3. Grabación, modificación e intercambio de información.

La información se puede intercambiar, grabar o modificar; para realizar estas acciones podemos utilizar diversos documentos y procedimientos, que son los siguientes:

3.1. Documentos estáticos y dinámicos.

Un documento dinámico está diseñado para "recolocar el contenido" dependiendo del tamaño de la ventana, la resolución del dispositivo y otras variables. Los documentos dinámicos tienen varias características integradas que incluyen la búsqueda, modos de presentación que optimizan la legibilidad y la capacidad de cambiar el tamaño y la apariencia de las fuentes. Estos documentos son óptimos para su uso cuando la facilidad de lectura constituye el principal escenario de consumo del documento. Ejemplo: un documento dinámico al visualizarlo en varias ventanas de tamaños diferentes, a medida que el área de presentación cambia, el contenido se recoloca para utilizar el espacio disponible de la mejor forma posible.

Por el contrario, los documentos estáticos o fijos están diseñados para tener una presentación estática. Los documentos fijos son útiles cuando la fidelidad del contenido de origen resulta esencial. Ejemplo: un documento pdf.

3.2. Vinculación e incrustación de información.

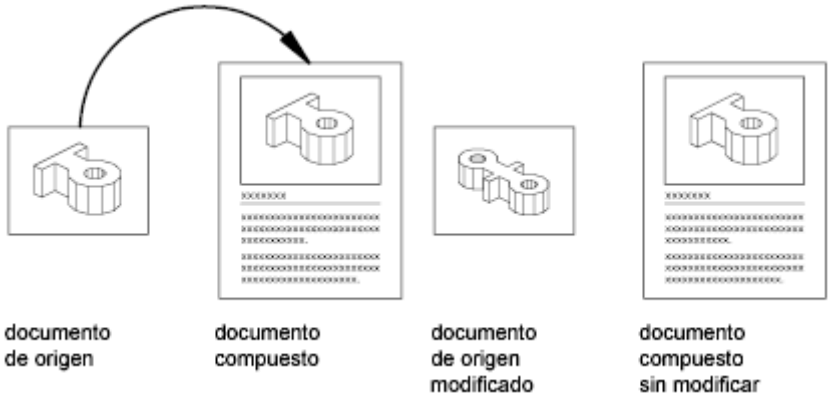
La incrustación y vinculación de objetos es una forma de utilizar información de una aplicación en una aplicación distinta. Para utilizar OLE, se necesitan aplicaciones de origen y destino que admitan OLE.

Tanto la vinculación como la incrustación insertan en un documento información procedente de otro. Además, los objetos OLE vinculados o incrustados se pueden editar desde la aplicación de destino. Sin embargo, la vinculación y la incrustación almacenan la información de forma diferente.

La relación entre incrustar y vincular es similar a la que existe entre insertar un bloque y crear una referencia externa.

Incrustación de objetos

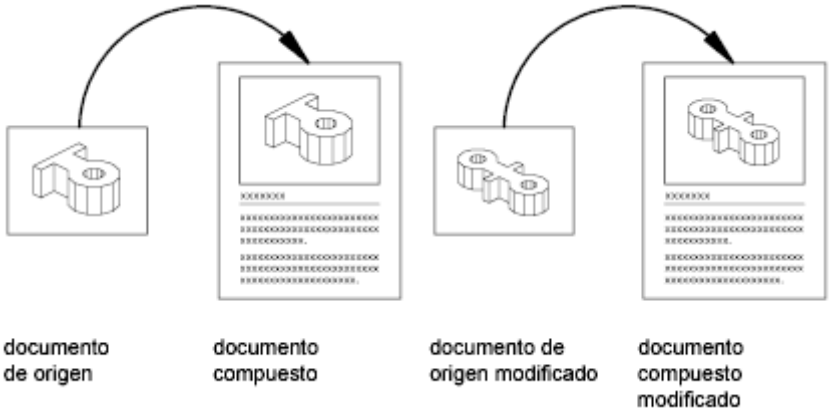
La incrustación de un objeto OLE consiste en la copia de información de otro documento. Cuando se incrustan objetos, no existe vínculo con el documento de origen, de modo que cualquier modificación que se haga en éste no se verá reflejada en los documentos de destino. Incruste objetos si desea utilizar la aplicación con la que los creó para editarlos, pero no desea que el objeto OLE se actualice si modifica información en el documento de origen.



Vinculación de objetos

Vincular un objeto consiste en una establecer una referencia a la información de otro documento. Vincule objetos si desea utilizar la misma información en más de un documento. Así, si modifica la información original, sólo tendrá que actualizar los vínculos para que se actualice el documento que contiene los objetos OLE. También puede establecer que los vínculos se actualicen automáticamente.

La vinculación de un dibujo requiere el mantenimiento del acceso al documento vinculado y a la aplicación de origen. Si cambia el nombre o desplaza cualquiera de ellos, quizá tenga que restablecer el vínculo.



6. **Pon un ejemplo de documento estático.**
7. **¿En qué consiste vincular un objeto?**

4. Procedimientos para usar y compartir recursos.

Vivimos en un mundo interconectado: casi todos los dispositivos digitales forman parte de una red. Y es precisamente esa función de los dispositivos —la conectividad— la que ha permitido que la revolución digital transforme nuestras sociedades.

¿Por qué? Porque el hecho de que tu ordenador pueda comunicarse con los de tus compañeros es extremadamente útil. Si esos ordenadores están interconectados, podéis compartir todos vuestros archivos. Así se ahorra mucho tiempo, porque no hace falta enviar tantos correos electrónicos. Además, con los ordenadores conectados en red, toda una oficina puede utilizar un mismo dispositivo, como una impresora. Esto reduce los costes y hace que las diferentes tareas sean muy cómodas para todos. Conectar los ordenadores en red aumenta la productividad y amplía las posibilidades, la capacidad y las funciones de cualquier ordenador. Piensa en todos los datos e información a los que tienes acceso a través de Internet porque puedes conectarte en red con todos esos otros ordenadores. ¿Podrías almacenar tanta información solo en tu ordenador? Imposible.

4.1. Conceptos básicos de las redes y la conectividad.

Una red informática es una configuración que conecta a dos o más ordenadores para que compartan una serie de servicios e información: por ejemplo, se pueden compartir archivos de audio o vídeo digital, servidores de aplicaciones y almacenamiento, impresoras, aplicaciones de correo electrónico y mensajería instantánea, acceso a Internet, etc.

Para que dos ordenadores se comuniquen entre sí y formen una red, se necesitan tres elementos:

1. Una conexión a través de un medio de conexión.

   El medio de conexión es un soporte que se usa para interconectar los ordenadores de una red, como un cable coaxial, un cable de par trenzado o un cable de fibra óptica. La conexión también puede establecerse de forma inalámbrica mediante señales de radio, tecnología láser o infrarroja o transmisión por satélite.

2. Un lenguaje común, que en las redes se denomina protocolo.

   Un protocolo es un conjunto de reglas definidas que permite a dos entidades comunicarse a través de una red. Sin protocolos no sería posible que los ordenadores intercambiaran y utilizaran la información; es lo que se llama interoperabilidad. Existen diferentes protocolos para distintos usos, por ejemplo, para las redes por cable (Ethernet), las redes inalámbricas (como 802.11ac) y la comunicación por Internet (por ejemplo, IP).

