EXAMEN 03/09/2024

DESCRIPCIÓN GENERAL DE LA PRÁCTICA:

Esta actividad evaluable consiste en cuatro apartados.

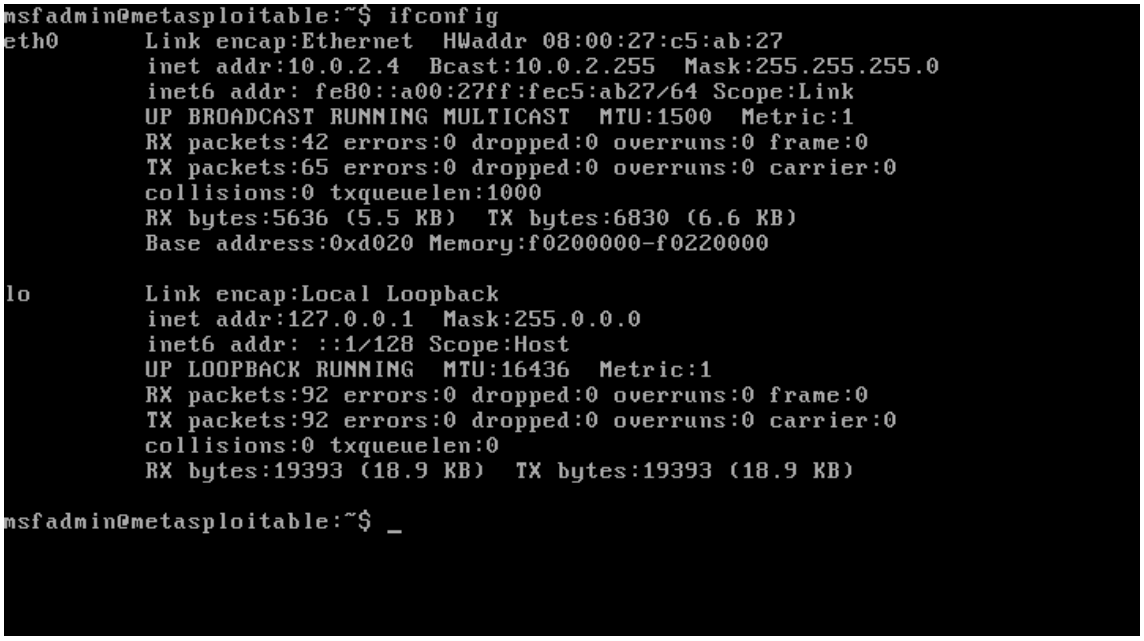
- En el primero se solicita información de las máquinas Metasploitable2 y Metasploitable3 Linux y Windows.
- En el segundo utilizar la herramienta Wireshark para analizar el tráfico de red al arrancar las máquinas en la red.
- En la tercera se trata sobre riesgos y controles de seguridad.
- En la cuarta 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:
    a. La información sobre la máquina (dirección IP, dirección MAC, etc.).
    b. Los puertos y servicios abiertos.
    c. Las vulnerabilidades.
2. Se pide:
    a. 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:
    a. Describir 10 riesgos de seguridad.
    b. Describir 10 controles de seguridad.
    c. Determina el riesgo inherente y residual de cada uno de ellos.
    d. Elabora matriz de riesgos inherente y residual.
    e. Explica que riesgos son prioritarios de tratar.
4. Se pide:
    a. Indicar la normativa aplicable para el tratamiento de datos de carácter personal.
    b. 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.

