módulo 1

Protección básica de sistemas, dispositivos y contenidos digitales

- Descripción de los principales riesgos asociados al uso de dispositivos tecnológicos
- Aplicación de medidas básicas de protección y seguridad
- Aplicación de medidas de seguridad a contenidos digitales
- Navegación dentro del entrono virtual de aprendizaje donde se realiza el programa formativo

---

OBJETIVOS:

- Concienciarse de la necesidad de estar informado de las principales amenazas y riesgos que ponen en peligro nuestra presencia y actividad en Internet y qué medidas prácticas tomar para evitarlos el máximo.
- Cómo mantener nuestros dispositivos digitales adecuadamente actualizados y cuáles son las ventajas de hacerlo.
- Aprender las principales características que nos ofrecen las plataformas de enseñanza y aprendizaje virtual, tomando como ejemplo la conocida plataforma educativa Moodle.

INTRODUCCIÓN

Internet y las nuevas tecnologías nos facilitan la realización de innumerables actividades y tareas de manera rápida y directa, pero su uso está amenazado por diferentes riesgos que ponen en peligro nuestra identidad, datos o información personal y profesional. Los ciberdelincuentes aprovechan el anonimato y acceso global de Internet para cometer sus delitos, entre los que se encuentran estafas y fraudes *online*, suplantación de identidad y robos de dispositivos y datos. Riesgos que podemos minimizar poniendo en práctica medidas de autoprotección como el uso correcto de contraseñas, bloqueo de dispositivos o programas de protección antivirus.

Otra de las puertas de entrada que utilizan son las redes WiFi públicas, muy útiles para conectarse a Internet de manera gratuita, pero abiertas a riesgos sino nos protegemos adecuadamente. Otra de las maneras de protección esencial es el mantenimiento correcto de nuestros dispositivos como ordenadores, tablets o teléfonos móviles. La actualización del *software* que utilizamos en dichos aparatos es una parte esencial de ese mantenimiento.

Finalmente, aprenderemos las principales características que definen a una plataforma educativa *online* o entorno virtual de aprendizaje. Una manera de aprender a distancia que nos facilita Internet y que permite la educación y formación flexible y de calidad para millones de personas en todo el mundo.

1. DESCRIPCIÓN DE LOS PRINCIPALES RIESGOS ASOCIADOS AL USO DE DISPOSITIVOS TECNOLÓGICOS

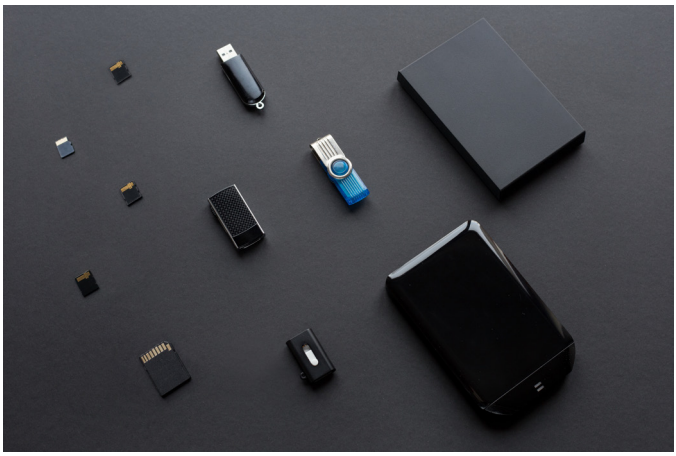
A medida que la tecnología sigue desempeñando un papel cada vez más importante en nuestra vida cotidiana, existen una serie de riesgos asociados al uso de los dispositivos tecnológicos. Para mitigar estos riesgos, es importante tomar medidas como utilizar contraseñas seguras, mantener los dispositivos actualizados con los últimos parches de seguridad, utilizar programas antivirus y ser precavido al abrir archivos adjuntos de correo electrónico o hacer clic en enlaces

de fuentes desconocidas. También es importante hacer copias de seguridad periódicas de los datos importantes e informar de cualquier actividad sospechosa o incidente a las autoridades competentes.

1.1 Robo y pérdida de dispositivos y datos

Cuando una persona, organización o empresa sufre la pérdida de un dispositivo como un móvil, una tarjeta de memoria o un ordenador, además del perjuicio por el valor económico del aparato (*hardware*), el peligro adicional es la pérdida de los datos que ese dispositivo pueda tener almacenados en su interior. Que en muchas ocasiones tienen un valor económico o personal mucho más grande que el propio aparato y que, dependiendo de la naturaleza de los datos, puede tener unas consecuencias muy graves. Los programas o *software* se pueden volver a instalar en un nuevo dispositivo, pero los datos o información se pueden perder definitivamente si no se han hecho las recomendadas copias de seguridad preventivas. Incluso si la información perdida o sustraída tiene esa copia de respaldo, su acceso por parte de personas no autorizadas puede tener graves consecuencias para una persona, organización o empresa. Por tanto, las pérdidas de dispositivos o robos intencionados constituyen un problema que se produce diariamente en todo tipo de entornos personales y profesionales.