Nota

Normalmente, los protocolos funcionan sin que los veamos, por lo que no es necesario que sepamos cómo funciona cada uno de ellos. Sin embargo, puede ser útil familiarizarse con algunos protocolos habituales para entender mejor la configuración de los programas de software, como los navegadores web y los clientes de correo electrónico.

- Protocolo de control de transmisión (TCP): divide el mensaje en una serie de paquetes y los envía desde el origen hasta el destino para volver a ensamblarlos en este último.
- Protocolo de Internet (IP): es un protocolo de direcciones y se utiliza principalmente con TCP. TCP/IP es el protocolo de conexión de redes más común.
- Protocolo de oficina de correos (POP): está diseñado para recibir correos electrónicos entrantes.
- Protocolo para la transferencia simple de correo (SMTP): envía y distribuye el correo electrónico saliente.
- Protocolo de transferencia de archivos (FTP): transfiere archivos de un sistema a otro, por ejemplo, archivos multimedia, archivos de texto, documentos, etc.
- Protocolo de transferencia de hipertexto (HTTP): transfiere documentos hipermedia, como el HTML. Se diseñó para la comunicación entre los navegadores y los servidores web, pero también se puede utilizar con otros fines. Al igual que HTTP, HTTPS transfiere los datos en formato de hipertexto, pero este último los transmite en un formato cifrado.

3. Una dirección única.

   En el contexto de las redes, es muy importante la relación entre el servidor y el cliente.

   Un servidor es un ordenador que alberga contenidos y servicios como un sitio web, un archivo multimedia o una aplicación de chat. Un buen ejemplo de servidor es el ordenador que contiene el sitio web de una pyme y que puedes visitar si escribes en tu navegador web el nombre de ese sitio web. El servidor tiene dentro esa página y la envía cuando se le solicita.

   Un cliente es otro ordenador, como tu portátil o tu teléfono móvil, que solicita ver, descargar o utilizar el contenido. El cliente puede conectarse a través de una red para intercambiar información. Por ejemplo, cuando solicitas ver la página de búsqueda de Google en el navegador web, tu ordenador es el cliente. Este es el modelo de red que se utiliza en la Web y en Internet.

   El envío y la recepción de mensajes entre ambos se conoce como el patrón de mensajería solicitud-respuesta. Utilizando un protocolo determinado, el cliente envía una solicitud y el servidor debe devolverle una respuesta.

   Esta relación es importante por varias razones. En primer lugar, todos los datos necesarios pueden estar en un mismo lugar, dentro del servidor, lo que ayuda a protegerlos y a autorizar a quienes quieran acceder a esos datos. Además, no es necesario que el servidor se encuentre cerca del cliente para que este pueda consultar los datos. Y, por último, con este modelo de cliente-servidor es fácil actualizar los sistemas de acceso, porque todo es independiente.

Nota

Breve resumen de la terminología habitual en el campo de las redes:

- Paquete: cuando hay que transmitir datos, antes de enviarlos, estos se dividen en pequeños segmentos de un mensaje, llamados paquetes. Una vez que llegan a su destino, se vuelven a ensamblar para formar el conjunto de datos original.
- Dirección de control de acceso al medio (MAC): la dirección MAC o dirección física identifica de forma exclusiva a cada host. Está asociada a la tarjeta de interfaz de red (NIC).
- Dirección IP: la dirección IP es un número de identificación que se asocia a un ordenador o a una red informática en concreto. Cuando el ordenador o la red se conectan a Internet, la dirección IP permite que los ordenadores envíen y reciban información, además de identificar los sistemas de origen y de destino. Una dirección IP no es más que un conjunto de cuatro números entre el 1 y el 254, separados por puntos. Un ejemplo de dirección IP es 192.084.15.1.

  La dirección IP es similar a una dirección postal. Existen diferentes clasificaciones, o tipos, de direcciones IP. Además, las redes pueden ser públicas o privadas; a las direcciones IP públicas se puede acceder desde cualquier lugar de Internet, pero no sucede lo mismo con las direcciones IP privadas.
- Router: los routers son elementos de hardware que transfieren datos entre diferentes redes para permitir que se comuniquen entre ellas. Los routers permiten transmitir datos de un extremo a otro estableciendo rutas entre los dispositivos de esos extremos y reenviando los datos a lo largo de la ruta, desde el nodo emisor hasta el de destino. Dicha ruta suele requerir varios saltos entre routers, que pueden tener lugar entre una red privada e Internet, entre una red privada y un servidor o entre diferentes redes conectadas entre sí.
- Cortafuegos: un cortafuegos (o firewall) es un dispositivo de seguridad de red que controla el tráfico entrante y saliente de acuerdo con unas reglas predeterminadas. Puede proteger cualquier red que esté conectada a Internet. Se puede configurar para que bloquee o permita el tráfico en función del estado, el puerto o el protocolo. Algunos cortafuegos también llevan incorporado un software antivirus y de detección de amenazas. El cortafuegos se puede colocar antes o después del router para proteger el sistema de las amenazas externas.
- Proveedores de servicios de Internet (ISP): los ISP (del inglés Internet Service Provider) son compañías que proporcionan conexión a Internet a todo tipo de usuarios, tanto a particulares como a empresas y otras organizaciones.
- Banda ancha: es la transmisión de datos a través de una conexión a Internet de alta velocidad y gran ancho de banda. La banda ancha proporciona un acceso muy rápido a Internet gracias a diversos tipos de tecnologías, como la fibra óptica, la tecnología inalámbrica, las conexiones de cable, el ADSL y las conexiones por satélite.
- Ethernet: es una tecnología que conecta las redes de área local (LAN) por cable y permite que los dispositivos se comuniquen entre sí mediante un protocolo que constituye el lenguaje común de la red.
- Hub: es un dispositivo de red que repite el tráfico que recibe a todos los dispositivos conectados.
- Switch: es un dispositivo de red que envía el tráfico que recibe a un dispositivo conectado específico, por ejemplo, a un ordenador determinado.

4.2. Tipos de redes.

A medida que las tecnologías han ido mejorando, se han desarrollado diversas versiones de los tres elementos que hemos mencionado más arriba para cubrir mejor las diferentes necesidades a la hora de conectarse, con funciones muy específicas que pueden combinarse para definir distintos tipos de redes.

Las redes informáticas no son todas iguales. La red que utilizamos para conectar un ordenador a un teléfono a través de Bluetooth es la más pequeña que podemos imaginar. A veces se denomina PAN (red de área personal) y, como su propio nombre indica, es una red unipersonal.

Si trabajas en una oficina, probablemente utilices una LAN (red de área local), que suele consistir en unos cuantos ordenadores independientes pero conectados a una o dos impresoras, un escáner y un dispositivo de almacenamiento local compartido. Pero las redes pueden ser mucho más grandes.

En el extremo opuesto, se habla de las MAN (redes de área metropolitana), que cubren todo un pueblo o ciudad, y de las WAN (redes de área amplia), que pueden abarcar cualquier zona geográfica. Internet es una WAN que cubre todo el planeta, pero en la práctica es una red de redes a la que se unen ordenadores.

Otra forma de diferenciar los tipos de redes es según si son de carácter público o privado.

