5

SEGURIDAD INTEGRAL EN EL ENTORNO DIGITAL

Como profesional que trabaja diariamente con tecnología, he comprobado cómo la seguridad digital ha evolucionado de ser un tema especializado a convertirse en una necesidad básica para cualquier usuario.

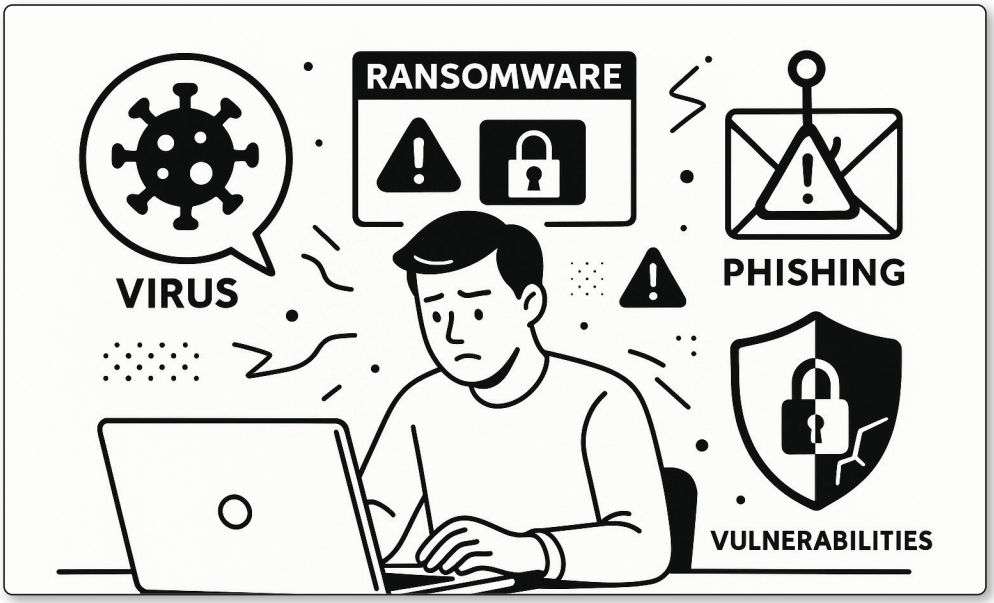
En este módulo, quiero compartir mi perspectiva acerca de dos pilares fundamentales que considero esenciales: por un lado, las estrategias prácticas que podemos implementar para proteger dispositivos y redes, desde la elección de antivirus hasta la configuración segura de conexiones WiFi; por otro, las medidas que usaremos para salvaguardar nuestra identidad digital y gestionar éticamente la información, especialmente en un mundo donde amenazas como el phishing son cada vez más sofisticadas.

El objetivo final es transmitir que la seguridad digital no es solo cuestión de expertos, sino una responsabilidad compartida donde cada uno de nosotros puede marcar la diferencia.

Requisitos previos

Para sacar el máximo provecho de este módulo, se requiere haber entendido los módulos anteriores o disponer de habilidades y conocimientos informáticos medios.

5.1 INTRODUCCIÓN



Los problemas de seguridad informática de este siglo han llevado al sector por el camino de la realización de grandes inversiones buscando minimizar las consecuencias tras la detección de incidencias en los sistemas.

Con sistemas, nos referimos no solo a los grandes equipos servidores que se utilizan en centros de datos y que se usan para los servicios de uso masivo en la actualidad como, por ejemplo, mensajería instantánea, páginas web, servicios online bancarios, ecommerce, email, juegos, redes sociales o plataformas de streaming; sino, también, para los dispositivos de uso personal que se conectan a esas fuentes y que transmiten datos personales de cualquier tipo.

La popularización y uso masivo de los dispositivos ha llegado a sectores de la población que pueden contar con diferentes niveles de conocimiento informático, desde expertos a usuario nóveles que, es probable, no sean conscientes de los peligros que enfrentan por el mero hecho de portar un teléfono móvil conectado a la red durante las 24 horas del día y que, lógicamente, envía y recibe paquetes de datos sin que el propio usuario sepa lo que ocurre.

Puesto que el ámbito de aplicación del conocimiento aprendido a través de este texto es el de las competencias avanzadas para la ciudadanía, vamos a centrar los

siguientes puntos en descubrir las técnicas y estrategias que debemos seguir, como usuarios, para minimizar la exposición a los riesgos inherentes al mundo etéreo del ciberespacio.

La tercera parte del primer módulo de este libro explica con bastante detalle los elementos fundamentales de la seguridad informática. Te recomiendo que repases ese módulo con objeto de que puedas entender mejor los siguientes puntos que se proponen.

5.2 PROTECCIÓN ACTIVA DE EQUIPOS Y REDES

Como propietarios de equipos informáticos y dispositivos móviles conectados a internet, tenemos que conocer los programas básicos que nos permitan mejorar la seguridad de los sistemas.

Nuestros dispositivos contienen datos personales, imágenes, vídeos, documentos y, probablemente, software de navegación a través de internet y aplicaciones que utilizamos para ingresar en redes sociales de todo tipo.

5.2.1 Métodos para asegurar dispositivos contra malware y accesos no autorizados

- Instalación y actualización regular de software antivirus y antimalware. Se puede elegir entre programas con licencia comercial de pago o de uso limitado y gratuito.
- Configuración de contraseñas robustas y procedimientos de autenticación de dos factores. El acceso al sistema operativo o cualquier otro dispositivo fijo o móvil debe realizarse ingresando un nombre de usuario y una contraseña fuerte de entre 8 y 12 caracteres alfanuméricos que incluyan letras mayúsculas, minúsculas y especiales (*$, %, _, #, +, -, etc*).
- Actualizaciones periódicas del sistema operativo y aplicaciones para corregir fallos y vulnerabilidades.
- Instalar solo aquellos programas que realmente vayamos a utilizar. Cada programa puede implicar añadir vulnerabilidades potenciales al sistema.

