# **EXAMEN 03/09/2024**

***DESCRIPCIÓN GENERAL DE LA PRÁCTICA:***

Esta actividad evaluable consiste en cuatro apartados.

* En el primero se solicita información de las máquinas Metasploitable2 y Metasploitable3 Linux y Windows.
* En el segundo utilizar la herramienta Wireshark para analizar el tráfico de red al arrancar las máquinas en la red.
* En la tercera se trata sobre riesgos y controles de seguridad.
* En la cuarta se trata sobre la normativa de protección de datos de carácter personal.

La actividad consta de 4 apartados:

1. Se pide que de la máquina Metasploitable muestres:
   1. La información sobre la máquina (dirección IP, dirección MAC, etc.).
   2. Los puertos y servicios abiertos.
   3. Las vulnerabilidades.
2. Se pide:
   1. Captura y guarda en un documento en texto plano (“ARP-DHCP”) el tráfico de paquetes ARP y DHCP del proceso de arranque de todas las máquinas de tu laboratorio.
3. Se pide:
   1. Describir 10 riesgos de seguridad.
   2. Describir 10 controles de seguridad.
   3. Determina el riesgo inherente y residual de cada uno de ellos.
   4. Elabora matriz de riesgos inherente y residual.
   5. Explica que riesgos son prioritarios de tratar.
4. Se pide:
   1. Indicar la normativa aplicable para el tratamiento de datos de carácter personal.
   2. Describir las figuras del delegado de Protección de Datos, responsable del Tratamiento y encargado del tratamiento. Elaborar un documento con la respuesta a los mismos.
5. METASPLOITABLE:
6. La información sobre la máquina:

Con el siguiente comando “*ifconfig*”,

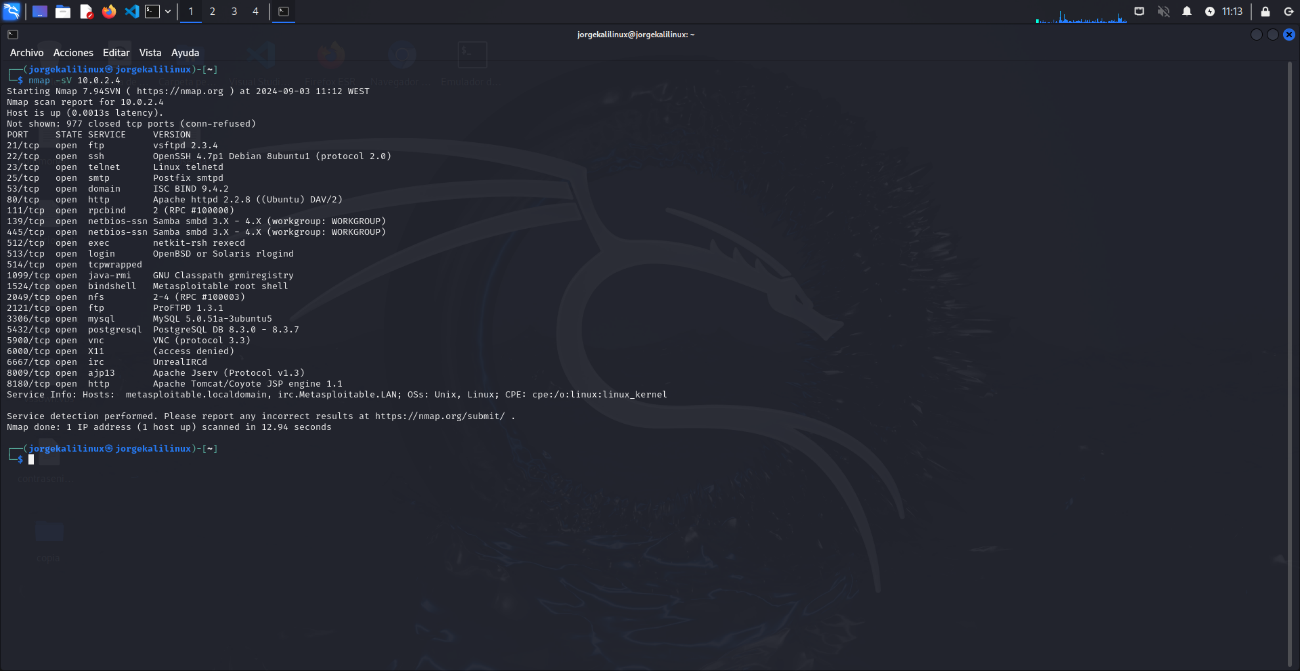
Texto

Descripción generada automáticamente

observamos que nuestra **dirección IP (inet addr)** es la **10.0.2.4**, el **broadcast (Bcast)** es hasta la **10.0.2.255**, y la **máscara (Mask)** es la **255.255.255.0**

1. Los puertos y servicios abiertos

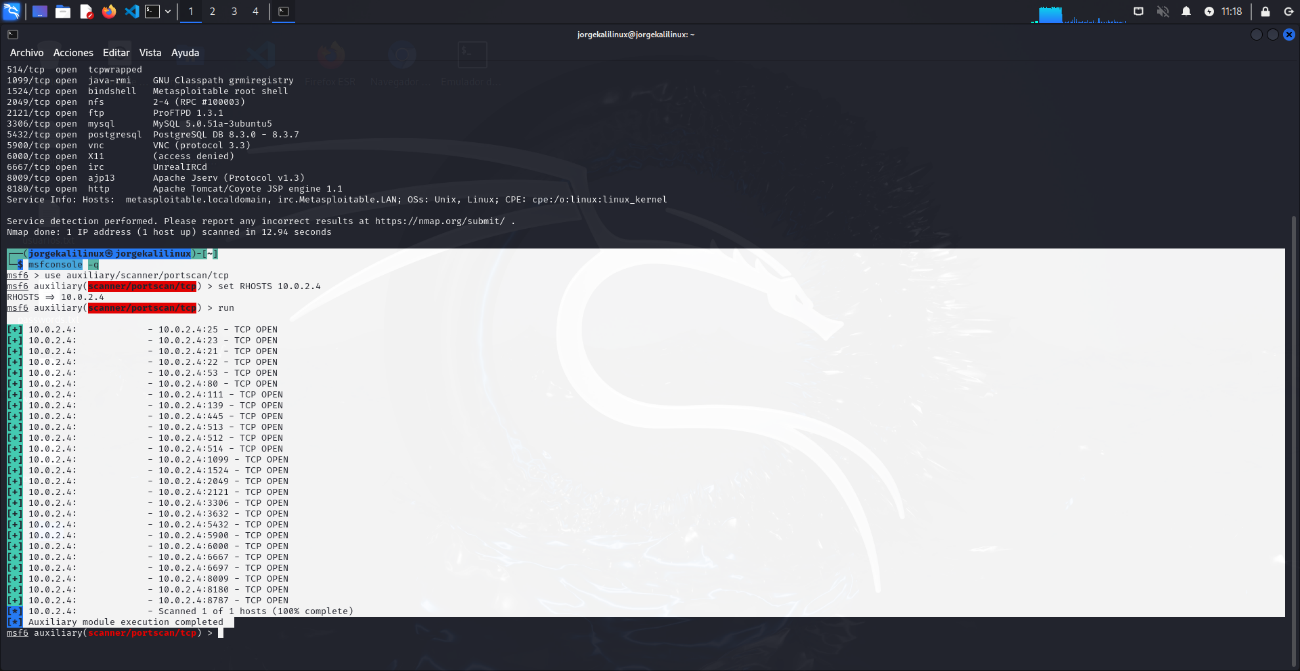
Nos vamos a la máquina Kali Linux y ejecutamos el siguiente comando “*nmap -sV IP*”, en este caso nuestra IP es la 10.0.2.4.