Una red pública es una red a la que puede conectarse cualquier persona. El mejor ejemplo de este tipo de red es Internet, donde la gente puede visitar los servidores públicos a través de sus direcciones IP públicas o mediante el nombre de dominio que se les ha asignado.

Una red privada es cualquier red de acceso restringido cuyos servidores solo tienen direcciones IP privadas. Una red corporativa o la red de un centro educativo son ejemplos de redes privadas. A veces no está muy claro el límite entre las redes públicas y las privadas: por ejemplo, al utilizar la World Wide Web, puedes encontrarte con archivos protegidos por contraseña o sitios web exclusivos para suscriptores. De modo que, incluso en una red totalmente pública, es posible ofrecer cierto grado de acceso selectivo y privado.

Si trabajas en una gran empresa, probablemente te hayas acostumbrado a la idea de que gran parte de la información que compartes con tus compañeros solo esté accesible a través de los ordenadores internos. Si accedéis a esa información más o menos igual que a la Web, significa que se trata de una intranet: una especie de Internet/Web privado e interno al que no se puede acceder a través de la red de Internet pública. Pero ¿qué ocurre si trabajas desde casa y necesitas entrar en las secciones privadas de esa red corporativa a través del Internet público? Para eso puedes utilizar algo llamado VPN (red privada virtual), que es un túnel seguro que te da acceso a la red privada de tu trabajo a través de una red pública.

A continuación, ilustramos el funcionamiento de una red observando un tipo de red que nos resulta más familiar: la red doméstica.

A. Proveedor de servicios de Internet; B. Teléfono móvil; C. Módem Wi-Fi; D. Televisor inteligente; E. Ordenador portátil.

8. **Pon ejemplos de lo que se puede compartir en una red informática.**
9. **Explica lo que es el protocolo de internet (IP).**
10. **Explica qué es la dirección IP.**

5. Optimización de los sistemas.

Optimizar los sistemas informáticos es fundamental para obtener mejores resultados en cualquier organización. En un mundo cada vez más competitivo, mantenerse a la vanguardia y contar con sistemas eficientes puede marcar la diferencia.

Realizar un diagnóstico completo de los sistemas

Uno de los primeros pasos para optimizar los sistemas es realizar un diagnóstico completo. Es importante identificar cualquier aspecto que esté afectando su rendimiento y eficiencia. Durante el diagnóstico, se debe evaluar tanto el hardware como el software. Examinar la velocidad de los equipos, la capacidad de almacenamiento, la presencia de virus y malware, entre otros factores. Existen muchas herramientas y métodos para realizar un diagnóstico efectivo, como programas de análisis de rendimiento y pruebas de velocidad de la conexión. Es bueno utilizar estas herramientas para obtener una visión clara de la situación actual de los sistemas.

Actualizar y modernizar los sistemas de manera regular

Mantener los sistemas actualizados es esencial para su rendimiento y seguridad. Las actualizaciones de software y hardware suelen incluir mejoras y correcciones importantes que mejoran la funcionalidad y evitan vulnerabilidades. No se debe esperar a que surjan problemas para actualizar los sistemas. Programar actualizaciones regulares y aprovechar las últimas tecnologías disponibles. Mantener los sistemas modernizados permitirá aprovechar al máximo su rendimiento y funcionalidad.

Optimizar el rendimiento de los equipos informáticos

Mejorar el rendimiento de tus equipos informáticos puede tener un impacto significativo en la eficiencia y productividad de la organización. Hay varias técnicas que se puede emplear para

optimizar el rendimiento de los equipos. Eliminar archivos y programas innecesarios, realizar la desfragmentación del disco duro y configurar los programas de inicio para que solo se ejecuten los necesarios. Además, hay que asegurarse de que los equipos tengan suficiente memoria RAM y espacio de almacenamiento, ya que esto también puede afectar a su rendimiento.

Implementar medidas de seguridad efectivas

La seguridad es una preocupación fundamental en cualquier sistema informático. Para optimizar los sistemas, es crucial implementar medidas de seguridad efectivas. Se debe tener un buen antivirus instalado y actualizado, utilizar firewalls para proteger la red, establecer políticas de contraseñas seguras y realizar copias de seguridad regulares de los datos. La seguridad es un tema en constante evolución, por lo que se debe estar al tanto de las últimas amenazas y realizar actualizaciones periódicas en las medidas de seguridad.

Realizar un adecuado mantenimiento preventivo

No esperar a que tus sistemas fallen para tomar medidas. Realizar un mantenimiento preventivo regular ayudará a evitar problemas y a mantener los sistemas en óptimas condiciones. El mantenimiento preventivo incluye la limpieza de hardware, la optimización de software y la monitorización del rendimiento. Limpiar regularmente los ventiladores y los componentes internos de los equipos, optimizar los programas y archivos innecesarios y monitorizar el uso de recursos y el rendimiento de los sistemas. Estas acciones permitirán prevenir problemas y mantener la eficiencia de los sistemas a largo plazo.

Optimizar la velocidad de carga del sitio web

Si se tiene un sitio web, optimizar su velocidad de carga es fundamental para brindar una buena experiencia a los usuarios. La velocidad de carga de un sitio web puede afectar directamente el número de visitantes y las conversiones. Para optimizar la velocidad de carga, hay que considerar técnicas como la compresión de imágenes, la minimización de solicitudes HTTP y el uso de una buena estructura de código. Realizar pruebas de velocidad regularmente para identificar áreas de mejora y asegurarse de mantener el sitio web siempre rápido y eficiente.

Mejorar la eficiencia en el trabajo

Además de optimizar los sistemas informáticos, también es importante mejorar la eficiencia en el trabajo. La manera en que se utilizan los sistemas y recursos puede marcar la diferencia en la productividad de la organización. Organízarse de manera efectiva, establecer prioridades claras, gestionar el tiempo y automatizar tareas repetitivas. Estas prácticas ayudarán a aumentar la eficiencia y a aprovechar al máximo los recursos.

Monitorear y analizar el rendimiento de los sistemas

El monitoreo y análisis del rendimiento de los sistemas es esencial para detectar problemas y tomar medidas correctivas. Utilizar herramientas de monitoreo para obtener datos sobre el rendimiento de los sistemas, como el uso de CPU, la memoria RAM y el ancho de banda. Analizar estos datos de manera regular para identificar cuellos de botella y áreas de mejora. Utilizar la información recopilada para optimizar los sistemas y obtener mejores resultados.

Mantener un respaldo regular de los datos

Realizar copias de seguridad regulares de los datos es una precaución fundamental para garantizar su seguridad y disponibilidad. Utilizar servicios en la nube o dispositivos de almacenamiento externo para respaldar los datos de manera segura. Además, es importante realizar pruebas de recuperación de datos periódicamente para asegurarse de que los respaldos sean efectivos. De esta manera, estaremos preparados para cualquier eventualidad y se podrá recuperar los datos sin problemas.

Capacitar al personal en el uso eficiente de los sistemas

Por último, pero no menos importante, capacitar al personal en el uso eficiente de los sistemas informáticos. La capacitación adecuada puede marcar la diferencia en la productividad y eficiencia de la organización. Implementar programas de capacitación efectivos y asegurarse de que todos los empleados estén familiarizados con las mejores prácticas y herramientas disponibles. Además, brindar recursos adicionales, como tutoriales en línea y cursos especializados, para que los empleados puedan mejorar continuamente sus conocimientos y habilidades.