5.2.2 Prácticas recomendadas para la gestión segura de redes Wi-Fi

Las conexiones utilizando Wi-Fi son especialmente cómodas ya que permiten el desplazamiento del dispositivo sin necesidad de utilizar cables. Este tipo de conexiones se convierten en una puerta de entrada crucial a nuestra información personal y profesional, por lo que es crítica su correcta configuración y gestión para proteger la privacidad y seguridad.

A continuación, te detallo las mejores prácticas para asegurar la red wifi:

- **Uso de protocolos de seguridad como WPA3**

  WPA3 (*Wi-Fi Protected Access 3*) es el protocolo de seguridad más avanzado para redes inalámbricas. Reemplaza a su predecesor, el WPA2, ofreciendo mayor protección contra ataques de fuerza bruta y mejor cifrado de datos.

  - Ventajas:
    - Cifrado más fuerte: WPA3 ofrece cifrado de 128 bits y elimina el uso de TKIP (*Temporal Key Integrity Protocol*) que ya está obsoleto y es inseguro.
    - Protección frente a ataques de diccionario: incluso si la contraseña es débil, WPA3 la hace mucho más difícil de descifrar. Para ello, el intercambio de claves usa SAE (*Simultaneous Authenticacion of*

Equals). Cada intento de contraseña obliga al atacante a interactuar en tiempo real con la red y cada intento fallido requiere un nuevo intercambio de claves con el router o punto de acceso, haciendo inviables los ataques mediante captura del tráfico.

- Autenticación individual de dispositivos: mejora la protección durante la conexión incluso en redes públicas.

- **Cambio regular de contraseñas y ocultación del SSID**

  Se recomienda modificar la contraseña de la red Wi-Fi de manera periódica para evitar que posibles atacantes obtengan acceso prolongado a la red.

  Usa contraseñas largas de forma similar a las que utilizas para el acceso con un usuario a un sistema. Evita contraseñas simples, comunes o fáciles de adivinar.

- **Ocultación del SSID (*Service Set Identifier*)**

  El SSID es el nombre de la red Wi-Fi y es visible para cualquier dispositivo que se encuentre dentro del alcance de tu red. Ocultar el SSID puede dificultar que personas ajenas detecten tu red. Eso sí, ten en cuenta que un atacante con medios y conocimiento suficiente no tendrá ningún problema en detectar la existencia de emisiones de radio Wi-Fi, por lo que esta precaución solo se aplicaría para usuarios normales.

  Aunque no proporciona una seguridad total, ocultar el SSID evita que se muestre tu red en el listado de redes existentes en el radio de alcance del dispositivo que escanea el entorno.

  Para ocultar el SSID, se deberá acceder a la configuración de router o punto de acceso y buscar la opción de "no difundir SSID".

- **Segmentación de la red para dispositivos invitados**

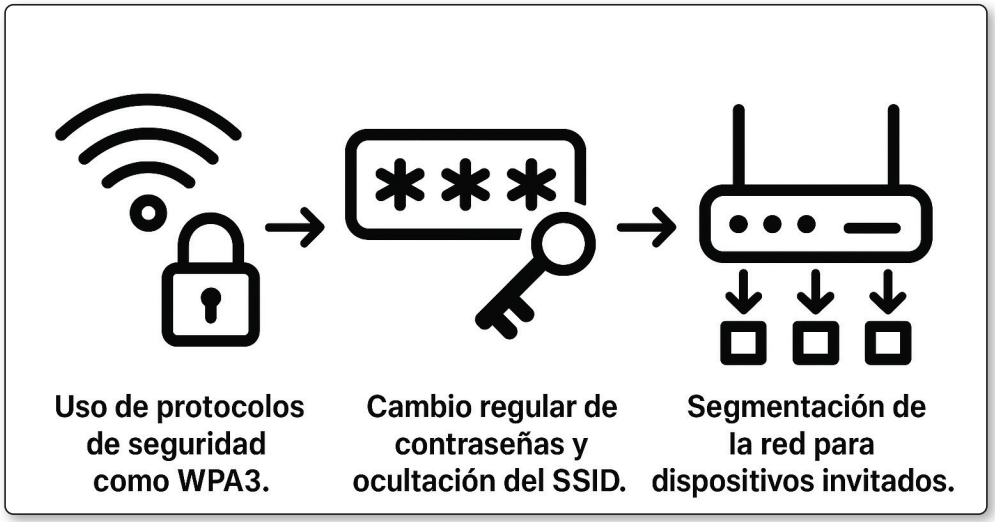
  Se refiere a la posibilidad de crear redes de invitados que usarán aquellas personas que no forman parte el núcleo familiar habitual o que acceden a las instalaciones de la empresa pero no tienen permisos de uso de los recursos existentes (ordenadores, impresoras, carpetas compartidas, documentos, etc).

  Los routers modernos permiten configurar redes Wi-Fi separadas o redes de invitados con configuraciones de acceso limitadas y, normalmente, con aislamiento de dispositivos en red.

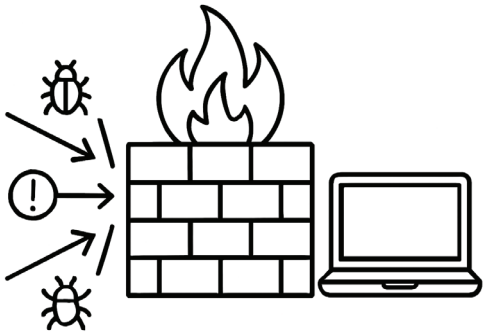
  Los beneficios que supone la segmentación son:

  - Aislamiento: los dispositivos conectados a la red de invitados no tienen acceso a los demás elementos de la red.

