AF4: Seguridad en la red

Recomendaciones de seguridad. Detección de vulnerabilidades

Digitalización aplicada al sector productivo.
Módulo formativo sobre competencias digitales transversales básicas.

Proyecto financiado por el Ministerio de Educación y Formación Profesional - *U.E. Next Generation*

Índice

1. INICIO

1.1 Introducción

El profundo cambio que ha supuesto Internet ha producido diversas transformaciones en nuestra sociedad, pero también en nuestra forma de comunicarnos, relacionarnos y trabajar. Para aprovechar todas las ventajas también debemos ser conscientes de los riesgos.

En la anterior unidad didáctica, Marta aprendió que en la web existen muchas amenazas, al igual que en el mundo real, como el acoso, las extorsiones o las estafas. Gracias a sus nuevos conocimientos, ha comprendido que **es necesario desenvolverse con precaución cada vez que se interactúa en línea.** Además, ha comprendido que es preciso asegurarse de no brindar toda la confianza a personas o entidades que no se conocen y a prestar mucha atención para no ser víctima de engaños y fraudes.

Y es que la tecnología ha cambiado profundamente la forma en la que nos relacionamos y ha dado lugar a nuevas formas de interactuar con nuestras amistades, compañeros y compañeras de trabajo, familia y pareja. También ha cambiado la forma en la que nos relacionamos con las empresas y organizaciones, cuando somos clientes o utilizamos sus servicios.

A lo largo de esta nueva unidad, Marta descubrirá algunos riesgos concretos como la suplantación de identidad, la extorsión y filtración de imágenes privadas a raíz del ***sexting*** y el ***grooming***. También revisará cómo funciona la tecnología para el desarrollo de fraudes y las campañas de ***phishing***. ¿Nos acompañas?

¿Qué vas a aprender en esta unidad?

OBJETIVO GENERAL DE LA ACCIÓN FORMATIVA

- Proteger la información y datos personales; proteger la identidad digital, de los contenidos digitales y de las aplicaciones informáticas; conocer las medidas de seguridad, así como el uso responsable y seguro de la información digital.

OBJETIVOS ESPECÍFICOS DE LA UNIDAD DIDÁCTICA

- Identificar formas de proteger dispositivos y contenidos digitales, diferenciando riesgos y amenazas en entornos digitales.
- Conocer medidas de seguridad y protección, identificando formas de asegurar la fiabilidad y la privacidad.
- Identificar cómo compartir información personal identificativa sin exponerse a uno mismo ni a terceros a riesgos.
- Conocer las políticas de privacidad sobre cómo se trata la información personal que se utiliza en servicios digitales.

2. VENTAJAS Y RIESGOS EN UN MUNDO INTERCONECTADO

2.1 Interacción en el mundo digital

A lo largo de las últimas décadas nuestra sociedad ha cambiado de una forma notable debido a la tecnología.

El uso de Internet y de las nuevas formas de comunicarnos han hecho que se transformen cuestiones tan esenciales como nuestro mercado laboral, la forma de acceder a la información, nuestras posibilidades para compartir ideas y, sobre todo, nuestra manera de comunicarnos e interactuar con otras personas.

- **Cambio en las relaciones humanas**

Las relaciones personales se han transformado de una manera evidente. Podemos comunicarnos tanto de forma personal como en grupo inmediatamente, llegando a miles de personas en un instante.

Pero el lenguaje también puede provocar numerosos malentendidos y desencuentros. Las redes sociales son una herramienta práctica para compartir información, de la misma manera que se pueden convertir en espacios de conflicto, por lo que es necesario que se usen atendiendo a una cierta **ética digital**.

- **Cambio en las relaciones laborales**

De la misma forma que se ha producido un gran cambio en la economía, también se han transformado de forma decisiva las acciones que desempeñamos en nuestros trabajos.

Hoy en día es común que un gran número de profesionales pueden trabajar desde casa, que las reuniones se hagan por videoconferencia y que se compartan documentos de

todo tipo para trabajar continuamente en tiempo real desde diferentes ubicaciones. Esto, evidentemente, ha implicado **la adquisición de toda una serie de competencias.**

- **Adquisición de nuevas habilidades y competencias digitales**

Compartir un documento y trabajarlo de forma simultánea requiere algo más que saber utilizar una aplicación.

Es necesario saber **trabajar en equipo, compartir los datos con responsabilidad y comportarse con educación ante comentarios y correcciones.** Las habilidades que vayas adquiriendo en ambos ámbitos, te permitirá reforzar tus competencias digitales.

- **Importancia de la seguridad**

Además, debemos **tener cuidado con la seguridad de los datos que manejamos,** seleccionando adecuadamente los entornos y las personas con las que los compartimos.

La pandemia del COVID - 19 ha provocado que todos estos cambios se aceleren. Marta, por ejemplo, no había teletrabajado hasta que empezó el confinamiento y tampoco realizaba videollamadas. Ahora, sin embargo, ¡maneja estas herramientas con soltura!

Esta revolución digital que estamos viviendo nos ha abierto un mundo de posibilidades, pero también ha venido acompañada de diversos peligros.

2.2 RGPD y políticas de privacidad

En 2016 se aprobó el RGPD (Reglamento General de Protección de Datos) para regular el derecho a la protección de los datos personales de las personas físicas y para que estos puedan circular de forma libre y segura.

Hace algunos años, cuando introducías tus datos, como tu nombre, tu edad o tu número de teléfono, en una página de Internet, la empresa en cuestión podía utilizarlos como quisiera, e incluso cederlos a otras. A medida que los productos y servicios digitales han ido evolucionando, también se iba haciendo patente la necesidad de crear **mecanismos de control que aseguraran la privacidad** de nuestros datos personales.

El **RGPD**, o Reglamento General de Protección de Datos es un reglamento europeo cuya finalidad es conseguir una **homogeneidad en el tratamiento de los datos privados** tanto dentro de los organismos públicos pero, sobre todo, en los privados. El RGDP hace posible que solo sean guardados los datos estrictamente necesarios para la finalidad legítima del tratamiento, evitando que estos sean conservados de manera indefinida o cedidos a terceros.

En España está en vigor desde 2021 la Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que establece el marco legislativo para la protección de datos personales.

¿Y qué son las políticas de privacidad?

Cuando visitas un sitio web, accedes a una tienda online o descargas una app, es normal que tengas que aceptar una serie de condiciones, entre ellas, lo que conocemos como **política de privacidad**.

Este tipo de políticas **deben manifestar qué datos van a recibir las empresas, cómo los van a almacenar y si van a ser compartidos** con terceros. De esta manera, podremos ser conscientes de cuáles de nuestros datos se están usando y para qué.

Una política de privacidad es un documento legal que expresa cómo utilizan nuestros datos las empresas. Suele ser usado en webs que requieren crear una cuenta.

¿Cómo se trata mi información personal?

