1. Introducción a PILAR

6.1 ¿Qué es PILAR?

PILAR (Practical Instrument for Legal Analysis of Risk) es una herramienta informática diseñada para la gestión y análisis de riesgos de seguridad en sistemas de información. Su principal objetivo es evaluar la seguridad de los sistemas, identificando amenazas, vulnerabilidades y posibles impactos. A continuación, se detallan sus características clave:

- **Gestión y Análisis de Riesgos de Seguridad:** PILAR proporciona un marco estructurado para identificar, evaluar y gestionar riesgos de seguridad. Permite a los usuarios realizar análisis detallados de los activos de información y evaluar las amenazas y vulnerabilidades que podrían afectarlos.
- **Evaluación de Seguridad de Sistemas de Información:** PILAR facilita la evaluación de la seguridad en sistemas de información, ayudando a los usuarios a identificar y priorizar las áreas de mayor riesgo y a implementar medidas de mitigación efectivas.
- **Desarrollada por el CCN-CERT:** PILAR fue desarrollada por el Centro Criptológico Nacional de España (CCN-CERT), lo que garantiza su alineación con las mejores prácticas y estándares internacionales en seguridad de la información.

6.3 Importancia de PILAR en Seguridad Informática

La importancia de PILAR en el campo de la seguridad informática se puede resumir en varios puntos clave:

- **Cumplimiento de Normativas y Estándares de Seguridad:** PILAR ayuda a las organizaciones a cumplir con diversas normativas y estándares de seguridad, como ISO 27001, NIST, GDPR, entre otros. Proporciona herramientas para documentar y demostrar la implementación de controles de seguridad efectivos.
- **Enfoque Sistemático para la Identificación y Gestión de Riesgos:** PILAR ofrece un enfoque estructurado y metodológico para la identificación y gestión de riesgos. Esto permite a las organizaciones abordar de manera proactiva los problemas de seguridad antes de que se conviertan en incidentes graves.
- **Facilitación de la Toma de Decisiones Informadas:** Al proporcionar un análisis detallado de las amenazas y vulnerabilidades, PILAR permite a los responsables de seguridad tomar decisiones informadas sobre las medidas de seguridad necesarias para proteger los activos críticos de la organización.

2. Instalación y Configuración de PILAR

3.1 Requisitos del Sistema

Para instalar y utilizar PILAR, es importante asegurarse de que el sistema cumple con los requisitos mínimos necesarios:

- **Sistema operativo compatible:**
  - PILAR es compatible principalmente con Windows.
  - Asegúrese de tener una versión actualizada de Windows (Windows 10 o superior recomendado).
- **Espacio de almacenamiento y memoria:**
  - **Espacio de almacenamiento:** Se recomienda tener al menos 1 GB de espacio libre en disco para la instalación y operación de PILAR.
  - **Memoria (RAM):** Se recomienda disponer de al menos 4 GB de memoria RAM para un rendimiento óptimo.

3.2 Proceso de Instalación

A continuación, se detallan los pasos para descargar, instalar y configurar PILAR:

Paso 1: Descargar PILAR

- **Visitar el sitio oficial del CCN-CERT:**
  - Abra su navegador web y diríjase al sitio oficial del Centro Criptológico Nacional (CCN-CERT).
  - En la sección de herramientas, busque PILAR y haga clic en el enlace de descarga.
- **Descargar el archivo instalador:**
  - Descargue el archivo instalador de PILAR en su computadora. Este archivo generalmente será un ejecutable (.exe) para sistemas Windows.

Paso 2: Ejecutar el Instalador

- **Ejecutar el archivo instalador:**
  - Navegue hasta la ubicación donde descargó el archivo instalador y haga doble clic en él para ejecutarlo.
  - Es posible que Windows le pida confirmar la ejecución del instalador; haga clic en "Sí" para continuar.
- **Seguir las instrucciones en pantalla:**
  - El instalador le guiará a través de varios pasos. Siga las instrucciones en pantalla para completar la instalación.

- Acepte los términos y condiciones, seleccione la ubicación de instalación (puede dejar la ubicación predeterminada) y haga clic en "Instalar".