- Mayor control: se pueden controlar los permisos de acceso y el ancho de banda que los dispositivos invitados pueden usar, sin comprometer la seguridad de la red principal.
- La red de invitados se puede activar mediante las opciones apropiadas en la configuración del router o punto de acceso. Se agrega un nombre, una contraseña, el aislamiento y el ancho de banda.



5.2.3 Uso de cortafuegos



La seguridad del sistema y de la red depende en gran medida de proteger las comunicaciones y controlar el acceso a nuestros datos.

5.2.3.1 ¿QUÉ ES UN CORTAFUEGOS?

En el mundo real, se utilizan muros y vallados para cerrar el perímetro de una zona, de forma que se puede controlar fácilmente la forma de acceder al sitio. Incluso se pueden agregar otros elementos de seguridad que impidan el paso a los que intentan saltar los muros fuera de las zonas de acceso habilitadas.

En el mundo informático, el cortafuegos es un programa que se utiliza como barrera de seguridad que actúa como un filtro entre la red interna y el tráfico proveniente del exterior (internet). Su función principal es monitorizar y controlar los paquetes de datos que entran y salen de la red.

5.2.3.2 CÓMO CONFIGURAR UN CORTAFUEGOS O FIREWALL

Para configurar un cortafuegos, se deben tener en cuenta los siguientes puntos:

- **Definir reglas de acceso:** se establecen ciertas reglas o normas que permiten o bloquean el tráfico en función de la dirección (entrante, saliente), el puerto o el protocolo utilizado en la comunicación.
- **Filtrar el tráfico entrante y saliente:** los firewalls pueden bloquear ataques externos como los intentos de intrusión o escaneos de puertos y, además, pueden filtrar el tráfico saliente para prevenir fugas de datos o comunicaciones no deseadas.
- **Aplicar un cortafuegos personal:** en dispositivos de uso individual, como ordenadores, smartphones o tablets, se puede configurar un firewall para protegerlos de amenazas externas cuando están conectados a redes públicas o no confiables.

Usar un cortafuegos tiene dos beneficios fundamentales: protegen contra los accesos no autorizados, evitando que un atacante aproveche una vulnerabilidad para acceder a la red; y la monitorización constante, que proporciona visibilidad en tiempo real del tráfico que pasa a través de la red, facilitando la detección de actividades sospechosas.

5.2.4 Cifrado de datos

El cifrado consiste en la manipulación de los datos aplicándoles unas reglas concretas para ofuscar el contenido de tal modo que solo emisor y receptor sean capaces de devolver el mensaje a su estado natural legible.

¿Qué es el cifrado de extremo a extremo?

Es una técnica de seguridad en la que los datos se cifran en el dispositivo del emisor y solo se descifran en el dispositivo del receptor. Esto significa que, incluso si los datos se interceptan en el camino, no pueden ser leídos por terceros.

¿Por qué es importante?

Garantiza la privacidad. Protege la información sensible como contraseñas, datos bancarios o comunicaciones personales que viajan a través de la red, evitando que alguien pueda visualizar los datos.

El cifrado previene los ataques de intermediarios que puedan encontrarse entre medias de la comunicación establecida. Asegura que los datos no pueden ser alterados o espiados por actores maliciosos ubicados entre el emisor y el receptor.

Aplicaciones comunes que usan cifrado de extremo a extremo

Se utiliza ampliamente en entornos WEB en los que el servidor cifra la información que envía al navegador utilizando certificados de seguridad. Así, cuando un usuario se identifica en una web, su nombre y contraseña no pueden ser leídos nada más que por el sistema receptor que conoce las claves de descifrado.

Es habitual en los servicios de mensajería instantánea como WhatsApp, Signal o Telegram. Solo el remitente y el emisor pueden leer los mensajes.

Existen servicios de email online con protección adicional con cifrado incluso de los mensajes almacenados en los buzones como, por ejemplo ProtonMail. Esta protección implica incluso que, en caso de perder la contraseña, ésta se puede recuperar pero se perdería la posibilidad de descifrar los mensajes almacenados y cifrados con la anterior contraseña.

Beneficios

El cifrado de extremo a extremo asegura que la comunicación se mantenga privada incluso cuando se transmite a través de canales inseguros como redes Wi-Fi públicas.

Ayuda a que usuarios y empresas puedan realizar transacciones o compartir información crítica sin temor a ser espiados.

Cifrado del disco duro o particiones

Como usuario del sistema operativo, tienes la opción de cifrar todo el contenido almacenado en el disco duro de tu ordenador.

Si trabajas con sistemas operativos de Microsoft modernos, puedes activar la herramienta *Bitlocker*, que se encarga de cifrar todo el contenido del disco duro o partición elegida.

En caso de pérdida del ordenador o intento de acceso al sistema operativo utilizando medios externos, la información queda totalmente preservada ya que se torna totalmente ilegible si no se utiliza la contraseña de Bitlocker.

Recuerda que ya hemos estudiado el concepto y uso de Bitlocker en el primer módulo.

5.2.5 Redes privadas virtuales (VPN)

Una VPN, o red privada virtual, es una herramienta que crea una conexión segura entre tu dispositivo y la red, cifrando todo el tráfico de datos. La VPN puede enmascarar la dirección IP de tu equipo y permitir que el dispositivo se conecte a internet de forma anónima, lo que agrega una capa extra de privacidad y seguridad.

¿Cómo funciona una VPN?

Cuando te conectas a internet mediante una VPN, el tráfico se redirige a través de un servidor seguro impidiendo al proveedor de internet o cualquier atacante detectar tu actividad en línea.

La VPN cifra la información asegurando que, incluso si alguien intercepta los datos en una red pública Wi-Fi (cafetería, hospital, aeropuerto, etc) no pueda leerlos ni robar información sensible.