Tradicionalmente, la protección de datos se relacionaba con enormes ficheros en los que se guardan grandes cantidades de datos. En la actualidad, se reconoce el tratamiento de datos personales como **cualquier operación** que se realiza sobre ellos, ya sea de manera manual o automática, y dentro o fuera de Internet.

Existen diferentes maneras de la que pueden ser tratados nuestros datos, y son las siguientes:

- **Recogida:** Se produce cuando se recogen datos, independientemente de que después sean usados o no, se puede llevar a cabo a través de correo electrónico, cumplimentación de impresos, apps, etc.

- **Registro:** Ocurre cuando se realiza algún tipo de registro de nuestros datos, como por ejemplo, con la grabación de una cámara de seguridad.

- **Organización y estructuración de la información:** Se trata de la clasificación de datos, normalmente con el fin de crear perfiles de usuarios.

- **Conservación de los datos:** Se refiere a la conservación de los datos en el tiempo y sobre cualquier formato de conservación, digital o físico.

- **Modificación o adaptación**: Se trata de modificar o adaptar los datos que ya se han registrado, como un cambio de domicilio o de compañía telefónica.

- **Extracción o consulta:** Se trata de la búsqueda de datos personales en bases de datos, redes sociales u otras plataformas.

- **Utilización:** Se da cuando, por ejemplo, enviamos un mail o imprimimos un documento que contiene datos de otra persona.

- **Comunicación, difusión o habilitación de acceso:** Esto ocurre cuando se comparten los datos de otra persona, por ejemplo, subiendo una foto de alguien a una red social o cuando damos permiso de acceso un documento en línea.

- **Cotejo o interconexión con otras administraciones:** Se produce cundo nos relacionamos con la Administración para cotejar o verificar datos.

- **Supresión o destrucción de datos:** La destrucción de soportes físicos o digitales, como un USB, también supone tratamiento de datos.

Derechos del las ciudadanas y ciudadanos

Para luchar contra el mal uso de nuestros datos por parte de terceros, las ciudadanas y ciudadanos cuentan con una serie de derechos sobre sus datos personales.

- **Derecho a la información.** Permite que el usuario o usuaria sepa si un organismo público o empresa posee sus datos, cómo los obtuvo y qué es lo que hace con ellos.

- **Derecho de acceso**. Si una organización gubernamental o empresa posee datos tuyos, tienes el derecho de solicitar el acceso a los mismos.

- **Derecho de rectificación, actualización o supresión.** Es el derecho de rectificar, actualizar o eliminar tu información de la base de datos que los contiene. Por ejemplo, que nuestro nombre no aparezca en listados de deudores si ya se ha pagado la deuda o que no figure en listados de empresas de publicidad si no lo hemos solicitado de manera expresa.

- **Derecho a que las decisiones que nos afectan sean tomadas por personas.** Por ejemplo, que cuando solicitamos un crédito a un banco, la decisión no dependa solo del resultado de un programa informático, sino que intervenga una persona en la valoración.

- **Consentimiento.** Cualquier empresa debe solicitar tu consentimiento a la hora de utilizar tus datos personales, y debe hacerlo de manera escrita u otros sistemas similares.

- **Datos sensibles.** Se consideran datos sensibles aquellos que revelan tu etnia, fe religiosa, salud, orientación sexual, afiliación sindical, etc., los cuales están protegidos y blindados con el fin de que nadie acceda a ellos.

2.3 Riesgos en entornos digitales

Marta ha estado reflexionando sobre cómo algunos de sus hábitos han cambiado a raíz de la digitalización. Y es que, hace ya mucho tiempo, que en lugar de cartas escribe y recibe mails, se comunica de forma pública a través de redes sociales, comparte documentos de forma *online* con sus compañeros, etc.

Marta nunca se había planteado que esas inofensivas acciones que realiza en Internet pueden ser susceptibles de diversos peligros. Acompáñala en su formación y descubre a qué riesgos te expones cada día al usar tus servicios digitales favoritos.

Principales riesgos en redes sociales

Las redes sociales nos permiten estar conectados, expresarnos, compartir contenidos... pero también entrañan ciertos riesgos. Estos son algunos de ellos:

- **Acceso a las apps de nuestros dispositivos**

Uno de los problemas más presentes en las redes sociales es el hecho de autorizar el acceso a ciertas aplicaciones, como la galería de imágenes o a la cámara de fotos, ya que podrían acceder a tu información personal y utilizarla sin que lo sepas.

- **Compartir demasiada información personal**

Muchas redes sociales permiten que mostremos nuestro nombre completo, sexo, teléfono... En las redes sociales se publican y es posible que los exploten terceros en su beneficio, por lo que es necesario que reflexiones muy bien sobre qué datos quieres compartir en tus redes.

- **Caer en trampas y ataques cibernéticos**

Existen distintos tipos de estafas digitales derivadas de ciberataques con *malware*, que también son posibles a través de las redes sociales.

- **Cambios en los permisos de privacidad**

En ocasiones, las redes sociales pueden cambiar sus permisos y privacidad, incluso de forma radical, por lo que hay que estar atentos a estos cambios.

- **Los bots en redes sociales**

Los bots son robots capaces de suplantar las acciones que pueden realizar las personas en las redes sociales. De esta manera, pueden hacerse pasar por una empresa o incluso por alguien que conoces.

Principales riesgos en páginas web

Algunos de los riesgos comunes derivados del uso de páginas web son los siguientes:

- **Secuestro de clics**

Es un ataque que se basa en que el usuario o usuaria haga clic en diferentes botones o enlaces de una web, lo que permite que realicemos ciertas acciones sin ser realmente

conscientes sobre ello. Pulsando sobre estos enlaces o botones, lo que hacemos es facilitar que un delincuente controle nuestro PC o redireccionarnos a web fraudulentas.

- **Ataque de inyección SQL**

Se trata de un tipo de ataque al *software* de una página web para, después, poder acceder a los datos de las personas que la usan.

- **Abrir una web que lleva a un lugar malicioso**

Cuando vas a entrar en una web, el sistema te redirecciona automáticamente a otro. Esto puede ser muy peligroso, ya que es la manera de la que funciona el ***phishing.***

Principales riesgos en gestores de correo electrónico

Algunos de los riesgos más comunes derivados de utilizar un servicio de correo electrónico son los siguientes:

- **Ataques Phishing**

A pesar de los múltiples filtros de seguridad, cabe la posibilidad de sufrir una suplantación de identidad a través del correo electrónico. Este tipo de ataque suele realizarse a través de correo electrónico. Normalmente en ese mail, se intenta suplantar a un organismo público o empresa y nos invita a facilitar una serie de datos. Recuerda que ninguna entidad pública o empresa te va a pedir, mediante correo electrónico, que les facilites datos sensibles que puedan afectar a tu seguridad

- **Publicidad engañosa**

Se tratan de aquellos mails que recibimos y que contienen publicidad engañosa o abusiva, y que no solo resulta molesta, sino que además puede suponer una puerta de entrada a los controles de nuestro ordenador.

