CUESTIONES TEÓRICAS SEGURIDAD INFORMÁTICA SMR

Tema 1 – SEGURIDAD INFORMÁTICA

Explica los **servicios que proporciona la seguridad informática**. Nombra dos técnicas de seguridad que proporcionan cada uno de los servicios,

Explica los **servicios que ofrece la seguridad informática**.

Explica para que sirve la **seguridad informática**.

Define el concepto de **riesgo de un sistema informático**, cuáles son los aspectos que influyen en el aumento del riesgo percibido de un sistema informático.

Explica la relación entre la **seguridad informática** y el **riesgo** de un sistema informático.

Explica el concepto de **confidencialidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la confidencialidad de los datos de un sistema informático.

Explica el concepto de **disponibilidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la disponibilidad de un sistema informático.

Explica el concepto de **integridad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la integridad de los datos de un sistema informático.

Explica el concepto de **responsabilidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la responsabilidad en un sistema informático.

Explica la diferencia entre **Vulnerabilidad** y **Amenaza** en un sistema informático.

Explica en que consiste el concepto de **Alta Disponibilidad (High Availability)** en seguridad informática.

Enumera y describe las **características de una red defendible** (Red de Área Local – LAN).

Explica las **fases de un compromiso (ataque) a un sistema informático**.

Describe el concepto de **seguridad pasiva** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

Explica dos **técnicas o herramientas de seguridad pasiva** que consideres importantes.

Describe el concepto de **seguridad activa** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

Explica dos **técnicas o herramientas de seguridad activa** que consideres importantes.

Describe el concepto de **seguridad física** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

Explica dos **técnicas o herramientas de seguridad física** que consideres importantes.

Describe el concepto de **seguridad lógica** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

Explica dos **técnicas o herramientas de seguridad lógica** que consideres importantes.

Explica todas las **técnicas de seguridad activa** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

Explica todas las **técnicas de seguridad pasiva** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

Explica todas las **técnicas de seguridad física** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

Explica todas las **técnicas de seguridad lógica** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

Explica la diferencia entre **seguridad física y seguridad lógica** poniendo además 2 ejemplos de herramientas de cada uno de estos tipos de seguridad informática.

Explica la diferencia entre **seguridad activa y seguridad pasiva** poniendo además 2 ejemplos de herramientas de cada uno de estos tipos de seguridad informática.

Describe cinco **técnicas de seguridad** que consideres imprescindibles en un equipo que va a utilizar una persona en su casa con conexión a Internet a través de una linea ADSL (**Configuración de seguridad para un hogar**). Indica cuales técnicas son imprescindibles y cuales opcionales.

Describe cinco **técnicas de seguridad** que consideres imprescindibles para una empresa pequeña (5 empleados con un ordenador cada uno , un servidor y una red local conectada a Internet con un router ADSL) (**Configuración de seguridad para una pequeña empresa**). Indica cuales técnicas son imprescindibles y cuales opcionales.

Tema 2 – SEGURIDAD PASIVA: HARDWARE Y ALMACENAMIENTO

Define el concepto de **seguridad pasiva** de un sistema informático:

Comenta tres técnicas o herramientas de seguridad **pasiva y física**.

Comenta tres técnicas o herramientas de seguridad **pasiva y lógica**.

Explica las características de un **CPD**.

Explica la diferencia entre **CPD** y **Centro de Respaldo**.

Explica el concepto, características y utilidad de un **SAI**.

Explica los conceptos de **almacenamiento**:

Local vs Remoto
Distribuido vs Centralizado
Redundante vs Único

Explica en que consiste el sistema **RAID**. Describe los tipos de RAID que conozcas.

Explica la técnica de almacenamiento en **RAID 0**. Concepto, características, ventajas e inconvenientes de utilizarla.

Explica la técnica de almacenamiento en **RAID 1**. Concepto, características, ventajas e inconvenientes de utilizarla.

Explica la técnica de almacenamiento en **RAID 5**. Concepto, características, ventajas e inconvenientes de utilizarla.

