3	Alta
22_2	Antivirus	Software	Vulnerabilidades no parcheadas	SV5	Normal
22_3	Antivirus	Software	Desactualización	SV5	Baja
23_1	Sistema operativo Windows 2019 Server	Software	Ataques de fuerza bruta	SV2	Alta
23_2	Sistema operativo Windows 2019 Server	Software	Vulnerabilidades del sistema operativo	SV5	Normal
23_3	Sistema operativo Windows 2019 Server	Software	Configuración insegura	SV5	Baja
24_1	Base de datos MySQL	Software	Inyección SQL	SV1	Normal
24_2	Base de datos MySQL	Software	Acceso no autorizado	SV1	Alta
24_3	Base de datos MySQL	Software	Ataque DDoS	SV2	Alta
24_4	Base de datos MySQL	Software	Fuga de información	No Detectada en el enunciado	No hay salvaguarda asociada al impacto

CONCLUSIONES RELATIVO A LAS SALVAGUARDAS

- Lógicamente, han quedado amenazas sin poderles detectar una salvaguarda relacionada. También indicar relativo a este punto que hay amenazas cuyo riesgo intrínseco es nulo o muy bajo, no tienen una salvaguarda asociada, y a su vez no es necesario aplicárselas. Esto demuestra que la seguridad de sus sistemas informáticos esta enfocado a lo verdaderamente importante.
- Cabe destacar que las tareas del Sr. Bacterio son fundamentales para la seguridad de los activos, siempre es conveniente tener un informático que realice estas tareas de manera profesional.

---

6. Calcula el riesgo residual y explica cómo lo has calculado.

Primero de todo, cabe destacar que hemos realizado un estudio del impacto de las salvaguardas sobre la amenaza, por tanto si una amenaza tiene una salvaguarda con un impacto muy alto, lógicamente mitigaría la salvaguarda.

La formula general del riesgo residual es:

- *Riesgo Residual = Riesgo Intrínseco - Impacto de la Salvaguarda*

Esta formula no valora la eficacia de la salvaguarda, que solo tiene en nuestro caso una dimension, frente a las 3 dimensiones del riesgo intrínseco (valor, impacto, probabilidad). Recordemos que el impacto en este caso se considera la capacidad de mitigar esa salvaguarda.

Realmente el impacto de la salvaguarda tal y como he explicado al principio del presente apartado, no es fidedigno. ya que la seguridad absoluta ante las amenazas no existe al 100%. Basándome en la asignatura M1.809 - Sistema de Gestión de la Seguridad de la Información, voy a ponderar la mitigación de las amenazas según la siguiente imagen dependiendo del impacto.

Clasificación de niveles

Variación impacto/vulnerabilidad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Según la tabla, la organización estima que, en caso de utilizar la mejor medida de seguridad para un determinado riesgo, ésta le ayudará a reducir su riesgo inicial en un 95%, y así para cada uno de los niveles que ha establecido.

Para ello voy a aplicar una formula que valora el impacto de la salvaguarda en la amenaza:

- ***RIESGO RESIDUAL = RIESGO INTRÍNSECO * (1 - IMPACTO DE LA SALVAGUARDA CUANTITATIVO)***

Un valor añadido de esta fórmula frente a la formula general del riesgo residual es que no presenta valores negativos, sin embargo la formula general del riesgo residual si puede resultar 0 o un numero menor que 0, resultados los cuales son utópicos en la vida real.

Por todo voy a proceder a cuantificar el impacto de las salvaguardas atendiendo a la imagen anterior.

