

# Construcción de nuestra Identidad Digital y perfiles digitales.

---



**Materiales formativos de FP Online propiedad del Ministerio de Educación,  
Formación Profesional y Deportes**

[Aviso Legal](#)

# 1.- ¿Qué es Identidad Digital?

## ¿Qué es Identidad Digital?

La Identidad Digital se refiere a la **suma total** de todas las **huellas digitales** y **perfiles** que una persona o entidad tiene en línea. Incluye **perfiles digitales**, pero también abarca otras actividades y rastros en línea.

## ¿Qué abarca la Identidad Digital?

La Identidad Digital es un concepto **integral** que abarca todas las formas en que una persona o entidad interactúa en línea y las huellas que deja en el mundo digital. Incluye perfiles digitales como una parte de esa identidad, pero va más allá de ellos.



Freepik. Identidad Digital (CC BY-NC-SA)

## ¿Qué actividad en la red incluye la Identidad Digital?

La Identidad Digital incluye **toda la actividad en línea pasada y presente**; como búsquedas en la web, historiales de navegación, comentarios en foros, correos electrónicos enviados y recibidos, registros de acceso, compras en línea y más.

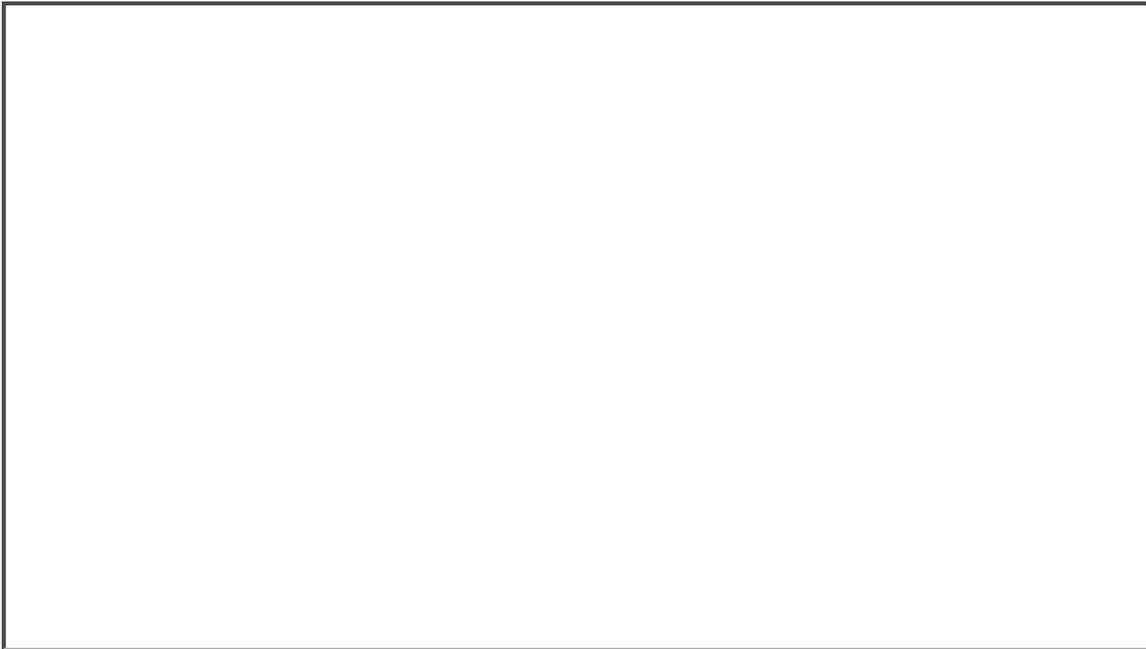
La construcción de nuestra Identidad Digital se refiere a cómo creamos y presentamos nuestra personalidad, intereses, y actividades en línea a través de diversos **medios digitales**, como redes sociales, blogs, foros y más.

## ¿Es lo mismo "Identidad digital" que "Ciudadanía digital"?

No, no es lo mismo.

## La Identidad Digital

La **Identidad Digital** es la imagen que proyectamos de nosotros mismos en el mundo virtual, así como cómo los demás nos perciben en función de esa información. La Identidad Digital puede incluir detalles como perfiles de redes sociales, fotos, comentarios y publicaciones que hacemos en línea. Es importante ser consciente de cómo construimos nuestra Identidad Digital, ya que puede influir en cómo los demás nos ven y nos juzgan en línea y en la vida real.



Freepik. *Identificar Digital* ([CC BY-NC-SA](#))

## Ciudadanía digital

La **ciudadanía digital** se refiere a la forma en que las personas se comportan y participan en línea de manera **responsable y ética**. Esto incluye respetar los derechos de privacidad de otros, no participar en el acoso cibernético, no difundir información falsa o engañosa y en general, ser un buen ciudadano en el entorno digital. La ciudadanía digital es esencial para mantener un ambiente en línea seguro y positivo.



Freepik. *Señales* ([CC BY-NC-SA](#))



## Reflexiona

¿En qué aspectos se diferencia la Identidad Digital de la identidad tradicional?

Mostrar retroalimentación

La Identidad Digital y la identidad tradicional comparten similitudes en cuanto a representar quién es una persona, pero difieren significativamente en sus características y en cómo se gestionan:

- ✓ **Alcance y Accesibilidad:** La Identidad Digital es globalmente accesible y puede ser consultada por cualquier persona con acceso a Internet. En cambio, la identidad tradicional suele estar restringida a documentos físicos y contextos específicos, como instituciones gubernamentales o educativas.
- ✓ **Temporalidad y Persistencia:** Las huellas digitales pueden persistir indefinidamente en la web, incluso después de que una persona intente eliminarlas o cambie de comportamiento. La identidad tradicional, como registros físicos, puede ser destruida o perderse con el tiempo.
- ✓ **Control y Privacidad:** Las personas tienen menos control sobre su Identidad Digital, ya que es fácil de compartir y difícil de eliminar por completo. La identidad tradicional, aunque también puede ser compartida, es más fácil de proteger mediante medidas físicas y legales.
- ✓ **Representación de Comportamiento:** La Identidad Digital incluye no solo información estática como nombre y fecha de nacimiento, sino también un registro dinámico del comportamiento en línea, como opiniones expresadas, compras realizadas y la interacción con otros usuarios.



## Autoevaluación

¿Qué es Identidad digital?

- La identidad digital es la forma en que las personas se comportan y participan en línea de manera responsable y ética.
- La identidad digital es la representación en línea de uno mismo.

- La identidad digital es la representación en línea de los demás.

Incorrecto

Opción correcta

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

### La identidad integral es un concepto:

- Incluye los perfiles digitales, pero no otras actividades y rastros en línea.
- No incluye los perfiles digitales, solo los rastros en línea.
- Es la suma total de todas las huellas digitales y perfiles que una persona o entidad tiene en línea.

La identidad digital se refiere a la suma total de todas las huellas digitales y perfiles que una persona o entidad tiene en línea. Incluye perfiles digitales, pero también abarca otras actividades y rastros en línea.

La identidad digital se refiere a la suma total de todas las huellas digitales y perfiles que una persona o entidad tiene en línea. Incluye perfiles digitales, pero también abarca otras actividades y rastros en línea.

La identidad digital se refiere a la suma total de todas las huellas digitales y perfiles que una persona o entidad tiene en línea. Incluye perfiles digitales, pero también abarca otras actividades y rastros en línea.

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

### ¿Qué incluye la identidad digital?

- Solo la actividad pasada en la red.
- Se puede personalizar y configurar según las preferencias del usuario
- Incluye actividad en línea pasada y presente.

Incorrecto

Incorrecto

La identidad digital incluye toda la actividad en línea pasada y presente, como búsquedas en la web, historiales de navegación, comentarios en foros, correos electrónicos enviados y recibidos, registros de acceso, compras en línea y más.

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta



## Autoevaluación

¿Es verdadero o falso?

**La ciudadanía digital se refiere a la forma en que las personas se comportan y participan en línea de manera responsable y ética. Implica el uso responsable y seguro de la tecnología y no participar en la sociedad digital.**

Verdadero  Falso

### Falso

La ciudadanía digital se refiere a la forma en que las personas se comportan y participan en línea de manera responsable y ética. Implica el uso responsable y seguro de la tecnología y la participación activa en la sociedad digital.

## 2.- ¿Por qué es importante la Identidad Digital?

### ¿Por qué es importante la Identidad Digital?

La Identidad Digital se refiere a la representación en línea de una persona. Es importante porque puede afectar la percepción que otros tienen de ti y puede ser relevante en cuestiones de privacidad y seguridad en línea.



Freepik. Ordenador (CC BY-NC-SA)

### ¿Cuáles son algunas prácticas clave de ciudadanía digital?

Algunas prácticas clave incluyen respetar la privacidad en línea, evitar el  ciberacoso, citar fuentes en línea adecuadamente y contribuir de manera positiva en comunidades en línea.

### ¿Cuál es la importancia de la alfabetización digital en la ciudadanía en línea?

La alfabetización digital es esencial para comprender cómo funcionan las tecnologías en línea, cómo protegerse y cómo participar de manera constructiva. Ayuda a las personas a tomar decisiones informadas y a ser ciudadanos digitales responsables.

### ¿Cuál es la relación entre la Identidad Digital y la privacidad en línea?

La Identidad Digital y la privacidad en línea están estrechamente relacionadas. La forma en que gestionas tu identidad en línea puede afectar tu privacidad. Es importante ser consciente de **qué información compartes y con quién**.



## Reflexiona

### ¿Cuál es la relación entre la identidad digital y la privacidad en línea?

Mostrar retroalimentación

La identidad digital y la privacidad en línea están intrínsecamente relacionadas. La identidad digital se compone de toda la información que una persona comparte y deja en línea, incluyendo perfiles en redes sociales, publicaciones, historial de navegación, y otros datos. Esta información puede ser utilizada para identificar y entender quién es una persona en el mundo digital.

La privacidad en línea, por otro lado, se refiere al control que una persona tiene sobre cómo se recopila, utiliza y comparte su información personal en

Internet. A medida que la identidad digital se construye a partir de la información disponible en línea, la privacidad en línea desempeña un papel crucial en la protección de esta información contra el acceso no autorizado, el mal uso y la divulgación indebida.

Una gestión adecuada de la privacidad en línea ayuda a proteger la identidad digital de una persona, permitiendo controlar qué información está disponible para el público, para empresas o para potenciales malintencionados. Por lo tanto, para proteger la identidad digital y evitar problemas como el robo de identidad, el acoso o la discriminación, es fundamental aplicar buenas prácticas de privacidad, como configurar opciones de privacidad en redes sociales, usar contraseñas seguras, y ser cauteloso con la información compartida en línea.



## Autoevaluación

¿Es verdadero o falso?

**La ciudadanía digital se refiere a ser un ciudadano en el sentido tradicional, sin relación con la tecnología digital.**

Verdadero  Falso

**Falso**

**La alfabetización digital implica comprender, utilizar y evaluar eficazmente la tecnología digital.**

Verdadero  Falso

**Verdadero**

**La ética digital no tiene nada que ver con el comportamiento ético y responsable en línea.**

Verdadero  Falso

**Falso**

**La seguridad en línea es un aspecto importante de la ciudadanía digital, que incluye proteger la información personal y evitar fraudes cibernéticos.**

Verdadero  Falso

**Verdadero**

**Los ciudadanos digitales no necesitan evaluar la información en línea, ya que todo en Internet es siempre preciso y confiable.**

Verdadero  Falso

**Falso**

**La participación activa en la sociedad digital no es un componente relevante de la ciudadanía digital.**

Verdadero  Falso

**Falso**

**La identidad digital es un aspecto fundamental de la ciudadanía digital y se refiere a construir una presencia en línea auténtica.**

Verdadero  Falso

**Verdadero**

**La educación no desempeña un papel importante en la ciudadanía digital y no se necesita enseñar a los estudiantes sobre aspectos éticos, técnicos y prácticos de la vida digital.**

Verdadero  Falso

**Falso**

## 3.- ¿Qué implica la Identidad Digital?

### ¿Qué implica la Identidad Digital?



Freepik. Huella Digital (CC BY-NC-SA)

La Identidad Digital es única y puede incluir información personal, perfiles en redes sociales, actividades en línea y una presencia en la web en general. Aquí se explora en detalle lo que implica la Identidad Digital:

### 1. Información personal:

La Identidad Digital puede incluir información básica, como nombre, fecha de nacimiento, género y detalles de contacto. Esta información es a menudo utilizada para crear cuentas en línea y perfiles de usuario.