Una gran mayoría de los dispositivos actuales son de tipo portátil, que los usuarios llevamos con nosotros y movemos continuamente de un lugar a otro. Una gran ventaja frente a los antiguos dispositivos fijos y pesados, pero que aumenta las posibilidades de pérdida o de sufrir un robo intencionado. Entre otros, los más comunes son: ordenadores portátiles, teléfonos móviles, tabletas, memorias USB, tarjetas de memoria, etc. Todos estos dispositivos pueden almacenar diversa cantidad de datos e información y, si esta es muy importante, es esencial tomar medidas para que en caso de pérdida o robo las consecuencias personales, económicas o profesionales sean las mínimas posibles. En los temas siguientes desarrollaremos con más detalle las diferentes medidas de prevención y protección más recomendadas para proteger lo más importante: los datos. Resumiremos ahora algunas de las medidas para evitar dichas consecuencias.



Tipos de dispositivos de datos que pueden ser objeto de robo o pérdida.

A. Medidas para minimizar las consecuencias de una pérdida o robo

Las dos recomendaciones básicas para proteger información confidencial en dispositivos tecnológicos son: realizar siempre una copia de seguridad o respaldo de esos datos y proteger los dispositivos con diversos sistemas de encriptación y contraseñas. Además de estas medidas esenciales, se recomiendan las siguientes:

- Conocer qué información guardamos en nuestros dispositivos, tanto portátiles como fijos: ordenadores, teléfonos móviles, memoria USB, ordenadores portátiles, etc. Tenemos que ser conscientes de que, si en estos dispositivos disponemos de información especialmente sensible, tendremos que protegerlos de una manera especial. Lo recomendable es solo mantener datos muy importantes en la memoria de estos dispositivos si es realmente imprescindible, de lo contrario lo más seguro es guardar la información esencial en discos duros virtuales - la llamada nube- donde no los podemos perder físicamente y están mucho más protegidos frente a cualquier intento de robo o consulta no autorizada. Si por ejemplo manejamos cuentas bancarias desde nuestro teléfono móvil, no se recomienda guardar las contraseñas y datos de acceso directamente en el teléfono, sino en uno de

estos servicios de acceso virtual solo accesible por nosotros. de esa manera, si perdemos o nos sustraen dicho teléfono nadie podrá acceder a dicha información bancaria.

- Cambiar las contraseñas de acceso. Si sufrimos la pérdida o robo de un dispositivo tipo teléfono móvil u ordenador portátil, debemos inmediatamente cambiar las contraseñas de acceso a servicios como el correo electrónico y otro tipo de cuentas. Accediendo desde otro dispositivo e identificándonos con los métodos de identidad que previamente y de forma recomendada deberíamos establecer en ese tipo de servicios.
- Mantener nuestros dispositivos siempre a mano y no dejarlos desatendidos en lugares desconocidos, especialmente en medios de transporte. Evitar acudir a lugares de ocio con teléfonos móviles si no es imprescindible.
- Conocer y guardar la información que identifica a estos dispositivos, como número de IMEI en el caso de las tarjetas de teléfono móvil, para poder anularlas inmediatamente después de una pérdida o robo. Por ejemplo, en el caso de los teléfonos tipo Android, podemos acceder al número IMEI de la tarjeta desde el menú Ajustes.
- Evitar el uso de dispositivos de memoria portátil (memorias USB, tarjetas de memoria) para guardar y trasladar información importante o confidencial, utilizando mejor en su lugar discos duros virtuales en la nube, donde se almacena la información y el dispositivo solo sirve para acceder a ella mediante identificación.
- Instalar programas o aplicaciones que permiten el rastreo *online* de dispositivos robados y que se activan automáticamente cuando ese teléfono móvil u ordenador portátil es encendido. Gracias a este *software* podemos localizar la posición de nuestro dispositivo en tiempo real, Gracias a las modernas técnicas que nos facilita Internet y los sistemas GPS.

1.2 Suplantación de identidad

A. Características y tipos

La tecnología actual de Internet permite que individuos o colectivos suplanten la identidad de otras personas y organizaciones con fines malintencionados. Desde delincuentes en busca de información valiosa como datos bancarios o víctimas de abuso *online* hasta grupos criminales que tratan de acceder a información privilegiada de empresas y gobiernos, todos ellos utilizan diferentes técnicas y estrategias para falsear su verdadera identidad *online*. Y poder así acceder más fácilmente a las víctimas objeto de su acción fraudulenta. Este tipo de acciones con fines maliciosos no debe confundirse con el uso de perfiles anónimos en redes sociales, que los usuarios podemos crear libremente para evitar utilizar nuestros datos personales reales como nombre, dirección, etc. El uso de este tipo de perfiles está autorizado por estas plataformas y tienen como objetivo el anonimato, no la realización de ninguna actividad ilícita o de acoso a otros usuarios.