Impacto de la salvaguarda	Impacto de la salvaguarda cuantitativo
Muy alto	0.95
Alto	0.75
Normal	0.5
Bajo	0.3
Muy bajo	0.1
No hay salvaguarda asociada al impacto	0

La tabla con el de salvaguarda cuantificado resulta la siguiente:

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
1_1	Datos de clientes	Información	Acceso no autorizado	SV1, SV2	0.75
1_2	Datos de clientes	Información	Manipulación de datos	SV1, SV4	0.5
1_3	Datos de clientes	Información	Pérdida de datos	SV3, SV5	0.3
1_4	Datos de clientes	Información	Divulgación involuntaria	SV1	0.5
2_1	Contabilidad y temas legales	Información	Acceso no autorizado	SV1, SV2	0.75
2_2	Contabilidad y temas legales	Información	Manipulación de datos	SV1, SV4	0.5
2_3	Contabilidad y temas legales	Información	Pérdida de datos	SV3, SV5	0.3
2_4	Contabilidad y temas legales	Información	Divulgación involuntaria	SV1	0.5
3_1	Datos de contratación de personal	Información	Acceso no autorizado	SV1, SV2	0.75
3_2	Datos de contratación de personal	Información	Manipulación de datos	SV1, SV4	0.5
3_3	Datos de contratación de personal	Información	Pérdida de datos	SV3, SV5	0.3

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
3_4	Datos de contratación de personal	Información	Divulgación involuntaria	SV1	0.5
4_1	Directora Ofelia	Personal	Amenaza interna	No Detectada en el enunciado	0
4_2	Directora Ofelia	Personal	Ingeniería social	No Detectada en el enunciado	0
4_3	Directora Ofelia	Personal	Errores humanos	No Detectada en el enunciado	0
5_1	Ayudante de oficina	Personal	Amenaza interna	No Detectada en el enunciado	0
5_2	Ayudante de oficina	Personal	Ingeniería social	No Detectada en el enunciado	0
5_3	Ayudante de oficina	Personal	Errores humanos	No Detectada en el enunciado	0
6_1	Técnico de sistemas Sr. Bacterio	Personal	Amenaza interna	No Detectada en el enunciado	0
6_2	Técnico de sistemas Sr. Bacterio	Personal	Ingeniería social	No Detectada en el enunciado	0
6_3	Técnico de sistemas Sr. Bacterio	Personal	Errores humanos	SV5	0.3

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
6_4	Técnico de sistemas Sr. Bacterio	Personal	Vulnerabilidades no parcheadas	SV5	0.5
7_1	Trabajador de campo Pepe	Personal	Robo o pérdida del smartphone	SV3	0.3
7_2	Trabajador de campo Pepe	Personal	Acceso no autorizado al smartphone	SV1	0.5
7_3	Trabajador de campo Pepe	Personal	Infección por malware o virus	SV3	0.5
8_1	Trabajador de campo Otilio	Personal	Robo o pérdida del smartphone	SV3	0.3
8_2	Trabajador de campo Otilio	Personal	Acceso no autorizado al smartphone	SV1	0.5
8_3	Trabajador de campo Otilio	Personal	Infección por malware o virus	SV3	0.5
9_1	Portátil Ofelia	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	0
9_2	Portátil Ofelia	Equipos y sistemas	Acceso no autorizado al portátil	SV1, SV2	0.75
9_3	Portátil Ofelia	Equipos y sistemas	Infección por malware o virus	SV3	0.5
9_4	Portátil Ofelia	Equipos y sistemas	Ataque de phishing	SV4, SV5	0.5
9_5	Portátil Ofelia	Equipos y sistemas	Ataque DDoS	SV2	0.75
9_6	Portátil Ofelia	Equipos y sistemas	Ataque de fuerza bruta	SV2	0.75
10_1	Portátil ayudante	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	0