Explica el concepto, utilidad y diferencias entre los sistemas de **almacenamiento y organización de disco(s) Windows**: Simple, Distribuido o Seccionado.

Explica el concepto de **recurso compartido en Windows**, utilidad y características.

Explica en que consiste la **virtualización**. Ejemplos de software de virtualización que conoces.

Explica las diferencias entre los sistemas de almacenamiento **DAS**, **NAS** y **SAN**.

Explica cuáles son las principales características y tecnologías utilizadas en los sistemas de almacenamiento **SAN**.

Explica la diferencia entre **cluster**, **granja de servidores** y **servidor de virtualización**.

Tema 3 – SEGURIDAD PASIVA: RECUPERACIÓN DE DATOS

Explica las diferencias, similitudes y relación entre los siguientes conceptos:

Copia de seguridad
Punto de restauración
Imagen de una partición
Imagen de un disco
Imagen del sistema
Clonación de un disco
Congelación de un sistema, partición o disco
Centro de respaldo
Servidor de imágenes

Explica las **características** que debe tener una buena **copia de seguridad** (Incluidas en la **política de copia de seguridad** de tu empresa).

Explica los **tipos de copia de seguridad de datos** que conozcas.

Explica la diferencia entre una **política de copia diferencial** y una **política de copia incremental**.

Explica la **política de almacenamiento y organización de la información** (datos de la empresa) que recomendarías a una pequeña empresa (5 empleados / 5 PC (iguales), un servidor w2012, una impresora de red y conexión a Internet a través de un router ADSL en todos los puestos).

Describe una **política de copia de seguridad** que recomendarías a una pequeña empresa (5 empleados / 5 PC (iguales), un servidor w2012, una impresora de red y conexión a Internet a través de un router ADSL en todos los puestos).

Explica el concepto y utilidad de **imagen del sistema** y un ejemplo de herramienta para poder hacerla.

Explica la diferencia entre una imagen de disco y una imagen de partición.

Si un equipo tiene una **partición de sistema** (donde está instalado el sistema operativo y los programas que utiliza) y una **partición de datos** (donde guardamos el trabajo que realizamos). ¿Cuál es la partición de la que debemos hacer la imagen para recuperar el equipo cuando se estropee? ¿Qué debemos hacer con la otra partición?

Explica la utilidad de un **punto de restauración en Windows**.

Describe las alternativas que conozcas para la **ubicación de las copias de seguridad.**

Explica los mecanismos de **protección y alta disponibilidad** de los equipos de tu empresa.

Explica el **protocolo de recuperación total o parcial de una copia de datos**.

Explica el **protocolo de recuperación de una imagen del sistema**.

Localiza **software** (programas) adecuados para realizar **copias de seguridad** de datos. ¿Cuál recomendarías?

Localiza **software** (programas) adecuados para realizar **imágenes del sistema**. ¿Cuál recomendarías?

Localiza webs que podamos utilizar para almacenar **copias de seguridad (en la nube)**.

Explica los mecanismos de **copia de seguridad de configuraciones especiales** que recomendarías en tu empresa. Ejemplos:

- **Copia de la configuración de un servicio**: DHCP, AD, DNS…
- Copia trimestral de datos después de cerrar la contabilidad…
- Copia de la **base de datos**…
- Copia en la nube de…

Tema 4 – CRIPTOGRAFÍA

Explica el concepto de **cifrado de clave privada**, su utilidad y algoritmos de clave privada que conoces.

Explica el concepto, utilidad y ejemplos de **algoritmos de cifrado simétrico**.

Explica el concepto de **cifrado de clave pública**, su utilidad y algoritmos de clave pública que conoces.

Explica el concepto, utilidad y ejemplos de **algoritmos de cifrado asimétrico**.

Explica el concepto de **certificado digital** y su utilidad. Ejemplos de uso.

Explica en qué consiste el mecanismo de **intercambio de claves de Diffie-Hellman**, tipo de cifrado que utiliza y en que famosos protocolos se utiliza esta forma de cifrado.