1. METASPLOITABLE:
   a. La información sobre la máquina:

Con el siguiente comando "*ifconfig*",



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**

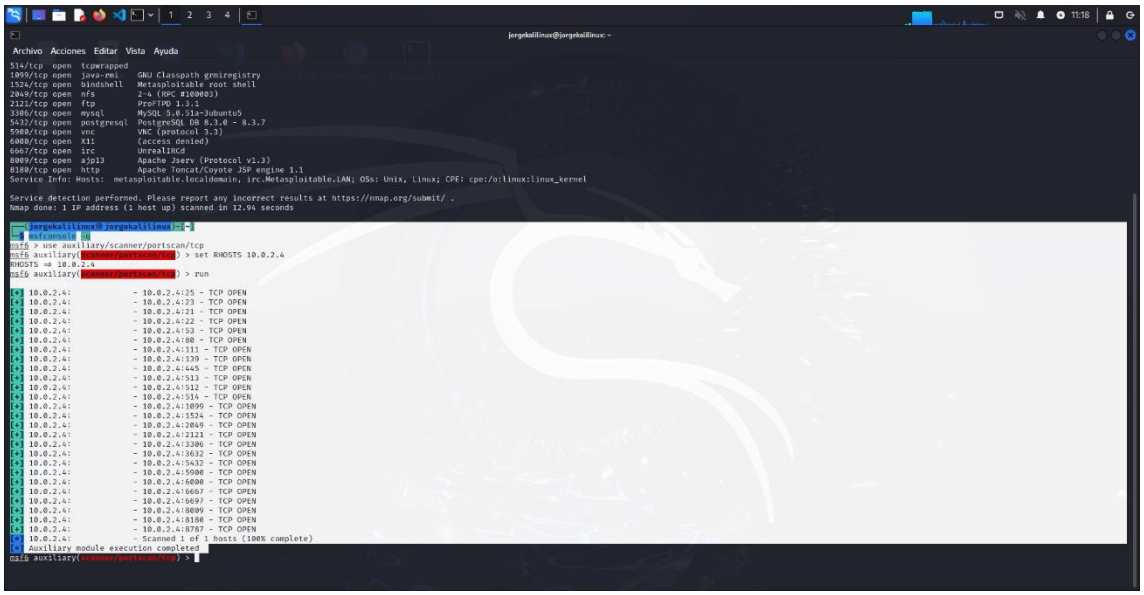
   b. Los puertos y servicios abiertos

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.

c. 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.

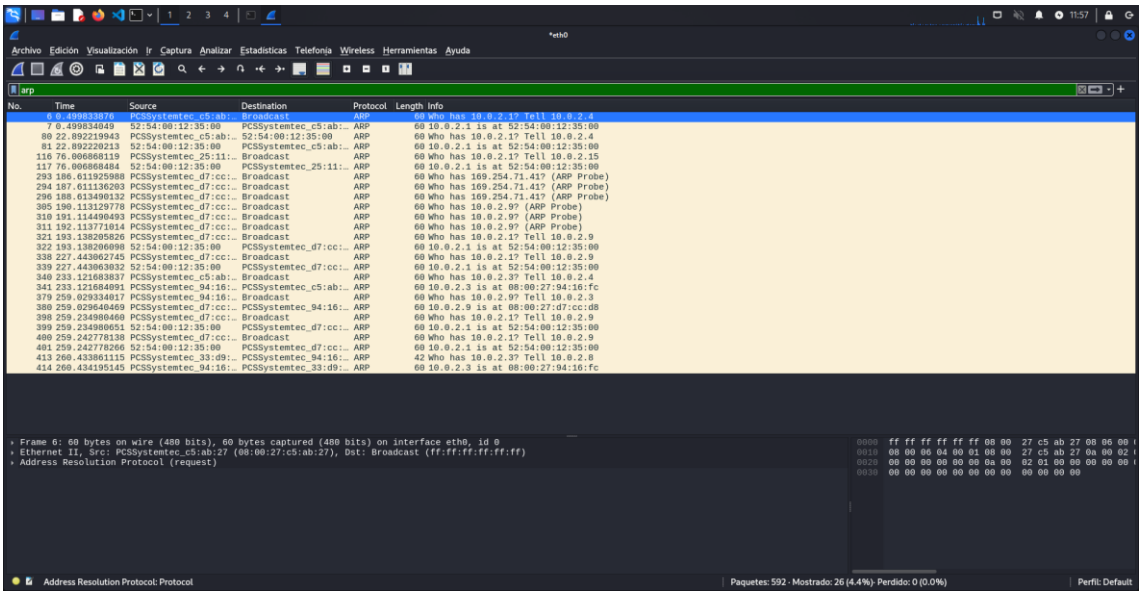
Estos son los siguientes comandos para realizar el escaneo ("*use auxiliary/scanner/portscan/tcp*", "*set RHOSTS IP*", "*run*"):