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
10_2	Portátil ayudante	Equipos y sistemas	Ataque de malware	SV3	0.5
10_3	Portátil ayudante	Equipos y sistemas	Acceso no autorizado	SV1, SV2	0.75
11_1	Portátil Sr. Bacterio	Equipos y sistemas	Robo o pérdida del portátil	No Detectada en el enunciado	0
11_2	Portátil Sr. Bacterio	Equipos y sistemas	Ataque de malware	SV3, SV5	0.5
11_3	Portátil Sr. Bacterio	Equipos y sistemas	Acceso no autorizado	SV1, SV2, SV5	0.75
12_1	Smartphone Pepe	Equipos y sistemas	Robo o pérdida del smartphone	SV3	0.3
12_2	Smartphone Pepe	Equipos y sistemas	Ataque de malware	SV3	0.5
12_3	Smartphone Pepe	Equipos y sistemas	Acceso no autorizado	SV1	0.5
12_4	Smartphone Pepe	Equipos y sistemas	Pérdida de conexión	No Detectada en el enunciado	0
13_1	Smartphone Otilio	Equipos y sistemas	Pérdida o robo del dispositivo	SV3	0.3
13_2	Smartphone Otilio	Equipos y sistemas	Infección por malware	SV3	0.3
13_3	Smartphone Otilio	Equipos y sistemas	Acceso no autorizado	SV1	0.5
14_1	Servidor correo/DNS	Infraestructura tecnológica	Ataque DDoS	SV2	0.75
14_2	Servidor correo/DNS	Infraestructura tecnológica	Vulnerabilidades no parcheadas	SV5	0.1
14_3	Servidor correo/DNS	Infraestructura tecnológica	Phishing y suplantación de identidad	SV5	0.5

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
15_1	Servidor portal/MySQL	Infraestructura tecnológica	Inyección SQL	SV5	0.1
15_2	Servidor portal/MySQL	Infraestructura tecnológica	Vulnerabilidades no parcheadas	SV5	0.1
15_3	Servidor portal/MySQL	Infraestructura tecnológica	Acceso no autorizado	SV1	0.5
16_1	Firewalls	Infraestructura tecnológica	Ataque externo	SV2	0.75
16_2	Firewalls	Infraestructura tecnológica	Vulnerabilidades de software	SV5	0.1
16_3	Firewalls	Infraestructura tecnológica	Configuración incorrecta	SV5	0.1
16_4	Firewalls	Infraestructura tecnológica	Fallo de hardware	No Detectada en el enunciado	0
17_1	Rack	Infraestructura tecnológica	Acceso físico no autorizado	SV1	0.5
17_2	Rack	Infraestructura tecnológica	Daños ambientales	No Detectada en el enunciado	0
18_1	Conexión a Internet	Infraestructura tecnológica	Interrupción del servicio	No Detectada en el enunciado	0
18_2	Conexión a Internet	Infraestructura tecnológica	Intercepción de datos	SV2	0.75
18_3	Conexión a Internet	Infraestructura tecnológica	Manipulación del tráfico	SV2	0.75
19_1	Puestos de trabajo cableados	Infraestructura tecnológica	Acceso no autorizado	SV1	0.5

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
19_2	Puestos de trabajo cableados	Infraestructura tecnológica	Manipulación física	No Detectada en el enunciado	0
19_3	Puestos de trabajo cableados	Infraestructura tecnológica	Intercepción de tráfico	SV2	0.3
20_1	Sistema operativo Windows 10	Software	Vulnerabilidades del sistema operativo	SV5	0.75
20_2	Sistema operativo Windows 10	Software	Malware	SV3	0.5
20_3	Sistema operativo Windows 10	Software	Ataques de fuerza bruta	SV1	0.5
21_1	Microsoft Office	Software	Vulnerabilidades de Microsoft Office	SV4	0.3
21_2	Microsoft Office	Software	Phishing y malware a través de documentos de Office	SV3	0.5
21_3	Microsoft Office	Software	Pérdida de datos	SV4	0.3
22_1	Antivirus	Software	Ataque de malware	SV3	0.5
22_2	Antivirus	Software	Vulnerabilidades no parcheadas	SV5	0.75
22_3	Antivirus	Software	Desactualización	SV5	0.3
23_1	Sistema operativo Windows 2019 Server	Software	Ataques de fuerza bruta	SV2	0.3
23_2	Sistema operativo Windows 2019 Server	Software	Vulnerabilidades del sistema operativo	SV5	0.75

ID de Amenaza	Activo	Tipo de Activo	Nombre de la amenaza	salvaguarda para la amenaza	Impacto de la salvaguarda
23_3	Sistema operativo Windows 2019 Server	Software	Configuración insegura	SV5	0.3
24_1	Base de datos MySQL	Software	Inyección SQL	SV1	0.5
24_2	Base de datos MySQL	Software	Acceso no autorizado	SV1	0.75
24_3	Base de datos MySQL	Software	Ataque DDoS	SV2	0.3
24_4	Base de datos MySQL	Software	Fuga de información	No Detectada en el enunciado	0

Una vez procedido al calculo del impacto cuantitativo de la salvaguarda procederemos a realizar una tabla donde se verá el calculo del valor residual.

ID de Amenaza	Riesgo_intrínseco	Impacto de la salvaguarda	Operación Riesgo residual	Resultado Riesgo residual
1_1	**9.375**	0.75	9.375 * (1 - 0.75)	***2.34375***
1_2	6.25	0.5	6.25 * (1 - 0.5)	3.125
1_3	8.75	0.3	8.75 * (1 - 0.3)	6.125
1_4	6.25	0.5	6.25 * (1 - 0.5)	3.125
2_1	**9.375**	0.75	9.375 * (1 - 0.75)	***2.34375***
2_2	6.25	0.5	6.25 * (1 - 0.5)	3.125
2_3	8.75	0.3	8.75 * (1 - 0.3)	6.125
2_4	6.25	0.5	6.25 * (1 - 0.5)	3.125
3_1	3.75	0.75	3.75 * (1 - 0.75)	0.9375
3_2	2.25	0.5	2.25 * (1 - 0.5)	1.125
3_3	3.75	0.3	3.75 * (1 - 0.3)	2.625
3_4	2.25	0.5	2.25 * (1 - 0.5)	1.125
4_1	**12.25**	0	12.25 * (1 - 0)	**12.25**
4_2	8.75	0	8.75 * (1 - 0)	**8.75**

ID de Amenaza	Riesgo_intrínseco	Impacto de la salvaguarda	Operación Riesgo residual	Resultado Riesgo residual
4_3	6.75	0	6.75 * (1 - 0)	6.75
5_1	2.25	0	2.25 * (1 - 0)	2.25
5_2	3.375	0	3.375 * (1 - 0)	3.375
5_3	3.375	0	3.375 * (1 - 0)	3.375
6_1	3.75	0	3.75 x (1 - 0)	3.75
6_2	5.625	0	5.625 x (1 - 0)	5.625
6_3	5.625	0.3	5.625 x (1 - 0.3)	3.9375
6_4	**9.375**	0.5	9.375 x (1 - 0.5)	***4.6875***
7_1	1.5	0.3	1.5 x (1 - 0.3)	1.05
7_2	1.5	0.5	1.5 x (1 - 0.5)	0.75
7_3	2.25	0.5	2.25 x (1 - 0.5)	1.125
8_1	1.5	0.3	1.5 x (1 - 0.3)	1.05
8_2	1.5	0.5	1.5 x (1 - 0.5)	0.75
8_3	2.25	0.5	2.25 x (1 - 0.5)	1.125
9_1	1.5	0	1.5 x (1 - 0)	1.5
9_2	2.25	0.75	2.25 x (1 - 0.75)	0.5625
9_3	3.375	0.5	3.375 x (1 - 0.5)	1.6875
9_4	3.375	0.5	3.375 x (1 - 0.5)	1.6875
9_5	0	0.75	0 x (1 - 0.75)	0
9_6	2.25	0.75	2.25 x (1 - 0.75)	0.5625
10_1	1.5	0	1.5 x (1 - 0)	1.5
10_2	3.375	0.5	3.375 x (1 - 0.5)	1.6875
10_3	1.5	0.75	1.5 x (1 - 0.75)	***0.375***
11_1	1.5	0	1.5 x (1 - 0)	1.5
11_2	3.375	0.5	3.375 x (1 - 0.5)	1.6875
11_3	1.5	0.75	1.5 x (1 - 0.75)	***0.375***
12_1	1	0.3	1 x (1 - 0.3)	0.7
12_2	1	0.5	1 x (1 - 0.5)	0.5
12_3	1	0.5	1 x (1 - 0.5)	0.5