La suplantación o usurpación de identidad *online* con fines deshonestos se lleva a cabo obteniendo datos personales concretos de las personas, organismos o empresas a suplantar. Los atacantes utilizan fallos en los sistemas de seguridad informática para penetrar en las cuentas e información confidencial de sus víctimas, roban dispositivos como ordenadores o teléfonos para robar esa información, o utilizan el envío de emails, mensajes de móvil SMS o aplicaciones de mensajería como WhatsApp y similares. Por eso es tan importante saber protegerse ante estos posibles ataques, la información es la mejor manera de defenderse ante posibles contactos utilizando una identidad falsa.

Los ciberdelincuentes pueden obtener esa información personal a través de diversos métodos, como el robo de equipos que almacenan información personal y diferentes técnicas de engaño. La suplantación de identidad es ilegal y, como consecuencia, está sujeta a diferentes penas.

Hay varias formas de hacerse pasar por otra persona o entidad:

- **Perfiles falsos**. Creando un perfil falso de otra persona en redes sociales y comunicándose con personas y organizaciones individuos comportándose como ellos.
- **Phishing**. Por medio de correos electrónicos, mensajes SMS, llamadas telefónicas o mensajes en apps de mensajería tipo WhatsApp. Los estafadores se pueden hacer pasar por bancos, empresas de suministro, proveedores, clientes, etc. Las víctimas son engañadas para revelar información confidencial, cuentas bancarias, contraseñas, etc. Esta técnica se conoce como *phishing* y es uno de los fraudes *online* más comunes en nuestros días. Los estafadores que utilizan el phishing pueden incluso intentar hacerse pasar por agencias del gobierno o administraciones: Seguridad Social, Hacienda, Tráfico…
- **Sitios web falsos**. Los sitios web falsos son creados por los estafadores como copias de páginas web auténticas y cuando los usuarios acceden a ellos e introducen sus claves de entrada, estas quedan registradas. Los estafadores pueden entonces utilizar estas claves para acceder a las cuentas de correo, perfiles de redes sociales, o incluso información bancaria de sus víctimas. Algunas estafas de compras *online* pueden utilizar incluso una aplicación móvil falsa que imita a una real y que incluye el nombre, colores, logotipo familiar y un dominio similar. Con el objetivo de apoderarse de los datos de las víctimas en estas tiendas *online* y realizar compras no autorizadas.

Atención

Los intentos de fraude por suplantación de identidad ocurren a diario y los ciberdelincuentes crean nuevas maneras de engañar a los ciudadanos mediante mensajes, falseando todo tipo de empresas y organismos públicos. En caso de duda, hay que contactar directamente con la entidad para comprobar la veracidad o falsedad de ese mensaje.

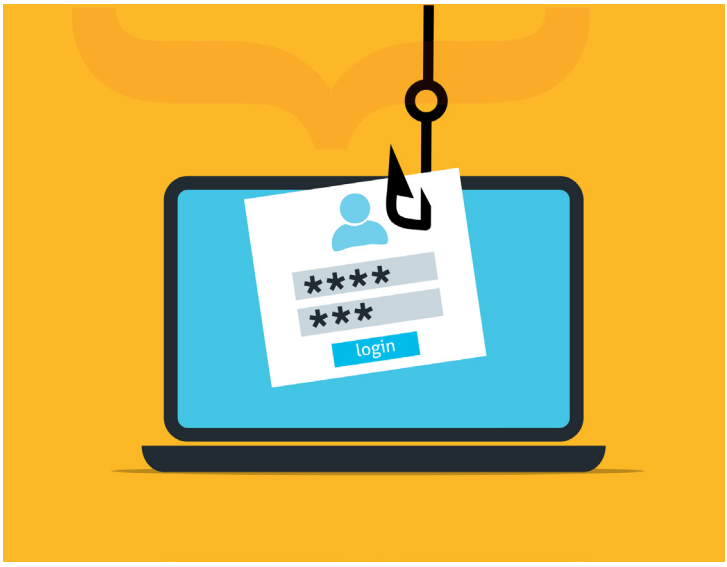
Los **objetivos** que persiguen los individuos o grupos que suplantan la identidad de personas, empresas u organizaciones son variados:

- Robo de datos e información confidencial.
- Sustracción de dinero, acciones,

- Compras no autorizadas a nuestro nombre.
- Falsificación de documentación.
- Robo de datos bancarios e información financiera.
- Robo de cuentas en redes sociales, para publicar información no autorizada en nuestro nombre.
- Contratar servicios financieros a nuestro nombre o nuestra empresa.
- Solicitud de Créditos a nuestro nombre o nuestra empresa.
- Realización de estafas o fraudes a nuestro nombre.