Como ves, es especialmente adecuado su uso si utilizamos conexiones de red Wi-Fi públicas y, además, muy útil para poder acceder a contenido restringido geográficamente o bloqueado en tu país ya que enmascara —cambia— la dirección IP real por una que forma parte de la red VPN y que puede estar ubicada en otra región.

El cifrado y enmascaramiento de la IP son buenas técnicas o estrategias para mejorar la privacidad en línea.

¿Quién ofrece este servicio?

Existen diversas entidades mundiales que ofrecen el servicio de conexión a sus VPNs ya sean de forma gratuita con limitaciones o mediante el pago de una cuota y acceso con mejoras en el servicio.

Las indicadas en la siguiente tabla son las más conocidas o habituales:

Servicio VPN	Tipo	Límite de datos	Características clave	Ideal para
ProtonVPN	Gratis	Sin límite	✅ Acceso a servidores en 3 países ✅ Velocidad reducida en plan gratis	Privacidad básica sin restricciones de volumen
Windscribe	Gratis	10 GB/ mes	🌍 Servidores en 10 países 🌍🚫 Bloqueador de anuncios integrado	Navegación privada + bloqueo de trackers/ anuncios
TunnelBear	Gratis	500 MB/ mes	🐻 Interfaz intuitiva 🐻🌐 +20 países disponibles	Primeros pasos con VPN (uso muy ocasional)
Hide.me	Gratis	10 GB/ mes	⚡ Velocidad moderada 🔒 5 ubicaciones disponibles	Equilibrio entre velocidad y seguridad
Atlas VPN	Gratis	2 GB/mes	🔒🚫 Enfoque en privacidad 📱 Optimizado para móviles	Navegación básica con protección mínima
ExpressVPN	Premium	Ilimitado	🔐 Cifrado AES-256 🚀 +90 países, velocidad ultrarrápida	Streaming 4K + máxima seguridad
NordVPN	Premium	Ilimitado	🚀🚫 Cifrado doble (Double VPN) 🎥 Optimizado para Netflix/YouTube	Privacidad extrema + acceso a contenido geo-restringido
CyberGhost	Premium	Ilimitado	🌐 +7000 servidores 🖥️ Servidores dedicados para streaming	Desbloquear plataformas internacionales
Surfshark	Premium	Ilimitado	💻 Conexiones simultáneas ilimitadas 💻✂️ CleanWeb (bloquea malware/ads)	Familias o usuarios con muchos dispositivos
Private Internet Access	Premium	Ilimitado	✂️⚙️ Configuración avanzada 🔗 Soporte P2P (torrents)	Usuarios técnicos que necesitan personalización detallada

5.3 SEGURIDAD PERSONAL Y GESTIÓN ÉTICA DE DATOS

En temas anteriores nos hemos acercado a conceptos tales como la ingeniería social, el "phishing", correos electrónicos fraudulentos, autenticidad de los sitios web, etc.

Dentro del punto de la seguridad personal, pasaremos a repasar las definiciones y estrategias que podemos seguir para mejorar nuestro entorno personal de trabajo, datos, privacidad y redes.

5.3.1 Prevención de riesgos como el phishing y el robo de identidad

El **phishing** y el robo o **suplantación de identidad** son dos de las amenazas más comunes en línea y su prevención requiere estar bien informado además de ser cauteloso con las interacciones digitales.

5.3.1.1 IDENTIFICACIÓN DE CORREOS ELECTRÓNICOS Y SITIOS WEB FRAUDULENTOS

- **El correo electrónico sospechoso**

  Ser capaz de identificar un correo electrónico fraudulento nos ayudará a evitar riesgos potenciales por lo que, en primer lugar, deberemos aprender cuáles son las características de este tipo de emails.

  Los emails de tipo fraudulento suelen tener los siguientes elementos:

  - **Señales de alerta:** la existencia de errores ortográficos, gramaticales, expresiones que no corresponden con el idioma en el que está redactado el texto o remitentes desconocidos son señales que deben activar las alarmas.
  - **Solicitudes sospechosas:** hay que desconfiar de correos que piden información personal o financiera, especialmente cuando hay cierta insistencia, urgencia o amenaza con consecuencias graves como el cierre de una cuenta en red social, anulación de servicios por falta de pago, solicitudes de cambio de contraseñas urgentes… etc.
  - **Verificación de direcciones:** siempre debemos verificar que el dominio del correo electrónico coincida con el oficial de la organización (por ejemplo: @paypal.com en lugar de *@paypa1.com*).
  - **Visualizar los emails en formato solo texto:** una forma excelente para mantener la seguridad es configurar el cliente de correo electrónico

para que muestre el email sin formato HTML, es decir, como texto plano. De ese modo, las imágenes no se descargan y los enlaces se muestran tal cual, sin posibilidad de ofuscarlos o disfrazarlos.

- **Sitios web fraudulentos**

  Son sitios web que se parecen bastante a los originales. Se llega a ellos mediante el engaño por pulsación de un enlace desde dentro de un email o enviado a través de algún sistema de mensajería instantánea. Se trata de sitios "*phishing*" diseñados para que el usuario crea que está en el lugar legítimo y realice las operaciones de ingreso que enviarían los datos al atacante para el robo de información.

  La mejor forma de protegerse contra estas webs es:

  - **La verificación de URL:** debemos asegurarnos de que la URL comienza con "https://" y localizar el icono del candado en la barra de direcciones.
  - **Certificados de seguridad:** son firmas de terceros de confianza que nos van a permitir detectar si el sitio es el original que estamos buscando. El candado verde indica que el sitio tiene un certificado SSL válido y, si la URL coincide con la empresa o servicio oficial, podremos descartar que se trate de un sitio web fraudulento.
  - **Revisión de la apariencia del sitio:** un sitio web fraudulento suele tener un diseño deficiente, ausencia de alguna imagen y/o errores gramaticales.

- **Herramientas para la verificación de la autenticidad de un sitio web**

  Podemos utilizar herramientas como Google Safe Browsing o extensiones para el navegador como WOT (Web Of Trust) para comprobar la fiabilidad de los sitios web.

  El uso de software de seguridad actualizado que ofrezca protección en tiempo real contra sitios web fraudulentos y con detección de phishing como antivirus y cortafuegos comerciales.

5.3.1.2 EDUCACIÓN SOBRE TÉCNICAS COMUNES DE INGENIERÍA SOCIAL

Denominamos "**ingeniería social**" a aquellas técnicas y estrategias que utilizan los ciberdelincuentes para manipular a las personas con el fin de obtener acceso a información sensible como contraseñas u otro tipo de datos personales.

Las técnicas más utilizadas para este fin son:

- **Pretexting:** el atacante crea una historia falsa para obtener información o ganarse la confianza del usuario (por ejemplo, diciendo que es un técnico de soporte técnico de un fabricante conocido).
- **Pharming:** consiste en el envío de enlaces a la víctima para que, al pulsar sobre ellos, se dirijan a sitios web falsos para el robo de datos.
- **Baiting:** es el ofrecimiento de algo gratis, como software o regalos, a cambio de que el usuario ingrese información personal. Se usa habitualmente el ofrecimiento de nuevos seguidores para la red social de la víctima, por ejemplo.

5.3.2 Configuración avanzada de privacidad en plataformas digitales

La privacidad digital debe considerarse como un derecho esencial y corresponde ser gestionada de forma cuidadosa en redes sociales y otros servicios en línea.

5.3.2.1 REVISIÓN Y AJUSTE DE CONFIGURACIONES DE PRIVACIDAD EN REDES SOCIALES Y SERVICIOS EN LÍNEA

Cada vez que ingresamos nuestros datos para darnos de alta en **alguna red social**, estamos creando un perfil que utilizará la empresa propietaria de la red para usos comerciales.

La propia aceptación de los términos y condiciones de uso de esa plataforma implica la firma de un contrato online por el servicio recibido y, a cambio, estaremos cediendo diversa cantidad de información que aprovechará la compañía en su propio beneficio.

No podemos controlar qué datos va a utilizar la red social pero sí acceder a algunas opciones para mejorar la privacidad del perfil creado.

Así, es importante revisar y personalizar las configuraciones de privacidad de cuentas en plataformas como Facebook, Twitter e Instagram para controlar quién puede ver las publicaciones y quién puede contactar con el usuario.

Por otro lado, limitar la visibilidad de la información personal como, por ejemplo, la fecha de nacimiento, dirección, email, etc, para que se muestre solo a familia, amigos cercanos o grupos de personas de confianza.

Los servicios de almacenamiento de archivos en línea o nube (Google Drive, Dropbox) deben estar correctamente configurados asegurándonos de que los documentos y fotos compartidos no tengan acceso para usuarios no autorizados.

Otras opciones importantes que debemos revisar es el ajuste de la configuración de las **cookies** en plataformas de comercio electrónico o navegación para proteger los datos de seguimiento.

5.3.2.2 GESTIÓN DE PERMISOS DE APLICACIONES Y EXTENSIONES DEL NAVEGADOR

Las aplicaciones que instalamos en los teléfonos inteligentes, ya sea con Android, con sistemas de Apple, o las extensiones para los navegadores web, solicitan permisos de uso al propietario del dispositivo.

Estos permisos que se le conceden a la aplicación o a la extensión abarcan desde los más inocuos (**bajo riesgo**), sensibles (**riesgo moderado**), peligrosos (**alto riesgo**) y críticos (**riesgo extremo**).

A continuación te muestro una tabla que resume los riesgos y su definición:

Nivel de riesgo	Permiso / Capacidad	¿Para qué lo solicita la app?	Riesgo potencial	Ejemplo legítimo	Ejemplo sospechoso / red flag
🔵 **Inocuo**	Acceso a Internet	Cargar contenido online, mostrar anuncios	Mínimo: solo tráfico de red	Juego que descarga niveles	—
🔵 **Inocuo**	Almacenamiento básico	Guardar ajustes o archivos propios de la app	Bajo: se limita a su carpeta	Editor de fotos que guarda imágenes	—
🔵 **Inocuo**	Vibración	Enviar notificaciones táctiles	Ninguno relevante	WhatsApp al recibir mensajes	—
🟡 **Sensible**	Ubicación	Mapas, clima, recomendaciones locales	Rastreo de movimientos y perfilado	Google Maps	Linterna que pide ubicación
🟡 **Sensible**	Cámara / Micrófono	Fotos, vídeollamadas, grabar audio	Espionaje visual o sonoro	Instagram (selfies, stories)	Calculadora que pide micrófono
🟡 **Sensible**	Contactos	Sincronizar redes sociales o mensajería	Robo de agenda → spam / phishing	WhatsApp para sugerir contactos	Juego que importa tus contactos

Nivel de riesgo	Permiso / Capacidad	¿Para qué lo solicita la app?	Riesgo potencial	Ejemplo legítimo	Ejemplo sospechoso / red flag
Peligroso	Acceso a SMS / Llamadas	Leer códigos 2FA, identificar llamadas	Lectura de mensajes privados, suplantación	App bancaria verificando SMS	Juego que lee tus SMS
Peligroso	Permisos de Administrador	Borrar datos remotos, antirrobo	Bloqueo total, instalación de malware	Gestor de dispositivos (MDM) corporativo	Wallpaper que se hace admin
Peligroso	Acceso a Notificaciones (extensión)	Mostrar/ responder mensajes en escritorio	Robo de credenciales, inyección de código	WhatsApp Web	Extensión "fondos de Chrome" que lee notificaciones
Crítico	Acceso raíz / superusuario	Recuperación de datos, personalización profunda	Control total del sistema	Herramienta de recuperación profesional	Cualquier app desconocida que pide root
Crítico	Instalar apps de orígenes desconocidos	Actualizar vía APK externa	Infección con malware o ransomware	Beta oficial de una app conocida	App "Premium gratis" que instala otras apps

Los permisos que solicita —y que se le conceden— una aplicación deben ser coherentes con el tipo de aplicación. Un exceso de permisos para una aplicación que, en principio, no los necesita, debe llevarnos a desconfiar.

Consejos de seguridad:

- **Revisar los permisos antes de instalar**: comprobar que estos son coherentes con las funciones de la aplicación.
- **Revisión periódica:** conviene repasar los permisos otorgados a aplicaciones de forma habitual.
- **Usar el principio de mínimo privilegio:** denegar permisos innecesarios. Ej.: ¿Necesita la linterna conocer la ubicación?
- **Actualizar apps y extensiones:** versiones más antiguas pueden tener vulnerabilidades.
- **Extensiones para navegadores:** utilizar las mínimas imprescindibles y verificadas por el desarrollador del navegador.

Ejemplo de alerta: si una extensión aparentemente trivial, como por ejemplo "cambiar el fondo de Chrome", solicita permisos críticos como acceso a contraseñas o notificaciones, ¡desinstala de inmediato!.

Una buena herramienta para comprobar el estado de las aplicaciones y qué permisos se les ha concedido es "*spytrap-adb*" aunque requiere algunos conocimientos técnicos avanzados para su instalación y uso.

Puedes encontrar un pequeño tutorial en este enlace:

"https://youtu.be/JqDfkpawnT8"

5.3.2.3 USO DE NAVEGADORES CENTRADOS EN LA PRIVACIDAD Y EXTENSIONES BLOQUEADORAS DE RASTREADORES

El modo más seguro de utilizar internet es mediante el uso de navegadores cuyo diseño se enfoque en la prevención de la fuga de datos y la privacidad.

Como recomendación, es interesante probar los navegadores "*Brave*" o "*Librewolf*" que existen para todas las plataformas. Cuentan con configuraciones avanzadas de seguridad y bloquean los rastreadores de forma automática ofreciendo una experiencia de navegación más segura y limpia.

Existen, además, extensiones o "*plugins*" de privacidad que se instalan en los navegadores habituales y se encargan de bloquear rastreadores, publicidad y asegurar conexiones cifradas en todas las páginas web. Ejemplo: **uBlock Origin, Privacy Badger o HTTP Everywhere**.

5.3.3 Normas éticas para la gestión y uso de información personal y de terceros

Como ya se estudió en el módulo 3, el manejo ético de los datos personales no es, simplemente, un requisito legal, sino una responsabilidad fundamental que protege tanto a los usuarios como a las organizaciones. Un uso inadecuado puede generar pérdida de confianza, sanciones económicas y daños en la reputación. Por todo ello, en esencial seguir unos principios éticos y conocer los marcos normativos (como el RGPD) que garanticen la transparencia, seguridad y respeto por los datos de los usuarios.

5.3.3.1 CUMPLIMIENTO DE LAS NORMATIVAS COMO EL RGPD

El Reglamento General de Protección de Datos es la normativa europea más estricta en materia de privacidad. Se aplica a cualquier organización que procese datos de los ciudadanos de la UE.

Sus principios clave giran en torno a:

- **Mínima cantidad de datos:** se deben recopilar únicamente los datos estrictamente necesarios para ofrecer el servicio.
- **Limitación de la finalidad:** los datos recogidos se deben usar exclusivamente para los fines declarados.
- **Seguridad:** las organizaciones deben implementar las medidas técnicas y organizativas adecuadas para proteger la información.
- **Transparencia:** los usuarios deben mantenerse informados de forma clara sobre cómo se tratan sus datos.

El reglamento define cuáles son los derechos fundamentales de los individuos:

- **Acceso:** todo usuario tiene derecho a una copia de los datos personales que la entidad u organización haya recopilado.
- **Rectificación**: los usuarios podrán solicitar la corrección de la información inexacta recogida.
- **Derecho al olvido**: podrán solicitar la eliminación de los datos.
- **Portabilidad**: los datos que requiera el usuario deben facilitarse en un formato transferible.
- **Oposición:** cualquier usuario tiene derecho a negarse al procesamiento de los datos para fines como el marketing directo.

Por ello, las organizaciones están obligadas a solicitar un consentimiento explícito, que debe ser libre, informado y específico.

En caso de que aparezca una brecha que derive en fuga de datos, la organización debe informar del hecho a las autoridades y a los afectados en las siguientes 72 horas.

El diseño de las plataformas de recogida de datos debe integrar la protección de los datos personales desde su planteamiento (*Privacy by Design*).

5.3.3.2 OBTENCIÓN DEL CONSENTIMIENTO INFORMADO PARA LA RECOPILACIÓN DE DATOS

La petición para la recogida de datos del ciudadano debe realizarse mediante la presentación de un formulario claro y verificable que permita su cancelación con la misma facilidad que su concesión.

Ejemplo de buenas prácticas

❌ **Incorrecto**:

"Al registrarse, acepta nuestros Términos y Condiciones" (sin detalles).

✅ **Correcto**:

"Al marcar esta casilla, acepta que usemos su email para enviarle ofertas. Puede darse de baja en cualquier momento. [Enlace a política de privacidad]".

El consentimiento tiene que estar escrito en un lenguaje claro y sencillo especificando qué datos se recopilan, para qué se van a utilizar y con quién se van a compartir en su caso.

5.3.3.3 TRANSPARENCIA EN LAS POLÍTICAS DE PRIVACIDAD Y TÉRMINOS DEL SERVICIO

Las políticas de privacidad y términos de servicio recogen la forma cómo la organización recopila, usa, protege y comparte los datos de las personas que hacen uso de los servicios que ofrece la entidad.

