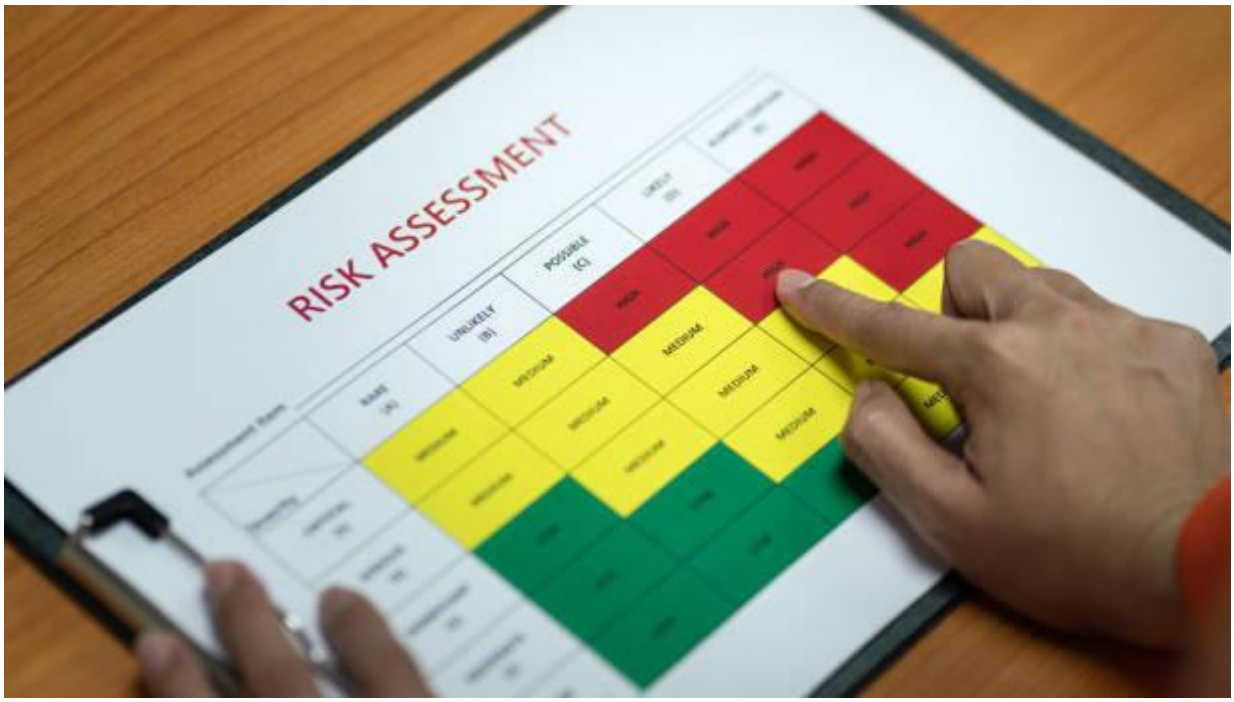
# EXAMEN PRÁCTICO

## Módulo III




Juan Carlos Vico López

# Índice

## INSTRUCCIONES

- Lee el enunciado del ejercicio y responde a las preguntas.
- Puedes consultar cualquier fuente para su realización.
- Una vez finalizado, entrega como respuesta un documento .pdf con tus soluciones justificadas.
- Dispones de 1 hora para tener subida la respuesta.

## EJERCICIO

- Ante el siguiente supuesto:
  - Se trata de una empresa que ofrece diariamente un resumen de prensa con las noticias relevantes para el cliente.
  - Para ello dispone de un programa que se ejecuta en un servidor situado en la sede de la empresa, en una ubicación remota de la España vaciada, que por la noche realiza búsquedas online en los distintos medios de prensa y extrae aquellas urls que están relacionadas con el cliente y las guarda en una BBDD, junto con los datos de contacto de los clientes.
  - A las 6 a.m. genera un correo con todas las urls encontradas para cliente y envía dicho correo.

- Dispone de una conexión a Internet por cobre, aún no llega la fibra, que es suficiente rápida como para el envío de los correos. Como contingencia tiene un router que dispone de una conexión 4G, por lo que la conexión, aunque no es rápida, es bastante estable, no habiendo sufrido ningún corte en los tres años que llevan operando.

- Sin embargo, los cortes de luz son muy frecuentes en el pueblo en la época de lluvia.

- El servidor no es un equipo dedicado, sino que lo usan también para la navegación habitual, así como para hacer la ofertas, la contabilidad, incluso para ver/descargar películas de vez en cuando.

- Responde a las siguientes cuestiones:

  - Caracteriza de forma cualitativa con la **probabilidad** las amenazas de corte de comunicaciones, corte de suministro y ataque por ransomware.

  - Asumiendo que todas las amenazas producen una degradación del 100% del valor del activo, crea una matriz de riesgo (impacto * probabilidad) y ordena las amenazas elegidas según el riesgo que implican en cuanto a la **disponibilidad**.

  - Realiza el análisis contemplando el **servicio de envío de noticias**, asumiendo que tiene una dependencia total de la BBDD, del servidor, de la electricidad y de las comunicaciones.

  - Propón alguna contramedida para mejorar la situación de riesgo resultante.

1. Como tenemos que caracterizar las amenazas en función de la probabilidad, vamos a enumerar primero estas para tenerlas identificadas.

<table>
<tr><th>Amenazas identificadas</th><th>Descripción</th></tr>
<tr><td>Corte de suministro</td><td>
5.2.7. [I.6] Corte del suministro eléctrico
<table>
<tr><th colspan="2">[I.6] Corte del suministro eléctrico</th></tr>
<tr><td>Tipos de activos:<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información (electrónicos)<br>• [AUX] equipamiento auxiliar</td><td>Dimensiones:<br>1. [D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:<br>cese de la alimentación de potencia<br>Origen:<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>Ver:<br>EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA</td></tr>
</table>
</td></tr>
<tr><td>Ransomware</td><td>
5.4.6. [A.8] Difusión de software dañino
<table>
<tr><th colspan="2">[A.8] Difusión de software dañino</th></tr>
<tr><td>Tipos de activos:<br>• [SW] aplicaciones (software)</td><td>Dimensiones:<br>1. [D] disponibilidad<br>2. [I] integridad<br>3. [C] confidencialidad</td></tr>
<tr><td colspan="2">Descripción:<br>propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.<br>Ver:<br>EBIOS: no disponible</td></tr>
</table>
</td></tr>
<tr><td>Corte comunicaciones</td><td>
5.2.9. [I.8] Fallo de servicios de comunicaciones
<table>
<tr><th colspan="2">[I.8] Fallo de servicios de comunicaciones</th></tr>
<tr><td>Tipos de activos:<br>• [COM] redes de comunicaciones</td><td>Dimensiones:<br>1. [D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:<br>cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.<br>Origen:<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>Ver:<br>EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN</td></tr>
</table>
</td></tr>
</table>

Ahora, vamos a caracterizar de forma cualitativa la probabilidad de estas amenazas, para ello vamos a crear una tabla de criterio de la probabilidad y su significado. Una vez expuesta, aplicaremos el criterio y valoraremos la probabilidad de las amenazas.

## Valoración de la probabilidad de ocurrencia de la amenaza:

| Valor | Probabilidad de ocurrencia de la amenaza |
|---|---|
| 1 | Una media de una vez cada 5 años (Muy baja) |
| 2 | Una media de una vez cada 2 años (Baja) |
| 3 | Una media de una vez al año (Media) |
| 4 | Una media de 3 veces al año (Alta) |
| 5 | Una media de 6 veces al año (Muy Alta) |

## Tabla de valoración probabilidad de amenaza:

| Activo | Amenaza | Probabilidad |
|---|---|---|
| Red | Corte de suministro | 5 |
| | Ransomware | 1 |
| | Corte de comunicaciones | 1 |
| Servidor/Equipo | Corte de suministro | 5 |
| | Ransomware | 3 |
| | Corte de comunicaciones | 1 |
| Electricidad | Corte de suministro | 5 |
| | Ransomware | 0 |

| Activo | Amenaza | Probabilidad |
|---|---|---|
| | Corte de comunicaciones | 0 |
| Oficina | Corte de suministro | 5 |
| | Ransomware | 0 |
| | Corte de comunicaciones | 1 |
| Personal | Corte de suministro | 0 |
| | Ransomware | 0 |
| | Corte de comunicaciones | 0 |
| Software buscador/envío | Corte de suministro | 5 |
| | Ransomware | 2 |
| | Corte de comunicaciones | 1 |
| BBDD | Corte de suministro | 5 |
| | Ransomware | 2 |
| | Corte de comunicaciones | 0 |

Una vez sacada la probabilidad, voy a añadir las tablas de valoración de la degradación y de cálculo del impacto, para mostrar cómo se calcula, pero el ejercicio nos dice que la degradación es del 100% por lo cual el impacto siempre será el máximo.

## Valoración de la degradación:

| Valor | Criterio |
|---|---|
| 0 | Sin degradación - 0% |
| 1 | Degradación baja - 25% |
| 2 | Degradación media - 50% |
| 3 | Degradación alta - 75% |
| 4 | Degradación máxima - 100% |

## Tabla de valoración para el cálculo del impacto:

| Degradación de la amenaza | Valor = 0 (No aplicable) | Valor = 1 (No impediría actividad) | Valor = 2 (Causaría trastornos leves) | Valor = 3 (Causaría trastornos graves) | Valor = 4 (Impediría actividad) |
|---|---|---|---|---|---|
| 0 - Sin degradación | 0 | 0 | 0 | 0 | 0 |
| 1 - Degradación baja | 0 | 1 | 2 | 3 | 4 |
| 2 - Degradación media | 0 | 2 | 3 | 4 | 5 |
| 3 - Degradación alta | 0 | 3 | 4 | 5 | 6 |
| 4 – Degradación Máxima | 0 | 4 | 5 | 6 | 7 |

Viendo estas tablas y sabiendo que el ejercicio nos dice que la degradación es del 100% podemos determinar que el valor del impacto será = 7.

2. Teniendo el impacto, ya podemos sacar la matriz de riesgo y ordenaré las amenazas según el riesgo en cuanto a la disponibilidad.

Tabla valoración del riesgo:

| Probabilidad | impacto 0 | Impacto 1 | Impacto 2 | Impacto 3 | Impacto 4 | Impacto 5 | Impacto 6 | Impacto 7 |
|---|---|---|---|---|---|---|---|---|
| 1 – Muy baja | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 – Baja | 0 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 3 – Media | 0 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 4 - Alta | 0 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 5 – Muy alta | 0 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

Tabla de riesgo ordenada según riesgo más alto:

🔴 **Riesgo Crítico (≥ 9)**

| Activo | Amenaza | Riesgo |
|---|---|---|
| Red | Corte de suministro | 11 |
| Servidor/Equipo | Corte de suministro | 11 |
| Electricidad | Corte de suministro | 11 |
| Oficina | Corte de suministro | 11 |
| Software buscador/envío | Corte de suministro | 11 |
| BBDD | Corte de suministro | 11 |
| Servidor/Equipo | Ransomware | 9 |

**Riesgo Alto (7 – 8)**

| Activo | Amenaza | Riesgo |
|---|---|---|
| Software buscador/envío | Ransomware | 8 |
| Red | Ransomware | 7 |
| Red | Corte de comunicaciones | 7 |
| Servidor/Equipo | Corte de comunicaciones | 7 |
| Oficina | Corte de comunicaciones | 7 |
| Software buscador/envío | Corte de comunicaciones | 7 |
| BBDD | Ransomware | 7 |

**Riesgo Bajo (0 – 6)**

| Activo | Amenaza | Riesgo |
|---|---|---|
| Electricidad | Ransomware | 0 |
| Electricidad | Corte de comunicaciones | 0 |
| Oficina | Ransomware | 0 |
| Personal | Corte de suministro | 0 |
| Personal | Ransomware | 0 |
| Personal | Corte de comunicaciones | 0 |
| BBDD | Corte comunicaciones | 0 |