ID de Amenaza	Riesgo_intrínseco	Impacto de la salvaguarda	Operación Riesgo residual	Resultado Riesgo residual
12_4	0	0	0 x (1 - 0)	0
13_1	1	0.3	1 x (1 - 0.3)	0.7
13_2	1	0.3	1 x (1 - 0.3)	0.7
13_3	1	0.5	1 x (1 - 0.5)	0.5
14_1	6.375	0.75	6.375 x (1 - 0.75)	1.59375
14_2	4.125	0.1	4.125 x (1 - 0.1)	3.7125
14_3	3.75	0.5	3.75 x (1 - 0.5)	1.875
15_1	6.375	0.1	6.375 x (1 - 0.1)	5.7375
15_2	4.125	0.1	4.125 x (1 - 0.1)	3.7125
15_3	3.75	0.5	3.75 x (1 - 0.5)	1.875
16_1	3.75	0.75	3.75 x (1 - 0.75)	0.9375
16_2	4.125	0.1	4.125 x (1 - 0.1)	3.7125
16_3	2.5	0.1	2.5 x (1 - 0.1)	2.25
16_4	0	0	0 x (1 - 0)	0
17_1	2.25	0.5	2.25 x (1 - 0.5)	1.125
17_2	0	0	0 x (1 - 0)	0
18_1	2.25	0	2.25 x (1 - 0)	2.25
18_2	2.25	0.75	2.25 x (1 - 0.75)	0.5625
18_3	2.25	0.75	2.25 x (1 - 0.75)	0.5625
19_1	2.25	0.5	2.25 x (1 - 0.5)	1.125
19_2	0	0	0 x (1 - 0)	0
19_3	2.25	0.3	2.25 x (1 - 0.3)	1.575
20_1	4.5	0.75	4.5 x (1 - 0.75)	1.125
20_2	4.5	0.5	4.5 x (1 - 0.5)	2.25
20_3	2.25	0.5	2.25 x (1 - 0.5)	1.125
21_1	4.5	0.3	4.5 x (1 - 0.3)	3.15
21_2	4.5	0.5	4.5 x (1 - 0.5)	2.25
21_3	2.25	0.3	2.25 x (1 - 0.3)	1.575
22_1	4.5	0.5	4.5 x (1 - 0.5)	2.25

ID de Amenaza	Riesgo_intrínseco	Impacto de la salvaguarda	Operación Riesgo residual	Resultado Riesgo residual
22_2	4.5	0.75	4.5 x (1 - 0.75)	1.125
22_3	2.25	0.3	2.25 x (1 - 0.3)	1.575
23_1	3.75	0.3	3.75 x (1 - 0.3)	2.625
23_2	6.375	0.75	6.375 x (1 - 0.75)	1.59375
23_3	3.75	0.3	3.75 x (1 - 0.3)	2.625
24_1	9.375	0.5	9.375 x (1 - 0.5)	4.6875
24_2	3.75	0.75	3.75 x (1 - 0.75)	0.9375
24_3	3.75	0.3	3.75 x (1 - 0.3)	2.625
24_4	3.75	0	3.75 x (1 - 0)	3.75

CONCLUSIONES RELATIVO AL RIESGO RESIDUAL

- El que una amenaza con un valor de riesgo elevado como puede ser Acceso no autorizado tanto a datos clientes como a contratos y temas legales es un mediante salvaguardas de alto impacto tengan una bajada de mas de 7 puntos es un valor muy importante, ya que se observa que tratan de mitigar lo mejor posible el riesgo de la amenaza poniendo medidas como en esta caso son el control de acceso basado en roles y la instalación de firewalls.
    - Amenazas con unos valores de riesgo que se podrían considerar de tipo bajo-moderados como pueden ser un ataque DDoS al servidor SQL tras ver su salvaguarda estos relativos a accesos no autorizados han quedado con menos puntuación que el citado ataque DDos.
- Se observa también que amenazas con un valor de riesgo bajo se le aplican salvaguardas que tienen un impacto alto tienen menos eficacia en la bajada del valor del riesgo.
    - Caso del ordenador de Sr. Bacterio y de la ayudante de la directora Ofelia relativo al acceso no autorizado.
    - Si que es cierto que las salvaguardas relacionadas son de son las mismas que la para mitigar las amenazas de acceso no autorizado, uso de sistemas basado en roles y el uso de firewalls, ademas que el Sr. Bacterio cuenta con el plus de que es su ordenador. Por tanto las salvaguardas están enfocadas mas a la información pero de manera indirecta también protegen a otras amenazas relacionadas con otros activos con mucha menos puntuación.