11. **Explica cómo se optimiza el rendimiento de los equipos informáticos.**
12. **Explica cómo se realiza un adecuado mantenimiento preventivo de los equipos informáticos.**

6. Técnicas de diagnóstico básico y solución de problemas.

A continuación, exponemos los problemas informáticos a los que las empresas suelen enfrentarse en su día a día. Hoy, queremos compartir algunos de los más relevantes, así como soluciones y propuestas que ayudarán a hacerles frente.

Problemas con la memoria RAM

Se trata de uno de los problemas más comunes con el que nos podemos encontrar en nuestro día a día de trabajo. De repente un día nuestra memoria nos dice que está llena. ¿Y ahora qué?

Si nuestro ordenador presenta problemas con la RAM puede ser debido a que tengamos un exceso de programas instalados o en ejecución, o por la presencia de troyanos que consumen recursos y de los que no somos ni conscientes.

¿Qué hacer en estos casos? Muchas veces sucede que no sabemos la cantidad de programas que tenemos instalados en nuestro ordenador, así que el primer paso será identificar qué nos está consumiendo tanta memoria para priorizar y seleccionar. Un proceso de optimización de recursos que muchas veces ya nos liberará memoria suficiente para poder trabajar con normalidad.

Si aun así seguimos con memoria insuficiente, siempre se podrá optar por añadir más RAM.

La pérdida de datos

Uno de los problemas informáticos en empresas más comunes. Son necesarias las copias de seguridad, incluso copias de las copias. La pérdida de datos e información es un inconveniente muy común en las Pymes, que muchas veces deciden actuar una vez tienen el susto.

De este modo, llegamos a una conclusión inexorable: contar con copias y con un sistema de seguridad es imprescindible para evitar cualquier posible incidente.

Los virus informáticos y los problemas de seguridad

Un dato curioso: cada mes se crean más de 6000 virus informáticos. No tener antivirus y cortafuegos instalados y actualizados es casi como dejar la puerta de nuestra casa con las llaves puestas.

Además, hay que tener en cuenta que muchos de los problemas informáticos derivados de este tema también vienen de la falta de actualización de los sistemas operativos. Ya no basta con antivirus, sino también con la actualización de nuestros sistemas.

Otra de las amenazas informáticas más comunes son los hackers: alguien consigue acceder a nuestras contraseñas y sacarnos información. Tener contraseñas difíciles de hackear y cambiarlas de vez en cuando puede ayudarnos a evitar este tipo de amenazas. En este sentido, os recomendamos no caer en la tentación del "123456" como contraseña y que seamos un poco creativos.

No contar con una red informática centralizada

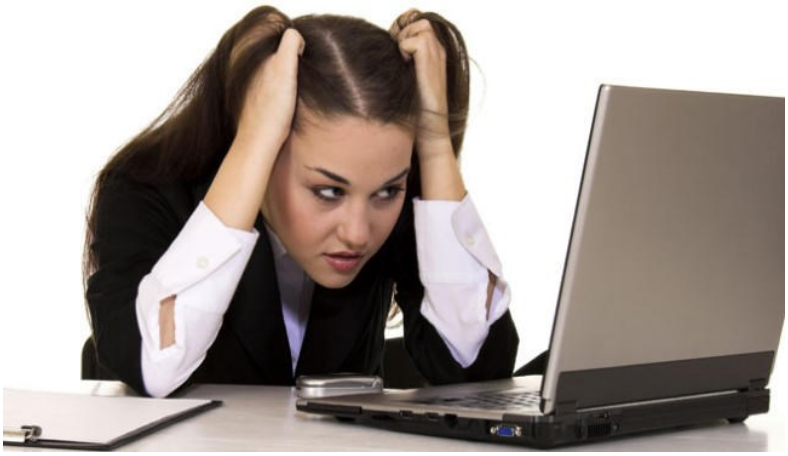
No contar con una red informática con los datos centralizados, es decir, que no cuenten con un almacenamiento de datos unificado, puede provocar que los procesos tecnológicos sean ineficientes. Acciones tan básicas como realizar o recuperar copias de seguridad o compartir recursos se pueden entorpecer y derivar a problemas mayores en una Pyme o gran empresa.

Falta de actualización de los ordenadores

No tener actualizados los ordenadores puede dar lugar a infinidad de problemas: desde riesgos de seguridad informática, hasta que la tecnología nos funcione más lenta o nos dé errores incomprensibles.

Cuando el sistema operativo pida ser actualizado, recomendamos que se haga sin tardar demasiado (siempre es una tentación la opción de "recordar más tarde") para evitar así cualquier incidencia.

El ordenador va muy lento



Sin duda alguna el principal problema al trabajar con ordenadores, es sentir que nuestro equipo va demasiado lento, hasta el punto de que hace que perdamos mucho tiempo y nos ralentiza enormemente nuestro ritmo de trabajo.

En la mayoría de casos esto ocurre por una sobrecarga de procesos, lo que hace que el equipo necesite de más tiempo para ejecutarse y que en ocasiones incluso se quede congelado, una sensación que con total seguridad habrás experimentado en alguna ocasión y que resulta tremendamente molesta. También puede ser que esta lentitud se deba a que nuestro ordenador haya sido infectado por algún tipo de virus, malware, spyware o troyanos.

La solución a esta lentitud dependerá del problema, pero por lo general consiste en descargar una versión del sistema operativo más avanzada de unos 64 bits aproximadamente. También puede pasar porque el procesador se sobrecaliente en exceso, y en este caso con limpiarlo o instalando uno nuevo debería ser suficiente.

Y por último, hay que echar un vistazo a la memoria del disco duro. Si ésta está demasiado llena y no cuenta con mucha capacidad, podría ser otra de las razones por las que funciona muy lentamente; hay que vaciarla con la con ayuda de un disco duro externo.

Ruidos extraños

Escuchar ruidos extraños al trabajar con el ordenador también es uno de los problemas más habituales. Es algo totalmente normal, y por lo general suele ocurrir debido a que el ordenador está demasiado sucio.

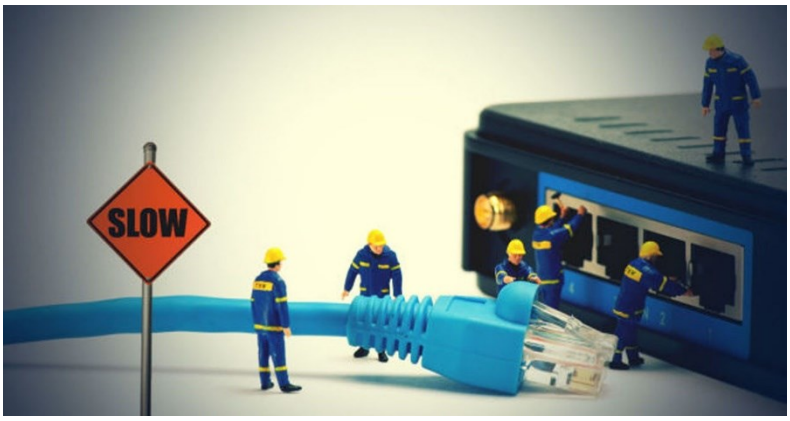
Si los ruidos extraños no cesan, recomendamos abrir el ordenador y hacernos con un trapo seco y con un spray de aire comprimido. Limpiamos todo el interior a fondo y prestamo una especial atención a la zona del ventilador.