Explica el concepto, utilidad y ejemplos de **algoritmos de función resumen** – hash – funciones condensadoras seguras.

Explica el concepto, utilidad y **proceso de la firma digital** de un documento.

Explica el concepto, utilidad y **proceso de comprobación de la firma digital** de un documento.

Explica el concepto de **firma digital** y su utilidad. Ejemplos de uso.

Explica la diferencia entre **firma digital** de un documento y **digitalizar la firma** sobre un documento.

Explica la utilidad de programas como **7zip**. Su relación con la seguridad informática y con los algoritmos criptográficos.

Explica la relación entre la criptografía y el protocolo **HTTPS**.

Explica la relación entre la criptografia y el protocolo **SSH**.

Explica la relación entre la criptografía y el protocolo **WPA2**.

Explica la relación entre la criptografía y el protocolo **SFTP**.

Explica la relación entre la criptografía y el protocolo **FTPS**.

Utilidad y características de una **Autoridad de Certificación**.

Explica la relación entre **PKI** y el estándar **X-509**.

Enumera las **aplicaciones de la criptografía** que conozcas indicando que tipo de cifrado o algoritmo criptográfico utilizan y para que sirven.

¿Qué es la **esteganografía**? ¿Conoces algún programa para implementarla?

¿Qué **programa** recomendarías en una pequeña empresa para **cifrar la información almacenada en el servidor de ficheros**?

¿Qué **protocolo** utilizarías para **administrar** los servidores de una pequeña empresa de forma **remota y segura**?

¿Cómo se almacenan las **contraseñas de las cuentas** de usuario en el sistema?

¿Podemos **crear y utilizar nuestros propios certificados digitales** o tenemos que acudir a una autoridad de certificación pública para que nos los genere?

Tema 5 – SEGURIDAD ACTIVA EN EL SISTEMA

Explica los siguientes conceptos:

Seguridad activa
Hacker - Analista de seguridad
Malware
Vulnerabilidad - Amenaza - Ataque

Explica en que consiste un **ataque de acceso**. Pon un ejemplo.

Explica en que consiste un **ataque de modificación**. Pon un ejemplo.

Explica en que consiste un **ataque de denegación de servicio (DoS)** (**Denial of Service**). Pon un ejemplo.

Explica en que consiste un ataque de **denegación de servicio distribuido (DdoS)**. Pon un ejemplo.

Explica en que consiste un ataque de **refutación**. Pon un ejemplo.

Explica la diferencia entre los siguientes tipos de software malintencionado: **Virus, Troyanos y Gusanos.**

Explica todas las técnicas de **seguridad acceso** que recomendarías para a un equipo de **hogar** conectado a Internet a través de un router ADSL.

Explica las técnicas que utilizarías como administrador de sistemas para mejorar la **seguridad de acceso** a los equipos de una pequeña **empresa**.

Explica porque podemos considerar **Active Directory** como una herramienta de seguridad. ¿En qué consiste? ¿Qué aspectos de la seguridad informática mejora esta herramienta?

Explica los mecanismos de **protección del arranque** de los sistemas de tu empresa.

Explica la **forma** en la que **accederías** a la información de la **partición de datos** (o a la información del disco duro) de un equipo del que no sabes (en principio) el sistema operativo que tiene ni conoces ninguna cuenta o password de usuario.

Explica la forma en la que comprobarías que un equipo **windows** está funcionando bien y está correctamente (seguro) configurado.

Explica la forma en la que comprobarías que un equipo **linux** está funcionando bien y está correctamente (seguro) configurado.

Explica la forma en la que comprobarías que un **servior linux** está funcionando bien y está correctamente (seguro) configurado y sus servicios funcionan correctamente.

Describe la forma en la que comprobarías el **log de Apache** para saber si el servicio funciona correctamente.

Describe la forma en la que comprobarías el **log del servicio SSH**.

Describe el **log de un servicio** (cualquiera de los que has estudiado durante el curso) explicando donde se encuentra, ¿para qué sirve?, ¿que podemos encontrar en él?

Describe la forma en la que comprobarías los **servicios instalados en un servidor de Ubuntu**.

Describe la forma en la que comprobarías los **servicios arrancados (running) en un servidor de Ubuntu**.

Describe la forma en la que comprobarías el propietario y los permisos de un directorio de un servidor Ubuntu.

Describe la forma en la que comprobarías los **grupos de usuarios y sus miembros** de un servidor Ubuntu.

Describe la forma en la que comprobarías los **usuarios y los grupos a los que pertenecen** de un servidor Ubuntu.

Describe la forma en la que **crearías, deshabilitarías y habilitarías una cuenta de usuario** en un servidor de Ubuntu.

Explica en qué consisten los siguientes ataques y localiza algún programa o mecanismo de seguridad que pueda servir para defendernos de ellos:

Virus
Troyanos
Gusanos
Keylogers
Dialers
Phishing
Spam
Sniffing o análisis de tráfico
Exploit
Hijacking
Ingeniería social
Robo de hardware
Conexión no autorizada a equipos o servidores
Conexión remota
Denegación de servicio
Inundación de peticiones SYN
Spoofing o suplantación de identidad
ARP Spoofing
DNS Spoofing
Zombie

Tema 6 – SEGURIDAD ACTIVA EN REDES

Describe las **características de una red defendible** (Red de Área Local:LAN).

Describe distintas técnicas de cifrado de las comunicaciones como herramienta de seguridad.

Enumera y describe:

Protocolos de aplicación que cifran las comunicaciones.

¿Cómo funciona HTTPS?

¿Cómo funciona SSH?

Protocolos de transporte que cifran la comunicación.

Protocolos de red que cifran la comunicación.

Protocolos de la capa de acceso a la red que cifran la comunicación.

Construir un mapa conceptual donde se encuentren los protocolos de comunicación seguros, su relación entre ellos, capa del modelo OSI...

Cortafuegos de red como herramienta de seguridad en la red.

Tablas y cadenas de reglas de **IPTABLES**

Proxy como herramienta de seguridad en la red.

DMZ como herramienta de seguridad en la red. Servicios que la empresa ofrece en Internet.

VPN como herramienta de protección de la red local para intervenciones remotas

Explica el proceso de instalación y configuración de un servicio de **administración remota segura con SSH en un servidor Ubuntu**. Explica también el software (cliente de administración remota SSH) necesario y su configuración en un cliente windows X para la conexión segura al servidor Ubuntu que hemos configurado. El cliente está en la misma red que el servidor y tienen conectividad.

Explica el proceso de instalación y configuración de un servicio de **administración remota segura con el servicio escritorio remoto en un servidor Windows**. Explica también el software necesario y su configuración en un cliente windows X para la conexión segura al servidor Windows que hemos configurado. El cliente está en la misma red que servidor y tienen conectividad.

Explica el **establecimiento de conexión entre un cliente y un servidor HTTPS**, señalando los elementos necesarios en ambas partes para que pueda establecerse la conexión.

Explica la diferencia entre los protocolos **HTTP** y **HTTPS**.

Explica las técnicas que utilizarías para garantizar y mejorar la **seguridad de la red cableada** de una pequeña empresa de la que eres el administrador.

Explica las técnicas que utilizarías para garantizar y mejorar la **seguridad de la red wi-fi** de un hogar.

Describe los mecanismos de **seguridad** que utilizarías en una red **Wi-Fi 802.11g** constituida por un router Wi-Fi que da acceso a Internet a los portátiles de dos usuarios de una oficina de abogados.

Explica el **establecimiento de conexión a una red Wi-Fi WPA2 personal**, señalando los elementos necesarios en ambas partes para que pueda establecerse la conexión.

Enumera y explica las **técnicas o herramientas de seguridad** que utilizarías para mejorar la seguridad de la **LAN de una pequeña empresa**.

¿Cuál es el puerto que utiliza el servidor **SSH** para comunicarse con sus clientes?.

¿Cuál es el puerto que utiliza el servidor **SFTP** para comunicarse con sus clientes?.

Explica el concepto de **VPN**. Tipos de VPN.

¿Qué software utilizarías para monitorizar (localizar, averiguar) los equipos conectados en la misma red que tu equipo?

¿Qué software utilizarías para monitorizar (localizar, averiguar) los puertos abiertos en un equipo que está en la misma red que tu equipo?

Ejercicio de **traducción de números binario – decimal – hexadecimal**.

BINARIO	HEXADECIMAL	DECIMAL
1101100		
	1E	
		121

Tema 7 – SEGURIDAD ACTIVA EN REDES: CORTAFUEGOS

Enumera y describe:

Cortafuegos de red como herramienta de seguridad en la red.
Tablas y cadenas de reglas de **IPTABLES**
Proxy como herramienta de seguridad en la red.
DMZ como herramienta de seguridad en la red. Servicios que la empresa ofrece en Internet.
VPN como herramienta de protección de la red local para intervenciones remotas

Explica el concepto de **cortafuegos**. Características de un cortafuegos como herramienta de seguridad.

Explica el concepto de **cortafuegos**. Tipos de cortafuegos. Características de un cortafuegos como herramienta de seguridad.

Explica la diferencia entre **cortafuegos local** y **cortafuegos de red** y la ubicación de estos dos tipos de cortafuegos en la red de una empresa.

Explica la utilidad de los siguientes servicios en la red local de una pequeña empresa: **router**, **cortafuegos de red** y **proxy**.

Explica la utilidad de las tres tablas de cadenas de IPTABLES.

Explica la utilidad de las reglas incluidas en cada una de las cadenas de la **tabla FILTER** de **IPTABLES**.

Explica las **acciones** (que recuerdas) que puede llevar al final una regla de **IPTABLES**.

¿Cómo se establece la **política por defecto** en una cadena de **IPTABLES**?

Explica el significado de los siguientes **comandos de IPTABLES**:

```
iptables -P INPUT DROP
iptables -t nat -A POSTROUTING -o ext -j MASQUERADE
```

Explica el concepto de **VPN**: utilidad, características, implementación y funcionamiento.

Explica un ejemplo en el que consideres necesaria la implementación de una **VPN** y los componentes que consideras necesarios para ponerla en marcha.

Explica el concepto de **DMZ**: utilidad, características, implementación y funcionamiento.

Explica un ejemplo en el que consideres necesaria la implementación de una **DMZ** y los componentes que consideras necesarios para ponerla en marcha.

Tema 8 – SEGURIDAD ACTIVA EN REDES: PROXY

Enumera y describe:

Cortafuegos de red como herramienta de seguridad en la red.
Tablas y cadenas de reglas de **IPTABLES**
Proxy como herramienta de seguridad en la red.
DMZ como herramienta de seguridad en la red. Servicios que la empresa ofrece en Internet.
VPN como herramienta de protección de la red local para intervenciones remotas

Explica el concepto de **cortafuegos**. Características de un cortafuegos como herramienta de seguridad.

Explica el concepto de **cortafuegos**. Tipos de cortafuegos. Características de un cortafuegos como herramienta de seguridad.

Explica la utilidad de los siguientes servicios en la red local de una pequeña empresa: **router**, **cortafuegos de red** y **proxy**.

Explica el concepto de **Proxy**: utilidad, características, implementación y funcionamiento.

Explica los **tipos de Proxy** que conozcas y su utilidad.

Describe la utilidad y características de un **servidor proxy web, caché y transparente**.

Explica el concepto y utilidad de un **proxy inverso.**

Enumera los **software** que recuerdes que podamos utilizar en una pequeña empresa como **servidores proxy**.

Tema 9 – NORMATIVA EN SEGURIDAD INFORMÁTICA

Explica la utilidad y finalidad de la **Ley Orgánica de protección de datos de carácter personal 15/1999 (LOPD).** **Sustituida por el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD)**

Explica las siguientes definiciones incluidas en la **Ley Orgánica de protección de datos de carácter personal**:

Datos de carácter personal
Consentimiento del interesado
AEPD
Prestador de servicios (en la LSSI/CE)

Explica la utilidad de la AEPD: **Agencia Española de Protección de Datos.**

Explica las medidas que tomarías para **realizar de forma legal en tu empresa un tratamiento con datos de carácter personal** (Nombre, Apellidos, Fecha de nacimiento, Teléfono, Dirección) de una serie de personas. El tratamiento consiste en llamar por teléfono a las personas para felicitarles en el día de su cumpleaños y enviarles un regalo.

Comenta el siguiente texto:
"La normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas".

Explica la utilidad y finalidad de la **Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI/CE).**

Explica las siguientes definiciones incluidas en la **Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI/CE):**

Prestador de servicios (en la LSSI/CE)

Nueva legislación (pendiente de actualizar en los apuntes)

Protección de datos

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente en aquellos artículos que no contradigan el RGPD)
- Real Decreto1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos

Sociedad de la información y telecomunicaciones

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones

PREGUNTAS GENÉRICAS QUE RESUMEN EL CURSO

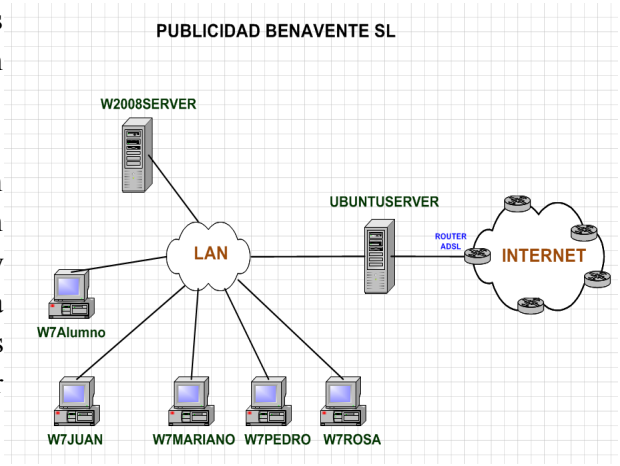
En la empresa Publicidad Benavente SL trabajan 5 personas:

Juan:	Dueño y jefe de la empresa.
Mariano, Pedro y Rosa:	Publicistas de la empresa
Tu:	Informático de la empresa.

La decisión sobre los equipos, sistemas operativos y redes de conexión necesarios ya está tomada e implementada como se acordó según el modelo adjunto.

En los próximos días debes poner en marcha cuatro técnicas de seguridad que permitan poner en marcha la empresa con las mínimas garantías para comenzar a trabajar.

La decisión sobre cuales son las cuatro técnicas y el orden en el que las vas a poner en marcha debes tomarla pensando en aquellas técnicas que reduzcan considerablemente el riesgo y aumenten considerablemente la seguridad informática; una vez puestas en marcha estas cuatro técnicas todos los empleados deben de estar en condiciones de poder comenzar a trabajar.



Describe de forma detallada la forma en la que implementarías y los equipos en los que trabajarías para poner en marcha **cada una de las cuatro técnicas que has elegido** indicando el trabajo que realizarías en cada uno de estos equipos.

Puedes mencionar otras técnicas de seguridad que implementarías en la empresa mas adelante indicando en que orden las pondrías en marcha, otras técnicas que consideras necesarias para mejorar la seguridad informática de la empresa.