6.1 Tabla final

Relativo al apartado 6.1 de las preguntas del ejercicio, se indica que pueden tener acceder al mismo en el haciendo click en este hipervínculo.

---

7. Si Ofelia preguntara qué puede hacer para mejorar la seguridad de la oficina, dado el informe que has elaborado, haz una propuesta de tres salvaguardas y justifícalas.

Viendo los resultados de la tabla anterior, lo mejor de este y ver que riesgos tras calcularse el riesgo residual son los que quedan mas altos. En este caso procedemos a ver cuales tienen mas puntuación, siendo este caso las amenazas asociadas a la directora ofelia:

- Amenaza interna.
    - Acciones malintencionadas o negligentes de la directora que pueden comprometer la seguridad de la información.
- Ingeniería social.
    - Manipulación por parte de atacantes externos para obtener información confidencial.
- Errores humanos.
    - Equivocaciones o descuidos al manejar información sensible Cabe destacar que ninguno de estas amenazas tenian salvaguarda alguna y, analizando el papel que juega Ofelia en la empresa, es de reseñar como aspectos a mejorar.

Las salvaguardas que se proponen para cada una de las amenazas pueden ser hasta validas en un conjunto u otro.

Enfocándonos a la amenaza interna se proponen las siguientes salvaguardas:

- Aunque se apliquen políticas de control de acceso basado en roles, se exija ademas, que estas se basen en el principio de mínimo privilegio.
- Se recomienda la realización de auditorias, de ambos tipos, internas y externas. Siendo por ejemplo una frecuencia semestral para las auditorias internas y una cada dos años externa.
- Realizar cursos de capacitación y concienciación en seguridad de la información a la directora, para asegurar que comprenda sus responsabilidades y las posibles consecuencias de sus acciones.

Relativo a las amenazas relativas a la ingeniería social, se recomiendan las siguientes salvaguardas.

- Capacitar al personal, no solo a la directora Ofeñia en la identificación de tácticas de ingeniería social, como phishing, pretexting y otros métodos de engaño, y cómo responder ante estos ataques. -Mi reflexión relativo a esta salvaguarda es que todos debemos de estar preparados para ser una posible victima de este tipo de ataques, no solo la directora, ya que un buen atacante puede hacer que el ayudante de Ofelia pueda ser estafado y entregue dinero a los estafadores creyendo que estaba cumpliendo órdenes de la directora.
- A parte de los firewalls que pueden son una medida de mitigacion de amenazas, se puede recomendar la implementacion de filtros de correo electronico para evitar estos intentos de ingeniería social.
- Establecer políticas y procedimientos claros para la verificación y autenticación de identidades antes de compartir información confidencial, especialmente en situaciones de contacto no solicitado.

Relativo a la amenaza de errores humanos cabe destacar las siguientes posibles salvaguardas.

- Como ya se indico en la ultima salvaguarda de la primera amenaza, el implementar programas de capacitación y concienciación en seguridad de la información para enseñar a los empleados las mejores prácticas al manejar información confidencial y los riesgos asociados con los errores humanos es muy positivo para mitigar este tipo de amenaza.

- Establecer políticas y procedimientos que exijan la verificación y revisión por parte de otro empleado antes de realizar acciones críticas o compartir información sensible.
    - Zero Trust.
    - Cifrado de documentos con infraestructura PKI.
- Para evitar la perdida de datos, es conveniente Utilizar soluciones tecnológicas, como el control de versiones y copias de seguridad automáticas, para minimizar el impacto de los errores humanos en la integridad y disponibilidad de los datos.
    - La elaboración de copas de seguridad de la documentacion, ya sea contratando servicios en la nube, puede ser una solcución factible.