- **Búsqueda de información y datos**

Se pueden recibir correos en los que te solicitan rellenar algún tipo de dato o información que parece inofensiva, pero que realmente es una información que se busca de manera intencionada.

- **Archivos maliciosos**

Una vez más, no podemos olvidar de los diferentes archivos maliciosos que pueden ser incluidos, de manera visible o no, en un correo electrónico.

Principales riesgos al descargar y compartir archivos

Compartir archivos a través de plataformas como OneDrive o Drive de Google lleva asociados los siguientes riesgos:

- **Fallos humanos**

La facilidad con la que compartimos documentos hace posible que se produzcan fallos humanos y que nuestros documentos terminen siendo compartidos con la persona equivocada.

- **Riesgos externos**

Como en el resto de casos que hemos visto, las plataformas para compartir documentos pueden ser atacadas por ciberdelincuentes.

2.4 Medidas de seguridad y protección

Marta es consciente de la necesidad de tomar medidas de seguridad y protección a la hora de navegar por Internet o al utilizar algunos de sus servicios. Como ella misma diría: "no hay mejor protección que una buena prevención". Por ello, a continuación, se profundizará en algunas medidas de seguridad que debemos tomar dentro de la "red de redes".

Muchos de los riesgos de seguridad en nuestra vida digital están motivados por las actuaciones de usuarios y usuarias.

Estas actuaciones están íntimamente relacionadas con el uso de Internet, la manera en la que utilizamos el correo electrónico, las redes sociales y las comunicaciones por videoconferencia. Para asegurarnos de hacer un buen uso de nuestros teléfonos, ordenadores y tabletas digitales, es recomendable seguir una serie de pautas. Son las siguientes:

- **Actualización de software**

Una de las primeras recomendaciones esenciales es mantener el **software de nuestros dispositivos actualizados.**

Es particularmente importante el sistema operativo, ya que es el software más importante del mismo, sobre el que funcionan el resto de las aplicaciones.

También es esencial tener actualizado el navegador, el gestor de correo electrónico o el lector de PDF.

Teniendo en cuenta que cualquier aplicación que usemos puede tener un fallo de seguridad, siempre se recomienda tener activadas las actualizaciones automáticas, lo que nos permitirá mejorar la estabilidad de nuestros dispositivos.

- **Evitar tener numerosas cuentas**

El hecho de que los ordenadores puedan ser utilizados por un gran número de personas hace que las preferencias de seguridad de los navegadores, de los programas y del correo electrónico sean muy diversas.

En un mismo sistema podemos tener **usuarios o usuarias que actúan correctamente** siguiendo las pautas de seguridad y **otros u otras que pongan en**

peligro al resto. Por eso, conviene limitar el número de personas con accesos diversos al equipo y consensuar el uso que va a hacerse del mismo.

- **Copias de seguridad**

Es esencial realizar **copias de seguridad** de nuestro sistema, ya que podemos perder nuestros datos por causas muy diversas, desde fallos físicos del disco duro hasta ataques donde se produce la eliminación de los datos o el "secuestro" de los mismos.

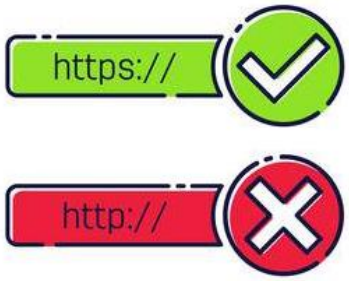
Es conveniente que la copia se realice en un **disco duro externo que encripte los datos,** de manera que no pueda leerse la información si no se tiene una clave elegida por el usuario o la usuaria.

- **Gestión de contraseñas**

Tanto las contraseñas de los dispositivos como las de las claves wifi se deben cambiar periódicamente para evitar que personas no autorizadas puedan conectarse a la red.

¿Visitamos páginas web seguras?
La manera más importante de establecer la seguridad en el uso de Internet es visitar páginas web seguras. El protocolo HTTPS nos va a permitir detectar la naturaleza de dichas páginas.

En la barra de navegación se encuentran las direcciones de las webs que visitamos. Delante de las direcciones veremos los caracteres "http" o "https". Son protocolos diferentes: en el primero de ellos los datos que viajan no están cifrados. En el segundo, que a veces no aparece directamente, sí que lo están.



Cuando decimos que una web está cifrada, significa que la información está protegida de manera que no cualquier persona puede acceder a ella.

HTTP son las siglas de *Hypertext Transfer Protocol* (protocolo de transferencia de hipertexto). HTTPS son las siglas de *Hypertext Transfer Protocol Secure* (protocolo de transferencia de hipertexto seguro). Los datos que se transmiten con este protocolo viajan encriptados, por lo que, si son interceptados, no podrán ser leídos.

Hay diversos tipos de ataque que se encargan de interceptar las “conversaciones” que tienen nuestros ordenadores. Por ejemplo, si la app de tu banco te solicita una contraseña, esta información que viaja del ordenador a la plataforma puede ser interceptada.

El hecho de que una página web sea segura y utilice el protocolo HTTPS viene respaldado por un certificado de seguridad.

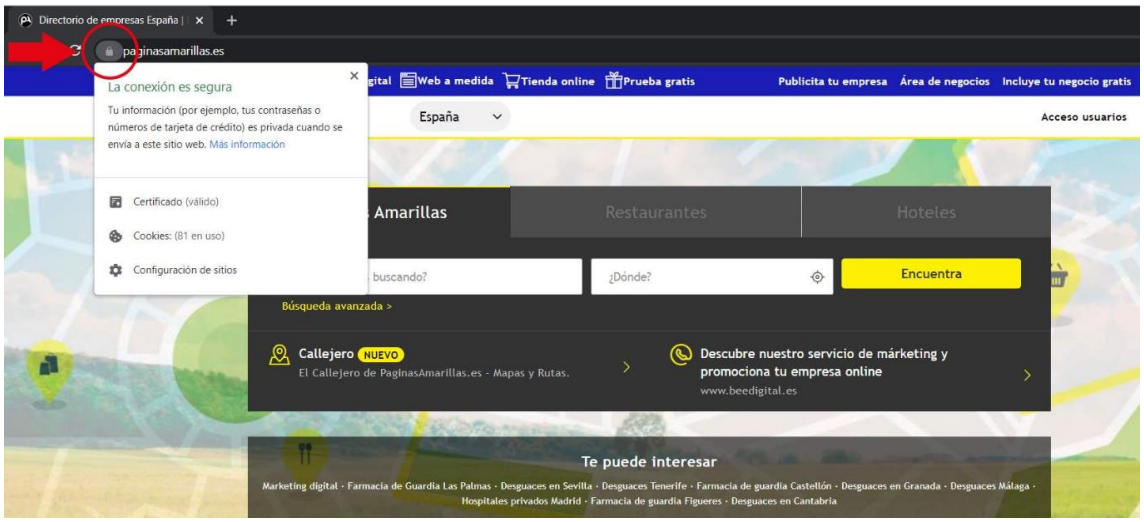
¿Cómo se puede comprobar el certificado de seguridad de una web?

Un **certificado de seguridad** es una medida de seguridad adicional que las páginas web pueden utilizar, y que garantiza que la información a la que acceden los usuarios y usuarias está cifrada.

En algunas ocasiones, para lograr la máxima impresión de veracidad cuando se produce un ataque de *phishing*, la página web es una copia exacta de la página de la empresa y, además, tiene una dirección HTTPS.

Si se dan todos estos casos y aun así se observa algo sospechoso, **es muy conveniente comprobar el certificado.**

Para hacerlo, simplemente hay que **pulsar sobre el candado** que se encuentra en la barra de navegación e inmediatamente se podrá confirmar quién es el dueño o la dueña del certificado.



Si un certificado no pertenece a la compañía de la que dice ser, estaremos ante un caso de estafa.

2.5 Suplantación de identidad

La suplantación de identidad se produce cuando una persona se apropia de la identidad digital de otra. Este tipo de acciones pueden ser llevadas a cabo por una persona o por una organización delictiva.

En una suplantación de identidad, el o la ciberdelincuente puede tener acceso a datos sensibles (particularmente fotografías o vídeos) **y desprestigiar a otra persona** publicando comentarios denigrantes utilizando sus perfiles en diferentes redes sociales.

Estas acciones se pueden llevar a cabo cuando se ha accedido, de forma ilícita, a una o varias cuentas ya creadas. También existe la posibilidad de que se cree **una cuenta nueva haciéndose pasar por otra persona.**

Este tipo de acciones suelen ser habituales en las cuentas de personas famosas y celebridades, aunque cada vez es más común encontrar este tipo de casos en las cuentas de cualquier usuaria y usuario, normalmente con el fin de desprestigiar.

Recientemente, saltó a los medios de comunicación una nueva oleada de casos de suplantación de identidad en la red social Instagram.
Un cierto número de delincuentes logró acceder a los perfiles de usuarios y usuarias que tienen sus cuentas abiertas y sin restricciones de acceso para robar sus fotografías y vídeos personales.
Con esta información, crean un nuevo perfil falso con el que suplantan a la víctima para estafar a sus contactos.

¿Cómo lo hacen?

Marta ha quedado profundamente impactada al descubrir que cualquier persona es susceptible de ser suplantada en Internet, pero... ¿Cómo se realizarán este tipo de ataques exactamente?

- **Usará un nombre similar con alguna pequeña variación difícil de percibir** Puede ser un pequeño cambio en una letra o símbolo.
- **Tendrá la misma foto de perfil**
- **Incluirá algunas de las últimas publicaciones de la cuenta clonada**
- **Intentarán volver a conectar con los seguidores de la cuenta original**

Marta ha recibido una petición de amistad de un contacto que ya tiene agregado en Facebook. En estos casos es recomendable comprobar por otros medios, como por ejemplo el teléfono o por Whatsapp, si esa persona realmente ha cambiado de cuenta o si se trata de un engaño.

La suplantación de identidad puede tener un objetivo delictivo cuando se suplanta a una persona para generar engaños y estafas.

Las redes sociales están cargadas de información. Por esta razón es fundamental seguir las recomendaciones de seguridad.

¿Cómo puedo protegerme?

Figuras políticas, cantantes, actores y actrices, *influencers*, deportistas, modelos son víctimas frecuentes de estas estafas. Pero también pueden serlo las empresas e incluso tú. Nadie está a salvo de sufrir una suplantación de identidad en el mundo digital.

Desde hace años, Facebook se encuentra a la cabeza del ranking de aplicaciones más utilizadas a nivel mundial, llegando a superar los dos mil millones de personas usuarias. Una red tan grande, en la que es relativamente sencillo acceder a la información de los usuarios y usuarias, resulta un foco perfecto a la hora de realizar ataques de suplantación de identidad.

Por suerte, cuentas con una serie de opciones y buenas prácticas que te ayudarán a protegerte de este tipo de ataques.

- **Minimizar la exposición de nuestros datos personales:** las redes sociales tienen opciones de configuración donde podemos elegir cuáles de nuestros datos son mostrados de modo público y cuáles compartimos en privado. Difundir la menor cantidad de datos posibles ayudará a que haya menos herramientas disponibles para suplantar nuestra identidad.

- **Iniciar sesión en las redes desde dispositivos y redes seguros:** es importante que el equipo que utilizamos esté actualizado y cuente con una protección antivirus, así como la conexión esté protegida y no se trate de una red abierta o pública.

- **Proteger la cuenta:** las propias redes suelen establecer los criterios mínimos de seguridad y evaluar la fortaleza de las contraseñas, de todos modos, hay que intentar hacerlas lo más complejas de descifrar. A su vez, con métodos como la doble autenticación, se puede tener más seguridad de que ninguna otra persona la esté utilizando.

- **Eliminar las cuentas inactivas:** dejar perfiles que ya no utilicemos abiertos pueden generar una brecha de seguridad y que la información que habíamos colocado allí sea recuperada y utilizada en una suplantación de identidad. Por ello, siempre que deje de utilizarse una cuenta es conveniente cerrarla (luego de haber hecho una copia de seguridad en caso de que hubiese contenidos que se deseara conservar).

¡Recuerda!

La mayoría de redes sociales permiten aplicar estas acciones y recomendaciones con el fin de protegerte de ataques de suplantación de identidad.

2.6 "Grooming" y riesgos del "sexting"

Según datos de 2018, aproximadamente un 35% de adolescentes en España han recibido mensajes de tipo erótico o extorsiones eróticas, a través de mensajería instantánea o por redes sociales.

El ***grooming*** es un tipo de ciberacoso que es llevado a cabo por una persona adulta sobre un menor de edad y que puede derivar en un abuso sexual.

Las técnicas más habituales implican **convencer a la o el menor para que faciliten imágenes pornográficas**, estableciéndose una fase de búsqueda de confianza.

Posteriormente, dichas imágenes pueden ser utilizadas para **extorsionar y amenazar** a la o el menor, pidiéndole cada vez más imágenes con la amenaza de difundirlas en caso de que no siga facilitándolas. Estas acciones pueden derivar también en que la persona abusadora intente concertar una cita con el o la menor utilizando las mismas estrategias.

¿Cómo actuar frente a un caso de grooming?

La **comunicación con las y los menores**, sobre temáticas como los riesgos de Internet o las páginas que visitan, es esencial para que confíen en contar sus problemas a las personas de círculos cercanos. Junto a la **educación afectivo-sexual,** constituye el mejor mecanismo de prevención para evitar esta amenaza.

Establecer una buena comunicación también será útil en caso de que no se haya podido evitar el *grooming*, e incluso ayudará a detectarlo: cambios en el estado de ánimo, en el rendimiento escolar, su relación con otras personas o sus pasatiempos son algunos de los indicadores de que puede estar ocurriendo una situación de *grooming*. Para afrontar esta situación, es recomendable:

- **Brindar apoyo y contención a la víctima**, evitando generar un sentimiento de culpa o vergüenza.
- **Reunir toda la información posible** sobre la persona que ha cometido el acoso (conversaciones, imágenes, vídeos) y realizar una denuncia ante las autoridades.
- **No es aconsejable enfrentarse** al acosador o la acosadora, ni tampoco denunciar su cuenta de modo público, dado que podría cerrar su cuenta o bloquearla, haciendo más difícil su localización. A su vez, es importante pensar que, desde otra cuenta, esta persona podría seguir acosando a otras víctimas.
- También es importante **cambiar las claves de las redes sociales** en caso de que el acosador o la acosadora hubiera conseguido acceso, revisar los ajustes

de privacidad y dialogar con el o la menor para que no confíe en personas desconocidas.

Debemos estar muy pendientes como sociedad para evitar el *grooming* y tomar medidas preventivas y educativas, así como saber cómo actuar ante un caso de este tipo.

El ***sexting*** se puede definir a grandes rasgos como el envío de textos, imágenes o vídeos con contenido erótico personal.

Imagina la siguiente situación...

Sara y Juan se conocieron recientemente mientras pasaban las vacaciones en Bilbao. Enseguida conectaron y pasaron las mejores semanas de sus vidas. Se habían enamorado, pero las vacaciones llegaron a su fin.

Sara volvió a Madrid y Juan a Barcelona. Ambos continuaron con sus rutinas y trabajos, aunque siempre se hacían algunos minutos para conversar. Estaban muy felices de que la tecnología les permitiera mantenerse en contacto y cada día pasaban más tiempo frente al móvil. Un día, después de intercambiar muchos comentarios, Juan le pidió a Sara que le enviase alguna foto o vídeo íntimo.

Al principio a Sara le dio vergüenza la petición de realizar *sexting*, pero después de meditarlo, pensó que en el fondo no tenía nada de malo. Juan le parecía una buena persona y confiaba mucho en él. A partir de ese momento, empezaron a intercambiar fotos íntimas. Aún así, Sara siempre le pedía a Juan que después de verlas las borrase de su dispositivo.

Meses después, algo pasó. En una red social de alto contenido sexual aparecieron colgadas las fotografías de Sara. Alguien las había visto y reconocido a la joven. Sara estaba desesperada ya que muchas personas, incluso su familia y sus colegas del trabajo, podrían ver esas fotos. Muy decepcionada, la joven le pidió explicaciones a Juan, que sorprendido juraba que él no había sido quien publicó las imágenes. Sara no le creyó porque solo él las tenía.

Juan no entendía nada. Realmente él había custodiado las fotos. Sin embargo, recordó que unos días antes había conectado su móvil al ordenador de una librería para hacer algunas impresiones para el trabajo. Ese día también que se había conectado a una wifi gratuita para hablar con Sara, ya que no tenía datos en el teléfono. Era evidente que alguien había pirateado su teléfono y colgado las fotos en la página web. Juan ahora sabe dónde estuvo su error pero eso no soluciona que las imágenes sigan publicadas.

En la actualidad, muchas personas conocen a su pareja a través de webs y aplicaciones, mientras que otras utilizan la tecnología para mantener conversaciones y conductas privadas. En ocasiones, prácticas como el *sexting* se deben a una presión por parte de la pareja o la necesidad de impresionar o reforzar el autoestima, mientras que otras veces se hace por diversión.

En cualquier caso, siempre que compartas información privada o sensible a través de tus dispositivos, aunque sea con personas de confianza, debes ser consciente de que

no existe una garantía de que esa información no termine siendo filtrada o generando una situación de acoso.

Las consecuencias de la difusión pública de este tipo de contenidos pueden generar un **sentimiento de humillación** en la persona que aparece en las imágenes, así como **afectar su autoestima** derivada de la presión social. Esto, además, suele ir acompañado de un **sentimiento de indefensión** o incluso de culpa.

En ocasiones las personas comparten contenidos íntimos por llamar la atención, como prueba de afecto o como broma. El problema es que esas imágenes pueden ser usadas por otras personas para acosarla o extorsionarla, dando lugar a la sextorsión.

¿Qué hacer ante la sextorsión o la filtración de imágenes privadas?

En caso de ser víctima de extorsión o haber sufrido la exposición de fotografías o vídeos íntimos en Internet, la solución siempre se basa en almacenar las pruebas y dar aviso inmediato a las autoridades.

Resulta especialmente útil guardar **capturas de pantalla de conversaciones, fotografías, vídeos o cualquier dato** sobre la persona que realiza la amenaza o el sitio donde se han publicado las imágenes. Si las imágenes están colgadas en un sitio web, también se puede enviar una solicitud al mismo para que sean retiradas.

En caso de un chantaje, **no se debe pagar a quien realiza la extorsión**, dado que esto solo contribuye a potenciar las estafas y no da garantía de que las imágenes no terminen publicándose de todos modos. En conclusión, siempre es mejor **mantener la calma y realizar una denuncia**, así como procurar adoptar los cuidados para que este tipo de situaciones no vuelvan a repetirse.

Muchas personas, especialmente adolescentes, comparten información, datos e imágenes de forma poco premeditada. Debemos ser conscientes de la importancia que tienen nuestros actos, así como poner límites éticos al uso de las redes.

Un caso de sexting mediático

En 2012, la exconcejala Olvido Hormigos saltó a las noticias por ser víctima de la difusión de un vídeo íntimo que había enviado a un hombre que no era su marido. Este caso quedó impune, pero se convirtió en un punto de inflexión para poner el foco en los límites de la privacidad, el honor y la difusión de documentos de carácter personal íntimo.

La repercusión mediática fue fundamental para cambiar la ley ante este tipo de delitos, de modo que se pueden prevenir daños irreparables en la imagen de las víctimas e incluso en su salud mental que le lleven al suicidio ante la presión social y moral a la que se ven sometidas tras la difusión de estas fotografías, conversaciones o vídeos eróticos.

En 2015 se modificó el Código Penal considerando estos actos como **un delito atendiendo a la gravedad de difundir de manera no autorizada imágenes íntimas**, aun

si previamente se habían remitido dichas imágenes con el consentimiento de la persona afectada.

Aún así, **la modificación del Código-Penal no previno el suicidio de una trabajadora** de la empresa CNH Industrial Pegaso-Iveco en 2019, cuando un compañero de trabajo con quien tuvo una relación sentimental difundió un vídeo íntimo que rápidamente se propagó por la empresa. Estas situaciones de acoso se ven amplificadas no sólo con el uso de la tecnología, sino de cómo las personas hacen uso de ella ante una situación de vulnerabilidad de la intimidad.

2.7 Ingeniería social

La ingeniería social se beneficia de las informaciones personales que pueden conseguirse en las redes sociales, como los gustos o intereses, de manera que resulte sencillo ganarse la confianza de la víctima.

La **ingeniería social** se basa en predecir las conductas de las personas para obtener información o provocar que realice acciones concretas y se basa en los principios psicológicos relacionados con las técnicas clásicas de estafa.