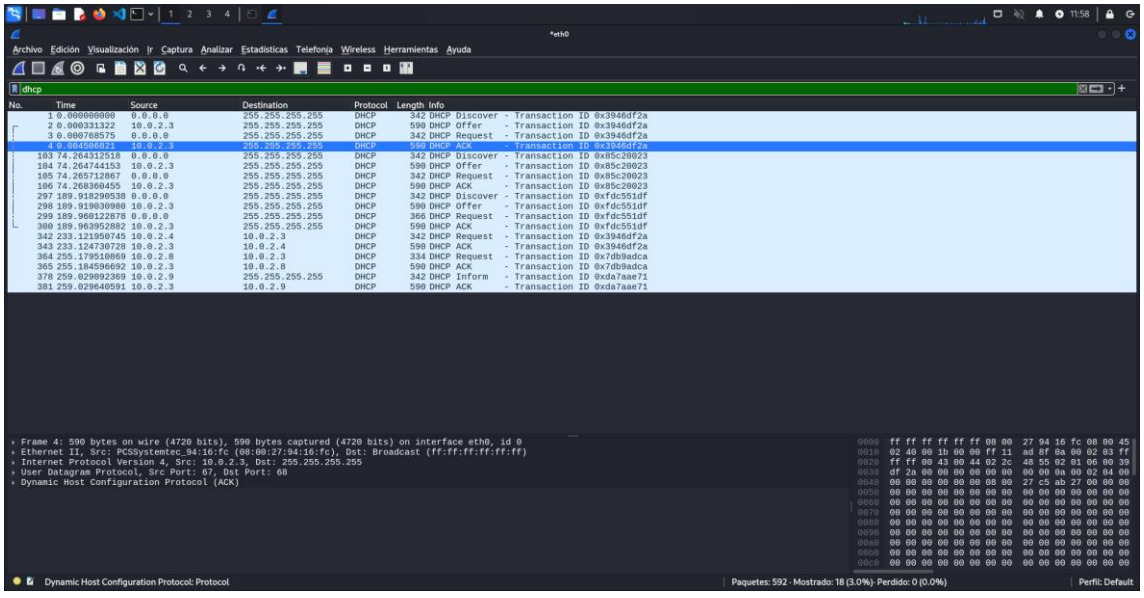


2. WIRESHARK:

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:





3. RIESGOS Y CONTROLES DE SEGURIDAD:

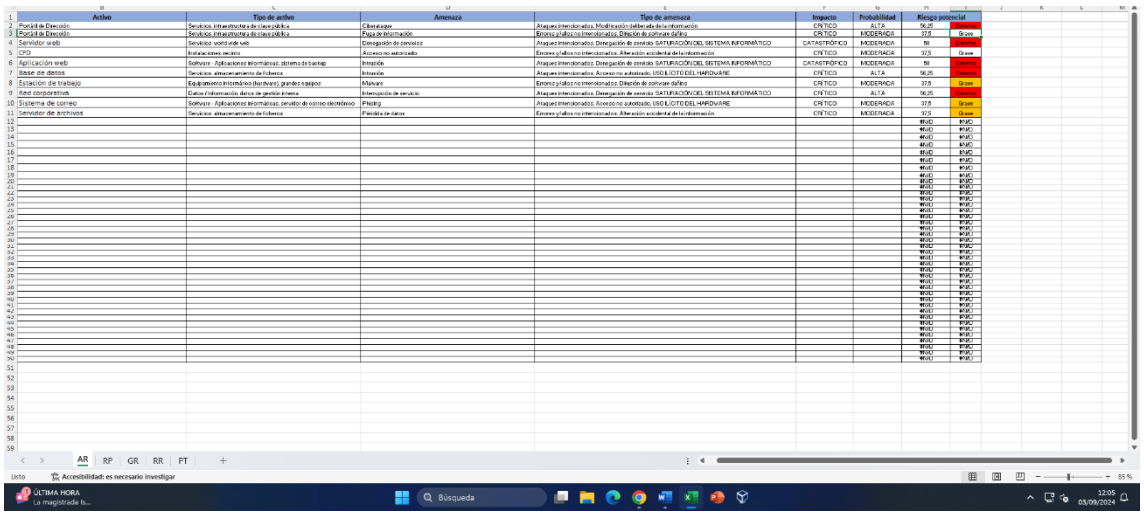
10 riesgos de seguridad:

10 controles de seguridad:

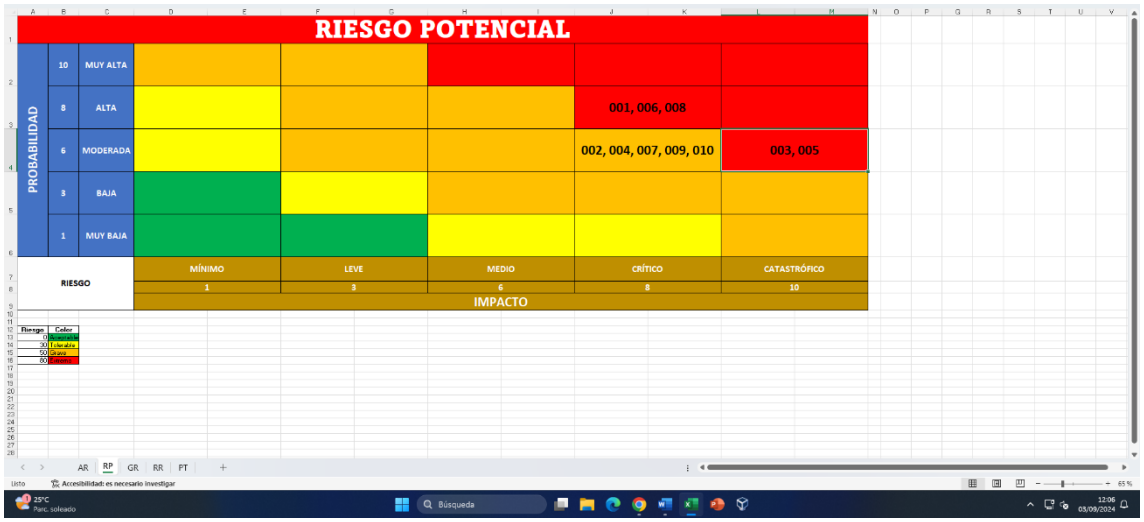
Riesgo inherente y residual de cada uno de ellos:

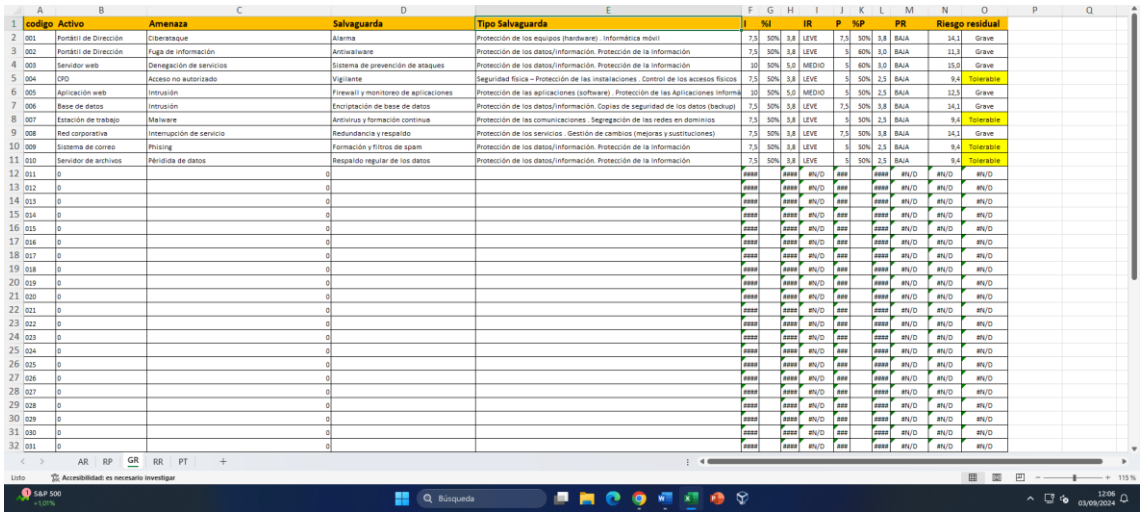
Matriz de riesgos inherente y residual:

Riesgos que son prioritarios de tratar:

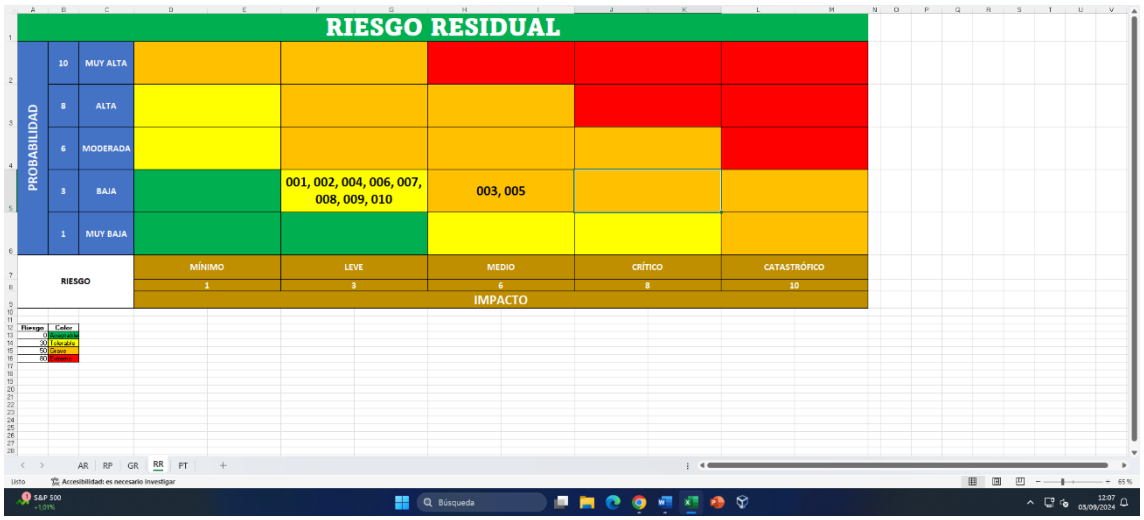


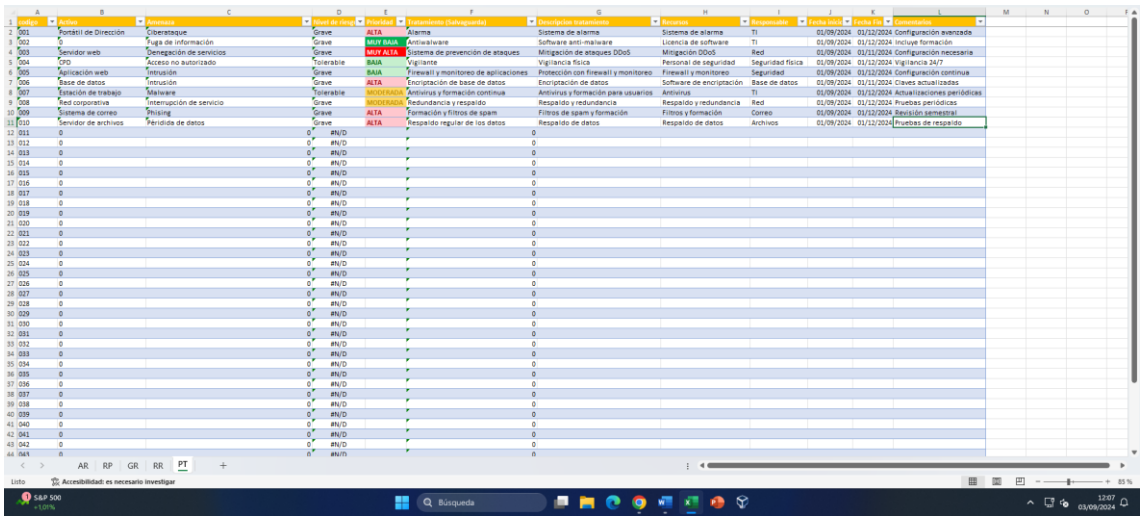
Activo	Tipo de activo	Amenaza	Tipo de amenaza	Impacto	Probabilidad	Riesgo potencial
Portal de Dirección	Servicios: Infraestructura de clase pública	Ciberataque	Ataques intencionados. Modificación deliberada de la información	CRÍTICO	ALTA	56,25 Extremo
Portal de Dirección	Servicios: Infraestructura de clase pública	Fuga de información	Errores y fallos no intencionados. Difusión de software dañino	CRÍTICO	MODERADA	37,5 Grave
Servidor web	Servicios: world wide web	Denegación de servicio	Ataques intencionados. Denegación de zombis. SATURACIÓN DEL SISTEMA INFORMÁTICO	CATASTRÓFICO	MODERADA	50 Extremo
CPD	Instalaciones: recinto	Acceso no autorizado	Errores y fallos no intencionados. Alteración accidental de la información	CRÍTICO	MODERADA	37,5 Grave
Aplicación web	Software - Aplicaciones informáticas: sistema de backup	Intrusión	Ataques intencionados. Denegación de zombis. SATURACIÓN DEL SISTEMA INFORMÁTICO	CATASTRÓFICO	MODERADA	50 Extremo
Base de datos	Servicios: almacenamiento de ficheros	Intrusión	Ataques intencionados. Acceso no autorizado. USO ILÍCITO DEL HARDWARE	CRÍTICO	ALTA	56,25 Extremo
Estación de trabajo	Equipamiento informático (hardware): grandes equipos	Malware	Errores y fallos no intencionados. Difusión de software dañino	CRÍTICO	MODERADA	37,5 Grave
Red corporativa	Datos / información: datos de gestión interna	Interrupción de servicio	Ataques intencionados. Denegación de zombis. SATURACIÓN DEL SISTEMA INFORMÁTICO	CRÍTICO	ALTA	56,25 Extremo
Sistema de correo	Software - Aplicaciones informáticas: servidor de correo electrónico	Phising	Ataques intencionados. Acceso no autorizado. USO ILÍCITO DEL HARDWARE	CRÍTICO	MODERADA	37,5 Grave
Servidor de archivos	Servicios: almacenamiento de ficheros	Pérdida de datos	Errores y fallos no intencionados. Alteración accidental de la información	CRÍTICO	MODERADA	37,5 Grave





codigo	Activo	Amenaza	Salvaguarda	Tipo Salvaguarda	I	%I	IR	P	%P	PR	Riesgo residual	
001	Portátil de Dirección	Ciberataque	Alarma	Protección de los equipos (hardware) . Informática móvil	7,5	50%	3,8	LEVE	7,5	50%	3,8	BAJA	14,1	Grave
002	Portátil de Dirección	Fuga de información	Antiwalware	Protección de los datos/información. Protección de la información	7,5	50%	3,8	LEVE	5	60%	3,0	BAJA	11,3	Grave
003	Servidor web	Denegación de servicios	Sistema de prevención de ataques	Protección de los datos/información. Protección de la información	10	50%	5,0	MEDIO	5	60%	3,0	BAJA	15,0	Grave