No se puede actualizar el sistema operativo

También es habitual ir a actualizar el sistema operativo del ordenador pero que, por razones desconocidas, resulte totalmente imposible. La solución a este problema dependerá del tipo de ordenador así como del sistema operativo, pero una de las principales razones es que no se dispone de una buena conexión a Internet, y es que para poder realizar la actualización es indispensable estar conectado a la red.

También puede ser que sea una versión del sistema operativo pirata y que Windows se haya percatado de ello. Si es así, la solución pasa por adquirir la versión original, ya que de lo contrario será imposible actualizar la versión del sistema operativo.

Internet va muy lento



Y aquí llega el mayor de los problemas a día de hoy, que no es otro que Internet vaya demasiado lento. Cuando esto ocurre, siempre pensamos que esto se debe a que nos están robando WiFi, que es muy posible, pero no siempre es ésta la razón.

Para asegurarnos de que no nos roban WiFi, se cambia la contraseña del router y nos acostumbramos a ir cambiándola cada cierto tiempo. Si aun así telproblema persiste, es posible que la tarjeta de red esté estropeada, por lo que habrá que comprar una nueva. Y para salir de dudas, nos aseguramos de que no dispongamos de programas que se encuentren compartiendo archivos vía P2P como los Torrent, ya que estos quitan un importante ancho de banda.

El ordenador se reinicia automáticamente

Si el ordenador se reinicia solo, esto se debe bien a que está infectado por algún tipo de virus que provoca un reinicio que se escapa de control, o a que hay cualquier tipo de error en tu sistema operativo que demanda el reinicio.

El navegador ha cambiado

Es muy posible que abramos Google Chrome (por ejemplo) y que todo haya cambiado de la noche a la mañana. Si esto es así, casi con total seguridad se deberá a que el ordenador ha sido infectado por un adware, uno de los tipos de virus más comunes hoy en día. El adware habrá infectado el ordenador a través de la descarga del navegador, por lo que desinstalamos ese programa y limpiamose el ordenador con algún programa tipo CCleaner.

13. **Busca en internet un antivirus gratuito y explícalo.**

7. Procedimientos de seguridad, integridad, acceso y protección de información.

7.1. Mantenimiento de los equipos informáticos seguros y actualizados en la empresa.

En un mundo cada vez más digital, la seguridad y la actualización de los equipos informáticos son vitales para el funcionamiento eficaz de cualquier empresa; debemos garantizar la seguridad y actualización de las infraestructuras informáticas.

Implementar políticas de actualización regular

En un entorno tecnológico en constante evolución, es esencial que las empresas implementen políticas de actualización regular para mantener seguros sus sistemas y equipos. Estas políticas deben incluir la instalación de las últimas actualizaciones de software, parches de seguridad y firmware.

Mantenerse actualizado con las últimas versiones de software y hardware ayuda a protegerse contra vulnerabilidades conocidas y garantiza un rendimiento óptimo de los equipos informáticos.

Es recomendable establecer un calendario regular de actualizaciones y asignar responsabilidades claras a los encargados de realizar dichas actualizaciones.

Además, es importante contar con un sistema de monitoreo y gestión de actualizaciones que permita automatizar y simplificar este proceso.

Invertir en software antivirus y firewalls de calidad

Un buen software antivirus y un firewall robusto son fundamentales para proteger los equipos contra malware, ransomware y otras amenazas informáticas. Debemos asegurarnos de invertir en soluciones de seguridad fiables y actualizadas, que ofrezcan una protección integral contra las últimas amenazas.

Estas herramientas deben ser capaces de detectar y bloquear malware, así como de analizar el tráfico de red en busca de posibles intrusiones.

Además de la instalación de software de seguridad, es importante mantenerlo actualizado de manera regular. Las actualizaciones periódicas garantizan que el software tenga las últimas definiciones de virus y parches de seguridad, lo que mejora su efectividad para detectar y neutralizar nuevas amenazas.

Capacitar adecuadamente al personal

Muchas amenazas a la seguridad informática provienen de errores humanos, como hacer clic en enlaces maliciosos o descargar archivos adjuntos infectados.

Capacitar al personal en buenas prácticas de seguridad informática puede ser una de las inversiones más efectivas que podemos hacer.

Debemos organizar sesiones de formación periódicas para educar a los empleados sobre los riesgos de seguridad y cómo identificar posibles amenazas. Enseñarles a reconocer correos electrónicos de phishing, a utilizar contraseñas seguras y a evitar el uso de dispositivos no autorizados en la red de la empresa.

Además, se debe fomentar la cultura de la responsabilidad compartida en cuanto a la seguridad informática, animando a los empleados a informar sobre cualquier incidente o actividad sospechosa.

Realizar copias de seguridad regularmente

Las copias de seguridad son esenciales para proteger los datos en caso de cualquier eventualidad o ataque informático.

Debemos realizar copias de seguridad con regularidad y almacenarlas en un lugar seguro. Esto garantiza que, en caso de pérdida de datos debido a un fallo del sistema, un ataque de malware o un desastre natural, se pueda recuperar la información importante de manera rápida y efectiva.

Es recomendable utilizar un enfoque de copia de seguridad en capas, que incluya tanto copias de seguridad locales como almacenamiento en la nube. De esta manera, los datos estarán protegidos contra pérdidas físicas y se podrá acceder a ellos desde cualquier lugar en caso de necesidad.

Utilizar contraseñas seguras y autenticación de dos factores

Las contraseñas débiles o fácilmente adivinables son una puerta abierta para los piratas informáticos.

Para aumentar la seguridad digital se debe fomentar el uso de contraseñas seguras entre los empleados, que incluyan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Además, es importante recordarles que no deben reutilizar contraseñas en diferentes cuentas y que deben cambiarlas periódicamente.

También es muy recomendable implementar la autenticación de dos factores (2FA) en los sistemas y aplicaciones. Esta medida de seguridad adicional requiere que los usuarios proporcionen dos formas de verificación, generalmente una contraseña y un código enviado a su dispositivo móvil, lo que dificulta el acceso no autorizado incluso en caso de que se haya comprometido una contraseña.

Mantener control sobre los dispositivos móviles

Con el auge del trabajo remoto y la adopción de la política BYOD (Bring Your Own Device), es más importante que nunca mantener un control riguroso sobre los dispositivos móviles que acceden a la red y a los datos.

Debemos establecer políticas claras para el uso de dispositivos personales en el entorno laboral y asegurarnos de que se cumplan.

Por último, implementar soluciones de gestión de dispositivos móviles (MDM) que permitan controlar y proteger los dispositivos que acceden a la red de la empresa. Estas soluciones permiten establecer políticas de seguridad, como la encriptación de datos, la eliminación remota en caso de pérdida o robo del dispositivo, y la restricción de acceso a determinadas aplicaciones y servicios.

Contratar a un profesional de seguridad informática

Si se tienen los recursos, contratar a un profesional específico de seguridad informática puede ser una excelente inversión para mantener los sistemas seguros y actualizados.

Un experto en seguridad informática puede evaluar los riesgos de la infraestructura, diseñar e implementar medidas de seguridad adecuadas, y monitorear continuamente la red en busca de posibles amenazas.