El uso de estas técnicas psicológicas hace que el ser humano se convierta en el "eslabón débil" dentro del proceso de seguridad. Esta manipulación hace que, en algunos momentos, los ***crackers*** prefieran intentar lograr una clave a partir de varias llamadas que haciendo un ataque para conseguirla.

Técnicas para un ataque de ingeniería social

Existen, fundamentalmente, dos técnicas para un ataque de ingeniería social:

- **ATAQUE UTILIZANDO EL TELÉFONO**

  En este tipo de acciones, la persona que llama **puede hacerse pasar por personal técnico que pregunta una serie de datos necesarios para poder llevar a cabo una acción requerida por el usuario o la usuaria.** Entre esos datos pueden estar contraseñas o datos sensibles que la persona facilita sin preocuparse por la seguridad de esa información.

  Se debe recordar que, para hacer estas llamadas más realistas, **las pueden llevar a cabo en el momento más oportuno.** Si hemos solicitado información a nuestra compañía para algún cambio y en ese momento nos llama alguien haciéndose pasar por un técnico de dicha empresa, sería muy sencillo que se diera esa información sin mucho problema.

  Muchas actuaciones de ingeniería social se basan en datos que pueden obtener mediante el uso de un *software espía*.

- **ATAQUE UTILIZANDO INTERNET**

  Es la técnica favorita de los ciberdelincuentes para plantear **ataques a gran escala.**

  Para dar verosimilitud al ataque siempre se intenta obtener datos y mover las actuaciones por bloques de usuarios y usuarias para facilitar "información de enganche" que pueda interesar a las posibles víctimas.

  Se pueden utilizar el **correo electrónico,** las redes sociales o las aplicaciones de mensajería.

¿Qué pueden conseguir los ciberdelincuentes a través de un ataque de ingeniería social?

Si caes en estos ataques de ingeniería social, su responsable puede obtener acceso a mucha información. Entre la información que buscan los y las ciberdelincuentes y pueden obtener con este sistema, son los siguientes tipos:

- PIN o contraseñas.
- Acceso a cuentas de correo.
- Número de la seguridad social.
- Datos sanitarios.
- Acceso a cuentas de redes sociales.
- Cuentas o tarjetas bancarias.

Ciberdelincuencia en banca online

La banca online es uno de los objetivos de la ciberdelincuencia, y su clientela conforma una de las **víctimas más habituales de las acciones de ingeniería social**. A continuación te presentamos una situación habitual y algunas observaciones sobre seguridad que lanzan algunos bancos a sus clientes para evitar ser defraudados.

Imagina la siguiente situación...

Actualización de cuenta

Antonio es un hombre de unos 70 años que tiene pocos conocimientos sobre tecnología.

Hace unos días recibió en su móvil un mensaje de su banco conforme debía realizar una actualización de su cuenta a través de Internet. Como no es muy hábil con la informática, siguió los pasos del mensaje al pie de la letra para no equivocarse.

La llamada

Antonio recibe una llamada telefónica.

Al otro lado de la línea una voz masculina se hace pasar por un empleado de su banco.

Buenos días, Antonio. Soy Jorge Andrés. Le llamo desde su banco ya que necesitamos verificar con usted unos datos de su cuenta corriente. Hace unos días le remitimos un correo informando de la actualización de su cuenta. Para finalizar dicho proceso de nuestros sistemas de seguridad necesitamos realizar un cambio en sus claves de acceso. Por esta razón, es necesario que nos indique su usuario y contraseña actual para hacer la modificación y después le remitiremos por correo sus nuevas claves de acceso.

¿Podría indicarme su usuario y a continuación su contraseña?

¿Qué hacer ante esta situación?

Como te has dado cuenta, la llamada es sospechosa de ser una estafa, por lo que Antonio no debería continuar con la conversación. Lo más sensato es negarse a aportar esa información privada, abandonar la llamada e inmediatamente comunicarse con su banco para verificar si el trámite es real o fraudulento.

Recuerda

Si te vas a comunicar con tu banco para verificar una posible estafa o fraude, hazlo a través de los teléfonos oficiales que se pueden localizar en la web corporativa o bien en las Páginas Amarillas. A veces, quienes realizan la estafa nos envían un documento falsificado con opciones de contacto ficticias o bien nos dan un número de teléfono que nos conduce a su compinche.

Las entidades bancarias jamás te solicitarán tus claves secretas o enlaces a la web por teléfono o correo.

Consejos para evitar los ataques de ingeniería social

Pare evitar caer en estos ataques de ingeniería social conviene seguir estas recomendaciones:

- Evitar ofrecer cualquier tipo de información personal en espacios digitales públicos (redes, foros, web, entre otros).
- Ante cualquier duda con respecto a la persona que te está contactando, pedirle que se identifique claramente.
- Establecer pautas de trabajo en la organización que permitan automatizar unos buenos hábitos de control de datos.

Como ya viste en la anterior unidad, existen organizaciones como INICIBE y OSI que trabajan a diario para la ciudadanía pueda hacer un uso de Internet seguro y libre de riesgos.

2.8 "Phishing"

Marta no sale de su asombro en cuanto a la creatividad de los ciberdelincuentes a la hora de cometer sus acciones y cree que es de vital importancia seguir aprendiendo las diferentes técnicas que emplean para "pescarnos". Por eso, a continuación, aprenderá todo sobre uno de los ciberataques más peligrosos que existen en la actualidad: el *phishing.*

El término "phishing" viene del inglés “fishing” (pesca) y hace referencia a la acción de “pescar” usuarios a través de “anzuelos” con el fin de conseguir contraseñas o datos bancarios.

El ***phishing*** *es* una de las actividades delictivas más destacadas de la Red. Se extendió principalmente para obtener datos bancarios de usuarios y usuarias, pero en los últimos años se ha utilizado en numerosas ocasiones para obtener contraseñas de redes sociales y servicios web.

Su forma de operar consiste en hacer llegar a la víctima un correo o mensaje aparentemente fiable. Ese mensaje conduce a un enlace que abrirá una réplica exacta de la web a la que se pensaba acceder.

Al introducir el nombre de usuario o usuaria y la contraseña del servicio se recibe un mensaje informando de que se ha producido un error. En ese momento, el nombre de usuario o usuaria y la contraseña ya han sido capturados por los cibercriminales. Para que la víctima no sospeche nada, es redirigida de nuevo a la web real, donde introduce de nuevo el nombre de usuario y la contraseña. Como todo seguirá funcionando, la persona no realiza ningún cambio. Quienes cometen el crimen, se han hecho con el nombre de usuario y la contraseña y los podrán utilizar para fines delictivos.

Un ejemplo de phishing es la técnica por la cual ciberdelincuentes se hacen pasar por una compañía que haya sido contratada por el usuario o la usuaria, con el fin de obtener datos bancarios o datos sensibles. Para hacerse pasar por esa compañía, necesitan saber que esa persona tiene, en efecto, un contrato con la misma o utiliza sus servicios.