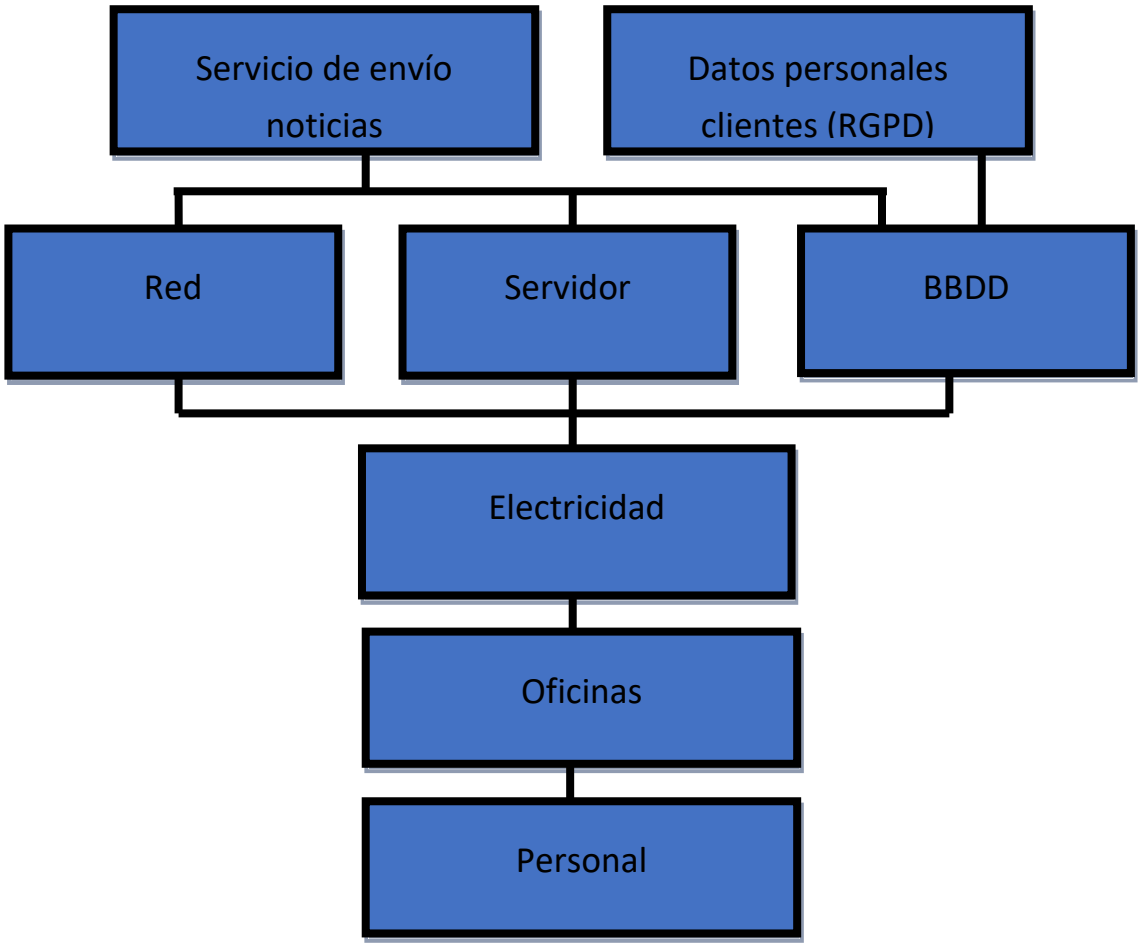
3. Ahora vamos hacer el organigrama sabiendo la dependencia del servicio y plasmando lo que nos dice el ejercicio. Con objeto de hacer el esquema, vamos a hacer el inventario de activos y los vamos a identificar para saber que vamos a añadir al organigrama.

| Activos | Tipo | Descripción |
|---|---|---|
| Red | COM | Conexión red y dispositivos |
| Servidor/Equipo | HW | Servidor |
| Electricidad | L | Red eléctrica |
| Oficina | L | Lugar de trabajo físico |
| Personal | P | Trabajadores |
| Software buscador/envío | SW | Software búsqueda y envío |
| BBDD | HW/SW | Base de datos contenido y clientes |

Determinados y descritos los activos de la empresa, vamos a pasar a hacer el organigrama según la dependencia descrita en el ejercicio.