Una buena hora de política de privacidad debe incluir, como mínimo el tipo de datos que va a recopilar (cookies, IP, datos de pago, etc), la finalidad del tratamiento de la información (mejora del servicio, marketing), con qué medidas de seguridad cuenta la entidad (cifrado, accesos restringidos) y cuáles son los derechos del usuario y cómo ejercerlos.

Por otro lado, los términos del servicio aglutinan las cláusulas que indican de qué manera se va a ofrecer el servicio de la organización pero evitando cláusulas abusivas (por ejemplo, evitar la cesión permanente de derechos sobre los contenidos cargados por el usuario) y se deben mostrar utilizando un lenguaje accesible y claro, evitando tecnicismos innecesarios.

Las políticas de privacidad y términos de uso deberían revisarse al menos una vez al año o cuando incluyan cambios relevantes y notificar a los usuarios estas modificaciones o actualizaciones en los términos.

5.4 MARCO LEGAL PARA LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA Y LA UNIÓN EUROPEA

Esta sección del módulo 5 no requiere su estudio. Se ha insertado con la única finalidad de que sirva como material de referencia y ofrezca al lector la posibilidad de ampliar conocimientos o de buscar cuestiones concretas en el articulado legal.

Legislación Española

- **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**

  Adapta el Reglamento General de Protección de Datos (RGPD) al ordenamiento jurídico español y reconoce derechos digitales como el derecho al olvido, la portabilidad de datos y la desconexión digital.

- **Ley Orgánica 7/2021, sobre protección de datos personales tratados con fines penales**

  Regula el tratamiento de datos en el ámbito de la prevención, detección, investigación y enjuiciamiento de infracciones penales.

- **Real Decreto 255/2025, sobre el DNI digital**

  Establece que el tratamiento de los datos personales asociados al Documento Nacional de Identidad digital se rige por el RGPD y la LOPDGDD, garantizando la seguridad y privacidad en su uso.

- **Nuevas medidas sobre el padrón municipal**

  Se han implementado restricciones al acceso de terceros, la obligatoriedad de consentimientos informados y auditorías periódicas para proteger los datos personales en los registros municipales.

- **Ley de protección de menores en entornos digitales**

  Incluye sanciones por la creación de contenido sexual con inteligencia artificial y grooming, establece controles parentales obligatorios y eleva la edad mínima para el consentimiento en redes sociales a 16 años.

- **Registro obligatorio de datos de viajeros**

  Desde diciembre de 2024, hoteles y agencias de viajes deben registrar hasta 42 datos personales de los viajeros, medida que ha generado controversia por posibles conflictos con la normativa de protección de datos.

Legislación Europea

- **Reglamento General de Protección de Datos (RGPD) – Reglamento (UE) 2016/679**

  Establece el marco general para la protección de datos personales en la UE, incluyendo derechos como el acceso, rectificación, supresión y portabilidad de los datos.

- **Ley de Datos (Data Act)**

  Otorga a personas y empresas el derecho a acceder y compartir los datos generados por dispositivos conectados, promoviendo una economía de datos justa y transparente.

- **Reglamento (UE) 2025/327 sobre datos de salud electrónicos**

  Permite a los ciudadanos ejercer el derecho de autoexclusión para limitar el acceso a sus datos de salud electrónicos, garantizando la privacidad incluso en contextos transfronterizos.

- **Ley Europea de Inteligencia Artificial (AI Act)**

  Clasifica los sistemas de IA según su nivel de riesgo y establece requisitos para garantizar que su uso sea seguro, transparente y respete los derechos fundamentales, incluida la protección de datos personales.

- **Reglamento ePrivacy (pendiente de aprobación)**

  Busca reforzar la confidencialidad de las comunicaciones electrónicas, regulando aspectos como las cookies, el spam y la privacidad en servicios de mensajería.

5.5 EJERCICIO PRÁCTICO

La propuesta de ejercicio práctico para este módulo es, quizá, más compleja que en los anteriores debido a la profundidad del contenido que hemos abarcado. No obstante, y del mismo modo que en los capítulos previos, la práctica pretende servir como repaso y ayuda para entender un poco mejor los conceptos que has estudiado.

Este ejercicio práctico que te permitirá interiorizar un tema bastante denso pero imprescindible en el mundo etéreo del ciberespacio.

Ejercicio 1

"Mi entorno digital blindado"

Diseñado para que consolides *todas* las competencias del módulo: protección activa de equipos y redes, privacidad personal y gestión ética de los datos.

- **Objetivo general**

  Realizarás una mini-auditoría de tu propio ecosistema (PC, móvil y router Wi-Fi) y simularás un incidente de seguridad. Al terminar, entregarás un informe de 3–4 páginas con evidencias (capturas o extractos) y una reflexión ética/RGPD.

- **Escenario de partida**

  Imagina que mañana debes conectar tu portátil a la Wi-Fi pública de un aeropuerto para descargar un contrato confidencial. Además, en tu móvil usas varias apps de ocio y sueles instalar extensiones experimentales en Chrome.

- **Tareas (realizadas de modo secuencial)**

#	Bloque	Qué tienes que hacer	Evidencia mínima a incluir
1	**Inventario & hardening**	- Lista rápida de dispositivos que usas a diario. - Para cada uno: antivirus/firewall (marca, versión) + fecha de última actualización + autenticación (contraseña, biometría, 2FA). - Desinstala 2 programas que no uses y justifica por qué reducían la superficie de ataque.	Captura del panel "Aplicaciones instaladas" + tabla resumen.
2	**Wi-Fi segura en casa**	Accede al router y: - Activa WPA3 (o el protocolo más fuerte disponible). - Cambia contraseña y oculta el SSID. - Crea una red de invitados con aislamiento y ancho de banda limitado. - Explica en ≤ 80 palabras la utilidad de cada acción.	2 capturas del portal del router avec tintadas las credenciales.