A screenshot of a web form for personal information. The form has a header with tabs: "GENERAL", "CATEGORÍA", "SEGURIDAD Y CONTROL", and "MIR REGISTRO DE CAMBIOS". Below the header, there are several input fields: "Nombre:" with "PEDRO" entered, "Apellido:" with "ALVAREZ" entered, "Tipo de identificación:" with a dropdown menu, "Fecha de nacimiento:" with a date picker, and "Descripción:" with a text area. There are also buttons for "Guardar", "Cancelar", and "Volver".

Freepik. Identidad personal (CC BY-NC-SA)

### 2. Perfiles en redes sociales:

Las cuentas en redes sociales son una parte importante de la Identidad Digital. Los perfiles en plataformas como Facebook, Twitter, Instagram y LinkedIn contienen información personal, fotos y actividades

compartidas con otros usuarios.



Pixabay. *Perfiles en redes sociales* (CC BY-NC-SA)

### 3. Huella digital:

La actividad en línea deja una huella digital. Esto incluye los sitios web visitados, las búsquedas en motores de búsqueda, las publicaciones en redes sociales y otros rastros digitales que una persona crea mientras navega por la web.

### 4. Comunicación en línea:

Los correos electrónicos, mensajes de texto, conversaciones en redes sociales y otras formas de comunicación en línea también contribuyen a la Identidad Digital. Estas interacciones pueden ser archivadas y rastreadas.

### 5. Actividades en línea:

Las actividades en línea abarcan desde compras en línea hasta el registro en foros, blogs, participación en juegos en línea y más. Cada una de estas actividades puede contribuir a la Identidad Digital de una persona.

## 6. Publicaciones y contenido compartido:

La información compartida en blogs, sitios web personales, plataformas de video y otras formas de contenido en línea también forma parte de la Identidad Digital. Esto puede incluir artículos, videos, fotografías y otros medios creados y compartidos en línea.



Pixabay. Identidad Digital (CC BY-NC-SA)

## 7. Evaluación por terceros:

Las empresas, empleadores y otros individuos pueden evaluar la Identidad Digital de alguien para tomar decisiones importantes. Esto puede incluir verificar antecedentes, evaluar la idoneidad de una persona para un trabajo o juzgar la **confiabilidad** de una fuente en línea.

## 8. Privacidad y seguridad:

La gestión de la privacidad y la seguridad en línea es un componente importante de la Identidad Digital. La información personal y la actividad en línea deben protegerse contra el robo de identidad, el acoso cibernético y otras amenazas.

## 9. Autenticación y seguridad:

La Identidad Digital también se relaciona con la autenticación en línea. Esto se refiere a la forma en que una persona demuestra ser quien dice ser al iniciar sesión en cuentas en línea. Esto puede incluir contraseñas, autenticación de dos factores y otras medidas de seguridad.

## 10. Gestión de la reputación en línea:

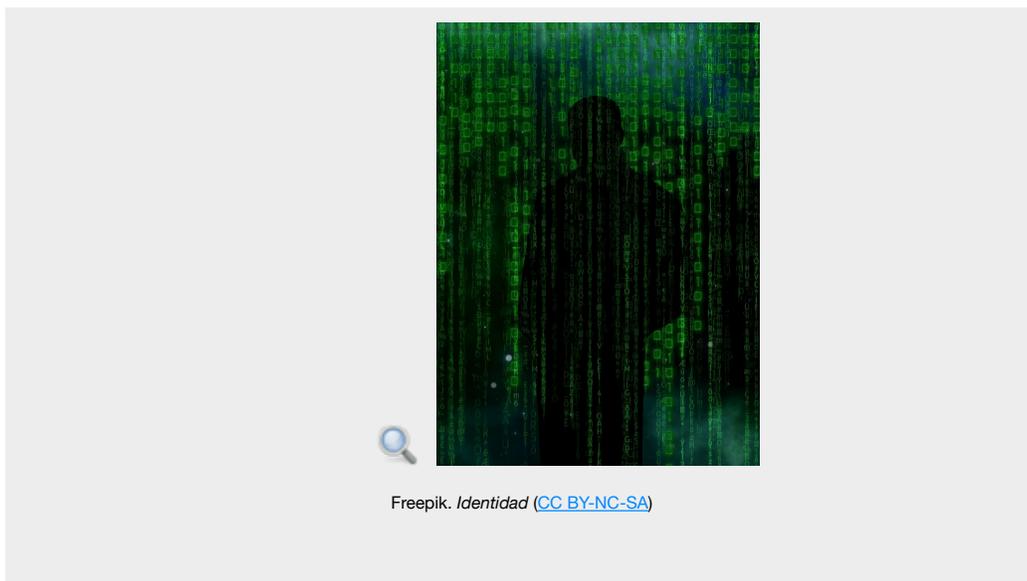
La gestión de la reputación en línea es el proceso de controlar y mantener una imagen positiva en línea. Las personas a menudo buscan mantener una reputación positiva en la web y eliminar o mitigar contenido negativo o perjudicial.



Freepik. *Gestión reputación línea* ([CC BY-NC-SA](#))

## 11. Continuidad de la identidad:

La Identidad Digital puede trascender la vida de una persona. Los datos y la información en línea pueden seguir existiendo mucho tiempo después de que una persona haya fallecido, lo que plantea cuestiones de privacidad y legales.



En resumen, la Identidad Digital es una parte integral de la vida moderna en línea. Cada vez más, nuestras actividades en la web contribuyen a la construcción y representación de nuestra identidad en el mundo digital. La gestión de la Identidad Digital es importante tanto para la privacidad como para la seguridad en línea, y se ha convertido en una parte fundamental de la vida en la era de la información y la tecnología.

En la siguiente tabla puedes ver ejemplos de Identidad Digital:

### Ejemplos de Identidad Digital

Aspecto de la Identidad Digital	Ejemplos
Información personal	Nombre, fecha de nacimiento, detalles de contacto.
Perfiles en redes sociales	Cuentas en Facebook, Instagram, LinkedIn.
Huella digital	Historial de navegación, búsquedas en Google.
Comunicación en línea	Emails, mensajes en redes sociales.
Actividades en línea	Compras, registro en foros.
Contenido compartido	Publicaciones en blogs, videos en YouTube.
Evaluación por terceros	Verificación de antecedentes por empleadores.
Privacidad y seguridad	Protección contra robo de identidad.
Autenticación y seguridad	Contraseñas, autenticación de dos factores.

Gestión de la reputación en línea	Control de la imagen en redes sociales.
Continuidad de la identidad	Datos en línea después del fallecimiento.



## Autoevaluación

¿Qué incluye la identidad digital de una persona?

- Solo la información personal como nombre y dirección.
- Solo los perfiles en redes sociales.
- Información personal, perfiles en redes sociales, huella digital y más.
- Solo las compras realizadas en línea.

Incorrecto

Incorrecto

La identidad digital abarca una amplia gama de aspectos, incluyendo información personal, perfiles en redes sociales, actividad en línea y contenido compartido. Es un reflejo completo de una persona en el ámbito digital.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

### ¿Qué es una huella digital?

- Un rastro físico dejado en dispositivos electrónicos.
- Las huellas de los dedos usadas para la autenticación.
- La actividad y los rastros que una persona deja en línea.
- La dirección IP de un usuario.

Incorrecto

Incorrecto

La huella digital incluye los sitios web visitados, las búsquedas, las publicaciones en redes sociales y otros rastros dejados en línea, formando una parte crucial de la identidad digital.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

### ¿Cómo pueden las empresas utilizar la identidad digital de una persona?

- Solo para enviar correos electrónicos publicitarios.
- Para evaluar la idoneidad de un candidato para un empleo.
- Para obtener acceso a las cuentas bancarias de una persona.
- Para realizar llamadas telefónicas automáticas.

Incorrecto

Las empresas pueden usar la identidad digital de una persona para verificar antecedentes, evaluar su reputación en línea y tomar decisiones informadas sobre contrataciones.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Qué aspecto de la identidad digital se relaciona con la protección contra el robo de identidad?**

- Gestión de la reputación en línea.
- Continuidad de la identidad.
- Autenticación y seguridad.
- Evaluación por terceros.

Incorrecto

Incorrecto

La autenticación y seguridad son fundamentales para proteger la identidad digital de una persona, asegurando que solo los usuarios autorizados puedan

acceder a sus cuentas y datos personales.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

### ¿Qué se entiende por "gestión de la reputación en línea"?

- Eliminar toda la información negativa de la web.
- Controlar y mantener una imagen positiva en línea.
- Crear perfiles falsos para mejorar la percepción pública.
- Ocultar toda la información personal en línea.

Incorrecto

La gestión de la reputación en línea implica cuidar cómo se percibe a una persona en el ámbito digital y tratar de mitigar cualquier contenido negativo o perjudicial que pueda afectar su imagen.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

### ¿Qué implica la "continuidad de la identidad" en el contexto digital?

- La transferencia de datos de una cuenta a otra.
- La existencia de datos e información en línea después de la muerte de una persona.
- La actualización continua de perfiles en redes sociales.
- La constante creación de nuevos contenidos en línea.

Incorrecto

La continuidad de la identidad digital plantea cuestiones sobre la gestión de datos y la privacidad, incluso después de la muerte de una persona, ya que la información en línea puede seguir existiendo indefinidamente. Estas preguntas ayudan a entender la amplitud y complejidad de la identidad digital,

Incorrecto

Incorrecto

## Solución

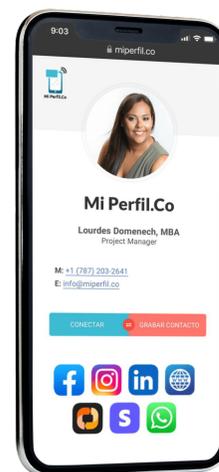
1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

## 4.- El Perfil Digital.

### ¿Qué es Perfil Digital?

Un perfil digital se refiere a la colección de información y datos personales que una persona u organización tiene en línea. Este perfil puede incluir una variedad de elementos, tales como:

1. **Información Personal:** Nombre, edad, ubicación, intereses y cualquier otra información demográfica que una persona pueda compartir en plataformas digitales.
2. **Actividad en Redes Sociales:** Publicaciones, comentarios, fotos, videos y otros contenidos compartidos en plataformas como Facebook, Instagram, Twitter, LinkedIn, entre otras.
3. **Historial de Navegación:** Datos sobre los sitios web visitados, búsquedas realizadas y actividades en línea, que pueden ser recopilados por empresas y servicios para personalizar la experiencia de usuario o con fines de publicidad.
4. **Información Profesional:** Datos relacionados con la carrera profesional, como experiencia laboral, habilidades, certificaciones y logros, comúnmente encontrados en perfiles de LinkedIn o en portafolios en línea.
5. **Preferencias y Hábitos de Consumo:** Información sobre compras en línea, preferencias de productos, servicios utilizados, etc.
6. **Interacciones en Línea:** Mensajes, correos electrónicos y otras formas de comunicación digital.



miperfilsite. Perfil Digital (CC BY-NC-SA)

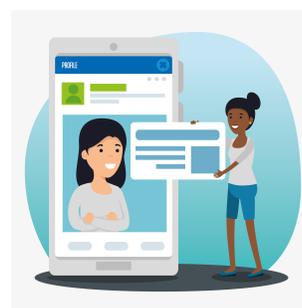
### ¿Es lo mismo identidad digital que perfil digital?

No, son conceptos diferentes.

El perfil digital y la identidad digital están estrechamente relacionados, pero se refieren a conceptos diferentes en el contexto de la presencia en línea:

#### Perfil Digital:

1. **Representación en línea:** Un perfil digital es una representación **específica** y a menudo **controlada por una persona, entidad o empresa en línea**. Puede incluir información personal, publicaciones, conexiones en redes sociales, contenido en sitios web y otros elementos que uno elige compartir o mostrar en línea.
2. **Enfoque más específico:** Un perfil digital tiende a centrarse en una plataforma o sitio web **en particular**. Por ejemplo, puedes tener un perfil digital en Facebook, otro en LinkedIn y otro en tu sitio web personal. Cada uno de estos perfiles digitales puede ser único y específico para su plataforma.



studiogstock. Perfil Digital (CC BY-NC-SA)

3. **Personalización:** Los perfiles digitales a menudo se pueden **personalizar y configurar** según las preferencias del usuario. Por ejemplo, puedes elegir qué información compartes en tu perfil de Facebook y qué contenido publicas en tu blog personal.

### Perfil digital versus Identidad digital

Perfil digital	Identidad digital
<p>Representación <b>específica y controlada</b> en línea en una plataforma particular, como una cuenta en una red social profesional (como linkedin) o un sitio web personal (como Instagram).</p>	<ul style="list-style-type: none"> <li>✔ La identidad digital es un concepto más <b>amplio y global</b> que engloba <b>todos los perfiles digitales y todas las actividades y rasgos</b> en línea de una persona.</li> <li>✔ Abarca <b>todas las actividades a lo largo del tiempo (presente y pasado) y en diversas plataformas.</b></li> </ul>



## Debes conocer

El perfil digital es creado a través de la **actividad en línea** y puede ser utilizado para diversas finalidades, como personalización de contenido, marketing dirigido, investigaciones de mercado o incluso en procesos de selección laboral. Es importante ser consciente de la cantidad de información personal que se comparte en línea, ya que esto puede tener implicaciones para la privacidad y seguridad personal.



## Ejercicio Resuelto

¿Cómo es el perfil digital de los tiktokers?

Mostrar retroalimentación

El perfil digital de un Tiktoker es esencial para atraer a una audiencia y construir una comunidad en la plataforma. La presentación, autenticidad y consistencia son importantes para establecer una marca personal sólida y atraer seguidores leales. Cada Tiktoker tiene su estilo y enfoque únicos, lo que se refleja en su perfil digital.

Aquí hay algunos de los componentes clave del perfil digital de un Tiktoker:



1. **Nombre de usuario:** Es el nombre con el que el Tiktoker se identifica en TikTok. A menudo, es único y refleja la personalidad o el tema del contenido.
2. **Biografía:** Una breve descripción o presentación del Tiktoker, que puede incluir información como su nombre, ubicación, intereses, enlaces a otras redes sociales y detalles relevantes.
3. **Foto de perfil:** Una imagen que representa al Tiktoker en la plataforma. La foto de perfil es una parte importante de la identidad digital y debe ser reconocible.
4. **Videos publicados:** El perfil digital muestra los videos que el Tiktoker ha publicado en su cuenta. Los seguidores pueden navegar por estos videos para ver su contenido anterior.
5. **Seguidores y seguidos:** El número de seguidores y las cuentas que el Tiktoker sigue se muestran en el perfil, lo que proporciona una idea de su popularidad y sus intereses.
6. **Interacción con otros usuarios:** Los comentarios y las interacciones del Tiktoker con otros usuarios, así como las respuestas a los comentarios en sus propios videos, también pueden estar visibles en el perfil.
7. **Enlaces a otras redes sociales:** Muchos Tiktokers enlazan sus perfiles de otras redes sociales, como Instagram, YouTube o Twitter, para que los seguidores puedan seguirlos en múltiples plataformas.
8. **Estadísticas y análisis:** TikTok proporciona estadísticas que muestran el número de me gusta, comentarios, compartidos y vistas que un Tiktoker ha recibido en sus videos. Esta información puede ayudar al Tiktoker a comprender su rendimiento en la plataforma.
9. **Pestañas y secciones específicas:** Los perfiles de TikTok a menudo incluyen pestañas o secciones específicas para organizar el contenido, como "Videos más populares" o "Listas de reproducción."
10. **Contenido destacado:** Algunos Tiktokers destacan videos específicos en su perfil para mostrar sus mejores trabajos o para resaltar ciertos temas.

## 4.1.- Tipos de Perfiles digitales.

---



Pixabay. Perfil Digital (CC BY-NC-SA)

Existen varios tipos de perfiles digitales, cada uno con un propósito específico y un conjunto de características distintas. A continuación, se presentan algunos de los tipos comunes de perfiles digitales:

### Tipos de Perfiles digitales.

---

<p><b>Perfil de Redes Sociales <u>Personal</u>:</b></p>	<p>Este es el tipo de perfil digital más común. Incluye perfiles en plataformas como Facebook, Twitter, Instagram, LinkedIn, entre otros, donde las personas comparten información personal, fotos, intereses y se conectan con amigos y contactos.</p> <div data-bbox="781 1413 1235 1675" data-label="Image"> </div> <p>Freepik. Redes sociales (CC BY-NC-SA)</p>
<p><b>Perfil de Redes Sociales <u>Profesional</u>:</b></p>	<p>Similar al perfil personal de redes sociales, pero se centra en la carrera y el  <u>networking</u> profesional. Ejemplos incluyen perfiles de LinkedIn, donde los usuarios resaltan su experiencia laboral, habilidades y logros.</p>

	 <p>Acaturnova. <i>Redes Sociales Profesionales</i> (<a href="#">CC BY-NC-SA</a>)</p>
<p><b>Perfil de Blog Personal:</b></p>	<p>Los blogueros crean perfiles digitales a través de sus blogs. Estos perfiles pueden incluir información sobre el autor, sus intereses y el contenido publicado en el blog.</p>
<p><b>Perfil de Plataformas de Contenido:</b></p>	<p>Los creadores de contenido en plataformas como YouTube, Instagram y TikTok tienen perfiles digitales donde comparten videos, fotos y otros contenidos relacionados con su especialidad.</p>
<p><b>Perfil de Empresa o Marca:</b></p>	<p>Las empresas y organizaciones crean perfiles digitales para promocionar sus productos, servicios y comunicarse con sus clientes en línea. Estos perfiles pueden incluir sitios web corporativos y perfiles en redes sociales.</p>
<p><b>Perfil de Juego en Línea:</b></p>	<p>Los jugadores que participan en juegos en línea suelen tener perfiles que muestran su progreso, logros y estadísticas en el juego.</p>  <p>Freepik. <i>Gamer</i> (<a href="#">CC BY-NC-SA</a>)</p>

<b>Perfil de Comprador en Línea:</b>	Los perfiles digitales en tiendas en línea almacenan información sobre las compras pasadas y las preferencias de los compradores.
<b>Perfil de Plataforma de Empleo:</b>	Los candidatos a empleo crean perfiles en sitios web de búsqueda de empleo para mostrar su experiencia laboral, habilidades y buscar oportunidades de trabajo.
<b>Perfil de Foro de Discusión:</b>	En los foros en línea, los usuarios tienen perfiles que muestran sus nombres de usuario, historial de actividad y participación en discusiones.
<b>Perfil de Aprendizaje en Línea:</b>	Los estudiantes pueden crear perfiles digitales en plataformas de aprendizaje en línea donde gestionan sus cursos, progreso y actividades educativas.
<b>Perfil de Correo Electrónico:</b>	Los servicios de correo electrónico permiten a los usuarios personalizar su información de perfil, incluyendo su nombre y firma.

Cada tipo de perfil digital tiene su propio propósito y audiencia específicos, y se utiliza para diferentes actividades en línea. La gestión de estos perfiles es importante para mantener una representación precisa y coherente en línea y para garantizar la privacidad y la seguridad en el entorno digital.



## Debes conocer

El **networking** es el proceso de establecer, desarrollar y mantener relaciones profesionales y personales con el fin de intercambiar información, recursos y apoyo, con el objetivo de avanzar en la carrera, encontrar oportunidades de negocio o colaboración, y mantenerse al día con las tendencias de la industria.

### Tipos de Networking con Definición y Ejemplos

Tipo de Networking	Definición	Ejemplos
<b>Operacional</b>	Relaciones para apoyo en tareas diarias.	Colaboración con otros departamentos.
<b>Estratégico</b>	Conexiones para perspectivas a largo plazo.	Asistencia a conferencias de la industria.
<b>Personal</b>	Contactos que ofrecen apoyo emocional.	Relaciones con amigos y familiares.

<b>En Línea</b>	Conexiones digitales a través de plataformas.	Uso de LinkedIn para expandir la red.
<b>Intraprofesional</b>	Interacción dentro de una profesión.	Participación en asociaciones profesionales.



## Autoevaluación

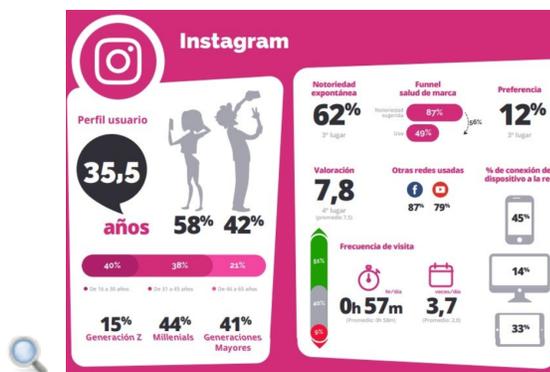
Rellenar huecos con las palabras adecuadas en cada caso.

1. Un [ ] de redes sociales personal incluye plataformas como Facebook, Instagram y Twitter, donde las personas comparten información personal y fotos.
2. Los perfiles en [ ] como LinkedIn se centran en la carrera y el networking profesional, resaltando la experiencia laboral, habilidades y logros.
3. Los blogueros crean perfiles digitales a través de sus [ ], donde pueden incluir información sobre el autor y sus intereses.
4. En plataformas como YouTube, Instagram y TikTok, los creadores de contenido tienen perfiles digitales para compartir [ ] y otros contenidos relacionados con su especialidad.
5. Las [ ] crean perfiles digitales para promocionar sus productos y servicios, y comunicarse con sus clientes en línea.
6. Los jugadores de [ ] suelen tener perfiles que muestran su progreso, logros y estadísticas en el juego.
7. Los perfiles digitales en tiendas en línea almacenan información sobre las compras pasadas y las [ ] de los compradores.
8. Los candidatos a empleo crean perfiles en sitios web de búsqueda de empleo para mostrar su [ ] laboral y habilidades.
9. En los [ ] en línea, los usuarios tienen perfiles que muestran sus nombres de usuario y participación en discusiones.
10. Los estudiantes pueden crear perfiles digitales en plataformas de [ ] en línea para gestionar sus cursos y progreso.
11. Los servicios de [ ] electrónico permiten a los usuarios personalizar su información de perfil, incluyendo su nombre y firma.
12. El [ ] es el proceso o habilidad que permite crear o ampliar una red de contactos profesionales y mantener esas conexiones para lograr beneficios a lo largo de una carrera laboral.

Enviar

## 4.2.- Perfiles en redes sociales

Los perfiles en redes sociales en el ámbito digital muestra un resumen de la representación en línea de individuos, organizaciones o entidades en plataformas de medios sociales.



Pixabay. Redes Sociales (CC BY-NC-SA)

Estos perfiles permiten a los usuarios crear una identidad virtual y participar en interacciones en línea con otras personas, compartir contenido, conectarse con amigos, colegas y seguidores, y estar al tanto de eventos, noticias y tendencias. Aquí se explora en detalle qué son y cómo funcionan los perfiles en redes sociales:

### ¿Cuales son los elementos clave de los perfiles en redes sociales?

#### 1. Información básica

Los perfiles en redes sociales suelen contener información básica sobre el usuario, como nombre, foto de perfil, género, fecha de nacimiento y ubicación. Esta información ayuda a otros usuarios a identificar y conectar con la persona.



**username**

**72 813** **9,6m** **45**  
posts followers following

Follow ▼

Pixabay. Perfil social (CC BY-NC-SA)

## 2. Foto de perfil

La foto de perfil es la imagen que representa al usuario en la plataforma. Puede ser una foto real de la persona o una imagen que el usuario elija como representación.

El tamaño ideal es 180 x 180 píxeles. La foto se verá en un móvil, por lo tanto será más pequeño todo.

### ¿Qué foto escoger si es una marca o personal?

En cuánto al tema de la foto, tenemos varias opciones:

- ✓ Si eres una **marca** lo más aconsejable es que se incluya el **logo**, así será mas reconocible.
- ✓ Si eres una **marca personal** hay dos opciones: **logo o foto**.

En este caso, si se usa una foto tuya, hazte unas fotos profesionales, que transmitan tu esencia. No se recomienda gafas de sol, de fotos de paisajes.

## 3. Nombre del perfil

En la mayoría de las redes sociales, los usuarios pueden proporcionar una breve descripción de sí mismos en su perfil. Esto a menudo incluye una biografía, intereses, ocupación y otros detalles personales.

El nombre de usuario trae de cabeza a muchas personas porque en muchas ocasiones el nombre de usuario que a ellos le gustaría poner está siendo utilizado ya por otro usuario o porque quieren transmitir información de su marca o de su actividad.

De hecho no se si os habéis fijado que últimamente muchos perfiles de influencers que se llamaban antes como el nombre de su blog, han cambiado al nombre de la persona real que gestiona el blog.

Lo ideal para mí es utilizar el **nombre de tu marca**.

**Límite 30 caracteres.** Consejos:

- ✔ Poner el nombre **de tu marca**.
- ✔ Utilizar una **palabra clave** que defina tu actividad. Instagram funciona con su buscador.
- ✔ Mezcla, combinación de marca personal y nombre.



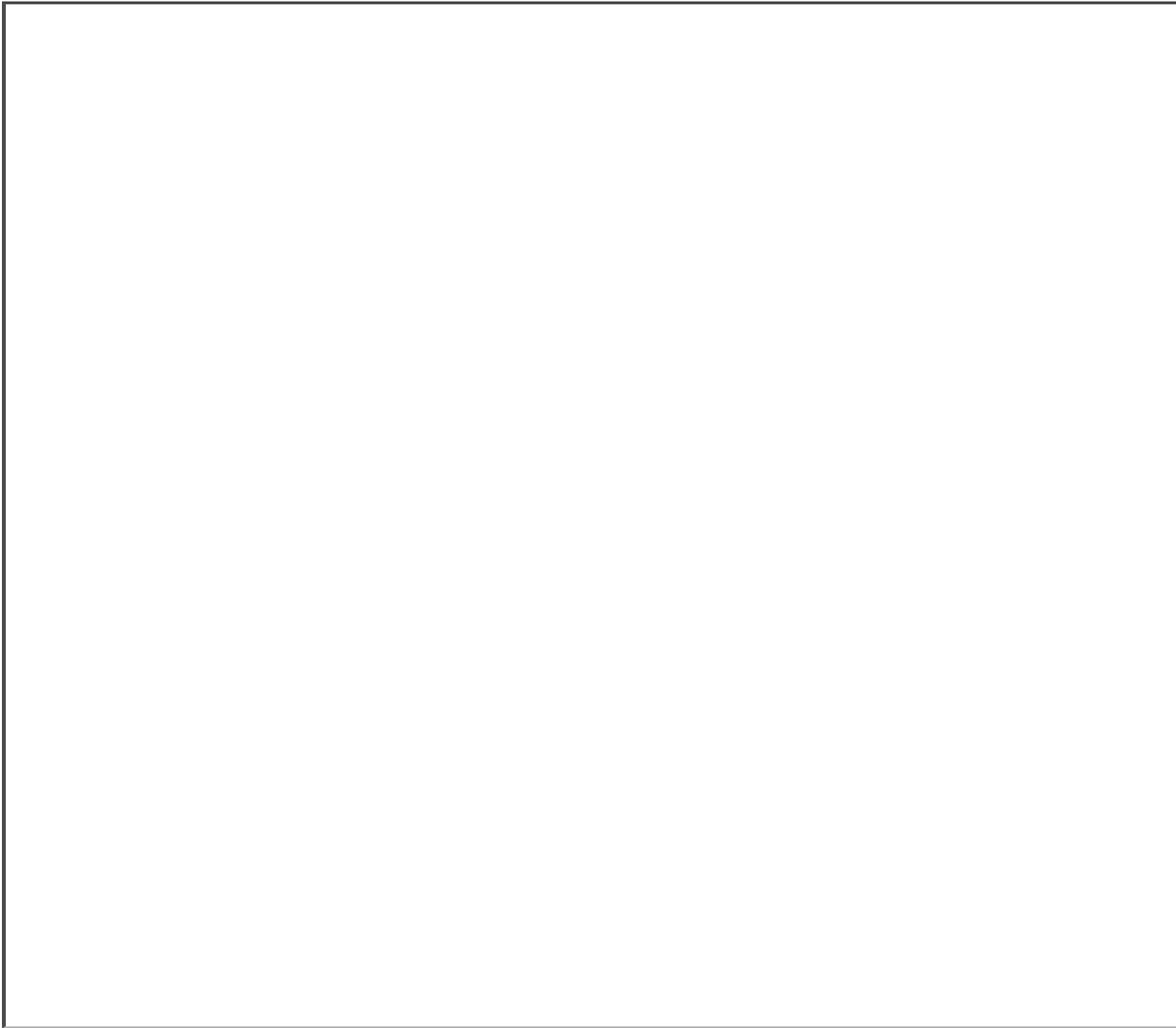
Acaturo Nova. Perfil Social (CC BY-NC-SA)

## 4. Biografía o descripción

En la mayoría de las redes sociales, los usuarios pueden proporcionar una breve descripción de sí mismos en su perfil. Esto a menudo incluye una biografía, intereses, ocupación y otros detalles personales.

**Límite 30 caracteres.** Consejos:

- ✔ Poner el nombre **de tu marca**.
- ✔ Utilizar una **palabra clave** que defina tu actividad. Instagram funciona con su buscador.



Acaturo Nova. Anatomía de un Perfil en Instagram ([CC BY-NC-SA](#))

## 5. Publicaciones y actividad

Los perfiles contienen una línea de tiempo o una sección de actividad donde se muestran las publicaciones y las interacciones del usuario, como comentarios, me gusta y compartidos. Esto refleja la actividad y la personalidad del usuario.

## 6. Conexiones y seguidores

Los perfiles en redes sociales permiten a los usuarios conectarse con otros usuarios, ya sea enviando solicitudes de amistad, siguiendo perfiles públicos o estableciendo conexiones de otro tipo. La cantidad de seguidores y seguidos a menudo se muestra en el perfil.

## 7. Galería de fotos y vídeos

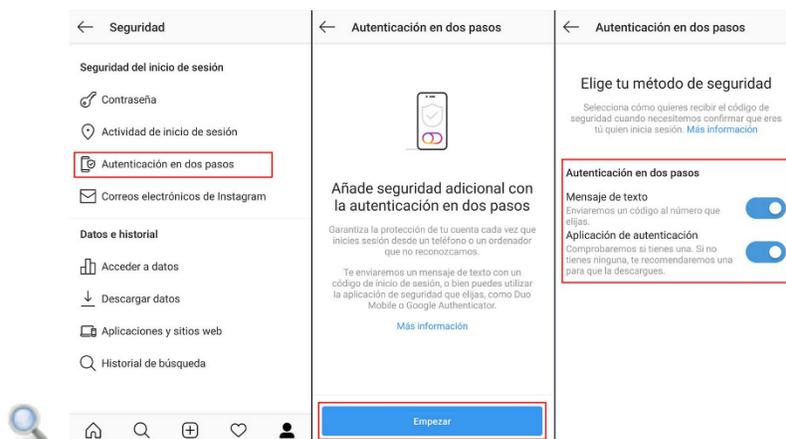
La mayoría de las plataformas de redes sociales permiten a los usuarios cargar y compartir fotos y videos en su perfil. Estos pueden ser imágenes personales, fotografías de eventos, videos caseros o contenido creativo.

## 8. Intereses y gustos

Los usuarios pueden indicar sus intereses, pasatiempos y gustos en su perfil. Esto facilita la conexión con otras personas que comparten intereses similares.

## 9. Privacidad y configuración

Los perfiles en redes sociales ofrecen opciones de privacidad para que los usuarios puedan controlar quién puede ver su contenido y quién puede interactuar con ellos. Esto es importante para mantener la seguridad en línea.



Acur Nova. Perfil social (CC BY-NC-SA)

En resumen, los perfiles en redes sociales en el ámbito digital son representaciones en línea de individuos y entidades que permiten la comunicación, la conexión y la interacción en un entorno virtual. Estos perfiles desempeñan un papel fundamental en la forma en que las personas se comunican, comparten contenido, establecen conexiones profesionales y personales, y participan en una variedad de actividades en línea.



## Reflexiona

¿Cuál es el propósito de la foto de perfil en una red social?

**Mostrar retroalimentación**

La foto de perfil sirve para representar visualmente al usuario en la plataforma. Puede ser una foto real de la persona, un logo de una marca, o una imagen que el usuario elija para representarse. Es importante para la identificación y la creación de una primera impresión.



## Reflexiona

**¿Qué se recomienda utilizar como nombre de perfil en las redes sociales?**

**Mostrar retroalimentación**

Se recomienda utilizar el nombre de la marca o una combinación de nombre personal y marca. Es importante que el nombre de perfil sea fácil de recordar y represente la identidad o la actividad del usuario, especialmente para fines de búsqueda y reconocimiento.



## Reflexiona

**¿Qué tipo de información se puede incluir en la biografía o descripción de un perfil de red social?**

**Mostrar retroalimentación**

En la biografía o descripción, los usuarios pueden incluir información sobre ellos mismos como su ocupación, intereses, pasatiempos, valores, y detalles relevantes sobre su marca o actividad profesional. Esto ayuda a otros usuarios a comprender mejor quiénes son y qué hacen.



## Reflexiona

**¿Qué opciones de privacidad suelen ofrecer los perfiles en redes sociales?**

Mostrar retroalimentación

Los perfiles en redes sociales suelen ofrecer opciones de privacidad que permiten a los usuarios controlar quién puede ver su contenido y quién puede interactuar con ellos. Estas configuraciones son importantes para proteger la seguridad y la privacidad en línea, permitiendo limitar la visibilidad a amigos, seguidores aprobados o al público en general.



## Autoevaluación

**¿Cuál de los siguientes elementos NO es típicamente parte de un perfil en redes sociales?**

- Foto de perfil
- Información básica
- Facturación y pagos
- Biografía o descripción

Incorrecto

Incorrecto

La facturación y pagos no suelen formar parte de un perfil de usuario en redes sociales, ya que estos perfiles se enfocan en la identidad, actividad y conexiones del usuario. La información básica, la foto de perfil y la biografía son elementos comunes que ayudan a otros usuarios a conocer más sobre la persona o entidad.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

**¿Qué se recomienda usar como foto de perfil para una marca en redes sociales?**

- Una foto de paisajes
- El logo de la marca
- Una imagen genérica
- Una caricatura

Incorrecto

Para una marca, lo más aconsejable es utilizar el logo como foto de perfil. Esto ayuda a establecer una identidad clara y reconocible, facilitando a los usuarios identificar y recordar la marca.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Cuál es el límite recomendado de caracteres para la biografía en redes sociales?**

- 10 caracteres
- 30 caracteres
- 100 caracteres
- 500 caracteres

Incorrecto

La biografía en redes sociales a menudo tiene un límite de 30 caracteres, lo cual obliga a los usuarios a ser concisos y claros al describirse. Es importante utilizar palabras clave relevantes que reflejen la identidad o la actividad del usuario.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Qué configuración de privacidad permite a un usuario limitar quién puede ver su contenido en redes sociales?**

- Público
- Amigos
- Personalizado
- Todos los anteriores

Incorrecto

Incorrecto

Incorrecto

Las plataformas de redes sociales suelen ofrecer varias opciones de privacidad, como "Público", "Amigos" y "Personalizado". Estas opciones permiten a los usuarios controlar quién puede ver su contenido, desde el público en general hasta un grupo específico de personas.

## Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

**¿Cuál de los siguientes es un propósito principal de los perfiles en redes sociales?**

- Realizar transacciones bancarias
- Compartir y conectar con otros
- Gestionar propiedades inmobiliarias
- Jugar videojuegos

Incorrecto

Los perfiles en redes sociales están diseñados principalmente para que los usuarios compartan contenido y se conecten con amigos, colegas y seguidores. Estas plataformas facilitan la comunicación y la interacción en un entorno virtual, permitiendo a los usuarios mantenerse informados y conectados.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

## 4.3.- Generación XYZ.

---

La identidad digital y el perfil digital está relacionado con la generación a la que pertenezcas.

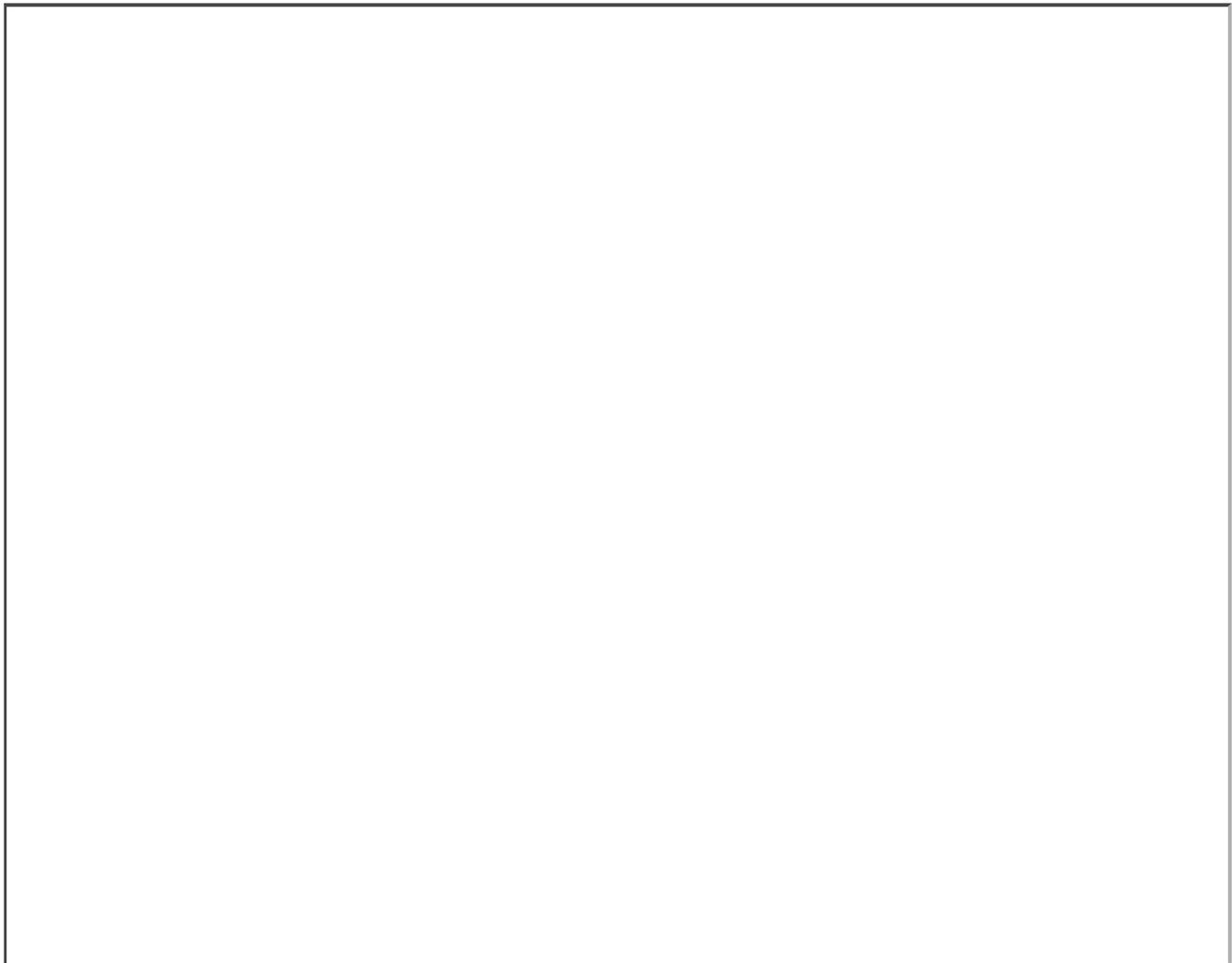
### ¿Qué es la Generación XYZ?

- ✓ **Generación X:** Los miembros de esta generación nacieron generalmente entre mediados de la década de 1960 y principios de la de 1980.
- ✓ **Generación Y (Millennials):** Si bien no hay un consenso claro sobre las fechas de inicio y finalización de esta generación, generalmente se considera que los Millennials nacieron entre principios de la década de 1980 y mediados de la de 1990.
- ✓ **Generación Z:** Esta generación sigue a los Millennials y generalmente se considera que nació a partir de mediados de la década de 1990 hasta principios de la de 2010.

### ¿Cuáles son las características de la Generación XYZ?

- ✓ **Tecnología:** Las generaciones XYZ han crecido en la era digital y tienen una fuerte familiaridad con la tecnología y las redes sociales. Los Millennials, en particular, son conocidos por su uso prolífico de las redes sociales y su adopción temprana de la tecnología móvil.
- ✓ **Valores:** Las generaciones XYZ suelen valorar la flexibilidad en el trabajo, la diversidad, la sostenibilidad y la autorrealización. Los Millennials, en particular, a menudo buscan un equilibrio entre el trabajo y la vida personal.
- ✓ **Cambio social:** Estas generaciones han sido testigos de avances significativos en derechos civiles, tecnología, medio ambiente y otras áreas. Han participado activamente en movimientos sociales y políticos.

En la siguiente presentación se puede ver un resumen de los principales conceptos de la Generación XYZ y Baby boomers:



Acatúr Nova. Generación XYZ ([CC BY-NC-SA](#))



## Reflexiona

**¿Cómo influyen las diferencias generacionales (Generación X, Millennials, Generación Z) en la manera en que cada grupo maneja su identidad digital y perfil en redes sociales?**

Mostrar retroalimentación

Las diferencias generacionales influyen significativamente en la forma en que cada grupo maneja su identidad digital y perfil en redes sociales debido a las distintas experiencias tecnológicas y culturales que han vivido.

## Generación X

La **Generación X**, que creció antes del auge de la era digital, generalmente adoptó la tecnología digital en su adultez. Aunque son competentes con la tecnología, tienden a ser más cautelosos y reservados en sus interacciones en línea. A menudo, prefieren mantener sus perfiles más privados y pueden utilizar redes sociales principalmente para conectarse con amigos y familiares cercanos, así como para mantenerse informados sobre eventos importantes.

## Millennials

Los **Millennials**, por otro lado, han sido testigos de la transición al mundo digital y han adoptado la tecnología móvil y las redes sociales como una parte integral de su vida diaria. Son más propensos a compartir detalles de su vida personal en línea y a utilizar las redes sociales como una herramienta para expresar sus identidades, conectar con una amplia red de amigos y colegas, y seguir las últimas tendencias y noticias. Valoran la autenticidad y la transparencia en línea, y buscan un equilibrio entre su vida laboral y personal a través de plataformas digitales.

## Generación Z

La **Generación Z**, nativa digital, ha crecido con smartphones y acceso constante a Internet. Este grupo es extremadamente fluido en el uso de tecnologías digitales y tiende a utilizar múltiples plataformas de redes sociales para diferentes propósitos, como entretenimiento, activismo, aprendizaje y comunicación. Son conocidos por su creatividad en la creación de contenido y su comodidad al compartir sus opiniones y experiencias en línea. Además, esta generación está altamente consciente de la privacidad y la seguridad digital, a menudo utilizando configuraciones de privacidad estrictas y siendo selectiva con la información que comparten.

En resumen, mientras que todas las generaciones usan redes sociales y manejan su identidad digital, las maneras en que lo hacen reflejan sus experiencias únicas con la tecnología. La Generación X es más privada, los Millennials buscan autenticidad y equilibrio, y la Generación Z combina creatividad y precaución con un dominio natural del entorno digital. Estas

diferencias subrayan la importancia de entender el contexto generacional al diseñar estrategias de comunicación y marketing digital.



## Autoevaluación

¿Es verdadero o falso?

**La identidad digital y el perfil digital de una persona están influenciados por la generación a la que pertenece.**

Verdadero  Falso

### Verdadero

Las generaciones como la X, Y (Millennials) y Z han crecido en diferentes contextos tecnológicos y sociales, lo que influye en cómo interactúan con la tecnología y construyen sus identidades digitales. Por ejemplo, los Millennials y la Generación Z son más propensos a utilizar redes sociales y a adoptar nuevas tecnologías rápidamente.

**Los miembros de la Generación X suelen tener la misma facilidad para usar redes sociales y tecnología móvil que los Millennials.**

Verdadero  Falso

### Falso

Aunque la Generación X tiene un alto nivel de familiaridad con la tecnología, los Millennials y la Generación Z tienden a estar más integrados en el uso diario de redes sociales y tecnología móvil debido a su exposición desde una edad temprana. Las diferencias en el uso y adopción de la tecnología pueden estar relacionadas con las experiencias formativas de cada generación.

**Los Millennials valoran la flexibilidad en el trabajo y buscan un equilibrio entre la vida laboral y personal.**

Verdadero  Falso

### Verdadero

Una de las características destacadas de los Millennials es su preferencia por ambientes de trabajo flexibles y un fuerte deseo de equilibrar su vida laboral y personal. Esta generación valora la autonomía y la autorrealización,

y a menudo busca empleos que les permitan mantener un buen equilibrio entre ambos aspectos.

**La Generación Z, a diferencia de las generaciones anteriores, no se involucra en movimientos sociales y políticos.**

Verdadero  Falso

**Falso**

La Generación Z es conocida por su activa participación en movimientos sociales y políticos. Al igual que los Millennials, esta generación está muy comprometida con temas como la justicia social, el medio ambiente y los derechos civiles, y a menudo utiliza plataformas digitales para movilizarse y expresar sus opiniones.

**Las generaciones XYZ han crecido completamente en la era digital, sin ningún conocimiento de tecnologías analógicas.**

Verdadero  Falso

**Falso**

Mientras que la Generación Z ha crecido predominantemente en la era digital, los miembros de la Generación X y algunos de los primeros Millennials tienen experiencia con tecnologías analógicas. La transición de lo analógico a lo digital ha sido un proceso gradual, y muchas personas de estas generaciones tienen conocimientos en ambos tipos de tecnologías.

## 5.- ¿Qué es información personal y no personal?

### ¿Qué es **información personal**?

La información personal, también conocida como información personal identificable (IPI) o datos personales, se refiere a cualquier detalle o dato que pueda utilizarse para identificar, contactar o ubicar a una persona específica.

Estos datos personales suelen ser privados y están relacionados con la identidad de un individuo. La información personal puede incluir, pero no se limita a:

1. **Nombre completo:** El nombre completo de una persona, incluyendo el nombre y los apellidos.
2. **Fecha de nacimiento:** La fecha en la que una persona nació.
3. **Número de documento de identificación:** Números como el número de pasaporte, el número de seguro social, el número de identificación nacional u otros documentos de identificación emitidos por el gobierno.
4. **Dirección postal:** La dirección física donde una persona reside o recibe correspondencia.
5. **Número de teléfono:** Números de teléfono, ya sea fijo o móvil, que permiten la comunicación con la persona.
6. **Dirección de correo electrónico:** Las direcciones de correo electrónico utilizadas para comunicarse en línea.
7. **Número de tarjeta de crédito o débito:** Los números de tarjeta de crédito o débito utilizados para realizar pagos en línea o transacciones financieras.
8. **Información financiera:** Datos sobre ingresos, cuentas bancarias, historial crediticio y otros detalles financieros personales.
9. **Género:** La identificación de género de una persona (masculino, femenino, no binario, etc.).
10. **Estado civil:** Información sobre el estado civil de una persona, como soltero, casado, divorciado, etc.
11. **Información de salud:** Datos sobre la salud de una persona, como historial médico, alergias, condiciones médicas, etc.
12. **Datos biométricos:** Datos únicos relacionados con las características físicas o fisiológicas de una persona, como huellas dactilares, reconocimiento facial o ADN.



Freepik. Passports (CC BY-NC-SA)

### ¿Qué es **información NO personal**?

A continuación, se presentan ejemplos de lo que generalmente no se considera información personal:

1.

**Información anónima o desidentificada:** Los datos que se han despojado de cualquier conexión directa con una persona y que no pueden utilizarse para identificar a alguien se consideran no personales. Por ejemplo, datos agregados de usuarios en un sitio web.



Pixabay. Información no personal. (CC BY-NC-SA)

2. **Información pública:** La información que se encuentra disponible públicamente y que la persona ha compartido intencionalmente, como su nombre en una lista de miembros de una organización o detalles de contacto en un directorio empresarial, por lo general no se considera información personal.

3. **Información empresarial:** Los datos relacionados con una entidad comercial o una organización, en lugar de una persona individual, se consideran información no personal. Esto incluye datos sobre empresas, como nombres comerciales, direcciones de correo electrónico empresariales y números de teléfono de contacto de la empresa.

4. **Información estadística o demográfica:** Datos relacionados con estadísticas o características demográficas generales, como la edad promedio de los usuarios de un sitio web o el número de personas en una determinada área geográfica, generalmente no se consideran información personal.

5. **Datos que no se pueden utilizar para identificar a una persona:** Si los datos no contienen elementos que permitan la identificación de una persona, como nombres, direcciones, números de identificación o referencias personales, se consideran no personales. Por ejemplo, un registro de temperatura en una ciudad sin ninguna conexión a individuos específicos.



## Autoevaluación

**Los datos identificativos de una empresa es una información:**

- Personal.
- No personal.

Incorrecto

Opción correcta

## Solución

1. Incorrecto
2. Opción correcta

**El estado civil de una persona es una información:**

- Personal.
- No personal.

Opción correcta

Incorrecto

## Solución

1. Opción correcta
2. Incorrecto

**El DNI es una información:**

- Personal
- No personal.

Opción correcta

Incorrecto

## Solución

1. Opción correcta
2. Incorrecto

**Las aficiones de una persona es una información:**

- Personal
- No personal.

Incorrecto

Opción correcta

## Solución

1. Incorrecto
2. Opción correcta

# 6.- La gestión de la Identidad Digital en entornos educativos de Formación Profesional.

## ¿Cuáles son buenas prácticas en la gestión de la Identidad Digital en el ámbito educativo de Formación Profesional?

La gestión de la Identidad Digital en entornos educativos es crucial para fomentar un entorno seguro y constructivo. Aquí tienes algunos ejemplos de buenas prácticas en la gestión de la Identidad Digital en el ámbito educativo de Formación Profesional:

- 1. Educación en Ciudadanía Digital:** Introducir programas de educación en ciudadanía digital que ayuden a los estudiantes a comprender los conceptos de privacidad en línea, seguridad y respeto en internet. Esto puede incluir lecciones sobre el manejo de contraseñas, la prevención del ciberacoso y la identificación de fuentes de información confiables en línea.
- 2. Promoción de la Privacidad:** Enseñar a los estudiantes la importancia de configurar las opciones de privacidad en sus perfiles en redes sociales y otras plataformas en línea. Animarlos a revisar y ajustar regularmente su configuración de privacidad para controlar qué información es pública y quién puede acceder a ella.
- 3. Creación de  Portafolios Digitales:** Fomentar la creación de portafolios digitales en los que los estudiantes puedan mostrar su trabajo, logros y habilidades. Ayudarlos a construir perfiles digitales profesionales que reflejen sus capacidades y logros académicos.

El portafolio según sea de carácter privado (confidencial), de aprendizaje (público, abierto a todo el mundo) y continuo (público pero restringido). Con Google Sites, Edublogs, Evernote, Canva, Flipped Classroom, WordPress o en el propio Moodle podrás ser el creador y diseñador de un portafolio de una manera sencilla.

- 4. Fomentar la Responsabilidad en Línea:** Enseñar a los estudiantes a ser responsables de sus acciones en línea. Esto incluye promover la importancia de citar adecuadamente las fuentes en línea, respetar los derechos de autor y evitar el plagio.
- 5.  Monitoreo y Supervisión:** Los educadores y padres pueden monitorear y supervisar las actividades en línea de los estudiantes, especialmente en entornos más jóvenes, para garantizar su seguridad y orientarlos en la toma de decisiones adecuadas en línea.

- 6. Promoción de Comportamiento Ético:** Fomentar un comportamiento ético en línea, incluyendo el respeto por los demás, la tolerancia y la empatía. Esto puede incluir discusiones en clase sobre el ciberacoso y la importancia de tratar a los demás con cortesía



Freepik. Hacker (CC BY-NC-SA)



Pixabay. Monitoreo (CC BY-NC-SA)

en línea.

7. **Incentivar la Creación de Contenido Positivo:** Animar a los estudiantes a contribuir de manera positiva en línea, ya sea compartiendo contenido educativo, participando en discusiones constructivas o promoviendo causas sociales.
8. **Enseñar Autenticidad:** Ayudar a los estudiantes a comprender la importancia de ser auténticos en línea y no falsificar identidades. Destacar la necesidad de evitar la creación de perfiles falsos o la difusión de información engañosa.
9. **Respeto por la  Diversidad:** Fomentar el respeto por la diversidad en línea y la apreciación de diferentes perspectivas y culturas. Enseñar a los estudiantes a ser críticos con el contenido en línea y a evitar la difusión de discursos de odio.
10. **Mantener una Comunicación Abierta:** Establecer una comunicación abierta entre estudiantes, educadores y padres para abordar cualquier problema relacionado con la Identidad Digital y la seguridad en línea. Los estudiantes deben sentirse cómodos al informar sobre situaciones de acoso o amenazas en línea.



Redes. istockphoto (CC BY-NC-SA)



## Debes conocer

Estas buenas prácticas pueden ayudar a crear un entorno educativo en línea más seguro y positivo, donde los estudiantes puedan desarrollar habilidades de gestión de su Identidad Digital y ciudadanía digital.



## Para saber más

En el siguiente enlace se puede ver Canvas con plantilla gratuitas:

 [Canvas](#)

Experiencia con Porfolio en Moodle:

 [Experiencia con Porfolio en Moodle](#)



## Autoevaluación

**¿Qué es una práctica recomendada para fomentar la seguridad en línea en estudiantes de formación profesional?**

- Compartir contraseñas con amigos de confianza
- Configurar y revisar regularmente las opciones de privacidad en redes sociales
- Publicar toda la información personal para ser fácilmente identificable
- Utilizar siempre perfiles anónimos para proteger la identidad

Incorrecto

Revisar y ajustar las opciones de privacidad es esencial para controlar quién puede acceder a la información personal en línea. Esto ayuda a proteger la seguridad de los estudiantes y su información personal, evitando que esta sea accesible a personas no autorizadas.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Cuál de las siguientes opciones es una buena práctica para la creación de portafolios digitales en educación?**

- Publicar documentos sin citas o referencias adecuadas
- Crear perfiles digitales que reflejen las habilidades y logros académicos
- Evitar mostrar trabajos o proyectos realizados
- No utilizar ninguna plataforma en línea para la creación de portafolios

Incorrecto

Fomentar la creación de portafolios digitales permite a los estudiantes mostrar sus habilidades, logros y proyectos de manera profesional. Es una excelente manera de construir una presencia en línea que refleje su desarrollo académico y profesional.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Cuál es una práctica positiva que se debe incentivar entre los estudiantes en el ámbito digital?**

- Compartir contenido que promueva el odio o la discriminación
- Contribuir con contenido educativo y participar en discusiones constructivas

- Crear perfiles para suplantar a otras personas
- Mantener sus opiniones en línea privadas para evitar conflictos

Incorrecto

Incentivar la creación de contenido positivo y la participación en discusiones constructivas en línea ayuda a los estudiantes a contribuir de manera valiosa a la comunidad digital. Fomentar estas prácticas promueve un entorno en línea más saludable y educativo.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

## 7.- ¿Cómo deben proteger las empresas la información personal?

### ¿Cómo deben proteger las entidades la información personal de sus usuarios?

Existen muchas leyes de protección de datos que limitan la cantidad de información personal que puede contener una entidad como una entidad educativa de Formación Profesional. Si una entidad necesita la recopilación o acumulación de información personal para funcionar, debe tomar las precauciones suficientes para mantener esos datos seguros y privados.

Entre algunas de las medidas más importantes para proteger la información personal se incluyen:

- ✓ **Limitar la recopilación y retención de datos.** Los datos no deben conservarse más tiempo del necesario, ya que cuantos más datos posea una empresa, mayor será el impacto potencial de una fuga de datos.
- ✓ **Asegurar los datos frente a posibles fugas.** Una de las tecnologías más importantes para asegurar los datos es la  encriptación; las organizaciones también pueden tomar otras medidas para proteger sus sistemas, desde el uso de  Firewall hasta el uso de  puertas de enlace web seguras.
- ✓ **Limitar el acceso interno con control de acceso.** El control de acceso garantiza que solo las partes autorizadas accedan a los sistemas y datos. El acceso no autorizado puede dar lugar a una fuga de datos o  vulneración de la privacidad.
- ✓ **Dar prioridad a la privacidad.** Las empresas deben incorporar la seguridad y la privacidad en sus servicios, tanto para evitar incumplir la normativa sobre privacidad como para proteger a sus clientes.
- ✓ Tener un **protocolo seguro de archivo de datos** con limitaciones y permisos de acceso a otros usuarios.



### Idoneidad de mantener la información personal y profesional por separado.

La causa principal por la que es necesario mantener la **información personal y la profesional** por separado se debe a que cada una de ellas tienen unos objetivos muy diferentes.

Los perfiles con información personal deben estar **restringidos** a un ámbito familiar y de amistades cercanas, evitando de esta manera todos los posibles problemas

que se pueden dar cuando la información sensible del usuario pasa de un entorno privado a uno público. Por el contrario, los perfiles con información profesional tienen el objetivo de alcanzar la mayor difusión posible y dar a conocer las destrezas y logros profesionales de una determinada persona.



Freepik. Redes Sociales (CC BY-NC-SA)



## Autoevaluación

¿Qué se entiende por "información personal" o "datos personales" en el contexto del texto?

- Cualquier información relacionada con una persona concreta.

-----

- Información relacionada con una persona concreta, excepto su historial médico.

-----

- Solo información identificativa, como nombre y dirección.

-----

Mostrar retroalimentación

## Solución

1. Correcto
2. Incorrecto
3. Incorrecto

¿Cuál es uno de los principales aspectos de la ciudadanía digital mencionados en el texto?

- La recopilación de datos personales.

- El comportamiento ético y responsable en línea.

- El uso de contraseñas seguras.

Mostrar retroalimentación

## Solución

1. Incorrecto
2. Correcto
3. Incorrecto

¿Cuál es una de las medidas clave que las empresas deben tomar para proteger la información personal según el texto?

- Limitar la recopilación y retención de datos.

- Utilizar solo sitios web HTTP en lugar de HTTPS.

- Compartir información con terceros sin consentimiento.

Mostrar retroalimentación

## Solución

1. Correcto
2. Incorrecto
3. Incorrecto

¿Qué es el "Warrant canary" mencionado en el texto?

- Una medida de seguridad para proteger datos en línea.

- Un indicador de cambio en las políticas de intercambio de información con entidades gubernamentales.

- Un tipo de autenticación de dos factores.

Mostrar retroalimentación

## Solución

1. Incorrecto
2. Correcto
3. Incorrecto

**¿Por qué se sugiere a las personas utilizar un solucionador de DNS centrado en la privacidad?**

- Para bloquear todas las cookies innecesarias.

- Para mantener su historial de navegación protegido de miradas indiscretas.

- Para garantizar la encriptación de extremo a extremo en las comunicaciones.

Mostrar retroalimentación

## Solución

1. Incorrecto
2. Correcto
3. Incorrecto

## 8.- Normativa que regula los derechos personales y digitales en la red.

La protección de la información personal es importante para garantizar la privacidad y la seguridad de las personas. Las regulaciones de privacidad, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y leyes de privacidad similares en otras regiones, establecen **pautas y requerimientos para la recopilación, el almacenamiento y el uso de información personal** por parte de organizaciones y empresas.

Estas leyes buscan **garantizar que los datos personales** se manejen de manera adecuada y segura, y que las personas tengan control sobre su información personal.



Freepik. Vista lateral de la mujer con casco de realidad virtual (CC BY-NC-SA)

### ¿Qué ley regula los derechos personales y digitales en la red?

La **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD)** es la normativa que adapta la legislación española al Reglamento Europeo de Protección de Datos (RGPD) y deroga la anterior LOPD de 1999.

### Aspectos Claves de los derechos personales y digitales en red

Aspectos Claves	Ejemplos
<b>Privacidad y Seguridad de Datos</b>	Uso de encriptación para proteger datos personales almacenados.
<b>Regulaciones de Privacidad</b>	Cumplimiento del RGPD en la UE para proteger la información personal.
<b>Derechos de los Individuos</b>	Derecho al acceso y rectificación de datos personales inexactos.
<b>Responsabilidad de las Organizaciones</b>	Implementación de políticas de privacidad y seguridad de datos.
<b>Notificación de Brechas de Seguridad</b>	Aviso a autoridades y afectados tras un hackeo de datos.
<b>Control y Autonomía de los Datos</b>	Derecho a retirar el consentimiento para el uso de datos personales.

**LOPDGDD**

Ley española que adapta la legislación al RGPD europeo.

**Debes conocer**

En el siguiente enlace puedes ver la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

 [Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.](#)

## 9.- ¿Qué formas tienen las personas puede proteger su información personal?

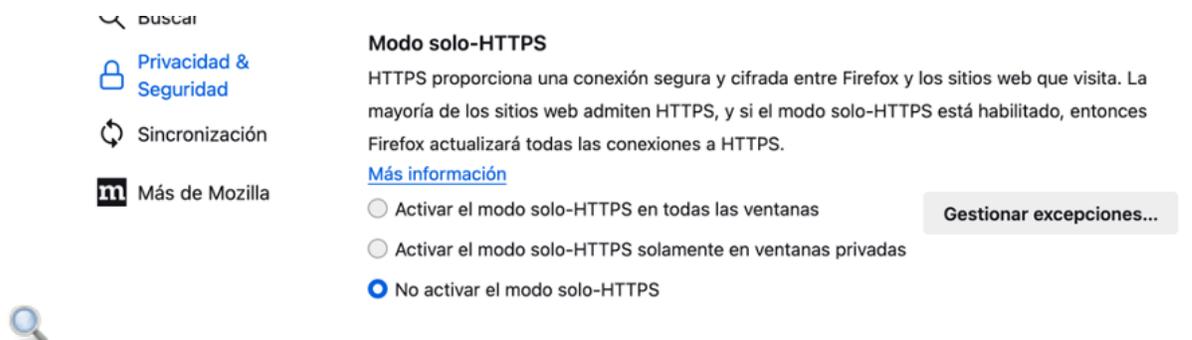
### ¿Qué formas tienen las personas puede proteger su información personal?

Hay varias medidas que las personas pueden tomar para asegurarse de que su información permanezca tan segura y privada como sea posible.



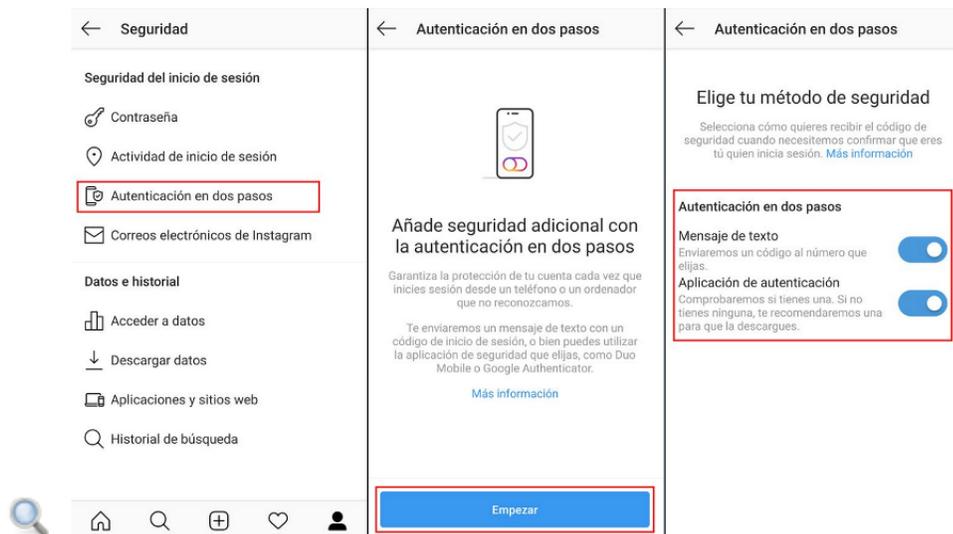
Freepik. Proteger información (CC BY-NC-SA)

- ✓ **Utilizar solo sitios web** 📁 **HTTPS:** Asegurarse de que las conexiones sean seguras, protegiendo la información transmitida. Evitar los sitios web que no utilicen la 📁 **encriptación TLS** para proteger los datos que entran y salen de sus servidores. Estos sitios web utilizan 📁 **HTTP** en lugar de HTTPS.



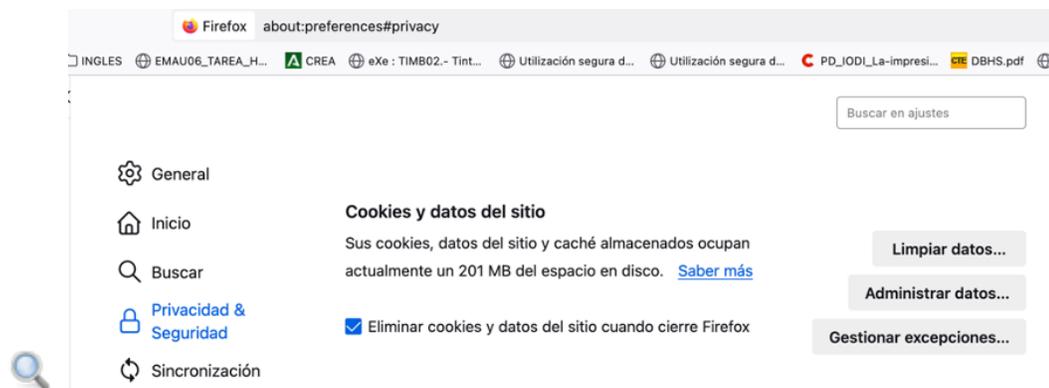
Acaturo Nova. HTTPS (CC BY-NC-SA)

- ✓ **Usar contraseñas seguras y** 📁 **autenticación de dos factores (2FA):** Crear 📁 **contraseñas robustas** combinando letras, números y símbolos, y activar la autenticación de dos factores (2FA) para una capa extra de seguridad. Los usuarios deben evitar reutilizar contraseñas o usar contraseñas débiles que puedan ser adivinadas con facilidad. Además, la 2FA hace que las cuentas en línea sean mucho más seguras.



Acaturnova. 2FA (CC BY-NC-SA)

- ✔ **Controlar el uso de cookies:** Gestionar y limitar las cookies en el navegador para proteger la privacidad. Algunas cookies del navegador son necesarias para que los sitios web funcionen correctamente, pero bloquear las cookies innecesarias, siempre que sea posible, ayuda a limitar el número de terceros que rastrean las actividades en línea de una persona. En la siguiente imagen puedes ver un ejemplo de cómo configurar las Cookies en el Navegador (Mozilla Firefox):



Acaturnova. Cookies (CC BY-NC-SA)

- ✔ **Usar un DNS seguro y centrado en la privacidad:** Optar por servicios DNS que prioricen la protección de datos personales. Los solucionadores de DNS a veces rastrean los dominios que visita una persona, a menudo para vender esta información a los anunciantes. En la siguiente imagen puedes ver un ejemplo de cómo configurar en el Navegador (Mozilla Firefox) el DNS:

## DNS sobre HTTPS

El sistema de nombres de dominio (DNS) sobre HTTPS envía los pedidos de un nombre de dominio a través de una conexión cifrada, lo que crea un DNS seguro y hace más difícil que otros vean que sitio web está tratando de acceder.

[Saber más](#)

Estado: Desactivado [Saber más](#)

Firefox no usará DNS seguro en estos sitios

[Administrar excepciones...](#)

### Activar DNS seguro usando:

#### Protección predeterminada

Firefox decide cuándo usar DNS seguro para proteger su privacidad.

- Usar DNS seguro en regiones donde esté disponible
- Use la resolución de DNS predeterminada si hay un problema con el proveedor de DNS seguro
- Usar un proveedor local si es posible [Saber más](#)
- Desactivar cuando una VPN, control parental o políticas de empresa estén activas
- Desactivar cuando una red le diga a Firefox que no debería usar DNS seguro [Saber más](#)

#### Protección aumentada

Usted controla cuándo usar DNS seguro y elige su proveedor.

#### Protección máxima

Firefox siempre usará DNS seguro. Se verá una advertencia de riesgo de seguridad antes de que usemos el DNS del sistema.

#### Desactivado

Usar la resolución de DNS predeterminada



Acaturo Nova. *DNS sobre HTTPS* (CC BY-NC-SA)

- ✓ **Utilizar la  encriptación de un extremo a otro:** Garantizar que solo los destinatarios autorizados puedan acceder a las comunicaciones. La encriptación de un extremo a otro garantiza que los mensajes permanezcan privados para todos, incluido el servicio de mensajería. Más información sobre la encriptación de un extremo a otro.
  - Ejemplo: El [cifrado de extremo a extremo de WhatsApp](#) se usa cuando chateas con otra persona a través de WhatsApp Messenger. Este cifrado garantiza que solo tú y la persona con quien te comuniqués puedan leer o escuchar lo que se envía, y que nadie más, ni siquiera WhatsApp, pueda hacerlo.
- ✓ **Revisar las Condiciones del servicio y la política de privacidad: Leer y entender los términos antes de usar cualquier servicio en línea:** Leer y entender los términos antes de usar cualquier servicio en línea. Las condiciones del servicio y su política son importantes para entender cuánta información personal recopila un sitio web o una aplicación, y qué ocurre con esa información personal.
- ✓ **Renunciar a compartir la información personal con terceros:** Limitar la divulgación de datos personales a empresas y servicios en todo tipo de redes sociales en Internet.

- ✓ **Busca los  Warrant canary** (literalmente canario garante o canario de seguridad): Verificar la existencia de alertas que indiquen acceso gubernamental a datos. Comprobar los Warrant carries de un servicio para ver si han cambiado sus políticas sobre el intercambio de información con entidades gubernamentales. En la actualidad describe un método mediante el cual un proveedor de servicios de Internet intenta informar a sus usuarios de que ha sido citado en secreto o requerido mediante orden gubernativa de los Estados Unidos.
- ✓ **Hacer copias de seguridad:** Realizar respaldos regulares de información importante en lugares seguros.
- ✓ **Mantener software actualizado:** Instalar siempre las últimas versiones de sistemas operativos y aplicaciones para evitar vulnerabilidades.

En la siguiente tabla puedes ver un resumen con ejemplos de las recomendaciones para Proteger la Información Personal en Internet:

### Recomendaciones Mejoradas para Proteger la Información Personal

Recomendación	Descripción	Ejemplos	Consejo Adicional
<b>Usar contraseñas seguras y 2FA</b>	Crear contraseñas únicas y complejas que combinan letras, números y símbolos. Utilizar autenticación de dos factores para añadir una capa adicional de seguridad.	Contraseña: R8&nY\$7z!2bQ; 2FA: Usar <a href="#">Google Authenticator</a> o <a href="#">Authy</a> .	No reutilizar contraseñas en diferentes sitios web y utilizar un gestor de contraseñas para mantenerlas organizadas.
<b>Utilizar solo sitios web HTTPS</b>	Verificar que los sitios web tengan un  certificado SSL/TLS, indicado por 'https://' en la URL, para garantizar una conexión segura.	Ejemplos: https://securebank.com, https://shopsecurely.com	Instalar extensiones como HTTPS Everywhere para forzar el uso de HTTPS siempre que sea posible.
<b>Controlar el uso de cookies</b>	Administrar las cookies para limitar el seguimiento y proteger la privacidad. Configurar el navegador para bloquear cookies de terceros.	Configurar en el navegador para bloquear todas las cookies de terceros o usar herramientas como Privacy Badger.	Limpiar las cookies y la caché regularmente y considerar el uso de modos de navegación privada.
<b>Usar un DNS seguro</b>	Utilizar un servicio de DNS que garantice la privacidad y la	Ejemplos de solucionadores DNS: Cloudflare DNS	Evitar usar los DNS de proveedores de internet que puedan

	seguridad de las solicitudes de dominio.	(1.1.1.1), Quad9 (9.9.9.9), OpenDNS.	registrar el historial de navegación.
<b>Utilizar la encriptación de un extremo a otro</b>	Proteger las comunicaciones para que solo el emisor y el receptor puedan leer el contenido.	Aplicaciones: WhatsApp, Signal, ProtonMail.	Preferir servicios que sean transparentes sobre su uso de encriptación y auditen su seguridad regularmente.
<b>Revisar Condiciones del servicio y políticas de privacidad</b>	Leer cuidadosamente los términos y políticas para comprender cómo se utilizarán los datos personales.	Revisar políticas en servicios como Facebook, Google, Amazon.	Buscar términos sobre compartición de datos con terceros y derechos del usuario para solicitar la eliminación de datos.
<b>Renunciar a compartir información personal con terceros</b>	Minimizar la cantidad de información personal compartida con aplicaciones y servicios.	No completar campos innecesarios en formularios en línea.	Usar datos ficticios o minimizados cuando sea posible, y siempre revisar los permisos solicitados por aplicaciones móviles.
<b>Buscar los warrant canary</b>	Verificar si las empresas utilizan canarios de orden judicial para alertar a los usuarios sobre órdenes de datos confidenciales.	Ejemplos: Políticas de transparencia de empresas como Dropbox, Apple, Signal.	Comprobar periódicamente la existencia y actualización de estos canarios como señal de que no se han recibido órdenes de silencio.
<b>Hacer copias de seguridad</b>	Realizar respaldos regulares de datos importantes para prevenir pérdidas.	Usar discos duros externos o servicios de almacenamiento en la nube como Google Drive, OneDrive.	Mantener al menos dos copias de seguridad en diferentes ubicaciones para mayor seguridad.
<b>Mantener software actualizado</b>	Instalar las últimas actualizaciones de software para protegerse contra vulnerabilidades de seguridad conocidas.	Actualizar sistemas operativos, aplicaciones y  firmware de dispositivos regularmente.	Habilitar las actualizaciones automáticas siempre que sea posible y revisar manualmente la disponibilidad de nuevas actualizaciones.



## Para saber más

En el siguiente enlace puedes ver más sobre la Privacidad y seguridad de Whatsapp:

 [Privacidad y seguridad de Whatsapp](#)



## Reflexiona

**¿Cómo puedo asegurarme de que mi información personal esté protegida cuando utilizo servicios en línea que requieren compartir datos sensibles?**

Mostrar retroalimentación

**Respuesta:** Para proteger tu información personal al usar servicios en línea, sigue estos pasos:

1. **Usa contraseñas seguras y únicas:** Crea contraseñas complejas que incluyan una combinación de letras, números y símbolos. Evita reutilizar contraseñas para diferentes cuentas.
2. **Habilita la autenticación de dos factores (2FA):** Esto añade una capa adicional de seguridad. Aunque alguien obtenga tu contraseña, necesitará un segundo factor (como un código enviado a tu teléfono) para acceder a tu cuenta.
3. **Verifica la seguridad del sitio web:** Asegúrate de que el sitio web utilice HTTPS, lo que indica que la conexión es segura y que tus datos están cifrados mientras se transmiten.
4. **Lee las políticas de privacidad y los términos de servicio:** Entiende cómo se recopilan, utilizan y comparten tus datos. Asegúrate de que el servicio respeta tu privacidad y no comparte tu información con terceros sin tu consentimiento.
5. **Limita la cantidad de información compartida:** Proporciona solo los datos esenciales y necesarios para el servicio. Cuanta menos información compartas, menor será el riesgo en caso de una filtración de datos.
6. **Utiliza servicios con encriptación de extremo a extremo:** Esto asegura que solo tú y la persona con la que te comunicas puedan leer

los mensajes, manteniendo tus conversaciones privadas.

7. **Mantén tu software y dispositivos actualizados:** Las actualizaciones de software suelen incluir parches de seguridad que protegen contra vulnerabilidades. Esto incluye sistemas operativos, navegadores y cualquier aplicación utilizada para acceder a servicios en línea.
8. **Usa un DNS seguro y centrado en la privacidad:** Servicios como Cloudflare (1.1.1.1) o Quad9 (9.9.9.9) no registran tu historial de navegación y protegen contra amenazas en línea.
9. **Realiza copias de seguridad de tus datos:** Mantén copias de seguridad de información importante en lugares seguros y separados, como discos duros externos o servicios de almacenamiento en la nube.
10. **Monitorea tus cuentas regularmente:** Revisa tus cuentas para detectar cualquier actividad inusual o no autorizada. Actúa rápidamente si notas algo sospechoso.



## Autoevaluación

¿Qué combinación se recomienda para crear contraseñas seguras?

- Solo letras
- Letras y números
- Letras, números y símbolos
- Solo símbolos

Incorrecto

Incorrecto

Las contraseñas seguras deben ser complejas y únicas, combinando letras, números y símbolos para dificultar su descifrado.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

¿Qué tecnología se utiliza para verificar la seguridad de un sitio web mediante la URL que comienza con "https://" ?

- Protocolo de transferencia de hipertexto (HTTP)
- Secure Sockets Layer (SSL)
- Protocolo de transferencia de archivos (FTP)
- Internet Protocol (IP)

Incorrecto

El uso de SSL/TLS cifra la conexión entre el navegador y el servidor, protegiendo la información transmitida, como datos personales y de pago. Es importante verificar la presencia de "https://" y un candado en la barra de direcciones para garantizar una navegación segura.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta

3. Incorrecto

4. Incorrecto

**¿Cuál es una herramienta recomendada para gestionar las cookies y proteger la privacidad?**

- Antivirus
- Firewall
- Privacy Badger
- Microsoft Word

Incorrecto

Incorrecto

Privacy Badger es una extensión del navegador que bloquea el rastreo de cookies de terceros, ayudando a proteger la privacidad del usuario al evitar el seguimiento de su actividad en línea.

Incorrecto

## Solución

- 1. Incorrecto
- 2. Incorrecto
- 3. Opción correcta
- 4. Incorrecto

**¿Qué tipo de DNS se recomienda para proteger la privacidad?**

- DNS proporcionado por el ISP

- DNS gratuito
- DNS seguro y centrado en la privacidad
- DNS público de cualquier proveedor

Incorrecto

Incorrecto

Usar un DNS seguro como Cloudflare (1.1.1.1) o Quad9 (9.9.9.9) ayuda a proteger la privacidad del usuario evitando el rastreo de actividades por parte de proveedores de internet o terceros.

Incorrecto

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

### ¿Qué significa la encriptación de un extremo a otro?

- Que los datos se encriptan en el servidor y se desencriptan en el cliente
- Que solo el emisor y el receptor pueden acceder al contenido de la comunicación
- Que los datos se almacenan en un formato encriptado en la nube
- Que los datos están encriptados mientras están en tránsito, pero no en reposo

Incorrecto

La encriptación de extremo a extremo asegura que solo las partes involucradas en la comunicación puedan leer los mensajes, protegiendo la privacidad de las conversaciones de posibles interceptores.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Por qué es importante revisar las Condiciones del servicio y las políticas de privacidad de los servicios en línea?**

- Para entender el diseño de la interfaz del usuario
- Para conocer cómo se utilizarán los datos personales
- Para aprender sobre las funcionalidades del servicio
- Para conocer los colores utilizados en el sitio web

Incorrecto

Las políticas de privacidad y condiciones del servicio explican cómo se recopilan, utilizan y comparten los datos personales. Es fundamental leer y entender estos documentos para tomar decisiones informadas sobre qué servicios utilizar y qué información compartir.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

**¿Cuál de las siguientes es una práctica recomendada para proteger la información personal al usar servicios en línea?**

- Compartir toda la información solicitada sin restricciones
- Renunciar a compartir información personal con terceros siempre que sea posible
- Utilizar la misma contraseña para todos los servicios
- Ignorar los permisos solicitados por las aplicaciones

Incorrecto

Limitar la cantidad de información personal compartida con servicios y aplicaciones minimiza los riesgos de exposición de datos sensibles. Es aconsejable revisar y restringir los permisos de acceso a datos que solicitan las aplicaciones.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

### ¿Qué son los "warrant canary" y por qué son importantes?

- Son alertas de nuevos productos en un servicio
- Son indicadores de que una empresa no ha recibido órdenes de divulgación de datos
- Son notificaciones de actualizaciones de software
- Son herramientas para eliminar cookies de los navegadores

Incorrecto

Los "warrant canary" son declaraciones publicadas regularmente por una empresa para indicar que no han recibido órdenes de divulgación de datos bajo secreto. La falta de actualización de estos puede indicar que la empresa ha sido obligada a entregar información sin poder notificar a sus usuarios.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta

- 3. Incorrecto
- 4. Incorrecto

**¿Cuál es una recomendación clave para la realización de copias de seguridad?**

- Guardar solo una copia de seguridad en el mismo dispositivo
- Realizar copias de seguridad esporádicamente
- Mantener múltiples copias de seguridad en diferentes ubicaciones
- Confiar únicamente en copias de seguridad automáticas

Incorrecto

Incorrecto

Es importante tener varias copias de seguridad almacenadas en diferentes ubicaciones para proteger los datos en caso de fallos de hardware, ataques cibernéticos o desastres naturales. Esto asegura que los datos puedan recuperarse si una copia se pierde o se corrompe.

Incorrecto

## Solución

- 1. Incorrecto
- 2. Incorrecto
- 3. Opción correcta
- 4. Incorrecto

**¿Por qué es crucial mantener el software actualizado?**

- Para tener acceso a nuevas funcionalidades de diseño

- Para protegerse contra vulnerabilidades de seguridad conocidas
- Para mejorar la velocidad de conexión a Internet
- Para reducir el consumo de energía del dispositivo

Incorrecto

Las actualizaciones de software suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas. Mantener el software actualizado es esencial para proteger los sistemas de ataques y mantener la seguridad de los datos personales.

Incorrecto

Incorrecto

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Licencia: licencia propietaria