



UD4. La Sociedad de la Información y del Conocimiento.



UD 1. LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO.

INDICE:

1. Hacia la Sociedad del Conocimiento Actual.
2. Evolución Tecnológica.
 - 2.1. Hacia la Sociedad del Conocimiento Actual.
 - 2.2. Evolución Tecnológica.
 - 2.3. Un Mundo Digital conectado a la Red.
 - 2.4. Identidad Digital.
 - 2.5. Conocimiento Colectivo.
3. Un Mundo Digital conectado a la Red.
 - 3.1. Hacia la Sociedad del Conocimiento Actual.
 - 3.2. Evolución Tecnológica.
 - 3.3. Un Mundo Digital conectado a la Red.
 - **Internet de las Cosas (IoT).**
 - **Dispositivos IoT en el hogar.**
 - **IoT: wearables.**
 - **IoTsmartcity.**
 - **IoT en medicina (IoMT).**
 - **IoT en la vida diaria.**
4. Identidad Digital.
 - ✓ **Componentes de la identidad digital.**
 - ✓ **Diferencia de la identidad física con la identidad digital.**
 - ✓ **Usos y beneficios.**
 - ✓ **Riesgos y protección.**
 - 4.1. DNI e.
 - **Características principales:**
 - **Importancia y uso.**
 - **Diferencia con otros documentos:**
 - 4.2. El Certificado Digital.
 - **¿Qué información contiene un certificado digital?**
 - **¿Para qué sirve un certificado digital?**
 - **Tipos comunes de certificados digitales:**
 - 4.3 Contraseñas.
 - a). **¿Por qué son importantes las contraseñas?**
 1. Protección de Información Sensible.
 2. Prevención de Ataques Cibernéticos.
 3. Control sobre tu Identidad Digital.
 4. Evitar Daños Colaterales.
 5. Cumplimiento Legal y Responsabilidad.
 6. Adaptación a las Amenazas Modernas.
 7. Confianza en los Servicios Digitales.



- b) El Peligro del SCAM y los Entornos No Verificados.
- c) Características de una Contraseña Segura:
- d) Malos Hábitos en la Gestión de Contraseñas.
- e) Herramientas para Evaluar la Calidad de tus Contraseñas.
- f) Verifica si tus Datos han sido Comprometidos.
- g) Consejos Adicionales para una Mejor Seguridad Digital.

5. Conocimiento Colectivo.

➤ Características principales:

5.1. Inteligencia Colectiva.

- Ejemplos de aplicaciones de la inteligencia colectiva.
- Características clave.
- Beneficios que aporta la inteligencia colectiva.
- ¿Cómo desarrollar la Inteligencia Colectiva?

5.2. Contenidos abiertos.

- Ejemplos de aplicaciones de la inteligencia colectiva.
- Características clave.

5.3 La Dimensión Social del Conocimiento.

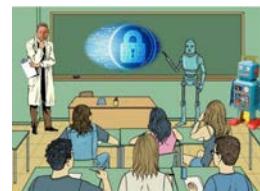
📘 Beneficios que aporta la inteligencia colectiva:

📘 ¿Cómo desarrollar la Inteligencia Colectiva?





UD4. La Sociedad de la Información y del Conocimiento.



1. Hacia la Sociedad del Conocimiento Actual.

La sociedad del conocimiento es aquella en la que **la fuente principal de riqueza, productividad y desarrollo social es la generación, el uso, la aplicación y la distribución de conocimiento**, especialmente científico y tecnológico. Se caracteriza por la innovación continua, el acceso a la información, la educación, el uso de las Tecnologías de la Información y Comunicación (TIC), y la capacidad de transformar datos en conocimiento para resolver problemas y crear un valor.



Elementos clave de la sociedad del conocimiento:

a). Conocimiento como recurso principal:

El conocimiento, en lugar del trabajo o las materias primas, es el factor más importante para el crecimiento económico y el progreso.

b). Innovación constante:

Existe un énfasis en la creación y aplicación de nuevos conocimientos y tecnologías para impulsar el desarrollo.

c). Rol de las TIC:

Las tecnologías de la información y la comunicación son fundamentales para facilitar la producción, distribución y acceso al conocimiento, superando barreras de tiempo y espacio.

d). Diferencia con la sociedad de la información:

Mientras que la sociedad de la información se centra en la acumulación de datos, la sociedad del conocimiento va más allá, ya que interpreta esos datos para crear entendimiento y generar acciones.



e). Educación y aprendizaje continuo:

La educación y la formación se vuelven cruciales para que los ciudadanos puedan acceder, procesar y aplicar el conocimiento de efectiva.

f). Capacidad de análisis:

Se desarrolla una mayor capacidad para el pensamiento crítico, el análisis y la integración de conocimientos para enfrentar los desafíos actuales.

En resumen, la sociedad del conocimiento es un modelo social que se enfoca en el saber compartido y la aplicación del conocimiento para el progreso integral de la sociedad.



Video 1: Definición de la sociedad del conocimiento (4 minutos)

Video 2: La revolución de los medios (5 minutos)

(5



Prometeus - La Revolución de los Medios



2. Evolución Tecnológica.

La evolución de la tecnología de la información (TIC) se puede dividir en etapas que van desde las herramientas mecánicas y eléctricas del siglo XIX y XX hasta la era digital y conectada actual, caracterizada por las computadoras personales, Internet, la inteligencia artificial y la integración del metaverso y la realidad aumentada. Los hitos clave incluyen la invención del teléfono, la creación de la primera computadora ([ENIAC](#) en 1946), la miniaturización con los microprocesadores, el nacimiento de [ARPANET](#), y la democratización del acceso a la información a través de Internet.

Veamos de forma resumida la evolución de la tecnología desde el siglo XIX.

1. Pre-Informática y Mecanización. (Siglo XIX - Principios Siglo XX).

Inicios de la comunicación:

Se introducen inventos como la imprenta, el telégrafo y el teléfono para reproducir y transmitir información de forma masiva y a distancia.

Herramientas mecánicas:

Aparecen máquinas de escribir y calculadoras, que facilitan el procesamiento de datos.

2. La Era Eléctrica y de los Sistemas (Años 40 - 60).

Primeros ordenadores:

Se desarrolla ENIAC (1946), la primera computadora, marcando un hito en la historia de la informática.

Surgimiento de la computación:

La tecnología de la información empieza a centrarse más en el contenido que en la forma, y aparecen los primeros sistemas de información.

Almacenamiento masivo:

IBM lanza el primer disco duro, un paso fundamental para el almacenamiento de datos.

3. La Era Electrónica y la Miniaturización (Años 70).

Desarrollo de componentes:

Se miniaturizan las computadoras y aparecen los primeros chips procesadores, permitiendo equipos más pequeños y potentes.

Sistemas avanzados:

Se crean sistemas de control automatizados (ACS) y sistemas de recuperación de información (IRS), que hacen hincapié en la creación de información significativa.

4. La Era de la Computadora Personal y de la Información (Años 80 - Actualidad)

4.1. Computadoras Personales (PC):

La computadora personal se convierte en la herramienta principal, democratizando el acceso a la computación.

4.2. Nacimiento de Internet:

En 1968 se crea [ARPANET](#), la primera red que dio paso a Internet y a la conexión global.

4.3. Conectividad y redes:

Se desarrollan las primeras redes y se expande la capacidad de conexión inalámbrica, haciendo la comunicación más instantánea.



UD4. La Sociedad de la Información y del Conocimiento.



5. La Era Digital y Conectada (Siglo XXI - Presente)

Ubicuidad de Internet:

Las tecnologías digitales, la telefonía móvil avanzada y la televisión por satélite/cable hacen la información más accesible.

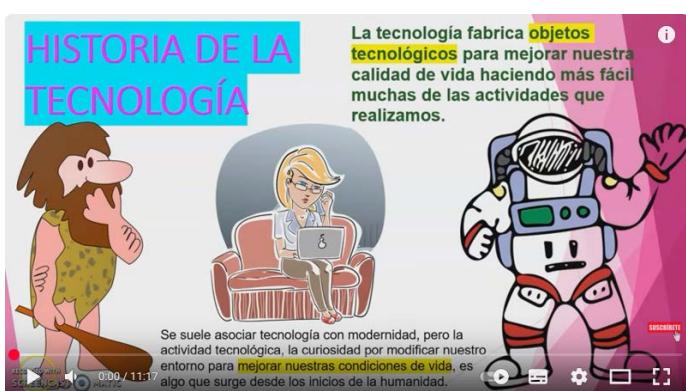
Avances recientes:

Se populariza la inteligencia artificial, el aprendizaje automático ([machine learning](#)), la realidad aumentada y el metaverso, transformando la interacción humana con el entorno digital.

Innovación constante:

Las TIC siguen evolucionando, con una innovación constante y la interconexión de nuevas tecnologías, que se adaptan a las necesidades de la sociedad.

[Video 1: Evolución de las tecnologías de la información \(4 minutos\)](#)



[Video 2: Historia de la tecnología \(11,16 minutos\).](#)



HISTORIA DE LA TECNOLOGÍA

[Video 3: Historia de la Computación \(26 minutos\)](#)



3. Un Mundo Digital conectado a la Red.

Un mundo digital conectado a la red **es una realidad en la que objetos, sistemas y personas están interconectados a través de internet**, permitiendo la recopilación y el intercambio de datos en tiempo real. Este concepto, conocido principalmente como el [**Internet de las Cosas**](#) (IoT), transforma nuestro entorno al integrar sensores, software y conectividad en elementos cotidianos, desde electrodomésticos hasta vehículos, para automatizar procesos y tomar decisiones más eficientes y estratégicas.

3.1. Componentes clave de un mundo digital conectado:

- 1) **Dispositivos con sensores:** Objetos cotidianos equipados con sensores que recopilan información sobre su entorno o funcionamiento.
- 2) **Conectividad:** La capacidad de estos dispositivos para conectarse a internet y a otras redes, permitiendo la transmisión de datos.
- 3) **Redes y plataformas:** La infraestructura de red (como 5G) y las plataformas en la nube que procesan, gestionan y analizan los datos recopilados.
- 4) **Intervención humana mínima:** El objetivo es automatizar acciones y proporcionar información para que los humanos puedan tomar decisiones informadas o actuar de manera más efectiva.

3.2. Beneficios y aplicaciones:

- Eficiencia y productividad: Las empresas pueden optimizar procesos, predecir fallos y reducir costes.
- Mejora de la vida diaria: Permite el control remoto de dispositivos en el hogar, la automatización de tareas y la creación de hogares inteligentes.
- Avances en diversas industrias: Se utiliza en la fabricación, transporte, agricultura, atención médica y más para mejorar la monitorización y el funcionamiento.

3.3. Desafíos y riesgos:

- a) Seguridad y privacidad: La gran cantidad de datos recopilados plantea desafíos en la protección de la información sensible.
- b) Mantenimiento: Asegurar el correcto funcionamiento y la seguridad de miles de dispositivos conectados es un reto importante

Internet de las Cosas (IoT).

¿Qué significa?

Significa que estamos rodeados de pequeñas redes y nuevas tecnologías que tienen una única finalidad: conectar el máximo de objetos que nos rodean, entre ellos y con nosotros. Básicamente es un concepto que hace referencia a la interconexión digital de objetos cotidianos con Internet.

¿Cuáles son las estimaciones de uso para un futuro corto? Creo que con el paso del tiempo el uso de Internet y de las nuevas tecnologías será cada vez más usual y seremos cada vez más dependientes de ellos, ya que, debido a su comodidad muchas



UD4. La Sociedad de la Información y del Conocimiento.



cosas serán reemplazadas por el IoT y nos acostumbraremos a los nuevos modelos, tanto físicos (objetos inteligentes) como virtuales (redes sociales, información, nube...)

¿Qué tipo de comunicación se utiliza?

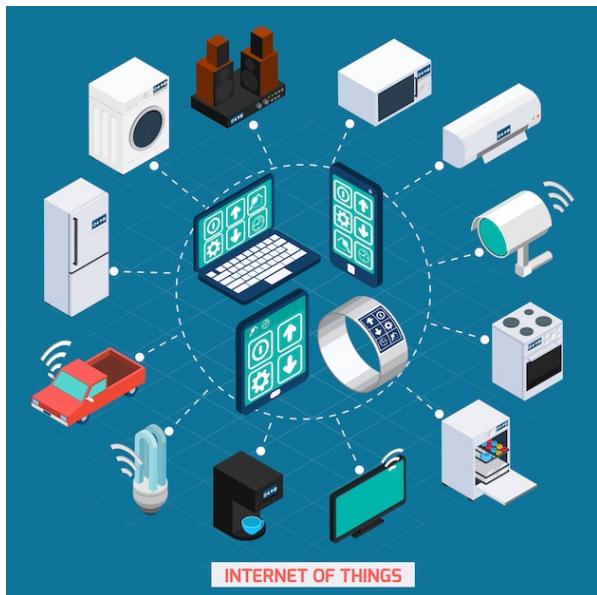
Redes Wi-Fi o Bluetooth

¿Qué evoluciones técnicas han hecho posible esta innovación en el campo de las tecnologías de la información y comunicación?

La población de la radio (1920-1940), aparición de la TV en los años 40, TV satelital y por cable en los años 70, la WEB en el 1993 y la WEB 2.0 en 2004. De esto han surgido las redes, ciudades hiperconectadas, revolución celular, movilidad empresarial...

¿Cómo se relaciona el elemento tecnológico Arduino con el IoT (“Internet of Things”)? El Arduino es una plataforma electrónica basada en el principio del hardware libre, no propietario, que permite su programación para el fin deseado. Realiza, precisamente, entre otras, la función de comunicar e interaccionar los objetos a través de internet.

Ejemplos con imágenes de dispositivos que formen parte del IoT



Ciudades Inteligentes.

Concepto “smartcities”: Es un sistema complejo e interconectado que aplica las nuevas tecnologías para gestionar desde el correcto funcionamiento de los sistemas de transporte público y privado, hasta el uso eficiente de los recursos energéticos o hídricos, pasando por los planes de protección civil, o aspectos socio-económicos, como la vitalidad de los espacios públicos y del tejido comercial, o la comunicación de incidencias a habitantes y visitantes



UD4. La Sociedad de la Información y del Conocimiento.



¿Cuáles son sus posibilidades o mejoras hacia el ciudadano que vive en ellas?

Sirven de infraestructuras, innovación y tecnología para disminuir el consumo energético y reducir las emisiones de CO₂.

Ejemplos de aplicaciones que usando las nuevas tecnologías se relacionan con un Mundo Digital conectado a la Red.:

- Tablets



- La [automatización del hogar](#) (termostatos y luces inteligentes).
- Las [ciudades inteligentes](#) (gestión de tráfico y alumbrado).
- El [Internet de las Cosas \(IoT\)](#) para la salud (wearables que monitorean la salud).
- **Los vehículos conectados** (diagnóstico remoto y mantenimiento predictivo).

Estas aplicaciones utilizan dispositivos inteligentes, sensores y redes de comunicación para recopilar y transmitir datos, permitiendo un control más eficiente y a distancia de múltiples sistemas.

En el hogar:

- ☞ **Smart home:** Controlar termostatos, luces y electrodomésticos a través de una aplicación para mejorar la eficiencia energética y la seguridad.
- ☞ **Seguridad:** Sistemas de alarma y cámaras de seguridad que se pueden monitorear de forma remota desde un teléfono inteligente.
- ☞ **Entretenimiento:** Altavoces inteligentes, televisores y sistemas de audio que pueden ser controlados de manera centralizada.

En la ciudad:

- ☞ **Gestión de tráfico:** Sensores y cámaras para monitorear el tráfico en tiempo real y optimizar los semáforos, así como aplicaciones que guían a los conductores hasta plazas de aparcamiento libres.
- ☞ **Servicios públicos:** Alumbrado público inteligente que ahorra energía y señalización digital.
- ☞ **Gestión de residuos:** Sensores en los contenedores para optimizar las rutas de recolección.

En la salud:

- ☞ **Wearables:** Relojes y pulseras inteligentes que monitorean la frecuencia cardíaca, la actividad física y el sueño.
- ☞ **Monitorización remota:** Dispositivos conectados a pacientes que permiten a los médicos hacer un seguimiento de su estado de salud a distancia.

En el transporte y la industria:

- ☞ **Vehículos conectados:** Los coches pueden reservar citas de mantenimiento automáticamente, además de permitir el control remoto de funciones como la climatización.
- ☞ **Gestión de flotas:** Seguimiento en tiempo real de vehículos para optimizar las rutas y la logística.



UD4. La Sociedad de la Información y del Conocimiento.



- ❖ **Industria (IIoT):** Sensores y dispositivos para el control de calidad digital, mantenimiento predictivo y monitorización remota en entornos peligrosos.

En la agricultura:

- ❖ **Agricultura de precisión:** Uso de sensores y drones para monitorear las condiciones del suelo y del clima, permitiendo un riego y una fertilización más eficientes.

El Internet de las Cosas (IoT):

Es para la gestión inteligente de ciudades, hogares y agricultura (sensores en aparcamientos, asistentes virtuales, drones).

Dispositivos IoT en el hogar:

Termostatos que regulan la temperatura si estamos o no en nuestro hogar o **bombillas regulables** son los dispositivos conectados más populares, pero también hay **cerraduras inteligentes, detectores de humos o comederos para animales**, que dispensan la ración si nosotros damos la orden desde el smartphone. Los aparatos de Penet, por ejemplo, nos envían alertas cuando el animal ha terminado de comer, con la cantidad que ha ingerido.

En los hogares es donde más ejemplos de IoT encontramos, con marcas ya muy asentadas. Los termostatos Nest o los **robots aspiradora** Roomba son dos de los productos más vendidos, gracias, entre otras razones, a su facilidad para ser controlados con una app. No se salva ni el cuarto de baño: en él encontramos los **cepillos de dientes** Kolibree

IoT: **wearables**:

Pulsera que cuenta tus pasos **o ese smartwatch que te da la hora a la vez que monitoriza tus latidos**.

IoT smartcity:

Mapas de ruido, iluminación más eficaz, gestión de los semáforos...

IoT en medicina (IoMT):

Audiómetros digitales. gran avance para mejorar los problemas de audición.

Monitores de glucosa continuos para informar en tiempo real del estado del paciente, pueden detectar patrones o tendencias

Inhaladores inteligentes podrían cambiar la manera en la que se maneja el asma.

IoT en la vida diaria:

Botellas de agua (Hidrate Sparkque te recuerda que bebas agua y que lleva la cuenta de cuánta has ingerido) **y plazas de aparcamiento**

- a) Inteligencia Artificial (IA) para asistentes personales, análisis de datos y automatización (Alexa, vehículos autónomos).
- b) Plataformas de colaboración en la nube como Google Meet y Microsoft Teams para la comunicación y el trabajo remoto.

La historia de internet origen (video de 8 minutos)



UD4. La Sociedad de la Información y del Conocimiento.



4. Identidad Digital.

La **identidad digital** es la [imagen virtual](#) que una persona o entidad proyecta en el entorno digital, formada por datos personales, comportamiento en línea y la información que otros comparten sobre ella. Es el equivalente a un documento de identidad en el mundo físico y se utiliza para la verificación segura en Internet, permitiendo el acceso a servicios y la realización de trámites.

Componentes de la identidad digital.

- 1) **Datos personales:** Información como nombre, fecha de nacimiento, número de identificación, datos biométricos o credenciales de acceso.
- 2) **Comportamiento en línea:** Acciones, gustos, opiniones y el uso de redes sociales (likes, comentarios, fotos, etc.).
- 3) **Huella digital:** Toda la información que se deja en internet, incluyendo la que no es visible directamente, pero está almacenada en bases de datos.

Diferencia de la identidad física con la identidad digital.

- **Identidad física:** Se basa en la persona en el mundo offline y se verifica con documentos como el DNI o pasaporte.
- **Identidad digital:** Es la representación de esa identidad en la red, completada por la interacción y la información compartida online.

Usos y beneficios:

- a) Identificación segura: Permite a individuos y empresas identificarse de forma segura y fiable en internet.
- b) Acceso a servicios: Facilita el acceso a servicios públicos y privados, desde la realización de trámites administrativos hasta el uso de servicios bancarios.
- c) Ciberseguridad: Mejora la seguridad y previene el fraude al establecer normas estrictas para la verificación de datos.

Riesgos y protección:

- ✓ **Robo de identidad:** La sustracción de datos digitales puede llevar al robo de identidad y a consecuencias negativas.
- ✓ **Gestión de la reputación:** Una mala gestión de la identidad digital puede afectar la reputación online y tener repercusiones en el ámbito personal y profesional

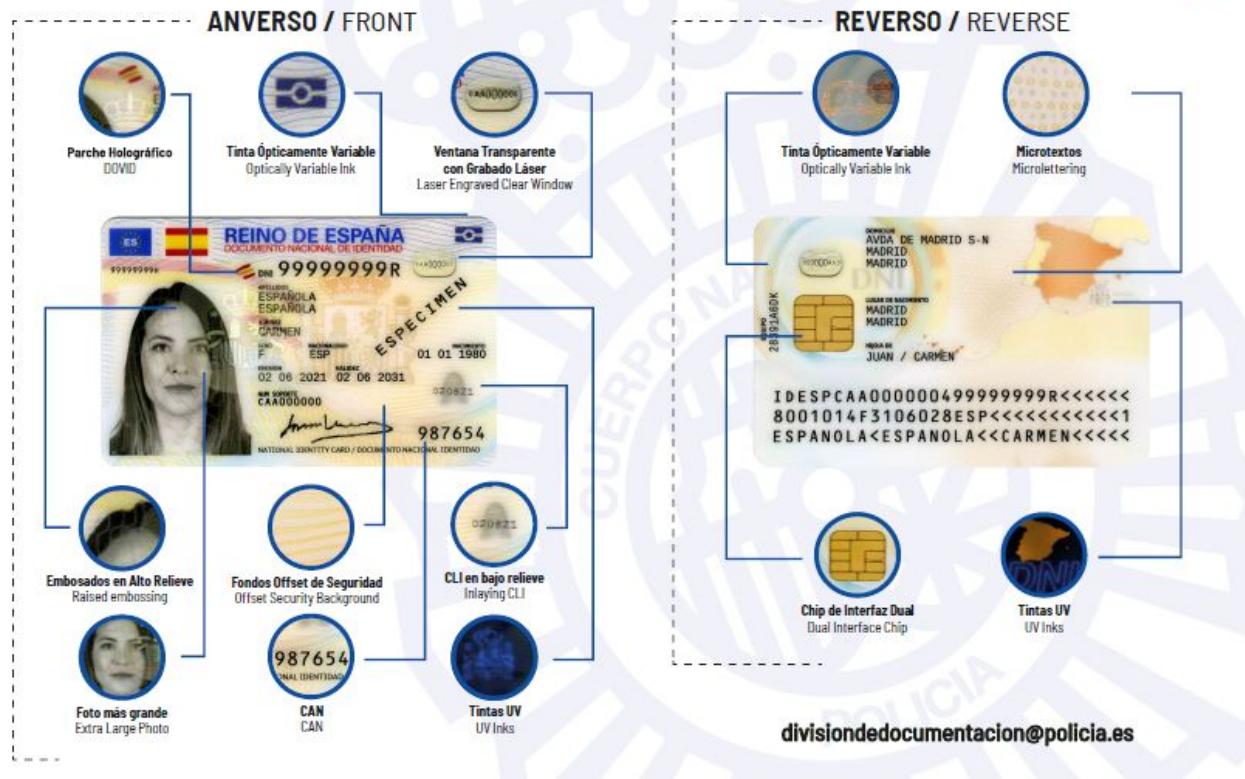


4.1. DNI e.

El **DNI (Documento Nacional de Identidad)** en España es un documento oficial y personal que acredita la identidad, los datos personales y la nacionalidad española de un ciudadano, siendo obligatorio a partir de los 14 años y necesario para la realización de diversos trámites oficiales dentro del país.

DNI ELECTRÓNICO 4.0

NATIONAL eID 4.0



Características principales:

- Propósito:**
Acreditar la identidad y la nacionalidad española de su titular.
- Emisor:**
Es emitido por la Dirección General de la Policía, del Ministerio del Interior.
- Obligatoriedad:**
La obtención del DNI es obligatoria para los españoles mayores de 14 años.
- Contenido:**
Incluye información personal como una foto, el nombre, la fecha y lugar de nacimiento, además de la firma del titular.
- Validez:**
Su validez depende de la edad, siendo generalmente de cinco años para jóvenes y diez para adultos, pero puede ser de dos años para menores de cinco o permanente para mayores de 70.



UD4. La Sociedad de la Información y del Conocimiento.



Importancia y uso.

➤ Trámites oficiales:

El DNI es indispensable para cualquier tipo de gestión o trámite oficial en España, desde gestiones bancarias hasta viajes dentro del territorio nacional.

➤ Identificación:

Es el documento por excelencia para la identificación de los ciudadanos españoles.

Diferencia con otros documentos:

1) NIF:

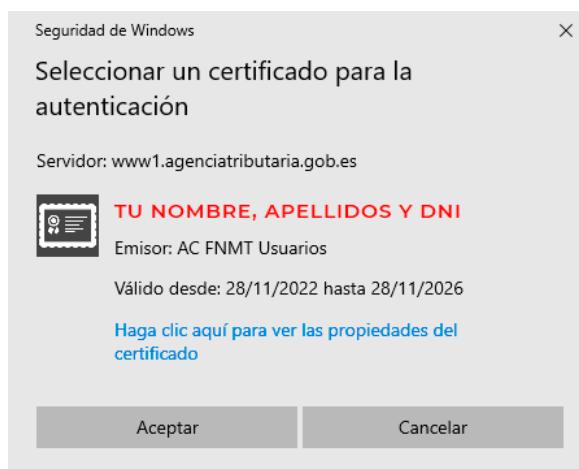
El Número de Identificación Fiscal (NIF) es un código que identifica a personas y entidades para fines fiscales. Para personas físicas, suele ser el mismo que el DNI.

2) NIE:

El Número de Identificación de Extranjero (NIE) es un documento similar al NIF en formato, pero se dirige a ciudadanos extranjeros que necesitan realizar trámites en España.

4.2. El Certificado Digital.

Un certificado digital es un archivo electrónico emitido por una entidad de confianza que valida tu identidad en Internet, permitiéndote firmar digitalmente documentos y realizar trámites online con la misma validez legal que en persona. Contiene información sobre el titular (como nombre y dirección), su clave pública, la de la entidad emisora, y su fecha de validez. Se utiliza para identificarse en plataformas de la administración pública y otras sedes electrónicas, y para firmar documentos de forma segura, garantizando la identidad del autor y la integridad del contenido.



Ejemplos de certificados digitales son:

- DNIE
- Fábrica Nacional de Moneda y Timbre



¿Qué información contiene un certificado digital?

- a) Identificación del titular: Datos como nombre y dirección del propietario del certificado.
- b) Clave pública: La clave pública que se utiliza para cifrar o verificar la firma digital.
- c) Fecha de validez: El período durante el cual el certificado es válido y se puede usar.
- d) Identificación del emisor: Los datos de la entidad certificadora que ha emitido el certificado.

¿Para qué sirve un certificado digital?

- 1) Identificación electrónica: Permite acreditar tu identidad ante organismos públicos, como hacienda o la DGT, para realizar trámites online.
- 2) Firma electrónica de documentos: Puedes firmar digitalmente cualquier documento electrónico, dándole la misma validez jurídica que una firma manuscrita en papel.
- 3) Garantizar la seguridad de las comunicaciones: Ayuda a asegurar que las transacciones y comunicaciones en Internet se realicen entre partes de confianza.

Tipos comunes de certificados digitales:

- 1) Certificado de DNI electrónico: Incluido en tu DNI, contiene certificados de autenticación y firma.
- 2) Certificados emitidos por la FNMT: Entidades públicas como la FNMT-RCM (Fábrica Nacional de Moneda y Timbre) emiten certificados para ciudadanos y empresas.

4.3 Contraseñas.

El método más extendido para identificarse y obtener acceso a la información personal es mediante contraseñas.

Para evitar que otros usuarios malintencionados consigan apoderarse de esta información es importante generar contraseñas seguras. En la era digital en la que vivimos, nuestras contraseñas son como las llaves de nuestra casa virtual. Controlan el acceso a nuestras cuentas bancarias, correos electrónicos, redes sociales y mucho más. Lo curioso es que muchas personas no le prestan la atención necesaria a la creación y gestión de sus contraseñas, lo que puede exponerlas a riesgos significativos. Es muy frecuente encontrarse con personas que usan la misma contraseña para todo, olvidando que si tienes la misma llave para todas las puertas estarás exponiendo todos los accesos que dependen de ello.



a). ¿Por qué son importantes las contraseñas?

Las contraseñas actúan como la **primera línea de defensa** contra accesos no autorizados a tus cuentas, pero su importancia va mucho más allá de simplemente “bloquear” nuestras cuentas. A continuación, puedes ver por qué las contraseñas son tan cruciales en este mundo que nos toca vivir:

1. Protección de Información Sensible.

Nuestras cuentas contienen **información extremadamente valiosa**: desde datos personales (como tu dirección o número de teléfono) hasta información financiera (como los detalles de tu cuenta bancaria o tarjetas de crédito). Una contraseña débil o comprometida puede permitir que los ciberdelincuentes accedan a esta información, exponiéndote a robos de identidad, fraudes o incluso chantajes.

Por ejemplo:

- ✓ Si un atacante obtiene acceso a tu correo electrónico, podría restablecer contraseñas de otras cuentas, bloqueándote fuera de ellas.
- ✓ Si acceden a tu cuenta bancaria, podrían realizar transacciones no autorizadas.



2. Prevención de Ataques Ciberneticos.

Los ciberdelincuentes utilizan técnicas sofisticadas, como **fuerza bruta**, **ataques de diccionario** o **phishing**, para intentar descifrar o robar tus contraseñas. Una contraseña segura dificulta enormemente estos ataques, lo que reduce el riesgo de que tus cuentas sean comprometidas.

Algunos métodos comunes de ataque incluyen:

- **Fuerza bruta**: Los atacantes prueban todas las combinaciones posibles de caracteres hasta encontrar la correcta.
- **Ataques de diccionario**: Se basan en listas predefinidas de palabras comunes o frases predecibles.
- **Phishing**: Intentan engañarte para que ingreses tus credenciales en sitios falsos o mediante correos fraudulentos.

3. Control sobre tu Identidad Digital

En la era de las redes sociales y los servicios en línea, nuestras cuentas representan nuestra **identidad digital**. Si alguien obtiene acceso a tus perfiles, podría publicar contenido en tu nombre, difundir información falsa o dañar tu reputación. Esto puede tener consecuencias graves tanto a nivel personal como profesional.

Por ejemplo:

- ❖ **Un atacante podría usar tu cuenta de redes sociales para enviar mensajes maliciosos a tus contactos.**
- ❖ **Podrían modificar tu perfil profesional en plataformas como LinkedIn, afectando tu carrera.**

4. Evitar Daños Colaterales

El uso de contraseñas inseguras o reutilizadas no solo pone en riesgo **tu propia seguridad, sino también la de otros** pudiendo tener un impacto amplio y perjudicial de lo que imaginas. Por ejemplo:

- Si usas la misma contraseña en tu cuenta de trabajo y en un servicio personal, un ataque exitoso en el servicio personal podría comprometer datos confidenciales de tu empresa.
- Si tus contactos confían en ti y reciben un mensaje falso desde tu cuenta comprometida, podrían caer en estafas.

5. Cumplimiento Legal y Responsabilidad

En muchos sectores, como la salud, las finanzas o la Administración Pública, existen **regulaciones estrictas sobre la protección de datos** (por ejemplo, el **GDPR**). Usar contraseñas inseguras o negligentes puede resultar en violaciones de estas normativas, lo que puede llevar a multas significativas o incluso responsabilidad legal.



UD4. La Sociedad de la Información y del Conocimiento.



Además, si eres responsable de gestionar cuentas en una organización, asegurarte de que las contraseñas sean seguras es parte de tu deber ético y profesional.

6. Adaptación a las Amenazas Modernas

Con el avance de la **tecnología**, los métodos de ataque también han evolucionado. Herramientas automatizadas y potentes ahora pueden probar millones de combinaciones de contraseñas por segundo. Esto significa que las contraseñas simples o predecibles ya no son suficientes para protegerte.

Sin embargo, al adoptar mejores prácticas (como usar contraseñas largas, únicas y aleatorias), puedes mantener una ventaja frente a estas amenazas.

7. Confianza en los Servicios Digitales

Imagina un mundo donde no pudieras **confiar** en que tus cuentas están seguras. No podrías hacer compras en línea, acceder a servicios bancarios o comunicarte con tus seres queridos sin preocuparte por ser hackeado. Las contraseñas son el mecanismo básico que nos permite confiar en los servicios digitales que usamos todos los días.

Cuando gestionas tus contraseñas correctamente, no solo proteges tus propios datos, sino que también contribuyes a un ecosistema digital más seguro para todos.

b) El Peligro del SCAM y los Entornos No Verificados.

Uno de los mayores riesgos relacionados con las contraseñas es caer en un **SCAM**, un tipo de **estafa diseñada para engañarte y obtener tus credenciales de manera fraudulenta**. Los atacantes suelen utilizar tácticas como correos electrónicos falsos, mensajes de texto o sitios web fraudulentos que imitan servicios legítimos (como tu banco, redes sociales o plataformas de correo electrónico) para convencerte de que ingreses tus datos. Este tipo de ataques, conocidos como **phishing**, son especialmente peligrosos porque explotan la confianza del usuario.

Por ejemplo, podrías recibir un correo electrónico aparentemente enviado por tu banco, indicando que hay un problema con tu cuenta y solicitando que ingreses tu contraseña para “verificar” tu identidad. Si caes en esta trampa y proporcionas tu contraseña en un entorno no verificado, los ciberdelincuentes obtendrán acceso completo a tu cuenta, poniendo en riesgo no solo tus datos personales, sino también tu seguridad financiera.

c) Características de una Contraseña Segura:

Para proteger tus cuentas, sigue estas recomendaciones al crear contraseñas:

1. **Longitud:** Usa contraseñas de al menos 12 caracteres. Cuanto más larga sea la contraseña, más difícil será de descifrar.
2. **Complejidad:** Combina letras mayúsculas, minúsculas, números y símbolos. Por ejemplo: C0ntr4s3ñ@Segur4!.



UD4. La Sociedad de la Información y del Conocimiento.



3. **Evita palabras comunes:** No uses palabras del diccionario, nombres propios, fechas de nacimiento o secuencias simples como “123456” o “password”.
4. **Única por cuenta:** Nunca reutilices la misma contraseña en múltiples sitios. Si un servicio es comprometido, todas tus cuentas estarán en riesgo.
5. **Aleatoriedad:** Genera contraseñas aleatorias en lugar de usar frases predecibles.

Un ejemplo de una buena contraseña podría ser: **G#7dL9@pXqT2.**

d) Malos Hábitos en la Gestión de Contraseñas.

A pesar de las advertencias, muchos usuarios siguen cometiendo errores graves al gestionar sus contraseñas. Aquí tienes un listado de los peores hábitos:

1. **Usar contraseñas simples:** Ejemplos como “123456”, “qwerty” o “password” son extremadamente inseguros.
2. **Uso de patrones repetitivos:** Usar un patrón que se repite en tus contraseñas es similar a usar una misma contraseña para todo. Por ejemplo, usar el patrón “miContraseña-Servicio” y emplearlo en el correo como “miContraseña-Correo” ó “MiContraseña-Banco”.
3. **Reutilizar contraseñas:** Si usas la misma contraseña en varias cuentas, un ataque exitoso en una de ellas comprometerá todas las demás.
4. **Guardar contraseñas en texto plano o en un Post-It:** Escribir tus contraseñas en notas físicas fáciles de encontrar o archivos sin cifrado es un riesgo innecesario.
5. **Compartir contraseñas:** Compartir tus credenciales con amigos, familiares o colegas puede aumentar el riesgo de exposición.
6. **No cambiar contraseñas regularmente :** Las contraseñas antiguas pueden volverse vulnerables con el tiempo debido a brechas de seguridad o avances tecnológicos.
7. **Usar información personal:** Evita usar nombres, apellidos, fechas de nacimiento u otros datos fácilmente adivinables.

e) Herramientas para Evaluar la Calidad de tus Contraseñas

Existen herramientas en línea que pueden ayudarte a verificar si tus contraseñas son seguras. Estas herramientas analizan la fortaleza de tus contraseñas y ofrecen sugerencias para mejorarlas. Algunas de las más populares son:

1. [**HowSecureIsMyPassword**](#): Calcula cuánto tiempo tardaría un atacante en descifrar tu contraseña.
2. [**Password Meter**](#) : Evalúa la fortaleza de tu contraseña basándose en varios criterios, como longitud, complejidad y patrones.
3. [**Kaspersky PasswordCheck**](#): Proporciona una estimación del tiempo necesario para crackear tu contraseña.

Estas herramientas son útiles, pero recuerda nunca ingresar contraseñas reales en sitios web no confiables.



UD4. La Sociedad de la Información y del Conocimiento.



f) Verifica si tus Datos han sido Comprometidos

Además de asegurar tus contraseñas, es importante verificar si alguna de tus cuentas ha sido afectada por una brecha de seguridad. Para ello, puedes usar servicios como:

1. [Have I BeenPwned](#): Esta herramienta verifica si tu correo electrónico o número de teléfono aparece en bases de datos filtradas de brechas de seguridad.
2. [Firefox Monitor](#) : Similar a Have I BeenPwned, esta herramienta te alerta si tus datos han sido expuestos.
3. [Google PasswordCheckup](#): Si usas Google Chrome, esta función verifica si tus contraseñas guardadas han sido comprometidas.

Si descubres que alguna de tus cuentas ha sido afectada, cambia inmediatamente las contraseñas asociadas.

g) Consejos Adicionales para una Mejor Seguridad Digital

1. **Usa un gestor de contraseñas** : Herramientas como [Keepass](#), [LastPass](#), [1Password](#) o [Bitwarden](#) generan y almacenan contraseñas seguras para ti.
2. **Activa la autenticación de dos factores (2FA)** : Añade una capa adicional de seguridad a tus cuentas mediante un código enviado a tu teléfono o una aplicación autenticadora.
3. **Actualiza regularmente tu software** : Mantén tus dispositivos y aplicaciones actualizados para protegerte contra vulnerabilidades conocidas.
4. **Sé cauteloso con los correos sospechosos** : Los ataques de phishing suelen intentar robar tus credenciales. Nunca hagas clic en enlaces ni ingreses tus datos en sitios no verificados.

En resumen...

Las contraseñas son una parte esencial de nuestra vida digital, pero también una de las áreas más vulnerables si no se gestionan correctamente. Siguiendo las mejores prácticas que hemos mencionado en este artículo, podrás reducir significativamente el riesgo de ser víctima de un ciberataque. Recuerda que la seguridad digital es una responsabilidad compartida, y cada pequeño paso que tomes puede marcar una gran diferencia.



5. Conocimiento Colectivo.

El conocimiento colectivo es la suma de habilidades, experiencias y saberes que se generan y comparten dentro de un grupo de personas a través de la interacción y la colaboración.

No pertenece a un solo individuo, sino que se construye y renueva constantemente, siendo clave para la innovación, la toma de decisiones y la resolución de problemas en diferentes contextos, desde organizaciones hasta comunidades indígenas.

Características principales:

- **Proceso de colaboración:** Se crea mediante la interacción, el diálogo y el intercambio de ideas entre múltiples personas, a diferencia de un monólogo.
- **Construcción en conjunto:** Es el resultado de sumar y combinar las perspectivas, conocimientos y experiencias individuales de cada miembro.
- **Cultura de intercambio:** Requiere una cultura de colaboración donde los miembros compartan abiertamente sus saberes para nutrir el conocimiento del grupo.
- **Motor de crecimiento:** Impulsa la innovación, la resolución de problemas, la toma de decisiones informadas y la agilidad en una organización.
- **Diversidad de formatos:** Se puede encontrar en distintos ámbitos:
 - **Empresas:** La experiencia acumulada de los empleados, consultores y socios.
 - **Comunidades:** Los saberes ancestrales y tradicionales transmitidos de generación en generación, a menudo relacionados con la biodiversidad.

5.1. Inteligencia Colectiva.

Aunque te pueda parecer un concepto nuevo, lo cierto es que **la inteligencia colectiva es algo antiguo**. Por ejemplo, Aristóteles, en la antigua Grecia, ya hablaba en su obra **Política** de que la aportación de muchas personas daba mejores resultados en la toma de decisiones. No obstante, **es con la revolución tecnológica actual cuando esta idea cobra máximo protagonismo**, debido precisamente a esa férrea interacción que propicia internet entre grupos de personas y sistemas.

De este modo, [Pierre Lévy](#), el responsable de la expansión del término “inteligencia colectiva”, la describe como “**una forma de inteligencia distribuida universalmente, constantemente mejorada, coordinada en tiempo real y que resulta en la movilización efectiva de habilidades**”. Mientras, Thomas W. Malone, autor de “**Handbook of Collective Intelligence**” y fundador del “[MIT Center for Collective Intelligence](#)”, se refiere a este mismo concepto como “grupos de individuos que actúan colectivamente de maneras que parecen inteligentes”.

Se trata, en definitiva, de **combinar las capacidades, conocimientos, puntos de vista y habilidades de varias personas para conseguir soluciones más enriquecedoras**.



En lugar de depender únicamente de una sola persona o experto, la inteligencia colectiva aboga por la colaboración y [participación activa de múltiples individuos](#) para lograr resultados más efectivos. Es decir, es un nuevo paradigma que hace **un cambio de mentalidad del “Yo” al “Nosotros”** basado en el principio de la mayor eficacia de la “sabiduría de la multitud”, término acuñado por **James Surowiecki** en su libro **“Wisdom of Crowds”**.

Ejemplos de aplicaciones de la inteligencia colectiva.

Aunque pueda parecer algo abstracto, seguro que, si escuchas algunos ejemplos de inteligencia colectiva, te sentirás muy familiarizado con el concepto.

- a) **Wikipedia:** utiliza esta filosofía para desarrollar contenidos, ya que aprovecha los conocimientos de millones de usuarios para ir creando, corrigiendo, ampliando sus entradas y mejorando una enciclopedia en línea.
- b) **Eyewire:** Se trata de un juego en línea que permite a los científicos obtener datos sobre las conexiones neuronales mientras los jugadores resuelven los rompecabezas propuestos. En Informática, por ejemplo, los **programas de código abierto** son también muestras de esta [inteligencia grupal](#), debido a que los softwares se van ajustando y desarrollando con la participación de expertos de todo el mundo. También lo son las [redes sociales](#), donde los miles de millones de datos que aportan los usuarios durante su navegación permiten crear perfiles y predicciones altamente fiables sobre su comportamiento como consumidor.
- c) **Software de código abierto:** Proyectos como Linux se desarrollan y mejoran colaborativamente por una comunidad global de programadores.
- d) **Crowdsourcing:** Externaliza tareas a una gran comunidad de personas, en lugar de hacerlo internamente.
- e) **Sesiones de brainstorming:** Una técnica de lluvia de ideas para generar soluciones creativas de forma colectiva.
- f) **Redes sociales:** Utilizan la información aportada por los usuarios para crear perfiles y hacer predicciones sobre su comportamiento

Como ves, las posibilidades de la inteligencia colectiva son tantas como situaciones en las que haya más de una persona implicada.



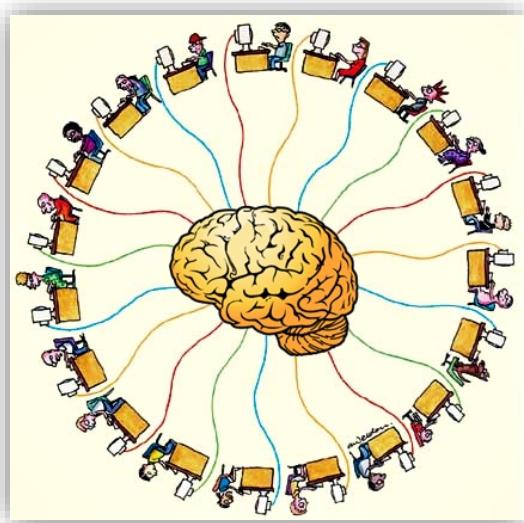


Características clave:

- **Colaboración:** La inteligencia colectiva se basa en la colaboración y el esfuerzo compartido entre los miembros del grupo.
- **Diversidad:** Fomenta la diversidad de pensamiento, lo que ayuda a reducir los sesgos cognitivos individuales y a generar ideas más innovadoras.
- **Sinergia:** El resultado de la colaboración es una sinergia donde el grupo es capaz de crear más valor conectando que sumando las partes por separado.
- **Toma de decisiones:** Permite tomar decisiones más informadas, acertadas y rápidas, aprovechando la experiencia de todos

Beneficios que aporta la inteligencia colectiva:

- 1) Logra resultados más sólidos, creativos y efectivos.
- 2) Optimiza la resolución de problemas complejos.
- 3) Aumenta la satisfacción de los miembros del equipo al sentirse parte de un éxito compartido.
- 4) Fortalece la cohesión y la confianza del grupo.



La clave del auge de la inteligencia colectiva radica en que podrás maximizar el potencial humano y lograr **resultados más sólidos, creativos y efectivos** al permitir que las habilidades y los conocimientos individuales se combinen y se aprovechen de manera colaborativa. No es de extrañar que el 78% de las compañías considere [la colaboración](#) como un aspecto esencial en el éxito empresarial, y que siete de cada diez organizaciones tengan planificado un aumento de la inversión en software social y comunicaciones grupales, según un [estudio](#) de IBM de 2021.

Ten en cuenta que la inteligencia colectiva engloba los conocimientos y las capacidades de todos los integrantes del grupo, lo que da lugar a ideas más innovadoras. Como consecuencia, **el resultado global será superior a la suma de los resultados individuales**. ¿Por qué, si no, hay equipos que, sobre el papel, deberían arrollar al rival por la calidad de sus integrantes en el plano individual y, sin embargo, no es raro ver sus derrotas ante formaciones más cohesionadas en el plano grupal?

Junto a esto, dado que cada integrante aportará habilidades complementarias y contará con información diferente, **la toma de decisiones será informada y acertada**, así como será más rápida y fácil **la resolución de problemas complejos**. Además, esta suma de mentes permite confrontar diferentes puntos de vista, reduciendo los sesgos cognitivos y aumentando **la satisfacción de los miembros del equipo**, ya que se sienten empoderados y parte activa del proceso, sin olvidar **las relaciones de confianza** que se generan en el ámbito interpersonal.



No obstante, para que los beneficios sean reales, hay que conocer y evitar también los **riesgos que plantea la inteligencia colectiva**. En este sentido, este trabajo conjunto puede provocar que los miembros del equipo tiendan a **ajustarse a las opiniones e ideas de la mayoría**. No olvides que no siempre la mayoría va a aportar la solución más acertada. Además, es importante tener en cuenta la **diversidad real** que presenta el grupo, así como el **grado de participación** de los integrantes, ya que, en ocasiones, determinadas personas acaparan las aportaciones, mientras otras permanecen calladas. Como señala Levy en su libro *[Inteligencia Colectiva. Por una antropología del ciberespacio](#)*, esa sinergia busca el reconocimiento y el enriquecimiento mutuo, no el culto de comunidades fetichizadas que dan lugar a totalitarismos.

¿Cómo desarrollar la Inteligencia Colectiva?

Es por esto que, para que puedas alcanzar el máximo potencial de la inteligencia de grupo o colaborativa, es recomendable tener en cuenta las siguientes **pautas a la hora de ponerla en práctica**:

- **Crea un entorno colaborativo.** Fomenta un entorno, físico o virtual, en el que se valore y se promueva la colaboración en un ambiente de respeto y confianza. Se trata de que las personas puedan reunirse, intercambiar ideas y trabajar juntas en proyectos comunes.
- **Impulsa la diversidad.** Procura que los grupos de trabajo sean heterogéneos. La [diversidad](#), en términos de habilidades, conocimientos, antecedentes y perspectivas, es esencial para enriquecer el proceso de colaboración y generación de ideas.
- **Propicia la comunicación.** Otro aspecto importante es que existan [canales de comunicación efectivos](#) que permitan el intercambio de información y el debate entre los miembros del grupo. Asimismo, no olvides garantizar una participación igualitaria durante este proceso, asegurándote de que todas las personas estén integradas.
- **Establece sistemas de toma de decisiones.** Para que el proceso deliberativo no se perpetúe eternamente, es necesario establecer los métodos que se van a utilizar para [adoptar decisiones](#).
- **Reconoce las aportaciones del grupo.** Por último, valora las contribuciones que se hagan tanto en el plano individual como grupal a través de alabanzas públicas, premios o incentivos tangibles. El reconocimiento fomentará la motivación y el compromiso de los miembros del grupo.

Siguiendo estos consejos, lograrás sacar el máximo partido a la inteligencia colectiva.



5.2. Contenidos abiertos.

Los contenidos abiertos son materiales (educativos, de investigación, etc.) que se comparten de forma gratuita en Internet bajo licencias abiertas, como las de [Creative Commons](#), lo que permite su reutilización, adaptación y redistribución sin restricciones o con restricciones mínimas. A diferencia de los contenidos disponibles en línea, que solo permiten el acceso, los contenidos abiertos también autorizan su modificación y uso para fines como la enseñanza, el aprendizaje o la investigación.

Características principales:

- **Acceso gratuito:** Son accesibles para cualquier persona de forma gratuita a través de Internet.
- **Licencias abiertas:** Se publican bajo licencias que permiten su uso y distribución libres, como las de Creative Commons o la [Licencia Pública General GNU](#). También pueden estar en dominio público.
- **Libertad de uso:** Permiten a los usuarios utilizar, modificar y redistribuir el contenido sin la necesidad de pedir permiso al autor, facilitando su reutilización.
- **Democratización del conocimiento:** Ayudan a reducir las barreras de acceso a la información y a los materiales educativos de alta calidad.

Ejemplos de contenidos abiertos:

1. Recursos Educativos Abiertos (REA): Son un tipo de contenido abierto diseñado específicamente para la enseñanza y el aprendizaje.

- ❖ Apuntes, guías didácticas y exámenes.
- ❖ Vídeos y cursos completos.
- ❖ Software educativo y simulaciones.

2. Investigación y otros materiales: Incluyen artículos científicos, datos de investigación, libros electrónicos y software en general que estén bajo licencias abiertas.

5.3 La Dimensión Social del Conocimiento.

La dimensión social del conocimiento es la idea de que todo saber se crea, se transmite y se valida dentro de un contexto social, cultural e histórico, siendo influenciado por las interacciones humanas, las estructuras sociales y los intereses de la comunidad. Esto significa que el conocimiento no es un producto aislado, sino un resultado de la colaboración, la comunicación y la negociación en una red de personas, instituciones y sistemas, como la ciencia y la tecnología.

Elementos clave de la dimensión social del conocimiento:

1. Contexto social e histórico: El conocimiento se forma y evoluciona en un momento y lugar específicos, lo que lo impregna de influencias sociales, políticas y culturales.



UD4. La Sociedad de la Información y del Conocimiento.



2. Interacción y colaboración: La creación y consolidación del conocimiento dependen de la participación de diversos actores sociales, como profesores, estudiantes, científicos y miembros de la comunidad.
3. Lenguaje y comunicación: El lenguaje y la capacidad de comunicar son esenciales para el intercambio de ideas y la construcción colectiva del conocimiento.
4. Propósito y valor social: El conocimiento tiene un valor social y se utiliza para el desarrollo económico, social y cultural de una sociedad, convirtiéndose incluso en un factor de producción.
5. Influencia mutua: Existe una relación bidireccional entre la sociedad y los sistemas de conocimiento; la sociedad moldea el conocimiento y, a su vez, este influye en las actividades, prioridades y necesidades sociales.

Implicaciones:

- a) Cultura científica: La cultura científica de una sociedad se construye no solo a partir de los hallazgos científicos, sino también de su integración en la vida diaria, la educación y la industria.
- b) Políticas públicas: El análisis de la dimensión social permite comprender las interconexiones entre ciencia, política, economía y sociedad, lo que es fundamental para el diseño y seguimiento de políticas públicas.
- c) Desarrollo social: Fomentar la creación y el uso del conocimiento de manera socialmente responsable contribuye a la prosperidad y al bienestar de las comunidades y culturas



UD4. La Sociedad de la Información y del Conocimiento.



TRABAJO DE INVESTIGACIÓN.

Este trabajo se realizará en Word, con tipo de texto arial 12, alineación izquierda, interlineado 1,15, con sangría izquierda y derecha de 6 puntos.

Encabezado (título “Trabajo de investigación la sociedad de la información y del conocimiento”) y pie de página (vuestro nombre con dos apellidos y el curso).

Ha de tener el trabajo imágenes e hipervínculos a páginas web y a videos.

TRABAJO DE INVESTIGACIÓN BLOQUES 6 Y 7.

6. Movilidad, ubicuidad y disponibilidad.

6.1. El teléfono inteligente

6.2. Tecnologías ubicuas

6.3. Navegar con dispositivos móviles

6.4. Correo electrónico

6.5. Geolocalización

6.6. Realidad aumentada

- Realidad aumentada y realidad virtual
- Realidad aumentada e inteligencia virtual

6.7. Apps

- Aplicaciones móviles para mejorar la productividad

7. Nuevos desarrollos de las TIC.

7.1. Robótica

7.2. Inteligencia artificial

7.3. Sistemas distribuidos

7.4. Litografía

7.5. Nanotecnología:

- Aplicaciones de la nanotecnología

7.6. Informática cuántica. ¿Qué es?

7.7. Bioinformática