Un profesional de seguridad informática también nos puede asesorar sobre las últimas tendencias y mejores prácticas en seguridad cibernética, manteniéndonos al tanto de las últimas amenazas y ayudándonos a adaptar las políticas y sistemas de seguridad en consecuencia.

Y, además, si quieres evaluar si tu organización es o no vulnerable a las amenazas cibernéticas y realizar un seguimiento de las medidas, utiliza esta checklist de ciberseguridad:

☐	Desarrollar un plan integral de gobernanza de datos que establezca políticas y estándares para la seguridad y privacidad de datos.
☐	Implementar una Política de Uso Aceptable y capacitar a los empleados sobre las políticas de seguridad.
☐	Asegurar la protección física de los recursos informáticos y controlar el acceso a áreas sensibles.
☐	Realizar un mapeo completo de la infraestructura de red para identificar posibles vulnerabilidades.
☐	Mantener un inventario actualizado de dispositivos autorizados y no autorizados.
☐	Implementar métodos de autenticación seguros y control de acceso para limitar el acceso no autorizado.
☐	Utilizar una arquitectura de defensa en profundidad con diversas herramientas de seguridad en diferentes capas.
☐	Garantizar configuraciones seguras y aplicar parches de seguridad de manera regular.
☐	Implementar firewalls y sistemas de detección/prevención de intrusiones para proteger la red.
☐	Escanear regularmente la red y los sistemas para identificar vulnerabilidades y tomar medidas correctivas.
☐	Encriptar datos sensibles almacenados en dispositivos móviles.
☐	Utilizar prácticas alternativas para proteger la transmisión de datos confidenciales por correo electrónico.
☐	Establecer procedimientos para manejar incidentes de seguridad y realizar auditorías periódicas para evaluar los controles de seguridad.

7.2. Herramientas de seguridad informática.

Muchas empresas se enfrentan a su proceso de transformación digital sin las debidas garantías. En el contexto en que vivimos es imprescindible para muchas organizaciones digitalizar sus archivos y apostar por nuevos sistemas que automaticen las tareas y les permitan ordenar más y mejor su información, para extraer insights con los que sumar inteligencia y estrategia colectiva al proyecto. Pero al volcar toda nuestra información en la red, nos hacemos mucho más vulnerables a los ciberataques y cualquier otro tipo de amenaza digital.

La seguridad informática se consigue a través de formación a los empleados para que sepan cómo tratar los datos de la empresa, protocolos de actuación y reacción frente a ciberamenazas y también, por supuesto, con el uso de softwares y otras herramientas de seguridad digital que nos proporcionan diversos proveedores.

Software antivirus

Parece básico, pero hay que recordarlo por si acaso. Todos los ordenadores corporativos conectados a la red de trabajo deben contar con un antivirus de calidad y fiable. Los antivirus aportan medidas de protección efectivas ante la detección de un malware o de otros elementos maliciosos, cierran posibles amenazas y son capaces de poner el dispositivo en cuarentena para evitar males mayores.

Una cosa importante es mantener el antivirus actualizado cuando lo adquirimos, para que realmente sea efectivo. De lo contrario, puede que nos sintamos protegidos ¡pero en realidad no!

Firewall perimetral de red

Una de las principales herramientas de seguridad informática es el firewall. Se dedica a escanear los paquetes de red y los bloquea o no según las reglas que previamente ha definido el administrador.

Gracias a los firewalls puedes inspeccionar el tráfico web, identificar usuarios, bloquear accesos no autorizados y muchas más acciones.

Servidor proxy

¿Qué es un proxy? Se trata de un dispositivo que actúa como intermediario entre Internet y las conexiones del navegador, y filtra los paquetes que circulan entre ambos puntos. Gracias al proxy se bloquean sitios web que se estima que pueden ser peligrosos o de los que esté prohibida su visita dentro del ambiente laboral. Gracias al proxy también se define un sistema de autentificación que limita el acceso a la red externa.

End Point Disk Encryption

También llamado cifrado de punto final, se trata de un proceso de codificación de datos para que nadie que no guarde la clave de descifrado pueda leerlo. Protege los sistemas operativos de la instalación de archivos corruptos, al bloquear los archivos almacenados en ordenadores, servidores y otros puntos finales.

Escáner de vulnerabilidades

Por último, el escáner de vulnerabilidades es una herramienta de seguridad informática fundamental para todo tipo de empresas, no importa el tamaño o el sector. El escáner es un software que detecta, analiza y gestiona los puntos débiles que tenga el sistema. Y muy importante, manda alertas en tiempo real al detectar problemas, lo que acorta mucho el tiempo de resolución de los conflictos.

14. **Busca en internet un software de copias de seguridad sencillo y económico y explícalo.**
15. **Explica por qué hay que mantener un control sobre los dispositivos móviles en la empresa.**

8. Normativa legal aplicable.

Código de Propiedad Intelectual

Exponemos el Código de Propiedad Intelectual, que pretende hacer una recopilación de las distintas leyes que afectan a la propiedad intelectual, así como a materias estrechamente relacionadas con las industrias culturales tales como las leyes del libro y del cine, el droit de suite en las obras de arte, el depósito legal o el reglamento del Registro General de la Propiedad Intelectual. En definitiva, se ha codificado electrónicamente la legislación vigente que el especialista en derechos de autor debe tener al alcance de la mano para dar respuesta a los problemas que se le plantean en su día a día.

No obstante, merece especial atención hacer referencia a una ley decimonónica formalmente derogada, pero que sigue desplegando sus efectos en la actualidad. Nos referimos a la Ley de Propiedad Intelectual de 10 de enero de 1879 (BOE núm. 12, de 12 de enero de 1879, págs. 107 a 108). Las disposiciones transitorias 2ª a 6ª del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (el "TRLPI") siguen dotado de eficacia al articulado de la ley de 1879 en determinados supuestos transitorios. La Ley de 1879 fue derogada y sustituida por la Ley 22/1987, cuyas disposiciones transitorias establecieron que la ley anterior continuaría rigiendo cualquier contrato concluido durante su vigencia. Adicionalmente, la Disposición Transitoria Cuarta del TRLPI respeta el plazo de protección de 80 años tras la muerte del autor que reconocía la ley de 1879 (10 años más que lo previsto en el TRLPI) para todas aquellas obras de autores fallecidos antes del 7 de diciembre de 1987.

A la vista de lo cual, la referida norma de 1879 continúa siendo de aplicación tanto para los contratos concluidos con anterioridad al 7 de diciembre de 1987, como a las obras de autores fallecidos antes de dicha fecha. Lo anterior hace que, como abogados especialistas en la materia, nos veamos obligados con relativa frecuencia a consultar la ley de 1879 y su peculiar régimen jurídico. Ésta es, además, aplicada por los tribunales.

Por todo ello, hemos creído conveniente advertir al lector de que, pese a no formar parte integrante de este Código, la Ley de Propiedad Intelectual de 1879 sigue siendo hoy un texto a tener en cuenta dentro del marco legislativo de la propiedad intelectual española.

DISPOSICIONES GENERALES

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Real Decreto de 3 de septiembre de 1880 por el que se aprueba el Reglamento para la ejecución de la Ley de 10 de enero de 1879 sobre propiedad intelectual. [Inclusión parcial].