- **Finalizar la instalación:**
  - Una vez completada la instalación, haga clic en "Finalizar" para cerrar el asistente de instalación.
  - Puede que se le solicite reiniciar su computadora para completar el proceso de instalación; si es así, hágalo.

Ejemplo Visual:

Descarga PILAR

3.3 Configuración Inicial

Una vez instalado PILAR, es necesario realizar algunas configuraciones iniciales para empezar a utilizarlo de manera efectiva.

Paso 1: Configuración de la Base de Datos de Activos

- **Abrir PILAR:**
  - Ejecute PILAR desde el menú de inicio o el acceso directo en su escritorio.
- **Crear una nueva base de datos de activos:**
  - En el menú principal, seleccione la opción "Nuevo Proyecto".
  - Asigne un nombre a su proyecto, por ejemplo, "Evaluación de Seguridad Corporativa".
  - Defina la ubicación donde desea guardar el archivo de la base de datos.
- **Añadir activos:**
  - Comience a añadir activos a la base de datos. Estos pueden incluir servidores, estaciones de trabajo, aplicaciones, datos críticos, etc.
  - Para cada activo, proporcione información detallada como nombre, descripción, ubicación, y propietario.

Paso 2: Definición del Ámbito del Análisis

- **Seleccionar el ámbito del análisis:**
  - Determine qué sistemas, redes y aplicaciones serán objeto del análisis de seguridad.
  - En la sección de "Ámbito", puede definir los límites del análisis incluyendo sólo los activos relevantes.
- **Configurar parámetros del análisis:**
  - Establezca los parámetros necesarios para el análisis, como el nivel de detalle, la profundidad del análisis y las métricas de evaluación.

Ejemplo de Configuración:

```
Ejemplo: Configuración de un proyecto en PILAR
-----------------------------------------
Nombre del proyecto: Evaluación de Seguridad Corporativa
Ubicación del archivo: C:\Proyectos\PILAR\SeguridadCorporativa.pdb
Activos añadidos:
1. Servidor de correo (Descripción: Servidor Exchange principal)
2. Estaciones de trabajo (Descripción: Equipos de empleados)
3. Datos financieros (Descripción: Base de datos financiera)
4. Aplicación web (Descripción: Portal de cliente)
```

3. Uso de PILAR: Pasos Básicos

4.1 Creación de un Proyecto

Paso a Paso:

1. **Abrir PILAR:**
   - Ejecute la herramienta PILAR desde el menú de inicio o el acceso directo en su escritorio.
2. **Seleccionar "Nuevo Proyecto":**
   - En la pantalla principal, seleccione la opción "Nuevo Proyecto".
3. **Introducir los datos básicos del proyecto:**
   - Nombre del Proyecto: "Evaluación de Seguridad Red Corporativa".
   - Descripción: "Análisis de riesgos de seguridad de la red corporativa para identificar y mitigar vulnerabilidades".

Ejemplo Visual:

```
-----------------------------------------
| Nombre del Proyecto:                  |
| Evaluación de Seguridad Red Corporativa |
|---------------------------------------|
| Descripción:                          |
| Análisis de riesgos de seguridad de   |
| la red corporativa para identificar   |
| y mitigar vulnerabilidades.           |
-----------------------------------------
```

4.2 Identificación de Activos

Paso a Paso:

1. **Añadir activos al proyecto:**
   - En el menú del proyecto, seleccione la opción "Activos" y luego "Añadir Activo".
   - Introduzca detalles del activo, como nombre, tipo, ubicación, y propietario.
2. **Clasificar los activos según su importancia y función:**
   - Clasifique los activos en categorías como hardware, software, datos y personas.
   - Asigne una clasificación de importancia a cada activo (crítico, alto, medio, bajo).