1. Las vulnerabilidades

Para detectar cuáles son las vulnerabilidades de la máquina, iniciamos Metasploit en Kali Linux con el comando “*msfconsole*”. Una vez entrado en Metasploit, realizamos un escaneo de ésta misma para detectar vulnerabilidades conocidas. Después del escaneo, se pueden usar módulos específicos de Metasploit para explotar o detectar vulnerabilidades en los servicios identificados.

Estos son los siguientes comandos para realizar el escaneo (“*use auxiliary/scanner/portscan/tcp”,* “*set RHOSTS IP*”, “*run*”):



1. WIRESHARK:

Para realizar este ejercicio, he encendido 3 máquinas: Kali Linux (para comprobar con Wireshark), Metasploitable2 de Linux y Metasploitable3 de Windows.

Ejecutamos Wireshark y vemos ARP y DHCP:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. RIESGOS Y CONTROLES DE SEGURIDAD:

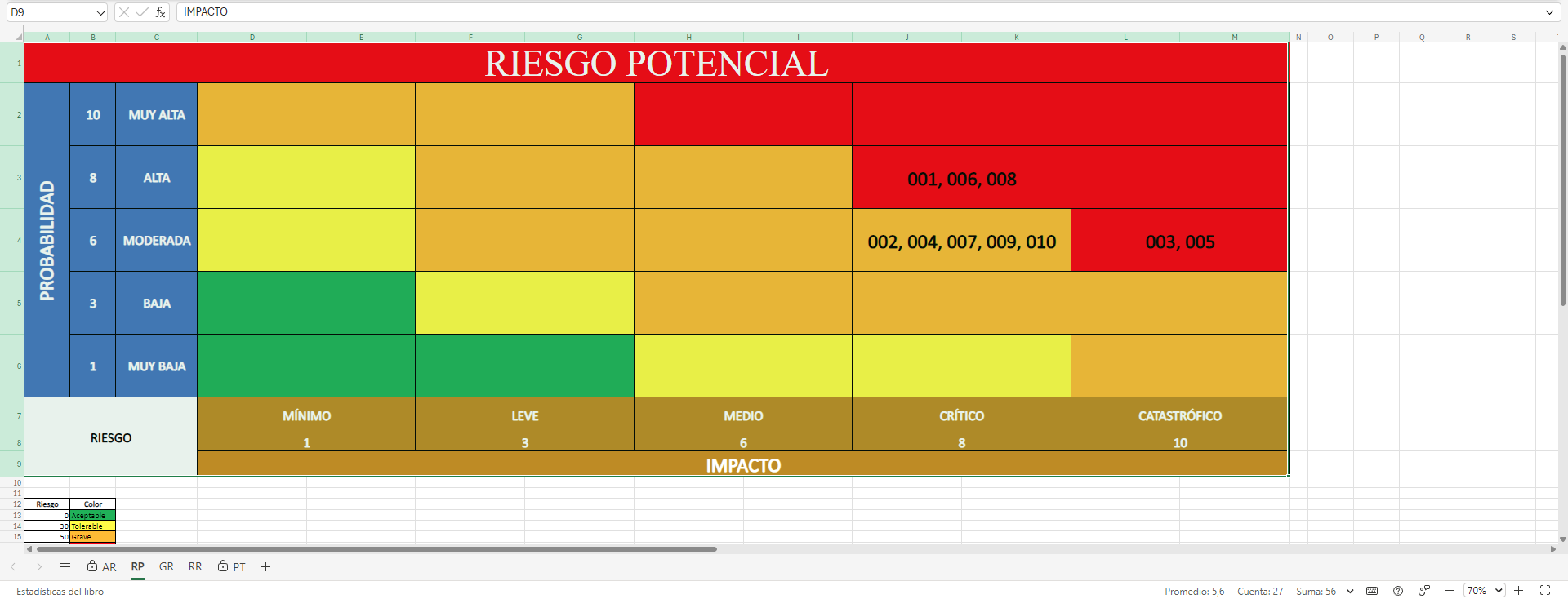
10 riesgos de seguridad:

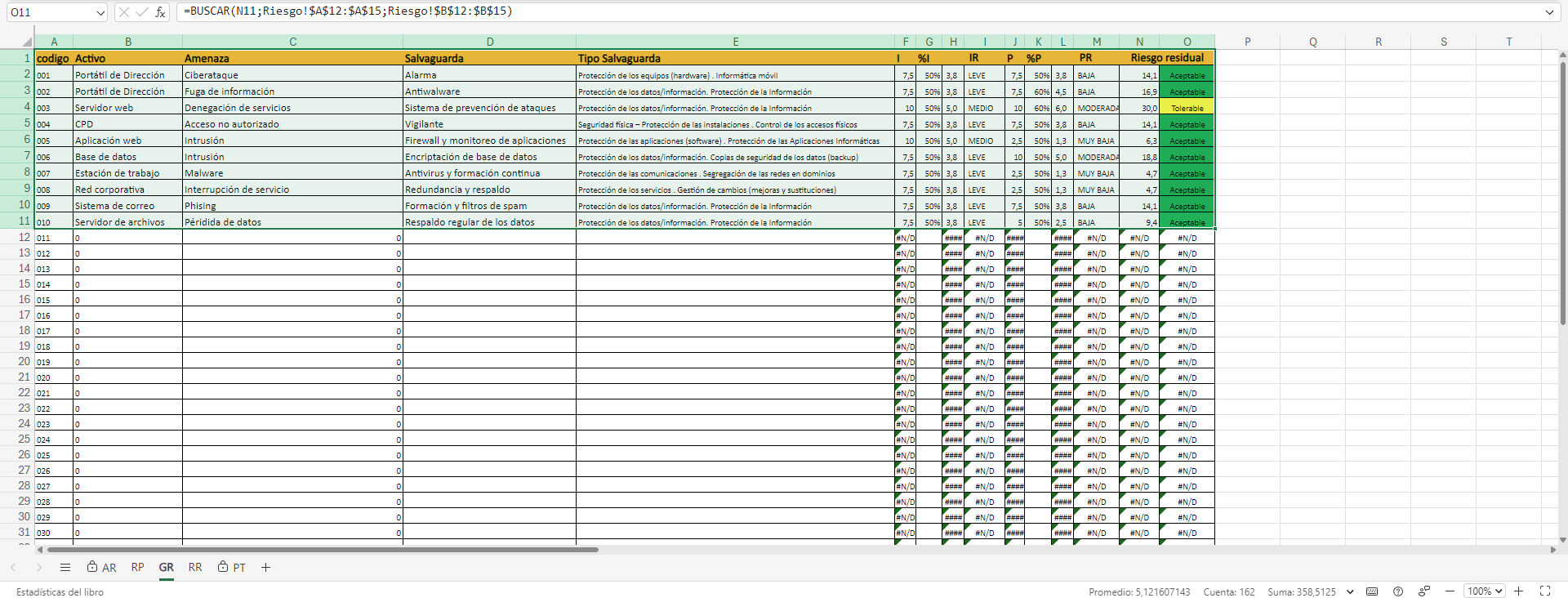
10 controles de seguridad:

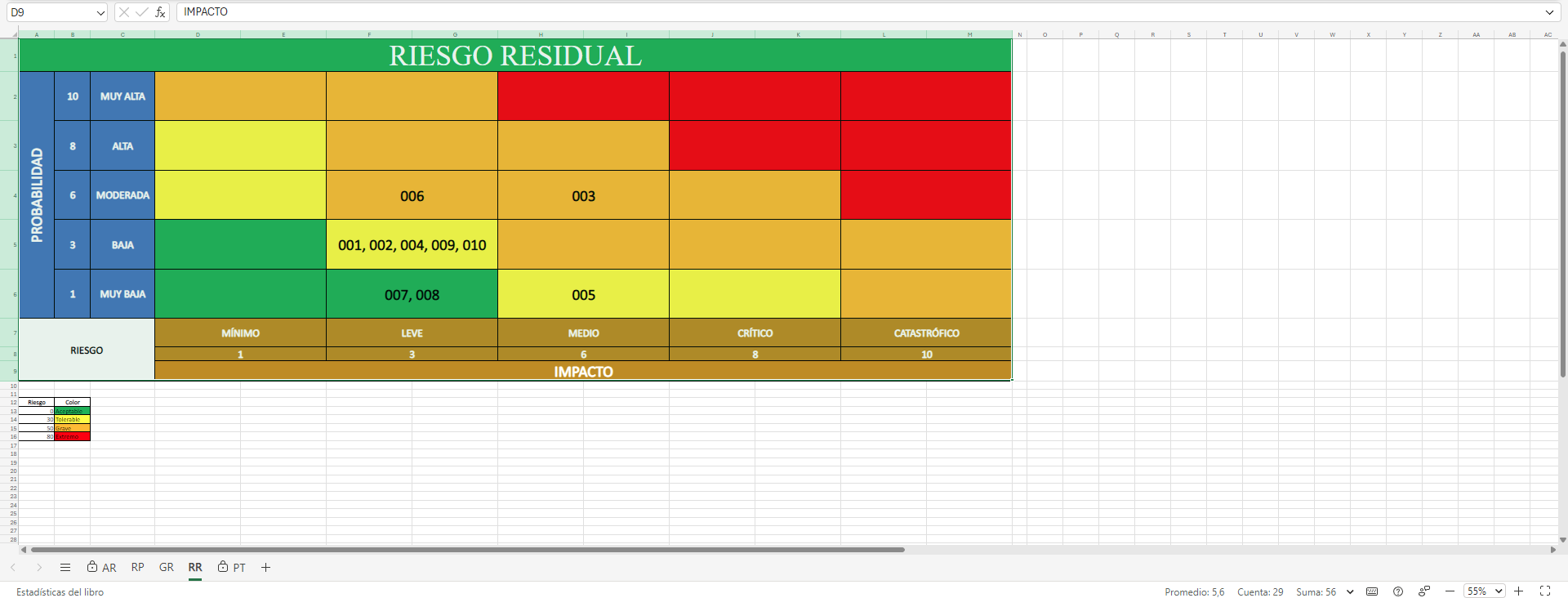
Riesgo inherente y residual de cada uno de ellos:

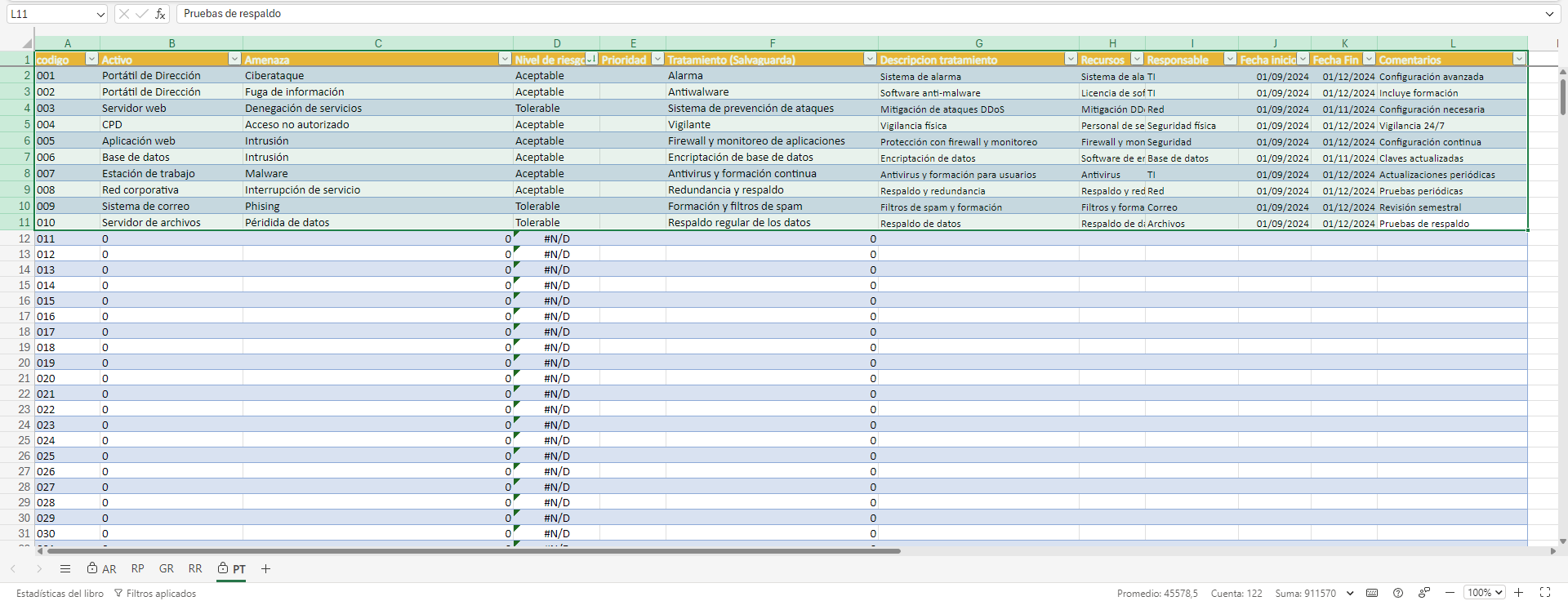
Matriz de riesgos inherente y residual:











Riesgos que son prioritarios de tratar: **001, 006, 008**.

Estos riesgos se encuentran en la zona de muy alta probabilidad y alto impacto, lo que los convierte en la mayor preocupación y tratar lo antes posible.

1. NORMATIVA APLICABLE PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL:

La normativa que regula el tratamiento de datos personales en España ha experimentado cambios significativos en los últimos años, buscando garantizar la protección de los derechos de las personas físicas en relación con el tratamiento de sus datos. Las normas son las siguientes:

* **Reglamento General de Protección de Datos (RGPD):** Este reglamento europeo (UE) 2016/679 es directamente aplicable en todos los estados miembros de la Unión Europea, incluyendo España. Establece un marco jurídico común y elevado para la protección de los datos personales.
* **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Esta ley española (Ley Orgánica 3/2018) adapta el RGPD al ordenamiento jurídico español y desarrolla algunos aspectos específicos.

La normativa implica lo siguiente:

* **Principios:** Establece principios fundamentales como la licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad, así como la responsabilidad proactiva del responsable del tratamiento.
* **Derechos de los interesados:** Reconoce y garantiza los derechos de los individuos sobre sus datos, como el derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos.
* **Obligaciones de los responsables del tratamiento:** Impone diversas obligaciones a quienes tratan datos personales, como la realización de evaluaciones de impacto, la designación de un delegado de protección de datos en determinados casos, la notificación de brechas de seguridad, etc.

**Figuras del delegado de Protección de Datos, responsable del tratamiento y encargado del tratamiento**

Dentro del marco normativo de protección de datos, encontramos tres figuras clave:

|  |  |
| --- | --- |
| ***FIGURA*** | ***RESPONSABILIDADES PRINCIPALES*** |
| Delegado de Protección de Datos | Figura obligatoria en determinadas organizaciones. Actúa como un punto de contacto interno y externo en materia de protección de datos.  Asesoramiento, supervisión, cooperación con la autoridad de control, etc. |
| Responsable del tratamiento | Persona física o jurídica, autoridad pública, servicio u organismo que, individualmente o conjuntamente con otros, determina los fines y medios del tratamiento de datos personales.  Determinación de los fines y medios del tratamiento, garantía del cumplimiento de la normativa. |
| Encargado del tratamiento | Persona física o jurídica, autoridad pública, servicio u organismo que trata datos personales por cuenta del responsable del tratamiento.  Tratamiento de datos por cuenta del responsable, bajo sus instrucciones. |