004	CPD	Acceso no autorizado	Vigilante	Seguridad física – Protección de las instalaciones . Control de los accesos físicos	7,5	50%	3,8	LEVE	5	50%	2,5	BAJA	9,4	Tolerable
005	Aplicación web	Intrusión	Firewall y monitoreo de aplicaciones	Protección de las aplicaciones (software) . Protección de las Aplicaciones Informa	10	50%	5,0	MEDIO	5	50%	2,5	BAJA	12,5	Grave
006	Base de datos	Intrusión	Encriptación de base de datos	Protección de los datos/información. Copias de seguridad de los datos (backup)	7,5	50%	3,8	LEVE	7,5	50%	3,8	BAJA	14,1	Grave
007	Estación de trabajo	Malware	Antivirus y formación continua	Protección de las comunicaciones . Segregación de las redes en dominios	7,5	50%	3,8	LEVE	5	50%	2,5	BAJA	9,4	Tolerable
008	Red corporativa	Interrupción de servicio	Redundancia y respaldo	Protección de los servicios . Gestión de cambios (mejoras y sustituciones)	7,5	50%	3,8	LEVE	7,5	50%	3,8	BAJA	14,1	Grave
009	Sistema de correo	Phising	Formación y filtros de spam	Protección de los datos/información. Protección de la información	7,5	50%	3,8	LEVE	5	50%	2,5	BAJA	9,4	Tolerable
010	Servidor de archivos	Pérdidda de datos	Respaldo regular de los datos	Protección de los datos/información. Protección de la información	7,5	50%	3,8	LEVE	5	50%	2,5	BAJA	9,4	Tolerable
011	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
012	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
013	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
014	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
015	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
016	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
017	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
018	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
019	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
020	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
021	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
022	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
023	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
024	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
025	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
026	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
027	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
028	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
029	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
030	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D
031	0		0		####	####	#N/D	###	####	#N/D	#N/D	#N/D