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Tipo: Hardware                         |
| Ubicación: Centro de Datos             |
| Propietario: Departamento de IT        |
| Importancia: Crítico                   |
-----------------------------------------
```

4.3 Evaluación de Amenazas y Vulnerabilidades

Paso a Paso:

1. **Seleccionar amenazas potenciales para cada activo:**
   - En el menú del activo, seleccione "Amenazas".
   - Añada posibles amenazas como "Acceso no autorizado", "Malware", "Fallo de hardware".
2. **Evaluar las vulnerabilidades presentes en el sistema:**
   - Identifique vulnerabilidades específicas asociadas a cada amenaza, como "Falta de autenticación fuerte" para "Acceso no autorizado".
   - Documente las vulnerabilidades en la herramienta.

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Amenaza: Acceso no autorizado          |
| Vulnerabilidad: Falta de autenticación|
| fuerte                                 |
-----------------------------------------
```

4.4 Análisis de Impacto

Paso a Paso:

1. **Definir el impacto de una amenaza en caso de materializarse:**
   - Clasifique el impacto en términos de confidencialidad, integridad y disponibilidad.
   - Utilice escalas de impacto como "Bajo", "Medio", "Alto".
2. **Utilizar plantillas y escenarios predefinidos:**
   - Aproveche las plantillas y escenarios disponibles en PILAR para facilitar el análisis de impacto.

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Amenaza: Acceso no autorizado          |
| Impacto:                               |
| Confidencialidad: Alto                 |
| Integridad: Medio                      |
| Disponibilidad: Alto                   |
-----------------------------------------
```

4.5 Gestión de Riesgos

Paso a Paso:

1. **Calcular el nivel de riesgo:**
   - Combine la probabilidad de una amenaza con su impacto para calcular el nivel de riesgo.
   - Use escalas de probabilidad como "Raro", "Posible", "Probable" y fórmulas para combinar estos factores.
2. **Priorizar los riesgos:**
   - Ordene los riesgos en función de su nivel para gestionar primero los más críticos.

Ejemplo:

```
----------------------------------------
| Activo: Servidor de Correo           |
| Amenaza: Acceso no autorizado        |
| Nivel de Riesgo: Alto                |
----------------------------------------
```

3.6 Planificación de Medidas de Seguridad

Paso a Paso:

1. **Proponer y documentar medidas de seguridad:**
   - Describa medidas específicas para mitigar cada riesgo identificado, como "Implementar autenticación multifactor" para "Acceso no autorizado".
2. **Asignar responsables y plazos:**
   - Asigne a personas específicas la responsabilidad de implementar las medidas.
   - Establezca plazos claros para la implementación.

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo            |
| Amenaza: Acceso no autorizado         |
| Medida de Seguridad:                  |
| Implementar autenticación multifactor |
| Responsable: Juan Pérez               |
| Plazo: 30 días                        |
-----------------------------------------
```

4. Ejemplos Prácticos con PILAR

5.1 Ejemplo 1: Evaluación de Seguridad en una Red Corporativa

Paso a Paso:

1. **Crear un Proyecto para una Red Corporativa:**
   - Abrir PILAR y seleccionar "Nuevo Proyecto".
   - Nombrar el proyecto como "Seguridad Red Corporativa" y proporcionar una breve descripción.

   Ejemplo:

```
-----------------------------------------
| Nombre del Proyecto: Seguridad Red Corporativa |
| Descripción: Evaluación de riesgos de seguridad en la red corporativa. |
-----------------------------------------
```

2. **Identificar y Clasificar Activos:**
   - Seleccionar la opción "Activos" y añadir activos clave:
     - Servidores (Servidor de Correo, Servidor de Archivos)
     - Estaciones de trabajo
     - Datos sensibles (Base de Datos de Clientes)

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Tipo: Hardware                         |
| Ubicación: Centro de Datos             |
| Importancia: Crítico                   |
-----------------------------------------
```

3. **Evaluar Amenazas:**
    - Seleccionar cada activo y añadir amenazas relevantes:
        - Malware (para servidores y estaciones de trabajo)
        - Acceso no autorizado (para servidores y datos sensibles)
        - Fallos de hardware (para todos los activos críticos)

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Amenaza: Acceso no autorizado          |
| Vulnerabilidad: Configuración de seguridad débil |
-----------------------------------------
```

4. **Analizar el Impacto y Calcular los Riesgos:**
    - Definir el impacto de cada amenaza en términos de confidencialidad, integridad y disponibilidad.
    - Calcular el riesgo combinando la probabilidad y el impacto.

    Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Amenaza: Acceso no autorizado          |
| Impacto:                               |
| Confidencialidad: Alto                 |
| Integridad: Medio                      |
| Disponibilidad: Alto                   |
| Nivel de Riesgo: Alto                  |
-----------------------------------------
```

5. **Proponer Medidas de Seguridad:**
    - Documentar medidas de seguridad específicas:
        - Actualizaciones de software
        - Implementación de firewalls
        - Configuración de copias de seguridad automáticas

Ejemplo:

```
-----------------------------------------
| Activo: Servidor de Correo             |
| Amenaza: Acceso no autorizado          |
| Medida de Seguridad: Implementar autenticación multifactor |
| Responsable: Departamento de IT        |
| Plazo: 30 días                         |
-----------------------------------------
```

4.2 Ejemplo 2: Análisis de Riesgos para una Aplicación Web

Paso a Paso:

1. **Crear un Proyecto Específico para una Aplicación Web:**
   - Abrir PILAR y seleccionar "Nuevo Proyecto".
   - Nombrar el proyecto como "Seguridad Aplicación Web" y proporcionar una breve descripción.

   Ejemplo:

```
-----------------------------------------------
| Nombre del Proyecto: Seguridad Aplicación Web |
| Descripción: Análisis de riesgos de seguridad |
| para una aplicación web.                      |
-----------------------------------------------
```

2. **Identificar Activos:**
   - Añadir activos relevantes:
     - Servidor web
     - Base de datos
     - Credenciales de usuario

Ejemplo:

```
-----------------------------------------
| Activo: Servidor Web                  |
| Tipo: Hardware                        |
| Ubicación: Centro de Datos            |
| Importancia: Crítico                  |
-----------------------------------------
```

3. Evaluar Amenazas:

- Seleccionar cada activo y añadir amenazas relevantes:
  - Inyecciones SQL (para la base de datos)
  - Cross-site scripting (XSS) (para la aplicación web)
  - Denegación de servicio (DoS) (para el servidor web)

Ejemplo:

```
-------------------------------------------------------
| Activo: Base de Datos                               |
| Amenaza: Inyección SQL                              |
| Vulnerabilidad: Validación insuficiente de entrada  |
-------------------------------------------------------
```

4. **Analizar el Impacto:**
   - Definir el impacto de cada amenaza:
     - Confidencialidad: Acceso no autorizado a datos sensibles.
     - Integridad: Modificación o corrupción de datos.
     - Disponibilidad: Interrupción del servicio.

   Ejemplo:

```
-----------------------------------------
| Activo: Base de Datos                 |
| Amenaza: Inyección SQL                |
| Impacto:                              |
| Confidencialidad: Alto                |
| Integridad: Alto                      |
| Disponibilidad: Medio                 |
| Nivel de Riesgo: Alto                 |
-----------------------------------------
```

5. **Proponer Medidas de Seguridad:**
   - Documentar medidas de seguridad específicas:
     - Validación de entrada para prevenir inyecciones SQL.
     - Uso de HTTPS para proteger la comunicación.
     - Implementación de políticas de contraseñas robustas.

Ejemplo:

```
-------------------------------------------
| Activo: Base de Datos                   |
| Amenaza: Inyección SQL                  |
| Medida de Seguridad:                    |
|Implementar validación de entrada sólida |
| Responsable: Desarrollador Web          |
| Plazo: 15 días                          |
-------------------------------------------
```

5. Generación de Informes

5.1 Tipos de Informes

PILAR proporciona una variedad de informes que son esenciales para diferentes audiencias dentro de una organización. Estos informes ayudan a comunicar los resultados del análisis de seguridad de manera clara y efectiva.

5.2.1. Informes Ejecutivos para la Alta Dirección

- **Propósito**: Brindar a los ejecutivos una visión general del estado de seguridad de la organización sin detalles técnicos complejos.
- **Contenido**: Resumen de los riesgos más críticos, impacto potencial y recomendaciones estratégicas.
- **Ejemplo**:

```
-----------------------------------------
| Informe Ejecutivo                     |
-----------------------------------------
| Proyecto: Seguridad Red Corporativa   |
| Fecha: 21/07/2024                     |
| ------------------------------------- |
| Riesgos Críticos:                     |
| - Acceso no autorizado a servidores   |
| - Inyección SQL en la base de datos   |
```