En este caso voy a seguir el criterio de Magerit de capas para hacerlo y voy a poner una pequeña guía para que se entienda en que capa está cada elemento.

- Capa 1 Activos esenciales
  - Información que se maneja
  - Servicios prestados
- Capa 2 Servicios internos
  - Que se estructuran ordenadamente el sistema de información
- Capa 3 Equipamiento informático
  - Aplicaciones (Software)
  - Equipos informáticos (Hardware)
  - Comunicaciones
  - Soportes de información: Discos, cientas….
- Capa 4 El entorno: activos que se precisan para garantizar las siguientes capas
  - Equipamiento y suministros: Energia, climatización, etc.
  - Mobiliario.
- Capa 5 Los servicios subcontratados a terceros
- Capa 6 Las instalaciones físicas
- Capa 7 Personal
  - Usuarios
  - Operadores y administradores
  - Desarrolladores



4. Como parte final del ejercicio, aportaremos contramedidas para el riesgo que hemos sacado en función del tipo de amenaza y priorizaremos las salvaguardas en función del riesgo.

**1. CORTE DE SUMINISTRO**

**Contramedidas:**

- **Sistemas de alimentación ininterrumpida (SAI):**
  Instalar SAI en equipos críticos para garantizar el suministro eléctrico durante interrupciones.
- **Generadores de respaldo:**
  Implementar generadores eléctricos para mantener operativas las infraestructuras esenciales.
- **Redundancia de infraestructuras:**
  Establecer sistemas redundantes para redes y servidores, permitiendo la continuidad del servicio en caso de fallos.
- **Planes de continuidad de negocio:**
  Desarrollar y probar regularmente planes que aseguren la operatividad ante cortes de suministro.
- **Monitoreo y alertas:**
  Implementar sistemas de monitoreo que alerten sobre fallos en el suministro eléctrico o interrupciones en la red.

**2. RANSOMWARE**

**Contramedidas:**

- **Copias de seguridad regulares:**
  Realizar backups frecuentes y almacenarlos en ubicaciones seguras y desconectadas de la red principal.
- **Actualizaciones y parches:**
  Mantener todos los sistemas y software actualizados para corregir vulnerabilidades conocidas.
- **Segmentación de la red:**
  Dividir la red en segmentos para limitar la propagación del ransomware en caso de infección.
- **Formación del personal:**
  Capacitar a los empleados sobre las prácticas seguras y la detección de correos electrónicos sospechosos.

- **Control de accesos:**
  Establecer políticas de acceso basadas en el principio de mínimo privilegio.
- **Autenticación multifactor (MFA):**
  Reforzar la seguridad de las cuentas mediante MFA, especialmente para accesos remotos.
- **Análisis de tráfico de red:**
  Utilizar herramientas que detecten comportamientos anómalos en la red que puedan indicar una infección.
- **Simulacros de ataque:**
  Realizar ejercicios periódicos para evaluar la respuesta ante incidentes de ransomware.

**3. CORTE DE COMUNICACIONES**

- **Redundancia de enlaces:**
  Contar con múltiples proveedores de servicios de internet para garantizar la conectividad.
- **Sistemas de comunicación alternativos:**
  Implementar canales de comunicación de respaldo, como redes móviles o satelitales.
- **Monitoreo de la red:**
  Supervisar continuamente el estado de la red para detectar y responder rápidamente a interrupciones.
- **Protocolos de comunicación de emergencia:**
  Establecer procedimientos claros para mantener la comunicación interna y externa durante incidentes.

Estas serían una serie de medidas que se podrían tomar para bajar mucho el riesgo de la empresa. Pero siendo objetivo con el ejercicio y viendo las características de la empresa es complicado que implementen tantas medidas de seguridad, aunque sea una mejora muy significativa del riesgo. Bajo mi punto de vista, creo que el objetivo principal de este informe sería concienciar al jefe o encargado de la seguridad de la empresa del estado de vulnerabilidad que tienen y de ahí ir implementando medidas además de concienciarse y formarse de los peligros y amenazas a las que pueden exponerse.