Real Decreto 1398/2018, de 23 de noviembre, por el que se desarrolla el artículo 25 del texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, en cuanto al sistema de compensación equitativa por copia privada.

Real Decreto 209/2023, de 28 de marzo, por el que se establecen la relación de equipos, aparatos y soportes materiales sujetos al pago de la compensación equitativa por copia privada, las cantidades aplicables a cada uno de ellos y la distribución entre las distintas modalidades de reproducción, previstas en el artículo 25 del texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril.

Orden CUD/330/2023, de 28 de marzo, por la que se aprueba la metodología para la determinación de las tarifas generales de las entidades de gestión de derechos de propiedad intelectual por la

utilización de su repertorio y el contenido de la memoria económica que debe acompañar a las tarifas generales.

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. [Inclusión parcial].

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. [Inclusión parcial].

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial].

Ley de 16 de diciembre de 1954 sobre hipoteca mobiliaria y prenda sin desplazamiento de posesión. [Inclusión parcial].

Decreto de 17 de junio de 1955 por el que se aprueba el Reglamento de la Ley de Hipoteca Mobiliaria y Prenda sin desplazamiento de posesión. [Inclusión parcial].

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial].

Ley 2/2011, de 4 de marzo, de Economía Sostenible. [Inclusión parcial].

LIBROS

Ley 9/1975, de 12 de marzo, del Libro. [Inclusión parcial].

Real Decreto 484/1990, de 30 de marzo, sobre precio de venta al público de libros. [Inclusión parcial].

Ley 10/2007, de 22 de junio, de la lectura, del libro y de las bibliotecas.

Real Decreto 2063/2008, de 12 de diciembre, por el que se desarrolla la Ley 10/2007, de 22 de junio, de la Lectura, del Libro y de las Bibliotecas en lo relativo al ISBN.

Decreto 2984/1972, de 2 de noviembre, por el que se establece la obligación de consignar en toda clase de libros y folletos el número ISBN.

Real Decreto 396/1988, de 25 de abril, por el que se desarrolla el artículo 72 de la Ley de Propiedad Intelectual sobre control de tirada.

Real Decreto 624/2014, de 18 de julio, por el que se desarrolla el derecho de remuneración a los autores por los préstamos de sus obras realizados en determinados establecimientos accesibles al público.

Real Decreto 224/2016, de 27 de mayo, por el que se desarrolla el régimen jurídico de las obras huérfanas.

OBRA AUDIOVISUAL

Ley 55/2007, de 28 de diciembre, del Cine.

Real Decreto 1084/2015, de 4 de diciembre, por el que se desarrolla la Ley 55/2007, de 28 de diciembre, del Cine.

Orden CUL/2834/2009, de 19 de octubre, por la que se dictan normas de aplicación del Real Decreto 2062/2008, de 12 de diciembre, por el que se desarrolla la Ley 55/2007, de 28 de diciembre, del Cine, en las materias de reconocimiento del coste de una película e inversión del productor, establecimiento de las bases reguladoras de las ayudas estatales y estructura del Registro Administrativo de Empresas Cinematográficas y Audiovisuales.

Orden ECD/2784/2015, de 18 de diciembre, por la que se regula el reconocimiento del coste de una película y la inversión del productor.

Real Decreto 448/1988, de 22 de abril, por el que se regula la difusión de películas cinematográficas y otras obras audiovisuales recogidas en soporte videográfico.

Orden CUL/1772/2011, de 21 de junio, por la que se establecen los procedimientos para el cómputo de espectadores de las películas cinematográficas, así como las obligaciones, requisitos y funcionalidades técnicas de los programas informáticos a efectos del control de asistencia y rendimiento de las obras cinematográficas en las salas de exhibición.

Decreto 3837/1970, de 31 de diciembre, por el que se regula la hipoteca mobiliaria de películas cinematográficas.

Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de bonos garantizados, distribución transfronteriza de organismos de inversión colectiva, datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de radio y televisión, exenciones temporales a determinadas importaciones y suministros, de personas consumidoras y para la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes. [Inclusión parcial].

ADMINISTRACIÓN PÚBLICA

Orden PRE/2418/2015, de 6 de noviembre, por la que se regula el número de identificación de las publicaciones oficiales.

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

Real Decreto 1778/1994, de 5 de agosto, por el que se adecuan a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las normas reguladoras de los procedimientos de otorgamiento, modificación y extinción de autorizaciones.

Real Decreto 1228/2005, de 13 de octubre, por el que se crea y regula la Comisión intersectorial para actuar contra las actividades vulneradoras de los derechos de propiedad intelectual.

DEPÓSITO LEGAL

Ley 23/2011, de 29 de julio, de depósito legal.

REGISTRO GENERAL DE LA PROPIEDAD INTELECTUAL

Real Decreto 635/2015, de 10 de julio, por el que se regula el depósito legal de las publicaciones en línea.

Real Decreto 611/2023, de 11 de julio, por el que se aprueba el Reglamento del Registro de la Propiedad Intelectual.

COMISIÓN DE PROPIEDAD INTELECTUAL

Real Decreto 1023/2015, de 13 de noviembre, por el que se desarrolla reglamentariamente la composición, organización y ejercicio de funciones de la Sección Primera de la Comisión de Propiedad Intelectual.

Real Decreto 1130/2023, de 19 de diciembre, por el que se desarrollan la composición y el funcionamiento de la Sección Segunda de la Comisión de Propiedad Intelectual y por el que se modifica el Real Decreto 1023/2015, de 13 de noviembre, por el que se desarrolla

reglamentariamente la composición, organización y ejercicio de funciones de la Sección Primera de la Comisión de Propiedad Intelectual.

Orden ECD/378/2012, de 28 de febrero, por la que se establece la obligatoriedad para los interesados en el procedimiento de salvaguarda de los derechos de propiedad intelectual, de comunicarse con la Sección Segunda de la Comisión de Propiedad Intelectual por medios electrónicos.

DELITOS CONTRA LA PROPIEDAD INTELECTUAL

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial].

OTRAS DISPOSICIONES RELACIONADAS

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. [Inclusión parcial].

Real Decreto-ley 2/2023, de 16 de marzo, de medidas urgentes para la ampliación de derechos de los pensionistas, la reducción de la brecha de género y el establecimiento de un nuevo marco de sostenibilidad del sistema público de pensiones. [Inclusión parcial].

Normativa sobre datos personales

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (Reglamento general de protección de datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establecen el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales. Queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo previsto en la disposición adicional decimocuarta de la LOPDGDD, y siguen vigentes las disposiciones de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que no contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y la LOPDGDD.

Para el tratamiento de datos personales relativos a condenas e infracciones penales, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales constituye la norma de referencia por la que se rige el tratamiento de este tipo de datos. Dicha Ley Orgánica traspone a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a esta misma materia.

En materia de seguridad del tratamiento, resulta de aplicación, en virtud de la disposición adicional primera de la LOPDGDD, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y, en el ámbito ministerial, la Política de Seguridad de la Información aprobada por la Orden HFP/873/2021, de 29 de julio.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vigente en los artículos referidos en la Disposición adicional decimocuarta y Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Orden HFP/873/2021, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública.