Otro tipo de suplantación de identidad dirigido especialmente a menores de edad y que veremos posteriormente, es el que tiene como objetivo el acoso y abuso sexual a través de Internet, el conocido como ***grooming***.

Todos los tipos de suplantación de identidad tienen efectos muy negativos sobre las víctimas que lo sufren ya sean ciudadanos particulares o empresas. Por esa razón, es importante que los usuarios de Internet pongamos en marcha medidas de protección a nuestro alcance para evitar o minimizar al máximo este tipo de riesgo.



El phishing trata de "pescar" víctimas en Internet para robar sus datos de acceso a bancos y similares

B. Cómo prevenir o evitar la suplantación

Después de ver todas esas formas de usurpar la identidad y los fines para los que se puede usar, no está de más saber cómo prevenir la suplantación de identidad. Para ello podemos tomar una serie de **medidas** que reduzcan el riesgo de que alguien se haga pasar por nosotros o nos roben datos para usarlos de manera fraudulenta:

- Denunciar inmediatamente a las autoridades la pérdida o sustracción de documentos de identidad como el DNI, carnet de conducir, pasaporte, etc.
- No entregar documentos de identidad a individuos o entidades para alguna gestión, si estos nos resultan sospechosos.
- Si recibimos un correo electrónico, llamada de teléfono o SMS y no estamos seguros de la identidad real del remitente, es mejor tomarse la molestia de contactar directamente con la persona o entidad real y verificar efectivamente que han sido ellos los que nos han enviado esa comunicación.
- No abrir, hacer clic, o introducir nuestras contraseñas en sitios o páginas web que nos parezcan sospechosas.
- No instalar en nuestro teléfono móvil o tableta aplicaciones o juegos gratuitos que nos parezcan sospechosos ya que muchos estafadores ofrecen esta gratuidad para captar a posibles víctimas.
- Utilizar contraseñas seguras, que sean difíciles de averiguar. si no queremos recordarlas podemos utilizar las aplicaciones conocidas como gestores de contraseñas, que nos facilitan la labor de guardar de forma segura las diferentes claves que utilizamos en nuestra actividad *online*. Se pueden asimismo activar sistemas de seguridad adicionales, como los factores de doble autenticación, que requieren el envío de un código a nuestro teléfono móvil además de la contraseña en una página web. Las preguntas y respuestas de seguridad que hemos de rellenar en algunos servicios que nos lo solicitan como método de identidad cuando olvidamos una contraseña, no deben de contener información que publicamos en redes sociales, como por ejemplo lugar de nacimiento, color favorito, nuestro primer colegio, etc.
- Mantener nuestros programas de protección antivirus y anti-*malware* actualizados en todos nuestros dispositivos.

- Asegurarnos de comprar *online* en sitios de confianza, e intentar utilizar métodos de pago no asociados directamente a nuestros datos bancarios.

1.3 Software malicioso

A. Descripción

Uno de los peligros más comunes que afectan a sistemas informáticos es el conocido como *malware*, o *software* malicioso. Se trata de un programa o código informático que se introduce dentro de un dispositivo como un ordenador o teléfono móvil con el objetivo de robar información, hacerse con el control de dicho aparato, espiar la actividad o producir un daño en el sistema. Se trata por tanto de una aplicación diseñada exclusivamente con fines malintencionados y que provoca numerosos daños y efectos negativos en millones de usuarios de todo el mundo.

Existen muchos tipos de *malware* en circulación y los conocidos virus informáticos podrían considerarse incluidos en este tipo de programas dañinos. Aunque por su importancia los virus tienen su propia clasificación y modos de actuar. Las características comunes a todo tipo de programas de *malware* son: se introducen en los equipos informáticos y teléfonos móviles sin que los usuarios se den cuenta de ello y realizan la labor dañina para la que fueron diseñados de manera oculta. El objetivo es permanecer invisibles y no ser detectados, por eso no interfieren de manera destacada en el rendimiento o actividad de los dispositivos infectados.

B. Cómo funciona el malware

Un programa tipo *malware* entra en un ordenador, redes o teléfono móvil de la misma manera que los virus. El usuario del dispositivo realiza alguna acción habitual pero que de forma involuntaria permite la infección de ese código maligno. Las acciones qué pueden llevar a la introducción del archivo *malware* en un ordenador o teléfono móvil pueden ser: