AF4: Seguridad en la red

Identidad digital. Presencia en las redes

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 3
1.1 Introducción 3
2. ¿QUÉ ES LA IDENTIDAD DIGITAL? 4
2.1 Identidad digital 4
2.2 Huella digital 5
2.3 Protección de datos 10
3. PROTEGE TU IDENTIDAD DIGITAL 11
3.1 Suplantación de identidad digital 11
4. AUTENTICACIÓN 14
4.1 Identidad digital y autenticación personal 14
4.2 Métodos básicos de autenticación 15
4.3 Biometría 16
5. IDENTIDAD EN REDES SOCIALES 17
5.1 Redes sociales y privacidad 17
6. CIERRE 19
6.1 Resumen 19
6.2 Referencias bibliográficas 20

1. INICIO

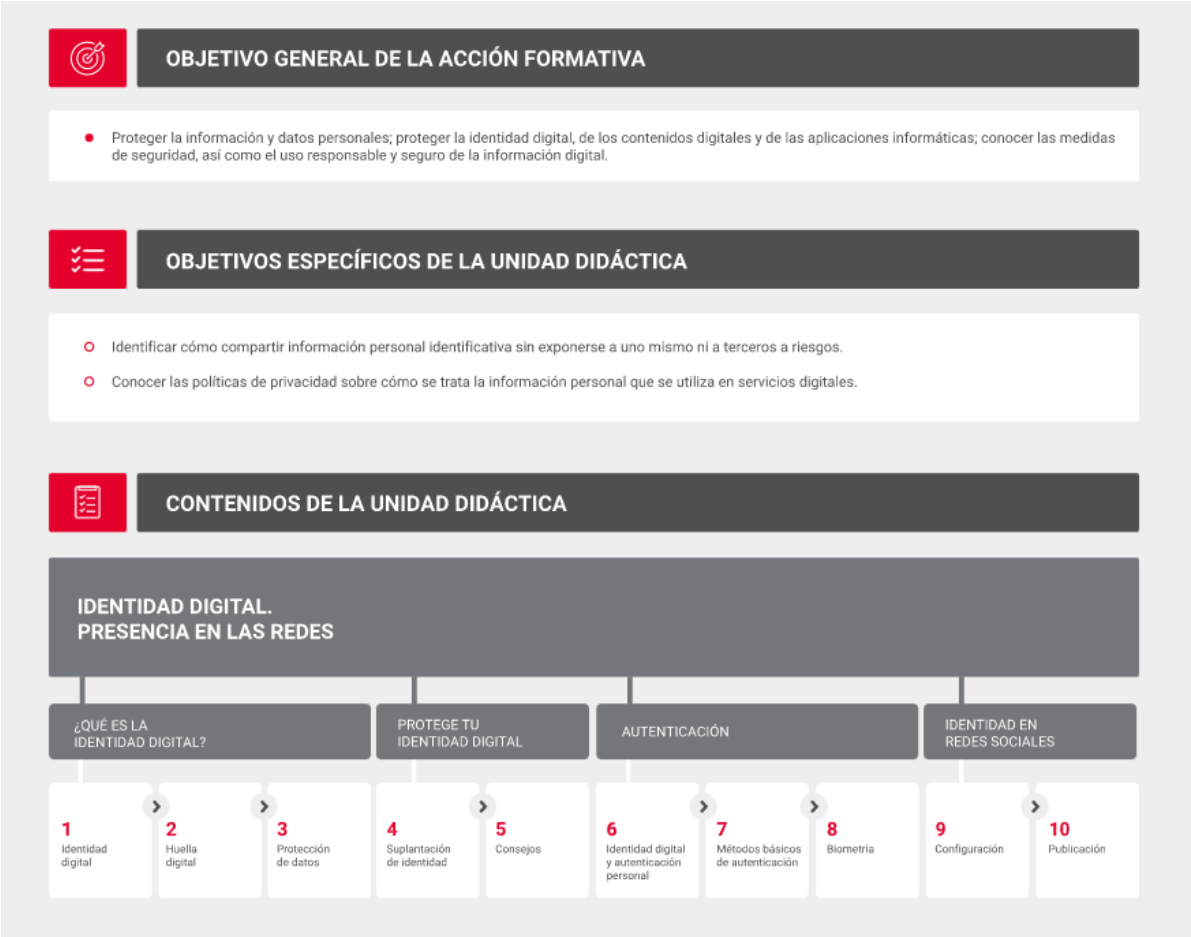
1.1 Introducción

Marta no era consciente del rastro que dejan sus acciones en internet y de la posible exposición de la información personal, propia y de terceros, que deja. Por otro lado, la ONG "Un mundo feliz" ha sufrido una suplantación de identidad recientemente, por lo que quiere conocer cómo actuar en estos casos para protegerse.

En esta unidad vamos a ver la **importancia que tiene la identidad digital** en nuestro mundo interconectado, **cómo se puede mejorar** a través de las publicaciones y las actuaciones que llevemos a cabo en el mundo digital y qué medidas aplicamos para **proteger nuestra información**.

También, vamos a aprender **cómo evitar la suplantación de identidad** y otro tipo de ciberdelincuencia en entornos laborales y personales, así como salvaguardar la privacidad en las redes sociales.

¿Qué vas a aprender en esta unidad?



2. ¿QUÉ ES LA IDENTIDAD DIGITAL?

2.1 Identidad digital

La información que aparece en internet sobre nuestra persona configura nuestra identidad digital. Nuestras acciones, como publicar contenidos y los comentarios que hacen los demás sobre nuestras acciones, conforman la idea de lo que somos en el entorno digital.

La **identidad digital**, por tanto, es la versión en internet de la identidad física de una persona. Está compuesta por los datos que proporcionamos en la red como la información de los perfiles en las redes sociales, comentarios, publicaciones, fotos, preferencias, compras online, etc.

Por ejemplo, Marta tiene un perfil personal en Facebook, otro en Instagram y para su vida profesional también ha creado uno en LinkedIn. Además, usa WhatsApp a diario para hablar y compartir información con sus contactos. En estos perfiles tiene distintas fotografías de su rostro, información sobre su fecha de nacimiento y su ocupación en la ONG.

Además, en Facebook e Instagram tiene imágenes de actividades en las que ha participado con otras personas y, en algunas, está etiquetada con su nombre. En estas redes suele publicar fotos y reaccionar a las publicaciones de sus amigos: pulsa en "Me gusta", comenta, comparte...

Toda esta información perfila su identidad digital.

Pero la información que se recopila sobre cada persona es mucho mayor que la que aparentemente vemos o conocemos. En un artículo publicado en Xataka (2018), Yúbal Fernández explica cómo al descargarse **una copia de seguridad de Facebook**, la red social había guardado toda esta información sobre él:

- Su **información personal**: nombre, número de teléfono, fecha de nacimiento, ciudad de residencia, situación sentimental, familia, etc.
- Todas las **fotos y vídeos**, con la ubicación e incluso la marca de la cámara con la que se hicieron las fotos.
- La **lista completa de sus contactos personales**, no solo los de Facebook, también los de su agenda, con sus teléfonos, direcciones de email, etc.
- Los **mensajes privados** de sus conversaciones a través de su aplicación de chat.
- Todas las **localizaciones**, las **direcciones IP** que es el número que identifica desde dónde se conecta un dispositivo a Internet, así como los dispositivos utilizados.
- Los anuncios que Facebook consideraba que le interesaban.

2.2 Huella digital

Cualquier persona en internet puede hacerse una idea de cómo es la vida de otras personas que publican sus inquietudes, los lugares que visita y sus gustos en las redes sociales.

Por huella digital se entiende el rastro que cada persona deja en internet con diferentes aportaciones.

Marta quiere profundizar en este tema de la huella digital, pues le preocupa el rastro que pueda dejar y de cómo esto puede afectar a terceras personas con las que trabaja.

La diferencia entre identidad digital y huella digital es que la primera es la representación de una persona a partir de su actividad en la red, la imagen que Marta proyecta de sí misma en las redes. Mientras que la segunda es el rastro de su actividad en la red y aquí podría involucrar a otras personas al manejar sus datos personales.

Cualquier acción en la web deja una serie de huellas:

Una recomendación de un restaurante.

Un voto favorable.

Las compras realizadas en tiendas online.

Comentarios en redes sociales.

Los teléfonos inteligentes se utilizan cada día para compartir información, fotografías y ubicaciones. En otras palabras, cada día es más grande nuestra exposición personal debido a la evolución de la tecnología.

Localización

Muchas aplicaciones móviles suelen pedirte permiso para conocer tu ubicación con el fin de mejorar el servicio. Esto hace que se pueda rastrear **tu ubicación** en cada momento. En algunas aplicaciones es necesario, como por ejemplo los navegadores GPS, pero en otras muchas aplicaciones proporcionar información sobre tu localización no condiciona su finalidad o funcionamiento.

Si tienes un iPhone o un iPad, puedes elegir que tu ubicación solo se comparta cuando abras y actives la aplicación, lo que resulta útil en el caso de los navegadores GPS.

Averigua qué tipo de permisos de acceso te requieren las distintas aplicaciones de tu dispositivo antes de concederlos.

¿Cómo podemos borrar nuestra huella digital?

Borrar nuestra huella digital es algo complejo, porque por mucho que intentemos eliminar un comentario o una imagen, es muy posible que esa misma información que deseamos borrar no desaparezca por completo.

Por esa razón, a este respecto, se proponen **dos posibilidades**:

Uso adecuado de internet: De forma preventiva, lo más adecuado es hacer un uso correcto de internet, y particularmente de las redes sociales.

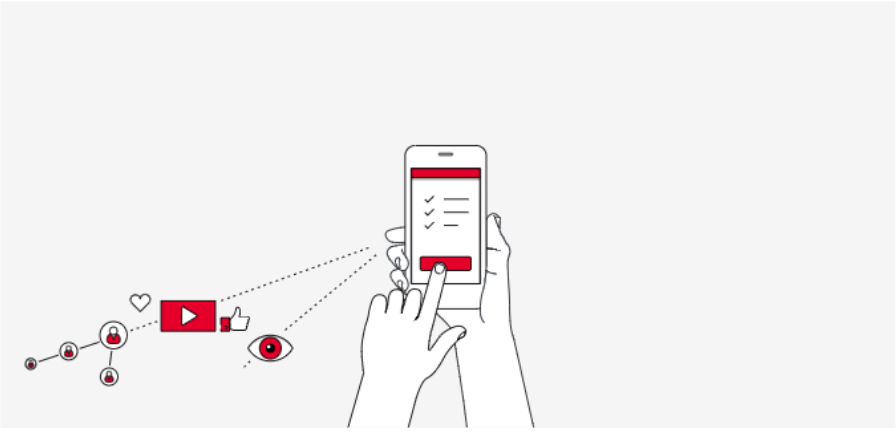
Para eso, es necesario cuidar las opciones de privacidad de los perfiles y pensar bien en lo que se quiere hacer público. Incluso antes de publicarlo, es conveniente saber que esa información puede permanecer en la red durante mucho tiempo, por lo que es necesario pensar dos veces antes de publicar cualquier elemento que pueda comprometer nuestra identidad digital. Por ejemplo, una foto en la que aparezca la ubicación de nuestra vivienda habitual o el colegio de nuestros hijos.

Generar otras informaciones: Por otro lado, cuando existe información que se desea eliminar de internet y no es posible, la opción más adecuada es **generar nueva información que pueda ir relegando progresivamente la información anterior**.

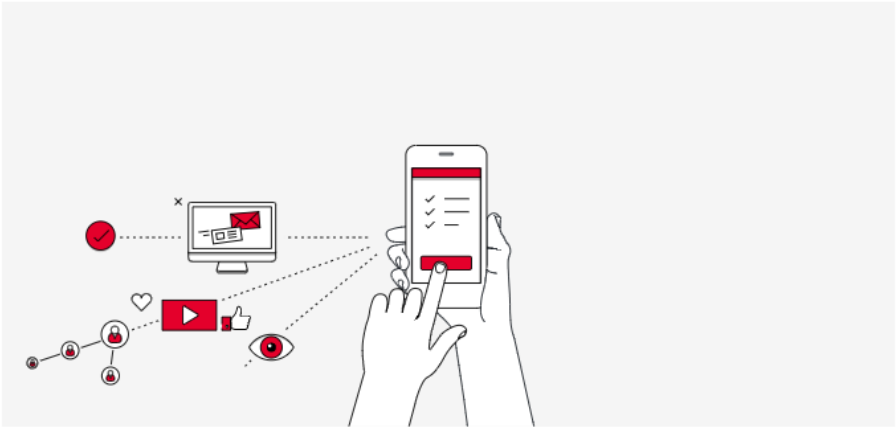
Esto se hace **creando una nueva reputación en redes sociales y en publicaciones web** para que, poco a poco, nuestra identidad digital se vea favorecida por nuevos aspectos positivos. Si estas publicaciones tienen relevancia, los buscadores las referenciarán en primer lugar, dejando relegada la información que no deseamos tener vinculada a nuestro perfil.

Consejos generales para reducir tu huella digital

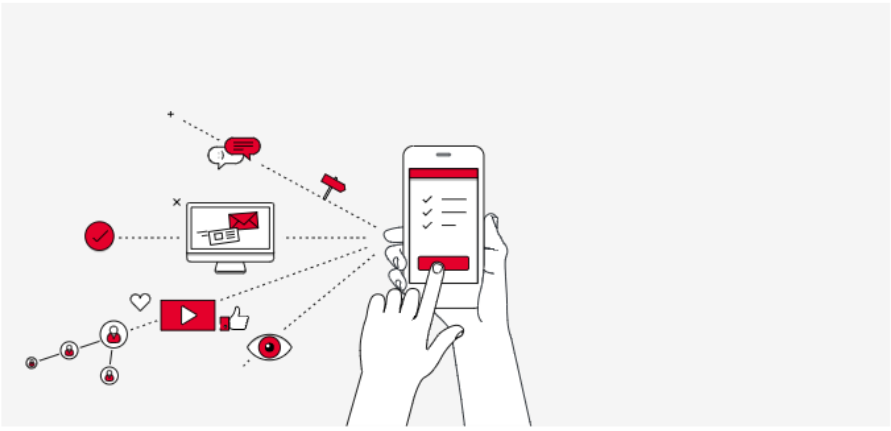
No compartas datos personales.



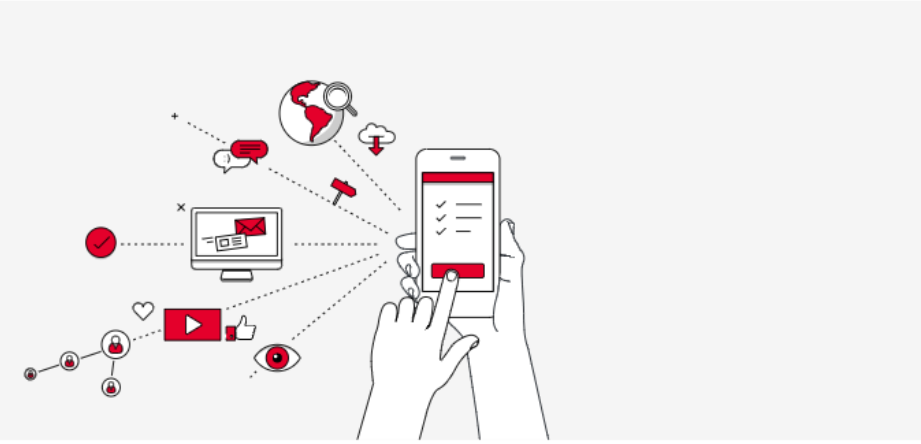
Cierra tu sesión de correo en lugares públicos.



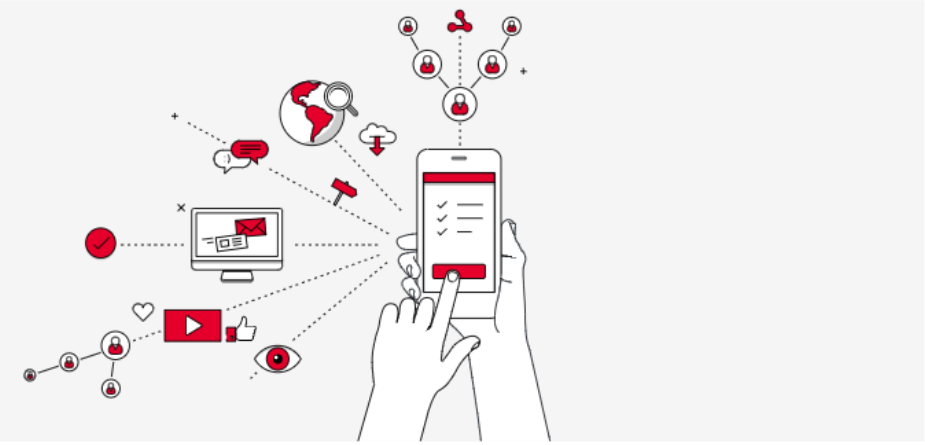
No aceptes amistad de extraños.



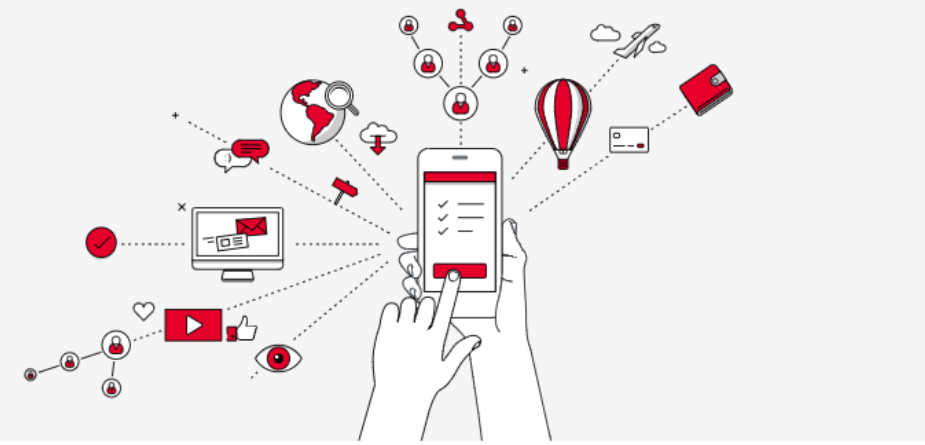
No compartas tu ubicación.



No compartas fotos o ubicación de terceros sin su permiso.



No compres en tiendas online no verificadas.



Utiliza una contraseña segura.

No uses redes wifi públicas.

No compartas datos sensibles a través de aplicaciones gratuitas.

La mayor parte de los datos que se dejan en internet no son solo nuestros, sino que nos relacionan o vinculan con otras personas.

Los datos se analizan de forma global, en conjunto con el resto de datos de otras personas con las que mantenemos un vínculo digital. El análisis puede incluir datos acerca de cuándo nos conectamos, quiénes son nuestros contactos, con quién hablamos, a quién seguimos en las redes, qué aspectos valoramos positivamente, etc.

Todas estas acciones generan una **huella digital colectiva**, que modela tanto la **identidad digital de una persona** como la identidad digital de **las personas con las que nos relacionamos.**

No me etiquetes

Es probable que haya personas que **no quieran aparecer en redes sociales** o no quieran que sus actividades sean públicas, pero a pesar de ello, se puede dar el caso de que acaben saliendo en las fotografías, textos o vídeos de otras personas, sin su conocimiento. Si etiquetamos personas, **debemos contar con su permiso** antes de hacerlo.

Respeta la privacidad de las demás personas y pide permiso antes de publicar cualquier material que las involucre.

2.3 Protección de datos

Las personas usuarias de internet son cada vez más conscientes de la importancia de su identidad digital y del poco control que, hasta hace poco, se ha tenido sobre ella.

La identidad digital no se ordena cronológicamente, sino por la notoriedad que han adquirido determinadas acciones con repercusión en la web.

A veces, esa **repercusión no siempre es predecible**, por lo que hay que tener la máxima cautela y el mayor cuidado posible con nuestra identidad en internet, ya que puede llegar a convertirse en un reflejo público de nuestra propia identidad.

El **prestigio personal** en la red, es decir, la estima pública que se obtiene en internet, tiene valor y está adquiriendo mucha importancia. Por esa razón, los robos de identidad no están únicamente relacionados con **la usurpación de los datos personales de las víctimas**, también están en riesgo nuestro **prestigio social, académico o laboral.**

¿Sabías que...?

España es el país de la Unión Europea con más víctimas de robo de identidad registradas, según cifras de la Oficina Europea de Estadística (Eurostat). El cuidado que debemos tener en este campo, por tanto, es muy grande.

Los datos que se ceden y se comparten a cambio de utilizar determinadas aplicaciones, como las de redes sociales, acaban perteneciendo, en la mayoría de los casos, a grandes corporaciones y quedan accesibles para realizar analítica de datos o big data.

Parece que las personas nos estamos viendo obligadas a esta entrega continua y pasiva de nuestros datos. Es por eso, que en estos momentos y desde todos los estamentos, se está tratando de **promover la capacidad de las personas para decidir cómo quiere que sus datos sean utilizados, almacenados y compartidos**.

Esta cuestión también se ve impulsada por el Reglamento General de Protección de Datos, relativo a la protección de los datos personales y su circulación para las empresas que tratan los datos de residentes en la Unión Europea, y por la Ley española de Protección de Datos Personales y garantía de los derechos digitales.

3. PROTEGE TU IDENTIDAD DIGITAL

3.1 Suplantación de identidad digital

Uno de los principales problemas relacionados con la seguridad en internet es la **suplantación de la identidad digital**, que consiste en hacerse pasar por otra persona con el fin de robar información sensible, estafar o cometer distintos tipos de acoso a través de internet.

Un caso claro de suplantación de identidad es cuando alguien utiliza los datos bancarios de otra persona para realizar compras online o movimientos en sus cuentas corrientes sin su autorización y aprobación.

También es frecuente pensar en casos de suplantación de identidad de personas famosas o "*celebrities*", pero cualquier identidad de una persona anónima corre el riesgo de ser robada.

Divulgar los datos personales de alguien a través de la red es una vulneración de su intimidad que puede dañar su reputación e imagen que tiene en la web.

Pero no solo se puede suplantar la identidad de una persona, los ciberdelincuentes también pueden usurpar la identidad de un banco, un servicio, una entidad pública o una empresa determinada.

Veamos qué le sucedió a la ONG donde trabaja nuestra protagonista, Marta:

La ONG "Un mundo feliz" está recibiendo quejas por parte de su voluntariado y de las personas socias a través de los distintos perfiles en redes sociales. La razón es que están recibiendo mensajes falsos a través de Facebook y WhatsApp, en los que simulan ser la ONG, para que realicen donaciones. Esta campaña resulta ser una estafa y la ONG, aunque no es la responsable, se ve envuelta en una crisis online.

Consejos para proteger la identidad digital

La identidad digital debe ser protegida, en primer lugar, con tus propias actuaciones.

Pero ¿qué podemos hacer para evitar la suplantación de identidad? ¿Cómo podemos actuar para que no nos ocurra? ¿Qué medidas puede aplicar la ONG en la que trabaja Marta para que no le vuelva a pasar?

Ten en cuenta las siguientes normas para proteger tu identidad digital:

CONFIDENCIALIDAD

Si dispones de cuentas con **preguntas de seguridad** para recuperar tus claves (como ocurre con las cuentas de Gmail), debes asegurarte de que las personas de tu entorno no sabrían responderlas y que solo las conoces tú.

Además, recuerda que debes cerrar la sesión cada vez que dejas el equipo. Por ejemplo, cuando te levantes al aseo o cuando finalices tu jornada laboral.

Por otro lado, en ningún caso almacenes **datos de acceso** si compartes tu ordenador.

CONTRASEÑAS FUERTES

Es importante que no comuniques a nadie los datos de usuario y contraseña, evita que la gente pueda mirar mientras tecleas la clave y crea contraseñas seguras.

Por supuesto, también es importante que no tengas datos relacionados con ellas en Internet. Es bastante común utilizar como contraseña el nombre de una mascota y, simultáneamente, tenerla etiquetada con su nombre en diversas fotografías en redes sociales.

Una contraseña fuerte, por tanto, tiene como **mínimo 8 caracteres, está formada por letras mayúsculas y minúsculas y números, además de caracteres especiales.**

Por ejemplo: #A%aGcPLajL48XZ.

USO DE WIFI PÚBLICAS

Se desaconseja totalmente conectarse a una **red wifi pública,** como la que puedes encontrar en un centro comercial o en un bar. Se debe a que su contraseña suele ser débil y, al mismo tiempo, los atacantes suelen estar preparados para robar datos en estas redes abiertas.

Una contraseña robusta deja de serlo si la apuntas en un papel o en un archivo del ordenador. Para evitar esto, los navegadores como Google ofrecen guardar y recordar tus datos de acceso en cada página, pero por contra, estás concediendo al navegador todos tus datos de acceso.

Javier, que también trabaja en la ONG "Un mundo feliz" con Marta, tenía configurado su correo electrónico con una contraseña bastante intuitiva, nunca consideró que tener una contraseña poco robusta le podría dar problemas.

Al cabo de un tiempo, Javier intentó entrar en su correo personal, pero su credencial y contraseña le daban error y no se lo permitía. Pensó que era un error del ordenador y no le dio más importancia.

Al poco tiempo, Marta, su compañera de trabajo y protagonista de nuestra historia, le recriminó que le había mandado un correo con un virus que le había estropeado su portátil nuevo. Javier no entendía lo que había pasado; él no le había mandado nada. De repente, comenzó a recibir llamadas de amistades y contactos explicándole el mismo problema que le había pasado a Marta. Cientos de correos infectados habían salido del buzón de Javier.

Javier decidió denunciar la situación ante la policía para intentar evitar más correos como estos. Unos días después, la policía le comunicaba que había sido víctima de usurpación de identidad, muy probablemente porque alguien averiguó la contraseña de acceso a su correo electrónico.

Javier reconoció que su contraseña era fácil de descubrir y fue consciente de la grave negligencia que había cometido por no haber configurado una contraseña más robusta.

Medidas de actuación en caso de suplantación de identidad

Si tenemos constancia de que ha ocurrido una usurpación de identidad, debemos actuar con rapidez para minimizar los daños.

¿Y cómo debemos actuar? ¿Cuáles serían los pasos a seguir? Veámoslos a continuación:

Paso 1

Cierra todas las sesiones que tengas activas (redes sociales, banco o, por ejemplo, correo electrónico) y cambia la contraseña de forma inmediata. En el caso de que te hayan cambiado la contraseña y no puedas entrar, ponte en contacto con el servicio en cuestión cuanto antes. Además, debes informarles para que tengan constancia de ello y, en el caso de que puedan, eliminen la cuenta falsa de inmediato.

Paso 2

Recopila toda la información que puedas en la que se evidencie la suplantación de identidad: haz capturas de pantalla, guarda correos electrónicos, conversaciones, etc.

Paso 3

Explica la situación a las personas que hayan podido ser afectadas por actuaciones realizadas en tu nombre y avisa de que podrían realizarse otras.

Paso 4

Si no se puede solucionar de forma rápida, denuncia lo sucedido ante las Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Puedes hacerlo de manera presencial o por Internet, en el Grupo de Delitos Telemáticos de la Guardia Civil.

También informa a la Oficina de Seguridad del Internauta (OSI), que depende del Instituto Nacional de Ciberseguridad (INCIBE).

Para más información, puedes dirigirte al teléfono gratuito del INCIBE, el 017, donde te darán toda la ayuda necesaria en materia de ciberseguridad.

4. AUTENTICACIÓN

4.1 Identidad digital y autenticación personal

La autenticación es el proceso que nos permite comprobar que la identidad que se presenta coincide con los datos de identidad previos que tiene la plataforma o servicio.

La forma más extendida de autenticación es el nombre de usuario y la contraseña, pero también es común usar herramientas que permiten leer datos biométricos.

La autenticación debe tener en cuenta, además de la seguridad del proceso, **lo operativo que sea su uso**. Esta cuestión no es menor, ya que muchos servicios requieren autenticarse en diversos momentos, y además una persona puede usar de manera

constante varios servicios. Esto impulsa la **necesidad de que estos procesos sean lo más rápidos posible**, para evitar que afecten al flujo de trabajo.

4.2 Métodos básicos de autenticación

¿Cuáles son los diversos mecanismos que existen para autentificar a las personas usuarias? ¿Cómo podemos comprobar la identidad de las personas?

Para que cualquier persona pueda autenticarse se pueden utilizar **diversos tipos de información**:

1. Algo que se conoce. Es el ejemplo habitual que se usa en la mayor parte de los servicios y que nos permite usar una contraseña para darnos de alta o acceder al servicio.

2. Algo que se posee. Este tipo de información sería el más tradicional, ya que se puede presentar un DNI, un pasaporte o una tarjeta.

3. Algo que se es. Esto nos permite un elevado grado de seguridad: utilizando elementos biométricos se puede autenticar a una persona con bastante seguridad.

4. Factores de contexto. Este método está relacionado con la ubicación actual o pasada, o el uso de determinadas funciones que facilitan los teléfonos móviles.

¿Sabías que...?

La combinación de diferentes elementos aumenta la seguridad del proceso de autenticación.

Métodos de autenticación

Según lo que hemos visto, existen diferentes informaciones que permiten comprobar la identidad de una persona. A estas informaciones las llamamos **factores de autenticación**. Debemos considerar tres opciones posibles:

- **La autenticación de factor único**
  Está basada en **un único tipo de credenciales**. Es la más extendida en la red y la que más se ha usado durante los últimos años. Al tener solo un elemento para autenticar a una persona, puede presentar problemas de seguridad.
- **La autenticación de factor doble**
  Este sistema combina **dos de las posibilidades de autenticación**. De esta forma, podríamos introducir algo que la persona sabe (una contraseña, por ejemplo) y algo que la persona es (una lectura de su huella dactilar).
- **La autenticación de factor múltiple**
  Permite contrastar algo que la persona sabe, algo que posee (por ejemplo, una tarjeta especial) y algo que es. Sería la fórmula de autenticación **más exigente**.

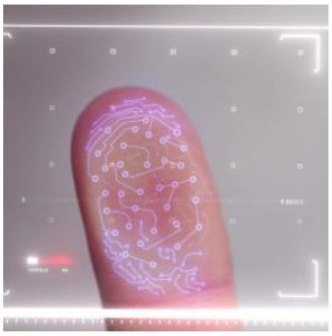
4.3 Biometría

La biometría permite la autenticación de una persona a través de su propio cuerpo.

No es un método nuevo, ya que las huellas dactilares y palmares se utilizan desde hace cientos de años para el sellado de documentos.

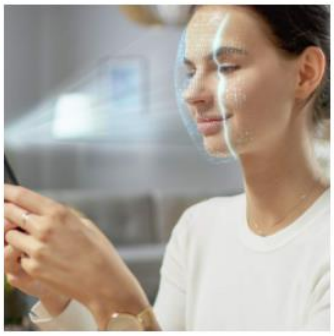
Ahora mismo, gracias a los avances técnicos, existen varias opciones para realizar una autenticación por medios biométricos. Además, la biometría se utiliza en numerosas **estrategias de seguridad**, tanto en sistema de **control** como en sistema de **reconocimiento**. De hecho, su uso indiscriminado por parte de algunos países ha levantado grandes críticas por la intromisión que puede suponer en la privacidad de las personas.

Ejemplos de pruebas de reconocimiento biométrico



Huella dactilar.

Reconocimiento ocular.



Reconocimiento facial.

Características de los métodos biométricos

La autenticación biométrica es muy común en la actualidad y presenta distintas posibilidades.

A continuación, veamos las características de los distintos métodos biométricos:

Huellas dactilares

Sigue siendo el método más usado, precisamente por lo extendido que está en los documentos oficiales. De la misma forma, también se utiliza en lectores de acceso y en los teléfonos móviles como método de autenticación y de pago.

Reconocimiento facial

El reconocimiento facial se ha extendido mucho en los últimos años. Además de usarse en el control de acceso de espacios como aeropuertos o edificios, también está extendido para la autenticación personal en teléfonos móviles, tabletas y ordenadores.

El problema principal que puede presentar son las dificultades ante los cambios de aspecto, ya que aumentar o disminuir de peso, usar o no gafas, llevar o no barba..., pueden influir en el proceso de autenticación.

Escaneo de retina

Este modelo hace un escaneado del patrón de vasos sanguíneos del globo ocular. Es uno de los métodos más seguros porque es imposible falsificar ese patrón y, por otro lado, los globos oculares no sufren variaciones con el tiempo.

Reconocimiento de voz

El reconocimiento de voz trabaja con los datos de timbre, resonancia e incluso expresiones de nuestra voz. Los problemas fundamentales pueden derivar de alguna afectación como afonía, resfriado, etc.

Según lo que hemos visto hasta ahora, acceder a una página con datos biométricos es más seguro, pero a cambio, las aplicaciones se guardan esta información privada y extremadamente sensible ya que nos identifica de manera única. En todas las acciones relacionadas con internet, debemos buscar un equilibrio entre la información que se confía y la que se mantiene privada.

5. IDENTIDAD EN REDES SOCIALES

5.1 Redes sociales y privacidad

Las redes sociales son utilizadas a diario por millones de personas. La conexión entre individuos permite compartir ideas, contenidos y diversas iniciativas casi en tiempo real.

Ya hemos visto el tipo de información que solemos compartir en redes:

- Fotografías.
- Localizaciones.
- Estados emocionales.

Generalmente aceptamos los **términos y condiciones** de las aplicaciones que queremos utilizar sin detenernos a revisar el grado de protección de nuestros datos que cedemos porque, normalmente, se trata de acuerdos complejos y extensos que no nos paramos a leer.

Las empresas están obligadas a cumplir con la normativa de la protección de datos y **las personas usuarias tienen el derecho de exigir más control sobre sus datos** para que las redes sociales se conviertan en un espacio más seguro y transparente.

Configuración de redes sociales

A veces se tiene toda la información, tanto del perfil como de las publicaciones, en abierto, lo que significa que todas las personas de la red pueden acceder a ellos. Si esa es la opción deseada no hay problema, pero en muchas ocasiones no solemos tener muy claro cuando empezamos a utilizar una red social qué es privado y qué es público.

Es también importante revisar otras posibilidades como, por ejemplo, **la opción de decidir si quieres que la información de tu perfil aparezca o no en los buscadores**, lo habitual es que desde Google se puedan localizar las redes sociales de una persona.

Decidir el **grado de exposición de tu perfil** también es una decisión tuya. Por ejemplo, si te interesa que tu perfil sea lo más público posible y que se pueda ver por todas las personas de la red, debes dejarlo en esa opción. Esto es interesante, por ejemplo, en las redes profesionales de búsqueda de trabajo. Sin embargo, si quieres **evitar una sobreexposición de tu perfil**, lo aconsejable es restringir la configuración en ese sentido.

¡Recuerda!

Es conveniente que revises la configuración de privacidad de tus perfiles en las redes sociales. Desde ahí puedes restringir determinada información y utilizar las redes sociales de una forma más adecuada a tus necesidades.

Publicación de información en redes sociales

Lo que publicas en la red es tu responsabilidad, por ello es importante que pienses bien qué quieres hacer público.

¿Sabías que...?

La gran mayoría de las redes sociales permite eliminar una publicación. Aun así, ha podido dar tiempo a que otra persona haga una captura de pantalla o descargue la imagen. La precaución es la única posibilidad de evitar hacer públicas informaciones que queremos que sean privadas.

Interacciones con otras personas

Recuerda que en Internet queda registro de las interacciones que tenemos con los demás.

Estas interacciones, aunque no son propiamente publicaciones, sí permiten que un atacante pueda acceder a ellas y hacer una captura. Esta información puede ser muy valiosa para cometer algún tipo de fraude. Las fotografías personales, así como los vídeos, incluso cuando se publican en servicios donde se pueden borrar automáticamente, pueden **ser grabados o descargados.**

Por esa razón, debemos pensar en cada publicación como si fuese a **permanecer accesible públicamente** para siempre.

Teniendo en cuenta esta idea, debemos publicar con la máxima prudencia.

Antes de hacer una publicación en redes sociales, piensa en los pros y contras que puede tener si cae en las manos equivocadas. Luego es muy complicado eliminar ese rastro digital.

6. CIERRE

6.1 Resumen

¿Qué le ha ocurrido a nuestra protagonista?

A lo largo de esta Unidad Didáctica, Marta ha comprendido **cómo se genera su imagen o identidad digital** en internet, **qué es la huella digital** y el rastro que deja. También empieza a ser consciente del **valor que tiene ceder sus datos** y cómo luego estos pueden llegar a ser accesibles y utilizados por grandes corporaciones.

Ha comprendido que debe **cuidar y proteger la información** que maneja, pues al trabajar con muchas personas y compartir dispositivos y herramientas digitales, se pueden correr algunos riesgos en cuanto a la seguridad de los datos confidenciales de especial sensibilidad.

En definitiva, Marta sabe **identificar cómo compartir información personal identificativa sin exponerse a ella misma ni a terceros a riesgos y conoce las políticas de privacidad sobre cómo se trata la información personal que se utiliza en servicios digitales.**

¿Y qué has aprendido a hacer?

En la siguiente unidad, Marta conocerá los principales impactos medioambientales que provocan las tecnologías digitales y su uso. ¿Qué puede hacer ella y la ONG donde trabaja para minimizar este impacto? ¿Cómo deben tratar los residuos tecnológicos? ¿Cómo pueden hacer un uso eficiente de la tecnología? Y, finalmente, ¿cómo acabará la historia de Marta? ¿Habrá resuelto las dudas que tenía sobre seguridad en la red? Veámoslo a continuación.

6.2 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:

- Agencia Española de Protección de Datos (2021). Configura tu privacidad en Facebook. Recuperado de: <https://www.youtube.com/watch?v=mjLV1qvkyZo> [10/02/2022].
- Europapress. Portal TIC. España es el país de la Unión Europea con más víctimas de robo de identidad en el último año, según el Eurostat. Recuperado de: <https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-pais-

union-europea-mas-victimas-robo-identidad-ultimo-ano-eurostat-20180102092136.html> [10/02/2022].

- Fernández, Yuba. (Septiembre del 2018). Me he bajado todos los datos que Facebook tiene sobre mí, y ahora sé que puede reconstruir mi vida cuando quiera. Xataka. Recuperado de: <https://www.xataka.com/privacidad/me-he-bajado-todos-los-datos-que-facebook-tiene-sobre-mi-y-ahora-se-que-puede-reconstruir-mi-vida-cuando-quiera> [10/02/2022].
- Google. Ayuda de cuenta de Google. Elegir qué aplicaciones pueden usar la ubicación de tu teléfono Android. Recuperado de <https://support.google.com/accounts/answer/6179507?hl=es> [10/02/2022].
- Grupo de Delitos Telemáticos de la Guardia Civil (2022). Recuperado de: <https://www.gdt.guardiacivil.es/webgdt/pinformar.php> [10/02/2022].
- Oficina de Seguridad del Internauta (2022). Recuperado de: <https://www.osi.es/es/reporte-de-fraude> [10/02/2022].
- Soporte de Apple. Activa o desactiva la Localización y el GPS en el iPhone, iPad y iPod touch. Recuperado de: <https://support.apple.com/es-es/HT207092#:~:text=Ve%20a%20Ajustes%20%3E%20Privacidad%20y,activa%20o%20desactiva%20Ubicaci%C3%B3n%20exacta> [10/02/2022].