Técnicas y recursos relacionados con el phishing

ROGUES: FALSOS ANTIVIRUS

Estos programas **generan una gran cantidad de alarmas sobre virus** informáticos en el sistema y, posteriormente, **ofrecen la solución dando la opción de descargar un antivirus gratuito**.

El método de estafa consiste en la proposición de la **descarga del antivirus de pago**, a través de páginas poco seguras **donde se pueden hacer con tus datos**.

Evidentemente, el antivirus, su búsqueda y la eliminación de los virus no han sido reales, sino datos completamente falsos.

ORDENADORES ZOMBIE

Es posible infectar una serie de ordenadores de manera que los usuarios o usuarias no sepan que están siendo utilizados para otros fines. La infección se puede desarrollar por webs falsas o correos electrónicos, y provoca que se instale un programa sin que el usuario o usuaria se percate.

Este programa se utiliza para el envío masivo de *spam* (desde el correo electrónico de la víctima) para obtener datos y credenciales en redes o, incluso, para perpetrar ciberataques.

En este caso, la víctima no sabe que le está pasando algo en su ordenador, por lo que es difícil de detectar si no usamos antivirus.

En caso de que se produzca un ataque, la **IP** del usuario o usuaria quedará registrada, por lo que tendrá que demostrar que su participación involuntaria se ha debido a una infección.

¿Cómo puedo saber si mi dispositivo está infectado?

Identificar algunas de las siguientes **anomalías en tus dispositivos** puede ser un indicador de que el dispositivo está infectado.

Mal funcionamiento

El equipo no se está comportando normalmente. Por ejemplo, se abren ventanas, o se cierran programas, entre otros.

Reinicio

El dispositivo se reinicia constantemente sin motivo aparente.

Cambios en sistema

Notas cambios en el sistema operativo, como menús que aparecen de forma diferente, disco duro con más actividad de lo normal, entre otras posibles situaciones.

Exceso de publicaciones

Hay exceso de publicidades que saltan en cualquier momento, principalmente con temática erótica.

Dispositivo lento

Notas que tu dispositivo está funcionando más lento de lo habitual.

Ventanas

Se abren sitios web sin que lo hayas solicitado.

¿Y qué debo hacer en caso de infección?

En estos casos debes **dejar de usar el dispositivo** cuanto antes **y proceder a su limpieza.** Tienes que **desconectar el dispositivo de Internet y eliminar los certificados**

digitales instalados, hacer una **copia de seguridad** de todo lo necesario y asegurarte de que esos **datos no están infectados usando un antivirus.**

También es conveniente restaurar el equipo a los **valores de fábrica**, si es posible, para devolver a la normalidad cualquier cambio en las preferencias que se haya llevado a cabo sin nuestro permiso.

2.9 Bulos o "fake news"

Siempre ha existido y se ha distribuido información falsa, pero la rapidez que ahora mismo otorgan las redes sociales hace que su impacto pueda ser enorme en pocas horas.

Debido a la velocidad y a la gran cantidad de información que circula por Internet, el peligro de las ***fake news***, traducido en español como **noticias falsas o bulos**, se ha vuelto preocupante en los últimos tiempos.

El objetivo de estos bulos no es otro que **desestabilizar, generar dudas y confusión** sobre una situación, una organización, una persona o incluso sobre una causa. Las formas más normales de difusión son el **correo electrónico, las redes sociales y las aplicaciones de mensajería instantánea**, como Whatsapp.

Cuando un bulo consigue extenderse, debido a la difusión por parte de un gran número de personas, se dice que se ha hecho viral. En un principio, las populares cadenas de correos electrónicos permitían hacer un seguimiento de las personas que habían realizado los reenvíos. Sin embargo, con las redes sociales, la difusión que llegan a tener algunos bulos llega a ser enorme.

La circulación de bulos a través de servicios como *Whatsapp* es bastante complicada de controlar ya que, en muchos casos, las personas reenvían el mensaje sin comprobar la veracidad del mismo.

Fake news y manipulación

Los bulos suponen un tema particularmente preocupante, ya que atentan contra la veracidad de los datos y pueden tener una **gran influencia** en las opiniones.

A este respecto, las redes sociales han tenido que adoptar, en varias ocasiones, **medidas contundentes** para parar algunos bulos que se estaban difundiendo por las mismas. Influir en referéndums, en elecciones o en la bolsa puede tener una importancia muy grande. Por ello, hay que tratar de garantizar la veracidad de las informaciones y considerar la amenaza de los bulos muy en serio.

El alcance de los bulos es tan grande que se ha comprobado que, incluso una vez que el bulo había sido descubierto y se publica su falsedad, el daño nunca llega a repararse.

Ejemplo de bulo relacionado con la Covid19

A raíz de la pandemia de la Covid19 las redes sociales experimentaron una avalancha de bulos y *fake news*. El miedo, la incertidumbre y la desinformación fueron el caldo de cultivo para esas noticias e informaciones tuvieran el efecto deseado.

En algunos casos, se produjo por el desconocimiento de la nueva enfermedad. Pero, en otros, tenían una clara orientación para desestabilizar a la sociedad, generar confusión e incluso provocar fraudes.

En este caso, con una acción de ingeniería social, se suplantó la identidad del Ministerio de Sanidad y se remitió por mensajería instantánea unas supuestas recomendaciones para luchar contra el virus y un **enlace con una estafa de venta de mascarillas**.

La Guardia Civil informó a la comunidad a través de las redes sociales del bulo para que las personas no cayesen en el engaño.

Para evitar la difusión de bulos hay que desconfiar de cualquier mensaje que solicite su reenvío o que haga declaraciones categóricas.

En la red también hay lugares donde informarse sobre la veracidad de las noticias que nos llegan. Muchas de ellas se investigan por páginas como Maldito Bulo, Newtral o VerificaRTVE. También en la Oficina de Seguridad del Internauta, tienes información sobre fraudes y bulos. Mira el apartado de referencias bibliográficas para acceder a estas páginas.

Hay que observar los detalles del mensaje: si no existe una referencia concreta y la información que ha llegado es anónima, debería evitarse su difusión.

2.10 La evolución del "ransomware"

A lo largo de su formación, Marta ha aprendido todo sobes los *malware*, los *spyware*, los *adware*... Pero aún le queda por descubrir a uno de los *"ware"* más molestos a los que se pueden enfrentar: el *rasomware*. Y es que este tipo de *software* malicioso es una de las ciberamenazas que más se han extendido en los últimos años.

Cuando hablamos de ***rasomware***, nos referimos a un tipo de *malware* que **impide a las usuarias y usuarios acceder a sus dispositivos o archivos** a menos que se realice un pago a modo de "rescate". Por lo general, estos pagos suelen realizarse a través de criptomonedas, como el Bitcoin, dificultando el seguimiento de las acciones ejecutadas por los ciberdelincuentes.

Previamente a las criptomonedas, los pagos se debían hacer a través de otros métodos (SMS incluidos), lo que dificultaba que el o la ciberdelincuente recibiera la cantidad económica. Los avances tecnológicos relacionados con las criptomonedas y el cifrado nos han traído, por desgracia, también este problema.