```
| ----------------------------------------|
| Impacto Potencial:                      |
| - Pérdida de datos sensibles            |
| - Interrupción del servicio             |
| ----------------------------------------|
| Recomendaciones:                        |
| - Implementar autenticación multifactor|
| - Validar entradas en aplicaciones web|
-------------------------------------------
```

5.2.2. Informes Técnicos Detallados para el Equipo de TI

- **Propósito**: Proveer al equipo técnico con detalles específicos sobre las vulnerabilidades, amenazas y medidas de seguridad recomendadas.
- **Contenido**: Descripción detallada de cada riesgo, métodos de evaluación, y medidas correctivas.
- **Ejemplo**:

```
-----------------------------------------------
| Informe Técnico Detallado                   |
-----------------------------------------------
| Proyecto: Seguridad Aplicación Web          |
| Fecha: 21/07/2024                           |
```

```
| ------------------------------------------|
| Activo: Base de Datos                     |
| Amenaza: Inyección SQL                    |
| Vulnerabilidad: Falta de validación de entrada|
| Riesgo: Alto                              |
| ------------------------------------------|
| Medidas de Seguridad:                     |
| - Implementar validación de entrada       |
| - Usar consultas preparadas               |
| - Revisión periódica de código            |
--------------------------------------------
```

5.2.3. Informes de Cumplimiento Normativo

- **Propósito**: Demostrar el cumplimiento de normativas y estándares de seguridad específicos (como ISO 27001, GDPR).
- **Contenido**: Evidencias del análisis de riesgos, medidas implementadas y auditorías realizadas.
- **Ejemplo**:

```
-----------------------------------------
| Informe de Cumplimiento Normativo     |
-----------------------------------------
```

```
| Proyecto: Seguridad Red Corporativa   |
| Fecha: 21/07/2024                     |
| ------------------------------------- |
| Normativa: ISO 27001                  |
| ------------------------------------- |
| Controles Implementados:              |
| - Control de acceso                   |
| - Protección de datos en tránsito     |
| ------------------------------------- |
| Auditorías Realizadas:                |
| - Evaluación de riesgos               |
| - Verificación de medidas de seguridad|
-----------------------------------------
```

5.2 Personalización de Informes

La personalización de informes es crucial para adaptar la información a las necesidades específicas de diferentes audiencias. PILAR permite seleccionar los componentes y niveles de detalle necesarios para cada tipo de informe.

5.2.1. Seleccionar Componentes y Niveles de Detalle

- **Proceso**:
  - **Paso 1**: Acceder a la sección de generación de informes en PILAR.
  - **Paso 2**: Seleccionar el tipo de informe (ejecutivo, técnico, cumplimiento).
  - **Paso 3**: Elegir los componentes a incluir (resumen de riesgos, análisis detallado, medidas de seguridad).
  - **Paso 4**: Ajustar el nivel de detalle según la audiencia.
- **Ejemplo**:
  - Para un informe ejecutivo: Seleccionar solo los riesgos críticos y las recomendaciones.
  - Para un informe técnico: Incluir detalles sobre cada vulnerabilidad y las técnicas de mitigación.

5.2.2. Exportar Informes en Diferentes Formatos

- **Formatos Disponibles**: PDF, Word, Excel.
- **Proceso de Exportación**:
  - **Paso 1**: Después de personalizar el informe, seleccionar la opción "Exportar".
  - **Paso 2**: Elegir el formato de exportación deseado.
  - **Paso 3**: Guardar el archivo en la ubicación deseada.
- **Ejemplo**:
  - Exportar un informe ejecutivo en PDF para una presentación a la alta dirección.
  - Exportar un informe técnico en Word para facilitar la edición y revisión por parte del equipo de TI.

6. Conclusiones y Recomendaciones

6.1 Beneficios de Usar PILAR

El uso de PILAR en la gestión y análisis de riesgos de seguridad informática aporta múltiples ventajas para las organizaciones. A continuación, se detallan algunos de los principales beneficios:

6.1.1 Mejora la Comprensión de los Riesgos de Seguridad

- **Descripción**: PILAR permite identificar, evaluar y entender mejor los riesgos a los que está expuesta una organización.
- **Ejemplo**: Al analizar una red corporativa, PILAR puede identificar amenazas como accesos no autorizados y fallos de hardware, proporcionando una visión clara de las áreas vulnerables.

6.1.2 Facilita la Planificación y Gestión de Medidas de Seguridad

- **Descripción**: La herramienta ayuda a planificar y priorizar medidas de seguridad basadas en el nivel de riesgo y el impacto potencial.
- **Ejemplo**: Después de evaluar los riesgos, PILAR puede recomendar la implementación de firewalls, autenticación multifactor y políticas de copias de seguridad para mitigar amenazas específicas.

6.1.3 Ayuda a Cumplir con Normativas y Estándares de Seguridad

- **Descripción**: PILAR soporta la conformidad con normativas y estándares de seguridad (como ISO 27001, GDPR), proporcionando informes detallados que demuestran el cumplimiento.
- **Ejemplo**: Generar informes de cumplimiento que evidencien la implementación de controles de seguridad requeridos por ISO 27001, facilitando auditorías y revisiones regulatorias.

6.2 Recomendaciones Finales

Para maximizar el valor de PILAR y asegurar una gestión eficaz de la seguridad informática, se sugieren las siguientes recomendaciones:

6.2.1 Realizar Análisis de Riesgos de Manera Periódica

- **Descripción**: Los riesgos de seguridad pueden cambiar con el tiempo debido a nuevas amenazas, cambios en la infraestructura, o actualizaciones de software. Es esencial realizar análisis de riesgos regularmente.
- **Ejemplo**: Programar revisiones trimestrales de los análisis de riesgos para asegurarse de que se consideren las últimas amenazas y vulnerabilidades.

6.2.2 Actualizar la Base de Datos de Activos y Amenazas Regularmente

- **Descripción**: Mantener la base de datos de activos y amenazas actualizada es crucial para la precisión del análisis de riesgos. Incorporar nuevos activos y actualizar las amenazas conocidas.
- **Ejemplo**: Después de añadir nuevos servidores o aplicaciones, actualizarlos en PILAR y reevaluar los riesgos asociados.

6.2.3 Integrar PILAR en el Ciclo de Vida de Desarrollo de Software y Operaciones de TI

- **Descripción**: La integración de PILAR en el ciclo de vida de desarrollo de software (SDLC) y las operaciones diarias de TI asegura que la seguridad se considere en cada etapa del proceso.
- **Ejemplo**: Utilizar PILAR durante la fase de diseño de nuevos proyectos para identificar y mitigar riesgos antes de la implementación, y realizar evaluaciones de seguridad periódicas durante el mantenimiento de sistemas.

7. Ejemplo Práctico Detallado: Evaluación de Seguridad en una Red Corporativa

1. Crear un Proyecto

Paso 1: Abrir PILAR y seleccionar "Nuevo Proyecto"

- **Ejemplo**: Al abrir PILAR, hacer clic en "Nuevo Proyecto" en la pantalla principal.

Paso 2: Introducir los datos básicos del proyecto

- **Ejemplo**: Rellenar los campos necesarios:
  - Nombre del Proyecto: "Seguridad de la Red Corporativa"
  - Descripción: "Evaluación de la seguridad para la red corporativa incluyendo servidores, estaciones de trabajo y bases de datos."

2. Identificación de Activos

Paso 1: Añadir activos al proyecto

- **Ejemplo**: En la sección de activos, hacer clic en "Añadir Activo" y registrar los siguientes activos:
  - Servidor de correo: Descripción y detalles técnicos.
  - Estaciones de trabajo de empleados: Número de estaciones, sistemas operativos.
  - Datos financieros: Tipo de datos, ubicación, importancia.
  - Base de datos de clientes: Detalles del servidor, tipo de base de datos.

Paso 2: Clasificar los activos según su importancia y función

- **Ejemplo**: Clasificar cada activo en categorías de importancia:
  - Alta: Datos financieros, Base de datos de clientes.

    - Media: Servidor de correo.
  - Baja: Estaciones de trabajo de empleados.

3. Evaluación de Amenazas y Vulnerabilidades

Paso 1: Seleccionar amenazas potenciales para cada activo

- **Ejemplo**:
  - Servidor de correo:
    - Amenaza: Ataques de malware.
    - Amenaza: Accesos no autorizados.
  - Estaciones de trabajo de empleados:
    - Amenaza: Fallos de hardware.
    - Amenaza: Malware.
  - Datos financieros y Base de datos de clientes:
    - Amenaza: Accesos no autorizados.
    - Amenaza: Inyección SQL.

Paso 2: Evaluar las vulnerabilidades en el software y la configuración de la red

- **Ejemplo**:
  - Servidor de correo:
    - Vulnerabilidad: Software desactualizado.
  - Estaciones de trabajo de empleados:
    - Vulnerabilidad: Falta de antivirus.

- Base de datos de clientes:
  - Vulnerabilidad: Configuración de permisos inapropiada.

4. Análisis de Impacto

Paso 1: Definir el impacto en caso de materialización de cada amenaza

- **Ejemplo**:
  - **Servidor de correo**:
    - Ataques de malware: Confidencialidad comprometida, Indisponibilidad del servicio.
  - **Estaciones de trabajo de empleados**:
    - Fallos de hardware: Indisponibilidad del sistema.
  - **Datos financieros**:
    - Accesos no autorizados: Pérdida de integridad de los datos, Confidencialidad comprometida.
  - **Base de datos de clientes**:
    - Inyección SQL: Pérdida de integridad de los datos.

5. Gestión de Riesgos

Paso 1: Calcular el nivel de riesgo combinando la probabilidad de la amenaza y su impacto

- **Ejemplo**:
  - **Servidor de correo**:
    - Ataques de malware: Probabilidad alta, Impacto alto = Riesgo alto.

- **Estaciones de trabajo de empleados**:
  - Fallos de hardware: Probabilidad media, Impacto medio = Riesgo medio.
- **Datos financieros**:
  - Accesos no autorizados: Probabilidad baja, Impacto alto = Riesgo medio-alto.

Paso 2: Priorizar los riesgos más críticos

- **Ejemplo**:
  - Priorizar riesgos altos como los ataques de malware en el servidor de correo y accesos no autorizados a los datos financieros.

6. Planificación de Medidas de Seguridad

Paso 1: Proponer medidas de seguridad

- **Ejemplo**:
  - **Servidor de correo**:
    - Medida: Actualizaciones de software regulares.
    - Medida: Implementación de firewalls.
  - **Estaciones de trabajo de empleados**:
    - Medida: Instalación de antivirus.
    - Medida: Mantenimiento y revisión periódica del hardware.
  - **Datos financieros**:
    - Medida: Control de acceso y auditorías regulares.
    - Medida: Cifrado de datos sensibles.

Paso 2: Asignar responsables y plazos

- **Ejemplo**:
  - **Servidor de correo**:
    - Responsable: Administrador de sistemas.
    - Plazo: 1 mes para implementar actualizaciones y firewalls.
  - **Estaciones de trabajo de empleados**:
    - Responsable: Equipo de soporte técnico.
    - Plazo: 2 semanas para instalar antivirus.
  - **Datos financieros**:
    - Responsable: Responsable de seguridad informática.
    - Plazo: 1 mes para implementar controles de acceso y cifrado.

7. Generación de Informes

Paso 1: Crear un informe ejecutivo para la alta dirección

- **Ejemplo**:
  - **Contenido**:
    - Resumen del análisis de riesgos.
    - Principales amenazas y vulnerabilidades identificadas.
    - Medidas de seguridad propuestas.
    - Prioridades y plazos.
  - **Formato**: PDF con gráficos y tablas resumiendo el análisis.

Paso 2: Crear un informe técnico detallado para el equipo de TI

- **Ejemplo**:
  - **Contenido**:
    - Detalle de cada activo y su clasificación.
    - Evaluación completa de amenazas y vulnerabilidades.
    - Análisis de impacto y cálculo de riesgos.
    - Medidas de seguridad detalladas con responsables y plazos.
  - **Formato**: Documento Word con anexos y referencias técnicas.