codigo	Activo	Amenaza	Nivel de riesgo	Prioridad	Tratamiento (Salvaguarda)	Descripcion tratamiento	Recursos	Responsable	Fecha inicio	Fecha Fin	Comentarios
001	Portátil de Dirección	Ciberataque	Grave	ALTA	Alarma	Sistema de alarma	Sistema de alarma	TI	01/09/2024	01/12/2024	Configuración avanzada
002	Portátil de Dirección	Fuga de información	Grave	MUY BAJA	Antiwalware	Software anti-malware	Licencia de software	TI	01/09/2024	01/12/2024	Incluye formación
003	Servidor web	Denegación de servicios	Grave	MUY ALTA	Sistema de prevención de ataques	Mitigación de ataques DDoS	Mitigación DDoS	Red	01/09/2024	01/11/2024	Configuración necesaria
004	CPD	Acceso no autorizado	Tolerable	BAJA	Vigilante	Vigilancia física	Personal de seguridad	Seguridad física	01/09/2024	01/12/2024	Vigilancia 24/7
005	Aplicación web	Intrusión	Grave	BAJA	Firewall y monitoreo de aplicaciones	Protección con Firewall y monitoreo	Firewall y monitoreo	Seguridad	01/09/2024	01/12/2024	Configuración continua
006	Base de datos	Intrusión	Grave	ALTA	Encriptación de base de datos	Encriptación de datos	Software de encriptación	Base de datos	01/09/2024	01/11/2024	Claves actualizadas
007	Estación de trabajo	Malware	Tolerable	MODERADA	Antivirus y formación continua	Antivirus y formación para usuarios	Antivirus	TI	01/09/2024	01/12/2024	Actualizaciones periódicas
008	Red corporativa	Interrupción de servicio	Grave	MODERADA	Redundancia y respaldo	Respaldo y redundancia	Respaldo y redundancia	Red	01/09/2024	01/12/2024	Pruebas periódicas
009	Sistema de correo	Phising	Grave	ALTA	Formación y filtros de spam	Filtros de spam y formación	Filtros y formación	Correo	01/09/2024	01/12/2024	Revisión semestral
010	Servidor de archivos	Pérdidda de datos	Grave	ALTA	Respaldo regular de los datos	Respaldo de datos	Respaldo de datos	Archivos	01/09/2024	01/12/2024	Pruebas de respaldo
011	0		0	#N/D		0					
012	0		0	#N/D		0					
013	0		0	#N/D		0					
014	0		0	#N/D		0					
015	0		0	#N/D		0					
016	0		0	#N/D		0					
017	0		0	#N/D		0					
018	0		0	#N/D		0					
019	0		0	#N/D		0					
020	0		0	#N/D		0					
021	0		0	#N/D		0					
022	0		0	#N/D		0					
023	0		0	#N/D		0					
024	0		0	#N/D		0					
025	0		0	#N/D		0					
026	0		0	#N/D		0					
027	0		0	#N/D		0					
028	0		0	#N/D		0					
029	0		0	#N/D		0					
030	0		0	#N/D		0					
031	0		0	#N/D		0					
032	0		0	#N/D		0					
033	0		0	#N/D		0					
034	0		0	#N/D		0					
035	0		0	#N/D		0					
036	0		0	#N/D		0					
037	0		0	#N/D		0					
038	0		0	#N/D		0					
039	0		0	#N/D		0					
040	0		0	#N/D		0					
041	0		0	#N/D		0					
042	0		0	#N/D		0					

4. 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.