Código de Comercio

El Código de Comercio en España es un conjunto de leyes y reglamentos utilizados para llevar a cabo todas las actividades comerciales en el país. Los inversores en España que quieran abrir una empresa deben observar las disposiciones de este Código, registrar su empresa en consecuencia y entablar contratos y relaciones comerciales según los requisitos de la ley.

El Código de Comercio español contiene importantes disposiciones relativas a los empresarios y a los actos de comercio que pueden realizar. Cuando ciertas actividades no están explícitamente contempladas en el Código, se rigen por el Derecho Civil común.

Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.

La primera versión consolidada, que se ofrece como texto original, se corresponde con la de fecha 1 de noviembre de 1996, aunque el texto original se publicó en la Gaceta de Madrid del 16 de octubre al 24 de noviembre de 1885. Ref. BOE-A-1885-6627.

Los principales tipos de comerciantes en España y el Registro Mercantil

El Registro Mercantil español tiene por objeto la inscripción de los principales tipos de personas jurídicas que pueden constituirse en España: empresarios individuales, sociedades anónimas y sociedades de préstamo o de seguros, instituciones de inversión colectiva y fondos de pensiones, así como sociedades civiles profesionales. El Registro depende del Ministerio de Justicia.

La inscripción no es obligatoria para los empresarios individuales, excepto para los armadores, pero sí lo es para todos los demás tipos de empresas en España. El procedimiento de registro debe realizarse en el plazo de un mes después de que la empresa haya obtenido todos los documentos necesarios. Tenga en cuenta que si una empresa desarrolla cualquier operación de importación-exportación, independientemente de si es una persona jurídica o un empresario individual, está obligada legalmente a solicitar un número EORI en España.

La información contenida en el Registro Mercantil es pública y las empresas deben poner parte de su información a disposición del público. Parte de esta información disponible al público incluye la forma jurídica de la empresa y/o su estado de insolvencia, su domicilio social en España, el capital desembolsado y otros.

Las obligaciones de un comerciante

El Código de Comercio contiene los derechos y las obligaciones de los comerciantes que realizan actividades comerciales y las estipulaciones de esta ley se completan con el Código Civil. Según el Código de Comercio, un comerciante debe llevar una contabilidad y disponer de los siguientes documentos:

- un diario
- libro de contabilidad o cuentas
- libro de balances
- libro de cartas.

También debe elaborarse un balance que incluya el activo de la empresa, el pasivo y el patrimonio neto (el valor final del activo una vez deducido el pasivo). La cuenta de pérdidas y ganancias es otro documento anual que presentan las empresas españolas y en él se recogen los ingresos y gastos realizados por la empresa en el respectivo ejercicio económico. El ejercicio fiscal en España suele coincidir con el año natural. Toda la información sobre la situación financiera de la empresa debe reflejar su verdadera situación. Las empresas pueden solicitar los servicios de un contable independiente o de una empresa de contabilidad para cumplir con la normativa vigente en materia de contabilidad e información.

Una parte de las nuevas normas del Código de Comercio, que completan el antiguo código, tienen como objetivo principal ayudar al país a recuperarse después de una crisis económica.

Otras disposiciones del Código de Comercio español

El Código de Comercio incluye directrices para la celebración de acuerdos comerciales. Las propuestas de negocios pueden hacerse verbalmente, pero cualquier relación comercial debe documentarse por escrito. Este documento servirá como prueba de las intenciones de ambas partes y la propuesta para hacer negocios podrá ser aceptada o rechazada.

Los contratos comerciales celebrados en España se consideran válidos independientemente de su formato e idioma y pueden ser vinculantes para las partes. Una excepción a la ejecutabilidad de cualquier contrato mercantil en España son aquellos acuerdos que se celebran en un país extranjero y a los que se les exigen unas formalidades, formatos o escrituras específicas para ser ejecutables, las cuales no se exigen en la legislación española.

El Código de Comercio define las obligaciones del vendedor y del comprador y también informa del contrato de compraventa obligatorio. El vendedor está obligado a entregar la mercancía según lo establecido y en el plazo previsto. El comprador puede solicitar el reconocimiento de los dioses.

Las bolsas de valores, las operaciones bursátiles y la actuación de los corredores de bolsa y de los agentes bursátiles están reguladas en el Código.

En resumen, un código de comercio trata de un conjunto de leyes destinadas a regular el comercio. Los códigos comerciales pueden ayudar en el comercio proporcionando “estándares” para solventar problemas y disputas. De hecho, un tema central es la resolución de disputas contractuales, ofreciendo directrices para la codificación de problemas y consejos sobre cómo proceder si se incumple un contrato.

El sentido común y las prácticas comerciales típicas del ámbito empresarial concreto son la fuente general de la mayoría de las transacciones prescritas, pero disponer de un código de comercio es un gran beneficio para los comerciantes y hace posible una transacción comercial fluida y eficiente.

No se puede confiar simplemente en el sentido común, sino que hay que aprender la ley básica que se aplica. Es un requisito para la persona de negocios eficaz como el aprendizaje de los principios básicos de la contabilidad.

16. **¿Qué es el Código de comercio?**
17. **¿Cuál es la función del Registro mercantil?**
18. **¿Cuáles son las obligaciones de un comerciante español?**

9. Test de repaso.

1. ¿Qué es un sistema operativo?
   a) Un sistema que opera
   b) Software que permite al ordenador el arranque, la gestión de los recursos y la comunicación usuario-dispositivos.
   c) Un sistema de navegación
   d) Ninguna es correcta

2. ¿Cuáles son sistemas operativos?
   a. MSDOS, Linux, Macintosh y Windows
   b. MSDOS, Google Chrome
   c. Explorer, Opera y Safari
   d. Yahoo, Hotmail

3. ¿Qué otro nombre recibe un controlador?
   a. Parche
   b. Programa
   c. Administrador
   d. Driver

4. ¿Qué clases de periféricos existen?
   a. De salida
   b. De entrada y salida
   c. De entrada, salida, entrada-salida y almacenamiento
   d. Almacenamiento

5. ¿A qué nos referimos con el término multimedia?
   a. A una tecnología
   b. Cualquier sistema que utiliza múltiples medios de expresión físicos o digitales para presentar o comunicar información.
   c. Medios electrónicos que almacenan y presentan contenidos multimedia
   d. Todas son correctas.

6. ¿Cuáles son de las siguientes amenazas que pueden dañar el sistema informático?
   a. Gusanos
   b. Virus, troyanos y spyware
   c. Adware, spam
   d. Todas las anteriores

7. ¿Qué normativa es de aplicación a la Propiedad intelectual?
   a. Real Decreto Legislativo 1/1996 de 12 de abril
   b. Real Decreto Legislativo 1/1996 de 12 de abril y Ley 21/2014 de 4 de noviembre
   c. Ley 21/2014 de 4 de noviembre
   d. L.O 15/1999 de 13 de diciembre

8. Según el Código de comercio quienes tienen la condición de comerciantes:
   a. Los que comercien en cualquier momento
   b. Las compañías mercantiles o industriales que se constituyan con arreglo al Código de Comercio
   c. Los que, teniendo capacidad legal para ejercer el comercio, se dedican a él habitualmente
   d. Las respuestas b y c son correctas.

9. ¿Con que otro nombre se conoce a la interfaz básica de usuario?
   a. GUI
   b. IBU