TÉCNICAS DE SEGURIDAD ELEGIDAS:

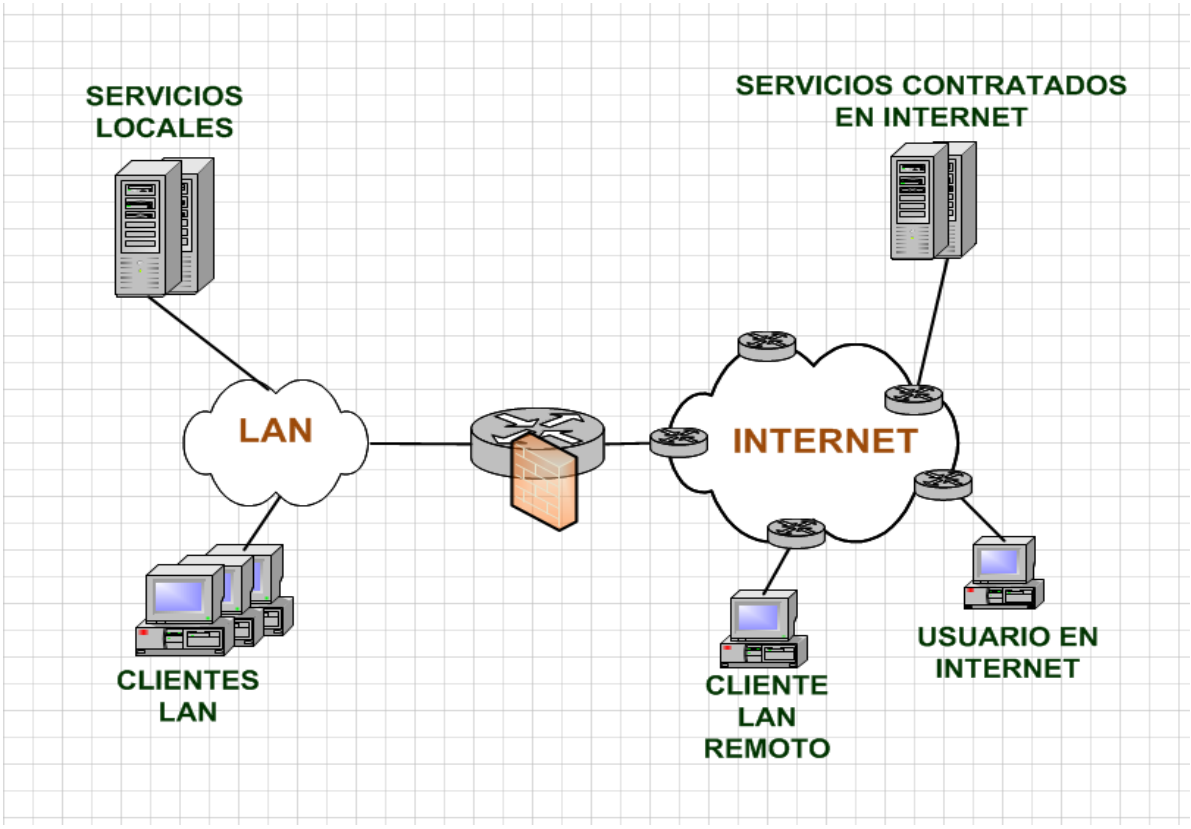
1:
2:
3:
4:

OTRAS TÉCNICAS PARA IMPLEMENTAR MÁS ADELANTE:

5:
6:
7:
8:
9:
10:

Prioriza y ubica en el siguiente modelo las **herramientas y técnicas de seguridad informática** que utilizarías en tu **empresa**... indicando además si son activas, pasivas, físicas y/o lógicas.

MÁS PRIORITARIO – MAS IMPORTANTE – OBLIGATORIO	ACTIVA	PASIVA	FÍSICA	LÓGICA
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
MENOS PRIORITARIO – MENOS IMPORTANTE - OPCIONAL				



Prioriza y ubica en el siguiente modelo las **herramientas y técnicas de seguridad informática** que utilizarías en tu **hogar**... indicando además si son activas, pasivas, físicas y/o lógicas.

MÁS PRIORITARIO – MAS IMPORTANTE – OBLIGATORIO	ACTIVA	PASIVA	FÍSICA	LÓGICA
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
MENOS PRIORITARIO – MENOS IMPORTANTE - OPCIONAL