#	Bloque	Qué tienes que hacer	Evidencia mínima a incluir
3	**Permisos de apps & extensiones**	- En tu smartphone, revisa los permisos de 5 apps al azar. - Clasifícalos con el semáforo 🔵🟡🔴🟥 y revoca al menos 1 permiso injustificado. - En tu navegador, elimina una extensión que pida más de lo necesario y justifica.	Tabla "App / Permiso / Nivel / Acción" + screenshot de la revocación.
4	**Simulación de phishing**	Descarga el fichero .txt que contiene **dos e-mails** (uno legítimo, uno falso) desde este repositorio de práctica (o crea tú mismo dos plantillas). - Señala 5 indicios que delatan al falso (URL, ortografía, urgencia…). - Reescribe el asunto del correo fraudulento para hacerlo *aún* más convincente → explica por qué es peligroso.	Copia de los e-mails con comentarios en color o marcados.
5	**VPN & red pública**	- Elige un servicio VPN gratuito de la tabla del módulo. - Conéctate desde tu móvil a un *hotspot* público compartido desde otro dispositivo. - Comprueba tu IP antes y después (whatismyip.com o similar). - Explica en 3 frases qué datos protege (y cuáles **no**).	Capturas con IP real vs. IP VPN + breve explicación.
6	**Reflexión ética & RGPD**	- Haz un diagrama (o lista numerada) del flujo de datos personales que generas cuando: a) envías ese contrato por e-mail b) lo almacenas en la nube corporativa. - Para cada punto, indica al menos una medida RGPD (mínima cantidad, cifrado, consentimiento…).	Foto/imagen del diagrama + párrafo de conclusiones (≈ 150 palabras).

Entregable

- **Informe PDF** con:
  - Portada (nombre y fecha).
  - Sección por bloque, evidencias incrustadas.
  - Conclusiones generacionales: **¿Qué ha cambiado en tu percepción de la seguridad digital?**
- **Opcional**: sube un vídeo corto (≤ 3 min) mostrando la prueba de VPN y comenta en voz alta lo que ocurre.
- **Recursos que puedes usar**
  - Panel de seguridad de Android / iOS ("Privacidad" → "Permisos").
  - Shodan o Wireshark (para usuarios avanzados) si quieres extra-puntos.
  - Herramientas online de diagrama (draw.io, Lucidchart) o simplemente PowerPoint.

5.6 AUTOEVALUACIÓN (10 PREGUNTAS)

Cada módulo incluye, al final, un pequeño cuestionario cuyo propósito no es otro que el de comprobar si has aprendido los conceptos estudiados. Te invitamos a realizarlo con tranquilidad y sin presión para que te sirva como recurso constructivo que te empuje en el camino del conocimiento.

Cuestionario (solo una respuesta es la correcta)

1. **¿Qué protocolo de seguridad Wi-Fi ofrece la protección más fuerte para redes domésticas?**
   a) WEP.
   b) WPA2.
   c) WPA3.
   d) WPS.

2. **Según la tabla de permisos, la cámara y el micrófono se clasifican como:**
   a) Inocuos (🔵)
   b) Sensibles (🟡)
   c) Peligrosos (🔴)
   d) Críticos (🚨)

3. ¿Cómo se denomina el proceso de cifrar los datos en el dispositivo del emisor y descifrarlos solo en el del receptor?

a) Cifrado simétrico.
b) SSL/TLS.
c) Cifrado de disco completo.
d) Cifrado de extremo a extremo.

4. ¿Qué herramienta de Windows permite cifrar todo el contenido de un disco duro o partición?

a) Defender SmartScreen.
b) BitLocker.
c) PowerShell.
d) Cortafuegos.

5. Un correo con urgencia, faltas y remitente extraño suele ser un ejemplo de:

a) Spam legítimo.
b) Sandbox.
c) Phishing.
d) Newsletter.

6. Al crear una red de invitados en tu router, el principal beneficio es:

a) Más velocidad en la red principal.
b) Aislar dispositivos externos de la red interna.
c) Ahorrar batería.
d) Eliminar contraseñas.

7. ¿Cuál de estos servicios VPN es de tipo *premium* según la tabla del módulo?

a) ProtonVPN.
b) Windscribe.
c) TunnelBear.
d) ExpressVPN.

8. ¿Qué permiso permitiría a una extensión de navegador leer tus credenciales guardadas y se considera «Peligroso»?

a) Acceso a notificaciones.
b) Vibración.
c) Acceso a Internet.
d) Ocultar pestañas.

9. ¿Qué derecho RGPD te permite solicitar la eliminación definitiva de tus datos personales?

a) Portabilidad.
b) Acceso.
c) Derecho al olvido.
d) Rectificación.

10. El principio de mínimo privilegio consiste en:

a) Conceder todos los permisos y retirarlos después.
b) Otorgar solo los permisos estrictamente necesarios.
c) Compartir credenciales entre apps fiables.
d) Usar la misma contraseña en todas partes.

Respuestas correctas

1 - C, 2 - B, 3 - D, 4 - B, 5 - C, 6 - B, 7 - D, 8 - A, 9 - C, 10 - B

¡Enhorabuena!

Has recorrido un camino lleno de conceptos técnicos y buenas prácticas, y lo has superado con nota. Cada paso que diste —desde blindar tu Wi-Fi hasta identificar un correo de phishing— demuestra tu compromiso con tu propia seguridad y la de quienes te rodean.

Sigue así. Cada contraseña fuerte, cada permiso revisado, cada actualización aplicada es una victoria que suma. La ciberseguridad no es un destino, sino un hábito, y tú ya lo estás convirtiendo en parte de tu día a día.

¡Orgulloso/a de tu progreso! Mantén la curiosidad encendida y celebra este logro.**Es la mejor señal de que vas por el camino correcto.**


TEMA 6
RESOLUCIÓN CREATIVA DE PROBLEMAS EN CONTEXTOS DIGITALES