La aparición de las criptomonedas ha permitido que se puedan realizar pagos de forma segura y sin seguimiento por parte de las autoridades. De esta manera, han

provocado que los y las ciberdelincuentes gocen de un método mucho más seguro para recibir los rescates.

Pautas para evitar ataques de rasomware

Para la máxima seguridad deberíamos cumplir con algunas buenas prácticas.

Copias de seguridad

Las copias de seguridad deberían ser frecuentes si queremos mantener nuestra información respaldada.

Si hay datos especialmente importantes, convendría tenerlos en otro disco duro o memoria USB que no se conectara con tanta frecuencia al equipo habitual. Esto permitirá tener una segunda copia de los datos más sensibles, por si acaso el disco duro de copias de seguridad más usado se viera comprometido.

Actualizaciones

Es fundamental actualizar el sistema operativo y los programas para evitar que los ciberdelincuentes puedan aprovechar los fallos de seguridad por tener un sistema operativo antiguo.

Descargas

Se debe revisar atentamente los sitios web desde donde se vaya a descargar un programa o archivo. Lo más conveniente es comprobar que la URL corresponde a un sitio reconocido, que la web usa protocolo HTTPS y que el certificado de seguridad de la web es correcto.

Correo electrónico

Revisar con cuidado cualquier archivo que provenga de un correo electrónico, especialmente si se trata de alguien desconocido. Es muy recomendable que se revise con un software antimalware todo el correo electrónico.

Red

Ante cualquier proceso extraño es importante desconectar inmediatamente el dispositivo de la Red.

Si sufres un ataque de *ransomware* y tienes una copia de seguridad solamente debes formatear el disco duro y, a continuación, volver a recuperar la información desde tu copia.

3. CIERRE

3.1 Resumen

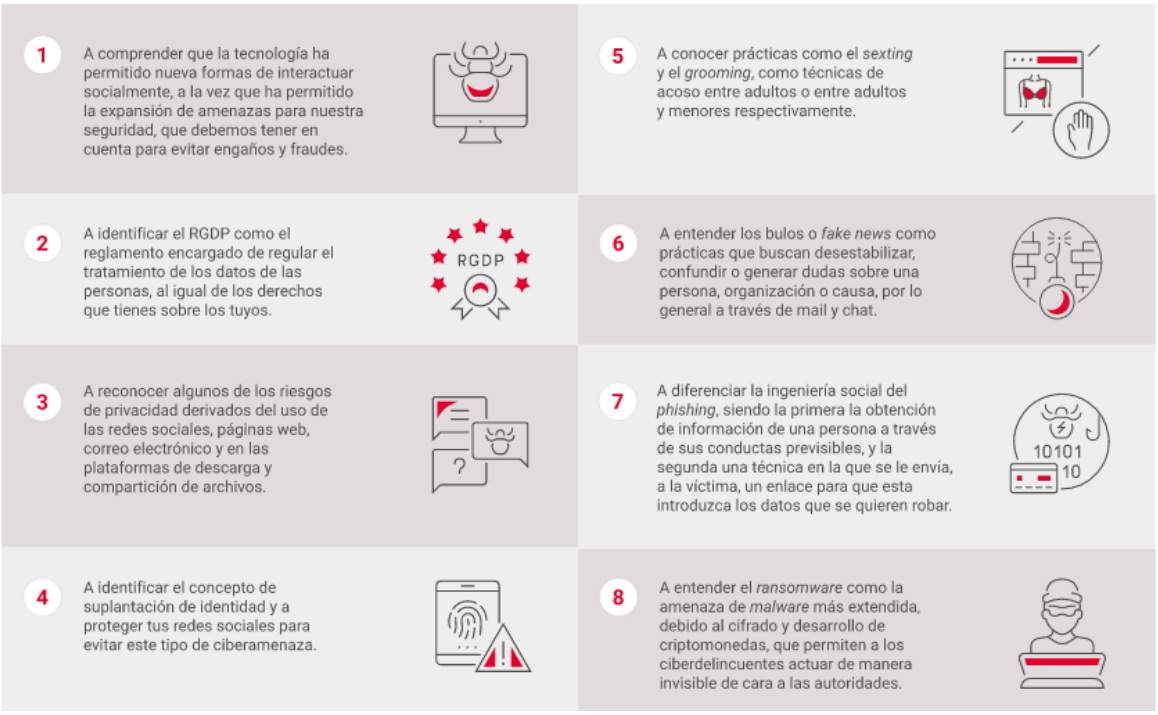
¿Qué le ha ocurrido a nuestra protagonista?

En esta unidad, Marta ha aprendido **cómo se trata la información personal que se utilizamos en los servicios digitales** gracias a las políticas de privacidad. Además, nuestra protagonista ha aprendido a proteger sus dispositivos, y los de la ONG, gracias a sus nuevos conocimientos sobre los riesgos y amenazas que existen en la red y las medidas de protección que deben aplicarse.

¿Y qué has aprendido a hacer?

Acción Formativa 4. Seguridad en la red.

UNIDAD DIDÁCTICA 4. RECOMENDACIONES DE SEGURIDAD. DETECCIÓN DE VULNERABILIDADES



Ahora que hemos aprendido todo sobre cómo la seguridad en Internet, en la siguiente unidad didáctica, Marta profundizará en todo lo relacionado con el *blockchain* y el uso de criptomonedas, con el fin de identificar las ventajas que puede esto suponer a una ONG como la suya.

3.2 Referencias bibliográficas

A continuación, puedes ver la relación de recursos (artículos, estudios, investigaciones, páginas web...) que se han consultado y citado para elaborar el contenido de esta Unidad Didáctica:

- ¿Qué puedes hacer si te ves afectado por una suplantación en redes sociales? Agencia Española de Protección de Datos. Recuperado de:

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-ministerio-consumo-campanna-suplantacion-identidad [31/01/2022].

- Línea de ayuda en ciberseguridad del Instituto de Ciberseguridad (INCIBE). Recuperado de: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad [31/01/2022].

- Maldito Bulo (2022). Recuperado de: <https://maldita.es/malditobulo/1> [14/02/2022].

- Newtral (2022). Recuperado de:: <https://www.newtral.es/fakes/> [14/02/2022].

- Guía de ciberataques. Recuperado de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf [14/02/2022].

- Sección "Protégete" de la Oficina de Seguridad del Internauta (OSI). Recuperado de: https://www.osi.es/es [31/01/2022].

- Sexting. Internet Segura For Kids (IS4K). Recuperado de: https://www.is4k.es/necesitas-saber/sexting [14/02/2022].

- Oficina de Seguridad del Internauta (OSI, 2022). Recuperado de: <https://www.osi.es/es/campanas/bulos-fake-news-fraudes> [14/02/2022].

- VerificaRTVE (2022). Recuperado de: <https://www.rtve.es/noticias/verificartve/> [14/02/2022].