DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel C2

ÍNDICE

DigitAll

Seguridad

4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel C2 4.1 Protección de dispositivos

Plan de respuesta a incidentes

Plan de respuesta a incidentes

Un plan de respuesta a incidentes es un conjunto de procedimientos y medidas diseñadas para manejar de manera eficiente y efectiva los incidentes de seguridad de la información o de ciberseguridad que puedan ocurrir en una organización.

Los objetivos de un plan de respuesta a incidentes son minimizar el impacto, restaurar la normalidad, proteger los activos de información, identificar la causa raíz, cumplir con los requisitos legales y normativos, y mejorar continuamente las capacidades de respuesta de la organización.

Las etapas de un plan de respuesta a incidentes pueden variar según la metodología o guía que se siga en su implementación, pero en todas ellas suelen existir las siguientes o una variante de estas:

1 | **Preparación:** esta etapa se enfoca en la preparación previa al incidente. Incluye la creación y documentación del plan de respuesta a incidentes, la designación y capacitación del equipo de respuesta, la identificación y clasificación de los activos críticos de la organización, y el establecimiento de políticas y procedimientos claros.

2 | **Detección y notificación:** en esta etapa, se monitorizan los sistemas y se utilizan herramientas de detección para identificar posibles incidentes que deberán ser notificados al equipo de respuesta.

3 | **Evaluación y clasificación:** en esta etapa, se lleva a cabo una evaluación inicial del incidente para determinar su naturaleza, alcance y gravedad.

4 | **Contención y mitigación:** en esta etapa, se toman medidas para contener y limitar el impacto del incidente. El objetivo es evitar que el incidente se propague y cause más daño.

5 | **Investigación y análisis:** después de contener el incidente, se lleva a cabo una investigación exhaustiva para comprender la causa raíz y el método de ataque. El análisis ayuda a comprender cómo ocurrió el incidente y qué medidas se deben tomar para evitar futuros incidentes similares.

GESTIÓN DE INCIDENTES

Gestión de incidentes y diseño de políticas de este tipo en las organizaciones. Tipos de incidentes de seguridad y pasos más comunes. Plan de contingencia y de continuidad de negocio.

e.digitall.org.es/A4C44C1V02

6 | **Recuperación y restauración:** una vez que se ha contenido y se ha realizado la investigación, se procede a la recuperación y restauración de los sistemas afectados.

7 | **Lecciones aprendidas:** después de completar la respuesta al incidente, se realiza una revisión y análisis exhaustivo de las acciones tomadas para mejorar el plan de respuesta a incidentes y fortalecer las medidas de seguridad de la organización.

Para ayudarnos en la implementación de este tipo de planes disponemos principalmente de dos herramientas, la norma ***ISO 27035*** (*e.digitall.org.es/iso-27035*) y la guía ***NIST SP 800-61*** (*e.digitall.org.es/nist-sp800-61*).

ISO 27035

La norma ISO 27035 es un estándar internacional de ISO que proporciona directrices y mejores prácticas para el manejo de incidentes, eventos y vulnerabilidades de seguridad de la información.

Se centra profundamente en la gestión de incidentes de seguridad de la información y abarca todo el ciclo de vida de un incidente, desde la preparación y detección hasta la respuesta, recuperación y aprendizaje.

Está diseñada para ayudar a las organizaciones a establecer y mejorar sus capacidades de respuesta a incidentes y a mitigar los impactos negativos de los incidentes de seguridad. Esta norma se puede considerar como una expansión de la sección de administración de incidentes de seguridad contemplada en la ISO 27002.

NIST SP 800-61

La NIST SP 800-61 es una guía publicada por el National Institute of Standards and Technology (NIST) de los Estados Unidos que pretende ayudar a las organizaciones en el establecimiento de la seguridad informática necesaria para tener la capacidad de respuesta ante incidentes y su tratamiento de manera eficiente. Esta publicación ofrece pautas para la gestión de incidentes, sobre todo para el análisis de datos y determinar la respuesta apropiada para cada tipo.

Estas directrices se pueden seguir de forma independiente según la plataforma de hardware, sistema operativo, protocolos o aplicaciones utilizadas

Al igual que la ISO 27035 aborda todos los aspectos del ciclo de vida de la gestión de incidentes y es ampliamente reconocida como una guía de referencia para el manejo de incidentes de seguridad de la información.

Seguridad

Nivel C2 4.1 Protección de dispositivos

Vulnerabilidades más extendidas: OWASP Top 10

Vulnerabilidades más extendidas: OWASP Top 10

Las tecnologías web son una parte fundamental de nuestra vida digital. La gran mayoría de los servicios que utilizamos diariamente, desde la banca electrónica o la gestión de la salud digital, están implementados sobre las tecnologías web: páginas, aplicaciones y servidores web que utilizan principalmente HTML, CSS y JavaScript para funcionar.

En esta sección se introduce la importancia de la seguridad de las aplicaciones web y las vulnerabilidades características de estas tecnologías. Para ello se profundiza en una de las referencias más extendidas y consensuadas de categorización de vulnerabilidades web, el OWASP Top 10.

El **OWASP Top Ten (Open Web Application Security Project Top Ten)** es una lista de las diez vulnerabilidades de seguridad más críticas en aplicaciones web. Fue creada por el Proyecto OWASP, una comunidad de expertos en seguridad de aplicaciones web que se dedica a mejorar la seguridad del software.

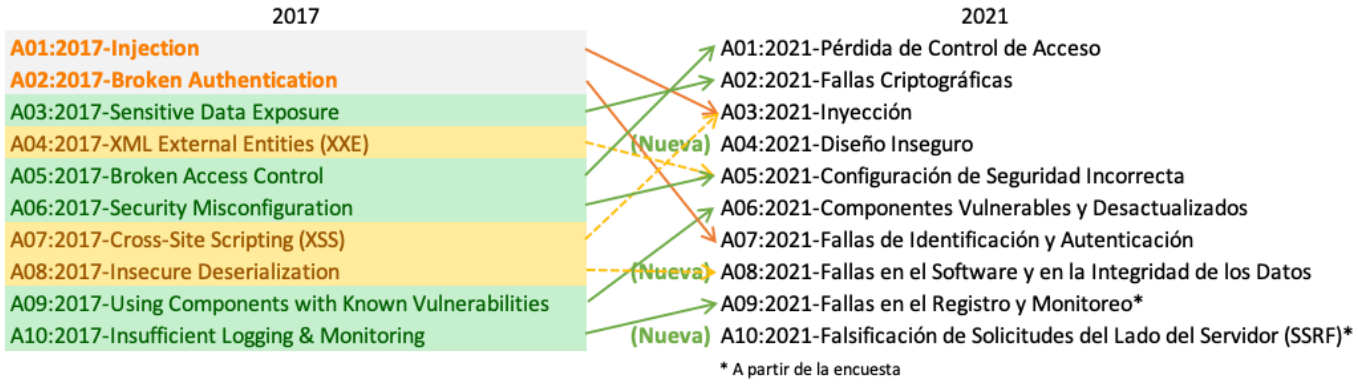
Web oficial del OWASP Top 10
owasp.org/www-project-top-ten

El propósito principal del OWASP Top Ten es proporcionar una guía para que los desarrolladores, profesionales de seguridad y organizaciones comprendan las **principales amenazas a las que se enfrentan las aplicaciones web** y tomen medidas para mitigar esos riesgos.

La lista se actualiza periódicamente para reflejar las nuevas amenazas y tendencias en seguridad de aplicaciones web. La última versión publicada, a fecha de elaboración de este documento, es la **OWASP Top 10 2021**. Sin embargo, un conocimiento muy interesante es el que nos brinda la posibilidad de comparar la versión anterior, el OWASP Top 10 2017, con la versión actual, para conocer cuáles son las tendencias en los últimos años a nivel de amenazas web. En los siguientes subapartados se explica en qué consisten las vulnerabilidades de cada categoría, las cuales están identificadas por un código, de la forma "A<ranking>:2021".

NOTA

La información utilizada para elaborar esta catalogación de las vulnerabilidades web proviene de diversas fuentes, como informes, análisis de incidentes, encuestas, etc. Estos datos son suministrados por expertos de seguridad y empresas especializadas en el sector, cuyo trabajo diario se basa en desarrollar y garantizar la seguridad de este tipo de aplicaciones.



Pérdida del control de acceso

La primera de las categorías del OWASP Top 10 2021 es "A01:2021-Broken Access Control", o pérdida del control de acceso. Este tipo de vulnerabilidades se refieren a situaciones en las que un sistema permite el acceso no autorizado, de forma equivocada, a ciertas funcionalidades o datos.

Un ejemplo de esto es cuando un usuario sin privilegios puede acceder a información confidencial o realizar acciones que deberían estar restringidas, como modificar registros de otros usuarios o acceder a secciones administrativas sin autorización adecuada.

Cabe destacar la tendencia que estamos viviendo en los últimos años con este tipo de vulnerabilidades, que han subido del puesto número cinco al primero desde la versión del 2017 del ranking.

Fallos criptográficos

La segunda categoría del OWASP Top 10 2021 es "A02:2021-Cryptographic Failures", en español, "fallos criptográficos". Esta categoría se enfoca en las debilidades relacionadas con el uso inadecuado de algoritmos criptográficos, gestión de claves y almacenamiento seguro de datos. Estas utilidades se utilizan para garantizar la confidencialidad e integridad de los datos, tanto de los usuarios como de las aplicaciones.

Un ejemplo común de fallos criptográficos es el uso de algoritmos de cifrado débiles o vulnerables, como el uso de cifrado obsoleto o el almacenamiento inseguro de claves, lo que podría permitir a un atacante descifrar datos confidenciales.

En la versión anterior de esta guía, esta categoría era conocida como “Sensitive Data Exposure”, o exposición de datos sensibles, situada en la tercera posición del mismo. En la versión actual, ha subido un puesto hasta colocarse en la segunda de las vulnerabilidades más críticas.

Inyección

El tercer tipo de vulnerabilidades se agrupan en la categoría “A03:2021-Injection”, las vulnerabilidades de inyección. Esta categoría agrupa aquellas vulnerabilidades que consisten en la inserción no deseada de código malicioso en aplicaciones web, generalmente a través de campos de entrada no filtrados o mal validados.

XSS Y SQL INJECTION

Conceptos de Cross-Site Scripting (XSS) y SQL Injection (SQLi), destacando su relevancia dentro del contexto de la seguridad de las aplicaciones web. Se explican las consecuencias de este tipo de ataques y cómo protegerse ante ellos.

e.digitall.org.es/A4C41C2V05

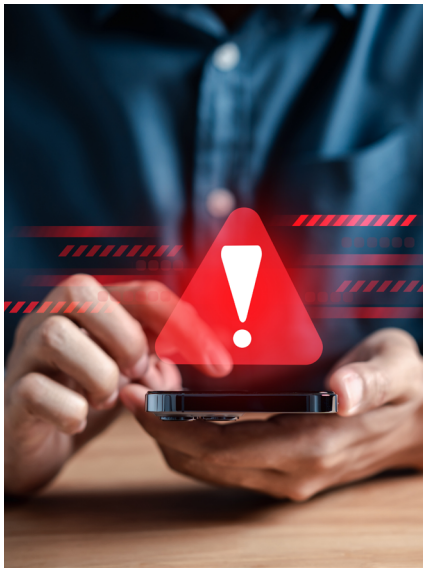
En OWASP Top Ten 2017 esta vulnerabilidad ostentaba la primera posición, y aunque en los últimos años haya caído en el ranking con respecto a otras categorías, sigue siendo una de las vulnerabilidades más críticas de la seguridad web.

Diseño inseguro

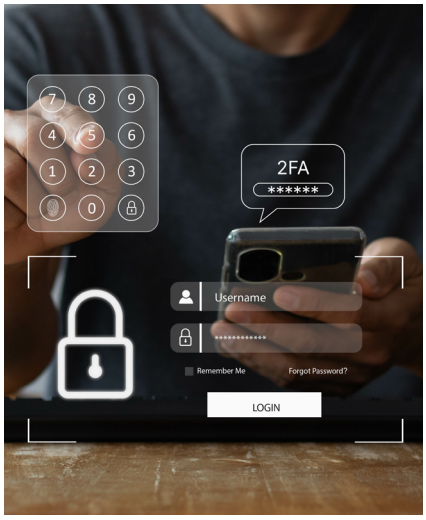
La categoría “A04:2021-Insecure Design” o diseño inseguro agrupa los fallos de diseño que pueden comprometer la seguridad de una aplicación. Esto implica la falta de consideración de los principios de seguridad desde el inicio del proceso de desarrollo.

Un ejemplo sería la falta de autenticación adecuada en un sistema, donde no se implementan medidas sólidas para verificar y autorizar a los usuarios, lo que permite el acceso no autorizado a recursos o datos confidenciales.

Esta es una de las categorías novedosas, que no existían en la versión de 2017, del ranking OWASP Top 10.



Configuración de seguridad incorrecta



En quinto lugar, se encuentran las vulnerabilidades "A05:2021-Security Misconfiguration" o de configuración de seguridad incorrecta. Estas se refieren a la configuración incorrecta de componentes de la aplicación y de los servidores que pueden permitir el acceso no autorizado o exponer información sensible.

Un ejemplo sería dejar accesibles directorios o archivos confidenciales a través de la configuración incorrecta de permisos de archivos o configuraciones de seguridad en un servidor web.

Componentes vulnerables y desactualizados

Esta categoría, "A06:2021-Vulnerable and Outdated Components" o componentes vulnerables y desactualizados, destaca los riesgos asociados con el uso de componentes de software que contienen vulnerabilidades conocidas o desactualizadas.

Un ejemplo sería utilizar una biblioteca o plugin obsoletos en una aplicación web, que tiene vulnerabilidades conocidas y que podrían ser explotadas por un atacante para comprometer la seguridad de la aplicación.

Fallos de identificación y autenticación

La séptima categoría del ranking es "A07:2021-Identification and Authentication Failures", que en español significa fallos de identificación y autenticación. Se refiere a debilidades en los mecanismos de identificación y autenticación de usuarios en una aplicación web. Esto puede incluir contraseñas débiles, falta de protección contra ataques de fuerza bruta o vulnerabilidades en el proceso de recuperación de contraseñas.

Un ejemplo es la falta de bloqueo de cuentas después de un número determinado de intentos fallidos de inicio de sesión, lo que facilita los ataques de fuerza bruta.

Fallos en el software y en la integridad de los datos

La octava categoría del OWASP Top 10 2021 es novedosa con respecto a la versión de 2017, y es "A08:2021-Software and Data Integrity Failures" o fallos en el software y en la integridad de los datos. Esta categoría se centra en los riesgos relacionados con la integridad y el comportamiento correcto del software, así como en la manipulación no autorizada de datos críticos.

Un ejemplo sería una aplicación que no realiza una validación adecuada de los datos de entrada, lo que podría permitir la introducción de datos maliciosos que podrían causar fallas en la aplicación o comprometer su integridad.

Fallos en los registros y monitorización de la seguridad

En la novena posición se encuentra "A09:2021-Security Logging and Monitoring Failures" o fallos en los registros y monitorización de la seguridad. Esta vulnerabilidad se refiere a la falta de un registro y monitoreo adecuados de eventos y actividades de una aplicación web. Esto puede dificultar la detección y respuesta ante incidentes de seguridad.

Un ejemplo sería la ausencia de un sistema de logs de eventos de seguridad, lo que dificulta la identificación de actividades sospechosas o ataques en curso.

Falsificación de solicitudes del lado del servidor

Por último, nos encontramos con una categoría muy específica, "A10:2021-Server-Side Request Forgery" o la falsificación de solicitudes del lado del servidor. Esta categoría se refiere a ataques en los que un atacante puede engañar al servidor para que realice acciones no deseadas en nombre del usuario legítimo.

Un ejemplo común es el ataque CSRF (Cross-Site Request Forgery), donde un atacante engaña al usuario para que realice acciones sin su consentimiento, como cambiar su contraseña o realizar transacciones no autorizadas.

Seguridad

Nivel **C2** 4.1 Protección de dispositivos

Red TOR

Red TOR

La red TOR es la red anónima en Internet más conocida. Permite navegar por servicios ocultos de la dark web, pero también acceder a cualquier servicio de Internet. Todo ello, de forma anónima. A continuación, se define qué es el anonimato, las redes anónimas y TOR.

Anonimato y privacidad

La privacidad y el anonimato son dos términos relacionados, pero su significado es diferente.

La privacidad se refiere al derecho de una persona a controlar la información que revela sobre sí misma y a decidir quién tiene acceso a ella. En el ámbito digital, la privacidad implica proteger los datos personales y asegurar que solo sean accesibles por las personas autorizadas. Esto implica tener control sobre qué información se recopila, cómo se utiliza, quién la utiliza y cómo se comparte.

El anonimato, por otro lado, se refiere a la capacidad de ocultar la identidad de una persona o mantenerla desconocida. Implica la posibilidad de realizar actividades en línea sin revelar información personal identificable, como nombre, dirección o cualquier otro dato que permita identificar a la persona detrás de una acción

Existen diferentes motivos por los que una persona necesita del anonimato en la red:

- **Libertad de expresión:** expresar las opiniones libremente sin temor a represalias, sobre todo de gobiernos u organizaciones represivas.
- **Conexión de personas:** conectarse en comunidades y grupos que compartan intereses similares sin miedo a la represión.
- **Libertad de investigación:** buscar información sin temor a ser juzgados o discriminados.
- **Periodismo y activismo:** filtraciones de información o publicación de noticias sobre gobiernos.

Tanto la privacidad como el anonimato son importantes como derechos digitales para proteger la información personal o identidad en el entorno digital. Sin embargo, es importante tener en cuenta que el anonimato absoluto puede plantear desafíos para la aplicación de la ley y la responsabilidad en línea, ya que puede permitir actividades ilegales sin dejar rastro.

Redes anónimas en Internet: Deep web y Dark web

Existen diferentes alternativas para conseguir anonimato en Internet. Ya hemos visto algunas opciones como el uso de redes virtuales (VPN) o proxies, lo que permiten ocultar la dirección IP de origen o ubicación geográfica. Sin embargo, esto requiere confianza en el proveedor de VPN o proxy.

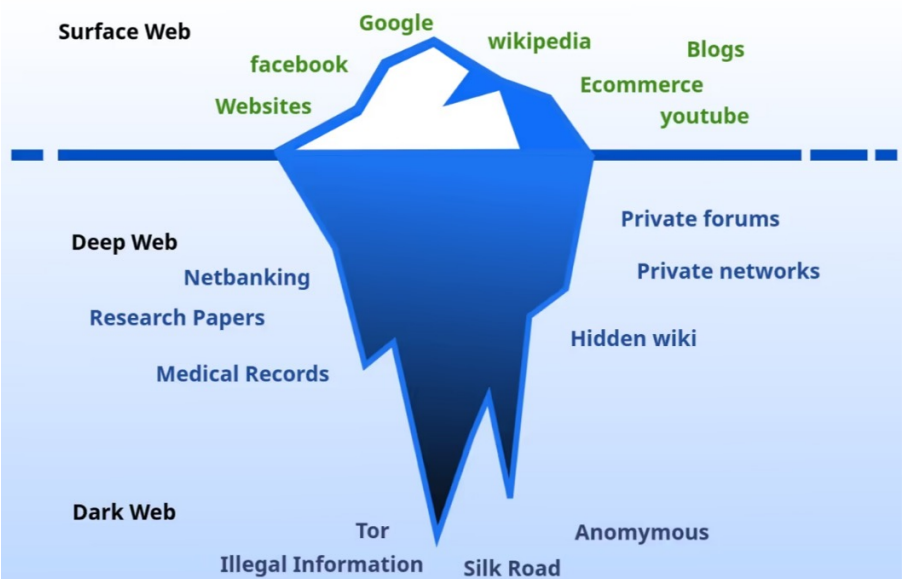
VPNS, PROXIES Y ANONIMATO EN LA RED

Las redes privadas virtuales o VPNs junto con los proxies permiten conectarse a diferentes redes o sitios web sin utilizar la dirección IP propia. De esta forma, permiten acceder a servicios y recursos en Internet con cierto nivel de anonimato.

e.digitall.org.es/A4C41C2V09

Por este motivo, varias iniciativas han creado lo que se conocen como redes anónimas. Las redes anónimas utilizan Internet para crear protocolos de comunicación que garanticen el anonimato de los usuarios. Por ejemplo, las redes Freenet e Invisible Internet Project (I2P) permiten a los usuarios conectados compartir contenidos y comunicarse de forma anónima. TOR, que veremos a continuación, es una red anónima que, además de permitir acceder a contenido dentro de la propia red, permite la conexión a servicios expuestos en Internet. Es decir, fuera de la red anónima.

Internet permite compartir información a través de la web, pero también crear redes anónimas que compartan contenido de forma anónima. La diferencia entre la web convencional y las redes anónimas se suele representar con la siguiente imagen.



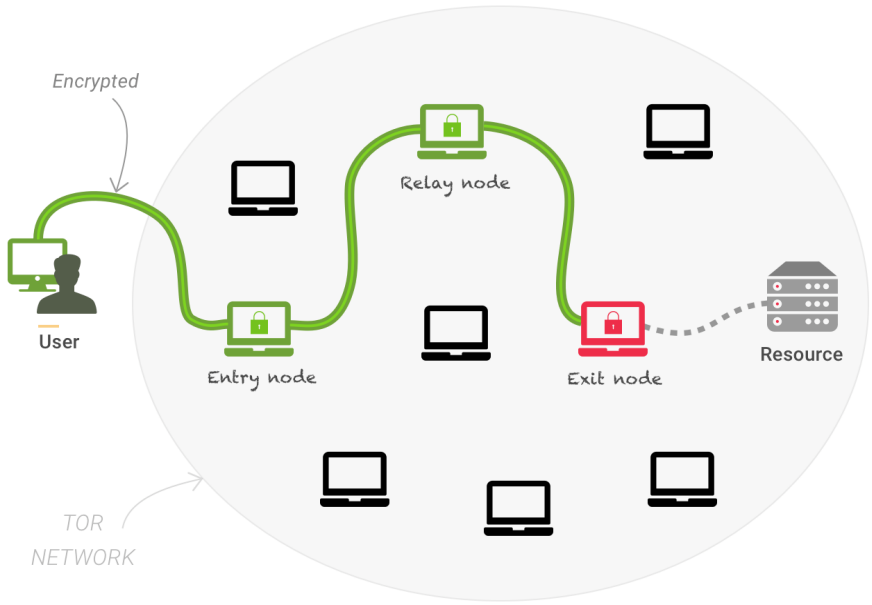
La web superficial o **Surface web** hace referencia a todas las páginas web a las que se puede acceder de forma convencional a través de Internet. Además, estos contenidos son indexados por los buscadores, como Google o Bing. Por lo tanto, se pueden encontrar y acceder fácilmente. Realmente, este tipo de contenido representa una pequeña parte de todo el contenido que puede accederse a través de Internet.
De esta forma, los contenidos como foros privados, redes privadas o cualquier contenido que no se pueda acceder sin pasar un control de acceso, se conoce como la **Deep web.** Esto es información que no está accesible de forma directa, ni que puede encontrarse usando buscadores como Google.

Por último, las redes anónimas forman parte de la **Dark web**. Estos contenidos sólo son accesibles a través de estas redes, utilizando esta tecnología.

The Onion Router (TOR)

El proyecto The Onion Router (TOR) ofrece un software que permite al usuario conectarse a la red TOR y acceder a contenidos de forma anónima. Este software utiliza el protocolo de comunicaciones “onion routing” o enrutamiento cebolla. Para asegurar el anonimato del usuario, el enrutamiento cebolla utiliza, al menos, dos nodos repetidores o “relays”.

Para conectarse a un sitio web, un usuario se conectará a un nodo repetidor quien, a su vez, se conectará a otro repetidor. El último nodo repetidor es quien, al final, se conectará al sitio web.



De esta forma, el primer nodo repetidor es el único que conoce al usuario, pero no sabe a dónde se conectará. Así mismo, sólo el último repetidor sabrá a dónde se está conectando, pero desconoce la identidad del usuario que ha iniciado la conexión. Para acceder a la red TOR sólo es necesario descargar el ***navegador TOR*** (*torproject.org*). Este navegador basado en Firefox permite conectarse y navegar por la red TOR, compuesta de servicios ocultos reconocibles por los dominios ".ONION".

⚠ ATENCIÓN

La Hidden Wiki es un servicio oculto accesible en la red TOR. Para acceder a él, es necesario utilizar el navegador TOR y usar el dominio ".ONION" de este sitio web:

http://paavlaytlfsqyvkg3yqj7hflfg5jw2jdg2fgkza5ruf6lplwseeqtvyd.onion/

Por último, es importante tener en cuenta algunas recomendaciones. Para navegar por TOR es recomendable hacerlo conectado a una VPN. Además, es muy importante tener en cuenta que en la red TOR prima el anonimato, por lo que hay que tener mucho cuidado con la ciberdelincuencia y navegar con cautela.

Seguridad

Nivel C2 4.1 Protección de dispositivos

Soluciones de anonimato en la red

Soluciones de anonimato en la red

Una vez hemos visto qué es el anonimato en la red, en este apartado se citarán diferentes utilidades que debes conocer para mantener tu identidad protegida.

RED TOR

Documento referenciado: ***A4C41C2D03***

Servicios VPN

Las redes privadas virtuales permiten conectarse de forma remota a una red. En el uso doméstico, los servicios VPN se utilizan para acceder a sitios web de forma anónima o para poder consultar contenido disponible sólo para ciertos países.

Es importante asegurarse de utilizar una VPN de pago que sean de confianza. Los servicios VPN deben tener una política de privacidad estricta, igual que los proveedores de conexión a Internet.

NordVPN

NordVPN es uno de los servicios más conocidos de VPN, con más de 5700 servidores alrededor de 60 países. Además, es compatible con multitud de dispositivos, incluyendo Linux, MacOS y Windows, pero también otros como dispositivos móviles e incluso Android TV.

NordVPN

NordVPN
nordvpn.com/es

ProtonVPN

ProtonVPN es un servicio ofrecido por una empresa suiza que apuesta por la privacidad de los usuarios. Permite usar hasta 10 dispositivos y ofrece altas velocidades. Además, permite configurar servicios como bloqueador de anuncios y privacidad avanzada. Igual que NordVPN, soporta un gran abanico de dispositivos.

Proton VPN

ProtonVPN
protonvpn.com/es

Mullvad VPN

Mullvad VPN es un servicio que promociona un alto nivel de privacidad y anonimato para sus usuarios, ya que permite registrarse y pagar el servicio de forma anónima. Tiene aplicaciones fáciles de usar y sencillas.

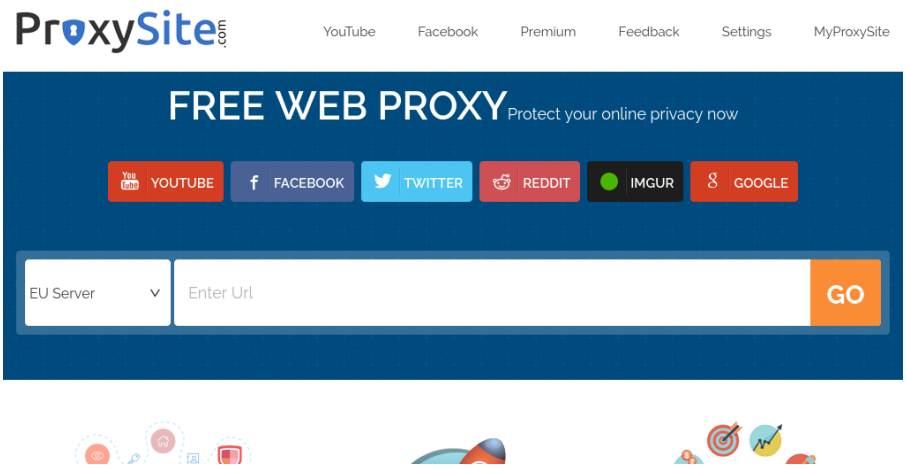
MULLVAD VPN

ProtonVPN
mullvad.net/es

Servicios Proxy

Por otro lado, existen servicios que permiten hacer consultas web en nuestro nombre. Es decir, permiten utilizar a un intermediario para navegar por webs sin exponer la dirección IP. Es destacable comentar que la mayoría de estos servicios ya se han mudado a servicios VPN.

ProxySite



Proxysite es un servicio que permite consultar cualquier web a través de su sitio web. Sólo con una dirección URL, se pueden visualizar contenidos bloqueados o disponibles exclusivamente en otros países.

ProxySite.com

ProxySite
proxysite.com

IP Vanish

Además de una VPN, IP Vanish ofrece un servicio de proxy con la tecnología SOCKS5. Esta tecnología se puede configurar como proxy en diferentes aplicaciones, como mensajería instantánea o el navegador web.

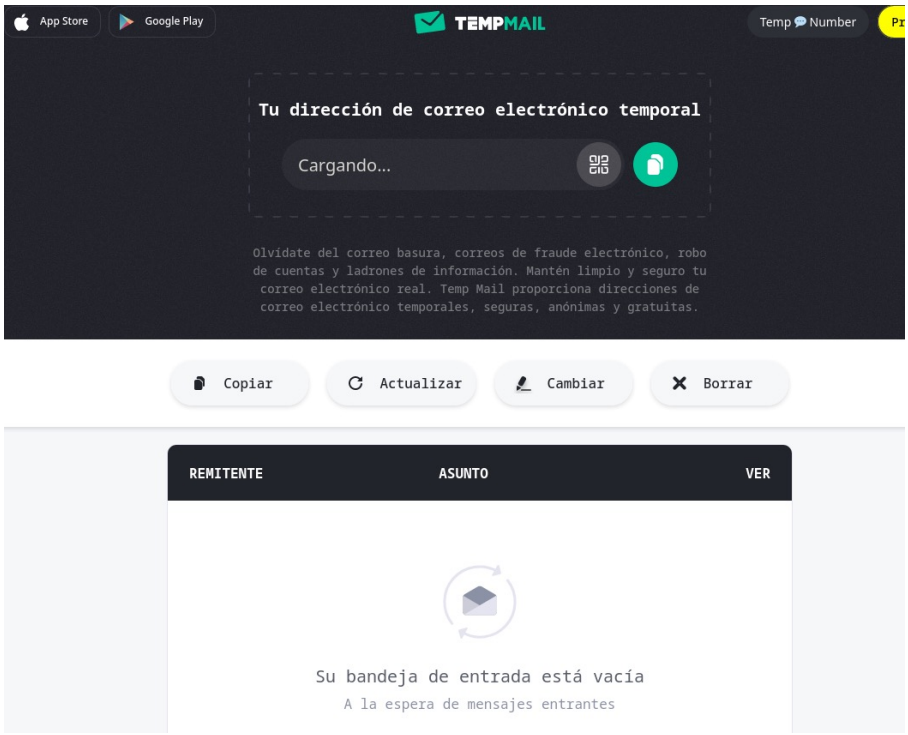
IPVANISH

IP VANISH
ipvanish.com/socks5-proxy

Mantener la identidad anónima

El anonimato en la red requiere de un esfuerzo considerable. Aunque se utilice TOR, para mantener el anonimato es muy importante mantener oculto cualquier dato personalmente identificable.

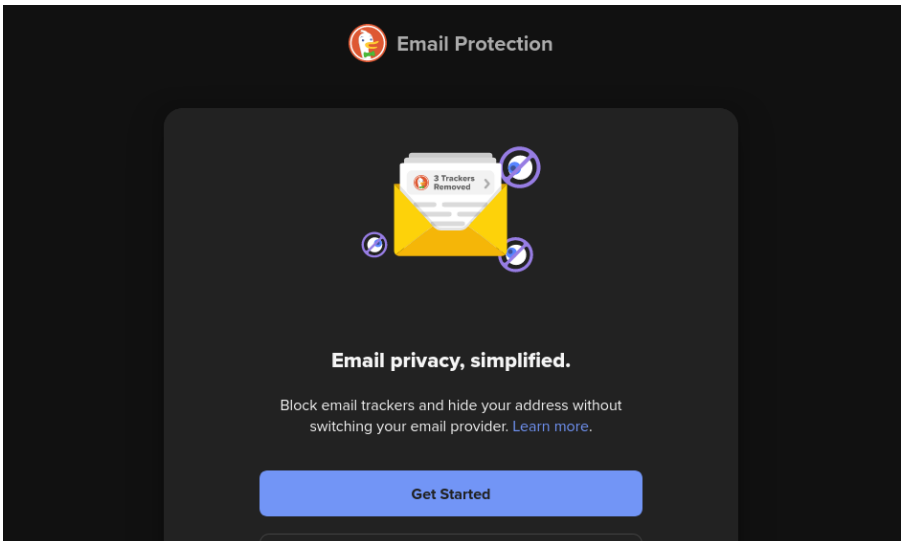
Bandeja de correo temporal



TEMPMAIL
temp-mail.org/es

En primer lugar, existen servicios online que requieren una dirección de correo electrónico para registrarse. Para evitar usar el correo personal, se pueden utilizar los servicios de correo temporal. Uno de los más conocidos es “Temp Mail”, aunque existen otros. Es importante tener en cuenta que este servicio es temporal, por lo que perderemos acceso a esa dirección de correo pasado el periodo de uso.

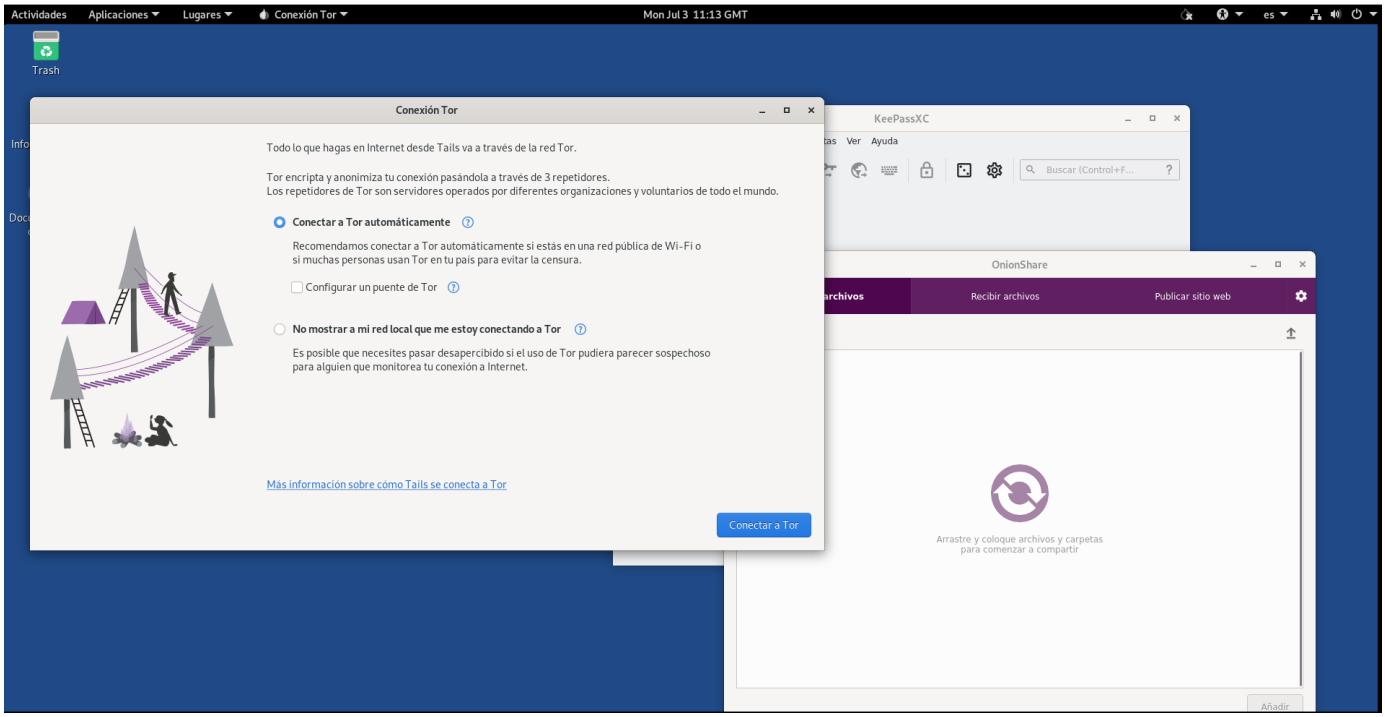
DuckDuckGo Email Protection



DuckDuckGO
duckduckgo.com/email

Si queremos mantener el acceso al correo temporal o utilizar nuestra cuenta sin revelar la dirección de correo real, podemos usar un proxy de correo electrónico. Esto nos permite ocultar la dirección de correo electrónico real tras una dirección de correo aleatoria. Uno de los servicios más conocidos es DuckDuckGo Email Protection, del famoso buscador. Una vez creada una cuenta, permite crear "alias" o pseudónimos de la dirección de correo real.

TailsOS: sistema operativo anónimo



TailsOS es un sistema operativo que unifica diversas tecnologías para ofrecer un nivel alto de privacidad y anonimato para el uso diario. Por defecto, usar TOR para la conexión a Internet.

Este sistema operativo pretende ejecutarse en cualquier ordenador desde un USB, intentando evitar cualquier sistema operativo no fiable y proporcionando "amnesia". Es decir, minimizando el registro de cualquier actividad.

TailsOS
tails.net

DigitAll

Seguridad

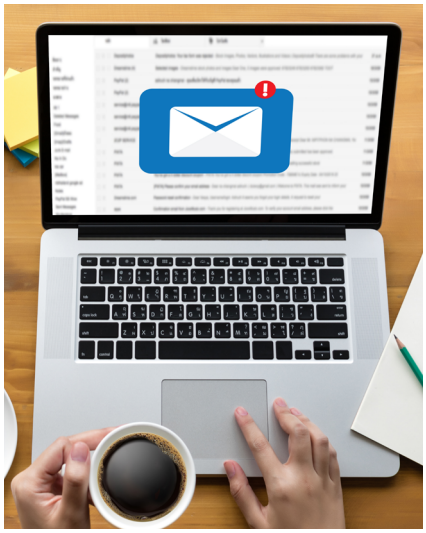
4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel C2 4.2 Protección de los datos personales y la privacidad

Privacidad en el email

Privacidad en el email



El uso del email está ampliamente extendido en la actualidad. Se estima que en el año 2022 se enviaron más de 330.000 millones de emails entre unos 4.000 millones de usuarios. Con tal volumen, el email es un negocio tan amplio que hay múltiples empresas involucradas. Incluso algunas que ofrecen de manera gratuita el servicio de email. Independientemente del número de emails y de la plataforma o aplicación de correo electrónico utilizado, es necesario garantizar que la privacidad de los usuarios no se vea comprometida.

Webmail

El correo electrónico o e-mail se puede utilizar tanto a través de aplicaciones como de plataformas web. Este último mecanismo es un servicio en la nube que se denomina webmail. Utilizando este sistema, los usuarios pueden enviar y recibir emails sin necesidad de instalar ninguna aplicación.

Existen muchas empresas que ofrecen webmail, algunas de pago y otras de forma gratuita. Estas ofrecen dirección de email para recibir y enviar correos electrónicos desde la web, aunque algunos proveedores proporcionan algunos servicios adicionales: conexión con clientes de correo electrónico, encriptación de correos, etc.

El webmail ofertado por muchas empresas no nos cuesta dinero, porque el coste se lo cobran con nuestra privacidad.

Estas empresas lo que desean son nuestros datos y nuestros perfiles de uso del email para poder vendérselo a terceros. Vamos a analizar algunas de las prácticas que pueden poner en riesgo nuestra privacidad.

Riesgos de privacidad en el uso de webmail

Al usar servicios webmail, si no tomamos algunas precauciones, podemos estar dejando desprotegida mucha información. El principal motivo es porque, salvo que se contrate y se active, los mensajes se envían sin encriptar.

⚠ ATENCIÓN

El contenido es accesible a cualquier sistema intermedio.

El segundo motivo es que los propios servidores webmail almacenan los mensajes desencriptados, por lo que, el propio servidor puede acceder al contenido con una potencial pérdida de privacidad. Los servidores argumentan la necesidad de dicho acceso para poder clasificar los mensajes recibidos e integrarlos en diferentes servicios en la nube, como el calendario personal, las notas, etc.

⚠ ATENCIÓN

Los servidores pueden acceder al contenido de nuestros mensajes y datos.

Por último, en función del país en el que se encuentre el servidor, los servicios de seguridad de dicho país podrían acceder al contenido de tus emails, simplemente con una solicitud al proveedor. Por ejemplo, si el servidor está en los EE.UU., la CIA o la NSA podrían obtener tus emails con una simple petición al proveedor.

⚠ ATENCIÓN

Entidades extranjeras pueden acceder a nuestros datos y mensajes, sin nuestra autorización.

Gmail

El servicio de email de Google se llama Gmail y, probablemente, es el servicio webmail más utilizado del mundo, precisamente por su integración con todo el ecosistema de servicios y aplicaciones de Google.

Desde 2017, Google no accede a tus emails por defecto, tienes que autorizarle para poder tener una integración efectiva. En estos casos, Gmail utiliza su servicio de análisis del contenido de tus emails para poder ofrecerte anuncios más adaptados a tus intereses, detectar posibles citas e incluirlas en tu calendario, cruzar perfiles de uso del navegador en el que estás accediendo a webmail con las búsquedas realizadas, etc.

En el caso de utilizar dispositivos con la ubicación activada, Gmail es capaz de establecer la localización desde donde se está accediendo al webmail, con la pérdida de privacidad que eso conlleva.

PRIVACIDAD EN LA NUBE

¿Cómo establecer medidas para evitar la pérdida de privacidad al usar servicios en la nube? Entre otras, ¿cómo evitar que ubiquen la localización desde donde estamos accediendo?

e.digitall.org.es/A4C42C2V04

Gmail no proporciona un sistema de encriptación de los mensajes ni de firma digital. Por lo que no es posible enviar mensajes cifrados ni firmados digitalmente sin el uso de extensiones.

Hotmail, Outlook.com

Microsoft lanzó diferentes plataformas webmail, aunque poco a poco todas ellas han ido migrando hacia un mismo servicio. Tal es así que si en el navegador buscas ***Hotmail*** (***hotmail.com***) te redirecciona hacia ***Outlook*** (***outlook.com***).

Outlook sí tiene un sistema reforzado de seguridad con la encriptación de los correos electrónicos.

Al igual que Gmail, el contenido del correo electrónico en Outlook se puede vincular al ecosistema de aplicaciones de Microsoft Office en la nube, aunque no es automático sino que el usuario debe activar en cada caso la transferencia del contenido hacia cada aplicación.

Outlook es un sistema webmail algo menos intrusivo que Gmail, aunque presenta características que afectan a la privacidad de los usuarios en cierta medida.

Otros sistemas webmail de mayor privacidad

Otros proveedores han tenido en cuenta las exigencias de algunos usuarios que solicitaban un mayor grado de privacidad que las plataformas webmail descritas en los puntos anteriores y lanzaron otras plataformas webmail de mayor privacidad.

Sistemas como ***ProtonMail*** (***proton.me***), con sede en Suiza, o ***tutanota*** (***tutanota.com/es***), con sede en Alemania, incorporan diferentes medidas de privacidad. El hecho de estar fuera del territorio de EE.UU. refuerza la privacidad, al no ser posible el acceso al contenido de los correos electrónicos, salvo por mandato judicial.

ProtonMail utiliza una doble contraseña: la primera para acceder al servicio y la segunda, para desencriptar el buzón. Así, se realiza un cifrado en el propio navegador del cliente usando esta segunda contraseña, desconocida totalmente por ProtonMail. Por tanto, todos los mensajes se envían cifrados desde el cliente y ProtonMail no puede acceder al contenido de los emails en ningún caso.

Tutanota es un servicio de webmail cifrado de extremo a extremo con muy alta seguridad, basado en el uso de Software Libre. En el caso de enviar mensajes a un usuario que no esté en Tutanota, se crea un hiperenlace a una cuenta temporal de Tutanota en la que, introduciendo una clave, previamente intercambiada con el usuario destinatario, podrá leer el mensaje desencriptado.

Aplicaciones de email

Otra opción es la utilización de aplicaciones en tu ordenador, tablet o smartphone que se encarguen del envío de los correos electrónicos directamente sin acceder a las plataformas webmail.

Si bien lo anterior es cierto con carácter general, de igual forma, hay que mantener algunas medidas para garantizar la privacidad. Estas medidas son aún más necesarias en el caso de dispositivos móviles.

⚠ ATENCIÓN

Las aplicaciones de email son más seguras y privadas que las versiones webmail.

PRIVACIDAD EN DISPOSITIVOS MÓVILES

Diversas consideraciones para garantizar nuestra privacidad en el uso de dispositivos móviles.

e.digitall.org.es/A4C42C2V03

Riesgos de privacidad en el uso de aplicaciones de email

Como se ha indicado, la utilización de aplicaciones de email es mucho más segura y tiene una mayor garantía de privacidad que el uso de webmail. Sin embargo, como cualquier servicio interconectado puede presentar algunos riesgos frente a la privacidad.

La inclusión de imágenes, vídeos y otros elementos HTML alojados en servidores remotos implica un riesgo. Al descargarse los diferentes elementos, el servidor donde está alojado es capaz de obtener información de la aplicación de correo electrónico: cuando se usa, dirección IP, sistema utilizado, etc.

⚠ ATENCIÓN

Lo ideal es tener configurado por defecto el bloqueo automático de descargas de remitentes desconocidos.

Otro riesgo es la respuesta automática de confirmación de recepción de mensaje. De esta manera, el emisor del email tiene constancia de que has recibido el correo electrónico y de que lo has abierto. Analizando la repuesta automática, el emisor original puede obtener información del receptor: que es una dirección de email activa, la dirección IP desde la que se ha mandado la respuesta automática, etc.

⚠ ATENCIÓN

Como recomendación, es preferible no activar por defecto la respuesta de confirmación de recepción de mensajes.

Microsoft Outlook 365

Una de las aplicaciones de correo electrónico más utilizada en el mundo es la versión en dispositivo del webmail Outlook, denominada en su última versión, **Microsoft Outlook 365**. Esta aplicación está desarrollada por Microsoft y permite una integración de este gestor de email con otras aplicaciones de la suite Office de esta empresa.

Microsoft Outlook 365
outlook.com

Esta aplicación incorpora en una sola aplicación el gestor de correo electrónico, junto con el calendario, un sistema de listas de tareas y la agenda de contactos.

La aplicación Outlook permite encriptar todos los mensajes utilizando el certificado digital, para realizar un cifrado asimétrico de llave pública y privada. Esto proporciona un nivel de privacidad muy alta extremo a extremo, es decir, que solo el receptor podrá leer el contenido del mensaje cifrado y no se guardará desencriptada en ningún servidor intermedio.

Hay versiones tanto para ordenador, versión Windows y para Mac, como para smartphone, en Android e iPhone.

Thunderbird

Thunderbird, desarrollado por Mozilla, que es la empresa detrás del famoso navegador Firefox, esta aplicación de correo electrónico es una opción muy interesante tanto en ordenadores personales, en Linux, Windows y Mac, como en dispositivos móviles, Android e iOS. Está construida usando Software Libre, siendo totalmente libre y gratuita.

Thunderbird
thunderbird.net/es-ES

Incorpora múltiples características de privacidad, como protección contra el rastreo de emails, bloqueo de contenido remoto, encriptación mediante certificado digital, etc.

The Bat!

Esta aplicación de correo electrónico es menos conocida que las anteriores, pero está diseñada para garantizar la máxima privacidad y seguridad. Utiliza la encriptación en todos los niveles: realiza todas las comunicaciones a través de canales seguros encriptados, cifra toda la información en el ordenador local, incorpora una encriptación extremo a extremo para el envío de los emails, etc.

Es capaz de funcionar sin respaldo de proveedores globales en la nube, para evitar dejar ningún mensaje fuera de tu ordenador.

The Bat! es de pago y solo tiene versiones para Windows.

The Bat!
e.digitall.org.es/thebat

Canary Mail

La aplicación **Canay Mail** integra tanto privacidad como productividad. La privacidad se garantiza con la combinación del cifrado asimétrico junto con la encriptación extremo a extremo. La productividad se fomenta con la incorporación de la Inteligencia Artificial para automatizar de manera inteligente muchas acciones, entre ellas, la detección de fraude por suplantación, eliminación de anuncios y descubrimiento de posibles emails de SPAM.

Esta aplicación tiene versiones tanto para ordenador, Windows y Mac, como para smartphones, Android e iOS.

Canary Mail
canarymail.io/es

Saber más

Privacidad en el email: algunas recomendaciones.
e.digitall.org.es/privacidad-email

Descubre 5 servicios de correo electrónico que respetan tu privacidad.
e.digitall.org.es/privacidad-email-2

ProtonMail. proton.me

tutanota. tutanota.com/es

Microsoft Outlook. outlook.com

Características de Thunderbird. e.digitall.org.es/thunderbird

The Bat! e.digitall.org.es/thebat

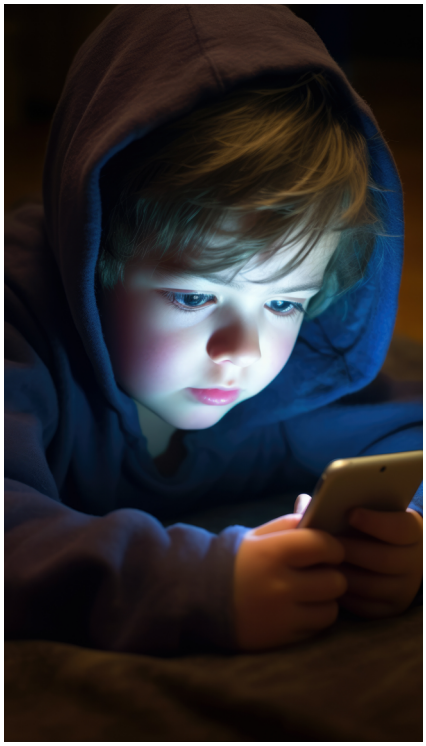
Canary Mail. canarymail.io/es

Seguridad

Nivel **C2** 4.2 Protección de los datos personales y la privacidad

Privacidad e Inteligencia Artificial

Privacidad e Inteligencia Artificial



Introducción

En la actualidad, los avances tecnológicos han permitido que pueda utilizarse una gran cantidad de información por parte de los sistemas informáticos, incrementando tanto la capacidad de computación como la de almacenamiento o comunicaciones. Esta información es captada de numerosas fuentes, entre ellas figuran, desde la información que directamente introducimos en nuestros ordenadores hasta la información que es adquirida o captada por innumerables dispositivos sensores (cámaras de vídeo, sensores ambientales, contadores de paso, sensores de peso, etc.), pasando por la propia información que nosotros mismos generamos en nuestra navegación cotidiana por redes sociales e internet en general (páginas que visitamos, vídeos visualizados, comentarios, preferencias de uso, etc.).

Toda esta información es recogida en servidores de datos que almacenan dicha información de forma más o menos estructurada, pero que permite establecer algoritmos o procesos de los que se pueden extraer información útil en la mayoría de los casos. Se trata del proceso de minado de datos que ayuda a instituciones y empresas a tomar decisiones sobre estrategias o desarrollos a implementar, o promociones y ofertas que ofrecer a determinados usuarios.

Estos avances tecnológicos, además, han permitido el establecimiento de sistemas automáticos para la presentación de información o toma de decisiones por parte de máquinas de forma autónoma en lo que se conoce como inteligencia artificial (IA).

Estas tecnologías, junto con los dispositivos móviles personales, las utilizamos cotidianamente y son elementos inseparables de nuestras vidas, interactuando entre ellas y afectando directamente a la información o contenidos con los que trabajamos o llegan directamente a nuestros dispositivos personales. Las redes sociales y el uso de dispositivos móviles que utilizamos diaria y asiduamente son una fuente importante de datos para tecnologías como la minería de datos o la inteligencia artificial, complementándose mutuamente y transformando la forma en la que consumimos contenido

digital. En este sentido, debemos contemplar, también, cómo de protegida está nuestra información particular y nuestros datos personales, en definitiva, nuestra privacidad y si ésta es utilizada de algún modo por estas tecnologías y en qué modo es utilizada. Para garantizar el uso responsable de estas tecnologías y contemplar los aspectos éticos que pudieran afectarles se trabaja actualmente en Europa, desarrollando y difundiendo una guía para adaptar al RGPD (reglamento general de protección de datos) los productos y servicios que utilizan inteligencia artificial.

La privacidad de la información y la protección de datos son conceptos que se han desarrollado en algunos vídeos, como los siguientes:

POLÍTICA DE PRIVACIDAD EN INTERNET Y EN LAS APLICACIONES

Se comenta el concepto de política de privacidad. Dónde encontrar el documento de políticas de privacidad tanto en Internet como en cualquier aplicación. Importancia de la política de privacidad. Contenido de un documento de política de privacidad.

e.digitall.org.es/A4C42A1V07

POLÍTICA DE PRIVACIDAD. INFORMACIÓN PRIVADA

El vídeo muestra generalidades en el uso de aplicaciones de mensajería instantánea, haciendo especial énfasis en las políticas de privacidad y compartición de datos.

e.digitall.org.es/A4C42A2V05

¿QUÉ INTRODUCIMOS EN NUESTRO ORDENADOR CUANDO NAVEGAMOS?

El concepto técnico de cookie, cómo se almacena en nuestro navegador la información que nos envían desde una web. Función inicial de las cookies y usos maliciosos (malware y gusanos). Cuidado con aceptar cookies de sistemas no confiables.

e.digitall.org.es/A4C42B2V06

Además, en el vídeo que se indica a continuación se desarrollan conceptos de inteligencia artificial (IA), minería de datos y cómo debemos proceder para proteger la privacidad de los individuos.

INTELIGENCIA ARTIFICIAL, MINERÍA DE DATOS Y PRIVACIDAD

El uso cada vez más generalizado de nuestros datos personales por parte de la Inteligencia Artificial, la Minería de Datos y los algoritmos en general, plantea nuevos retos frente a los que debemos estar atentos para preservar nuestra privacidad.

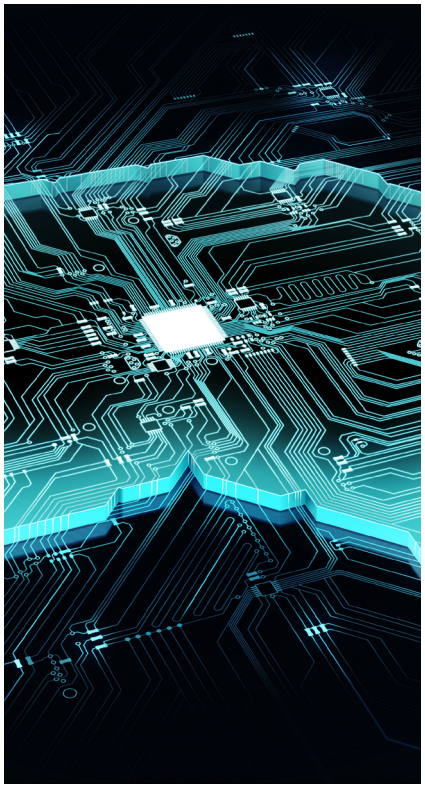
e.digitall.org.es/A4C42C2V06

En este documento se desarrollan, de forma resumida, los conceptos de inteligencia artificial, minería de datos y la relación que dichas tecnologías pudiera tener con la privacidad y protección de nuestros datos personales.

Inteligencia Artificial. Concepto y aplicaciones

La inteligencia artificial puede definirse, según diversos autores, como la habilidad de una máquina o sistema automático de presentar de forma autónoma las mismas capacidades de razonamiento, aprendizaje, planificación y creatividad que el ser humano. La inteligencia artificial permite a estos sistemas automáticos percibir su entorno a través de sensores, relacionarse con él, resolver problemas y actuar con un fin específico.

Los sistemas de inteligencia artificial son capaces de procesar la información de su entorno u otra información externa al mismo, adaptar una respuesta al comportamiento esperado y analizar los efectos que su decisión tendrá teniendo en cuenta las acciones previas realizadas.



El uso de la inteligencia artificial está en pleno auge debido al desarrollo de algunas aplicaciones, entre las más destacadas se encuentran aplicaciones, fundamentales a día de hoy, para diversos temas como: marketing, con aplicaciones IA específicas para comercio electrónico, envío de emails, o publicidad on-line; asistentes virtuales, que responden a preguntas, realizan determinadas tareas y recomendaciones como Siri o Alexa; automatización del hogar; sistemas de recomendación de visionado de contenido multimedia, como canales de televisión o preferencias web; sistemas de traducción automática; sistemas de conducción autónoma; asesoramiento y predicciones, desde predicciones meteorológicas a asesoramiento financiero; reconocimiento facial; y diagnósticos médicos.

Se puede resumir que los tipos de inteligencia artificial son dos, según la comisión de la Unión Europea: IA software, donde se incluyen análisis de imágenes, asistentes virtuales, motores de búsqueda y sistemas de reconocimiento de voz y rostro; e IA integrada, donde estarían los robots, drones, vehículos autónomos o internet de las cosas.

Minería de datos. Definición, métodos y técnicas

La minería de datos puede definirse como el análisis computacional automatizado de información en formato digital, según la comisión europea, e incluye en esta información textos, sonidos, imágenes y datos. La minería de datos hace posible el tratamiento de grandes cantidades de información con el fin de adquirir nuevos conocimientos y descubrir nuevas tendencias, pautas o correlaciones. Realmente, se trata de descubrir patrones de comportamiento y otra información valiosa en grandes conjuntos de datos.

La evolución tecnológica en almacenamiento de información y capacidades computacionales ha hecho posible que el procesamiento de grandes cantidades de datos (big data) evolucione y se desarrolle como materia propia, y la tecnología de procesado de grandes volúmenes de datos se ha convertido en una ciencia en sí misma. Previo a la aplicación de técnicas y modelos de búsqueda de resultados en los datos es preciso realizar un análisis de los mismos y preprocesado de datos para definir cuáles de ellos son realmente significativos y cuáles hay que obviar o eliminar del análisis final.

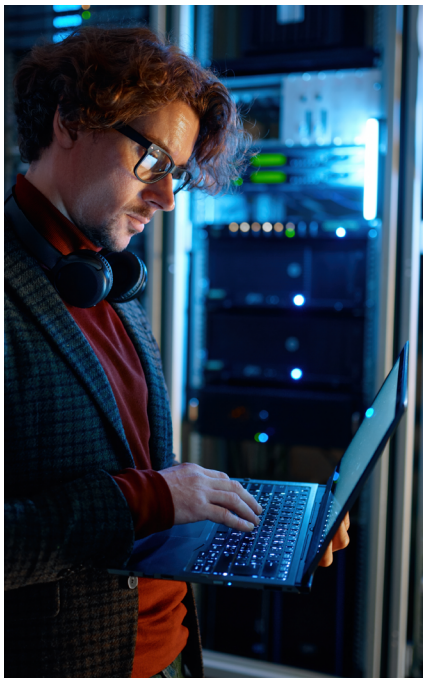
En la actualidad, empresas e instituciones utilizan técnicas y tecnología de minería de datos asiduamente en la toma de decisiones, a través de multitud de herramientas que analizan datos (desde el propio Excel, pasando que Qlik, Knime, R, o Tableau, hasta Oracle Data Mining).

Actualmente, se está desarrollando el concepto de “espacio de datos”, y desarrollo de los gemelos digitales, como un método de conocer previsiones certeras sobre distintos ámbitos o entornos de trabajo. Así, podemos encontrarnos el concepto de espacio de datos en temas de agricultura, ganadería, industria o socio-culturales. Un espacio de datos es el conjunto de

varias fuentes distintas de grandes cantidades de datos que ayudan a saber, por situaciones anteriores similares, qué va a suceder en el futuro y, de esta forma, tomar la decisión más certera para esto suceda o no. Es posible, por ejemplo, saber con antelación cuál va a ser la cosecha de aceite de oliva cuando tenemos todos los datos posibles sobre qué sucedió en campañas anteriores. Disponiendo de grandes cantidades de datos sobre meteorología, condiciones ambientales, características del terreno, humedad, fertilizantes, plagas, etc., podemos, en base a la información actual, predecir la cantidad y calidad de aceituna que será recogida. Aunque éste puede parecer un ejemplo sencillo, que es posible conocer con el análisis disponible en herramientas que utilizamos habitualmente como Excel (en su apartado de análisis de datos podemos encontrar diversas herramientas básicas de análisis como correlación, medias, histogramas, regresión, estadísticas descriptivas, covarianza, etc.), es bastante habitual utilizar herramientas más complejas y desarrolladas a medida dependiendo del tipo de sistema.

Interrelación entre IA y Minado de Datos

Tras las distintas etapas en las que se divide el proceso de minado de datos (como definir el objetivo de su proceso de minería y limpiar, analizar o preprocesar los datos) y llegar a determinar el conjunto de datos sobre el que se realizará el trabajo real de minería de datos es donde se necesita o utiliza la inteligencia artificial, en lo que se denomina aprendizaje automático, pudiendo ser éste supervisado o no supervisado.



La técnica más común utilizada en **aprendizaje supervisado** son las Redes neuronales, donde se dividen los datos en dos conjuntos y se deja que la red *aprenda* a clasificar sus datos, se entrena la red para clasificar los datos. **Por otro lado**, la técnica más común en **aprendizaje no supervisado** es el Algoritmo genético, no se supervisa porque no enseña nada, se ejecuta el algoritmo en el conjunto de datos y se espera a descubrir relaciones ocultas entre los datos.

Los grandes volúmenes de datos y el big data forman parte de la inteligencia artificial por cuanto supone de disponer de información que puede ser procesada. La inteligencia artificial analiza los datos de formas que los humanos son incapaces de hacer, para nosotros habría demasiadas personas con las que

comparar y demasiados puntos de información para mirar. Sin embargo, las soluciones de inteligencia artificial encuentran patrones donde las personas incluso nunca piensan en mirar. Pueden encontrar nuevas tendencias en cosas como datos de redes sociales, datos financieros e incluso datos geográficos. Por ejemplo, la inteligencia artificial puede saber si es probable que alguien compre un producto en función de sus inclinaciones políticas, para ello, solo necesita mirar a través de los perfiles de las redes sociales y compararlos con toda la información de la que dispone a través del big data, los datos son el combustible que mantiene la inteligencia artificial en funcionamiento. Además, la inteligencia artificial recopila información mientras busca patrones, y esta información se agrega a bases de datos llenas de información: infraestructura de big data. De este modo, el big data y la inteligencia artificial se apoyan mutuamente para crear una poderosa máquina de análisis. Por ejemplo, si alguna vez te han recomendado una serie en Netflix que te ha gustado, es porque la inteligencia artificial de la plataforma ha utilizado tus datos de consumo.

La privacidad de datos asociada al uso de inteligencia artificial, minería de datos

Nuestra identidad digital y hábitos de navegación en internet quedan registrados a través de cookies, que nosotros autorizamos, donde permitimos acceso a terceros a dicha información. Estos terceros son, habitualmente, empresas que trabajan y desarrollan técnicas de minería de datos e inteligencia artificial para ofrecernos ofertas, productos, promociones o servicios que puedan resultar de nuestro interés. Además, dependiendo de la información que compartimos en las redes sociales o en la autorización de nuestros datos podremos encontrarnos más o menos ofertas, productos o información dedicada específicamente a nosotros mismos en internet. En este sentido, nos ofrecerán productos que probablemente resulten de nuestro interés y no sepamos cómo o porqué se produce eso. Aunque todos conocemos cómo se utilizan nuestras preferencias en las redes sociales.

En contraposición a lo comentado, existe el Reglamento General de Protección de Datos, que protege o debería proteger nuestra información particular de la utilización por parte de los demás. En este sentido, y ante los cambios tecnológicos

y avances tanto en minería de datos como inteligencia artificial, se están proponiendo soluciones o respuestas a la desprotección que podamos tener en relación a estas tecnologías.

En concreto, la Agencia Española de Protección de Datos ha publicado una ***guía para adaptar al Reglamento General de Protección de Datos los productos y servicios que utilicen Inteligencia Artificial*** (*e.digitall.org.es/adecuacion-rgdp*). Este documento se centra en la adecuación al reglamento de protección de datos de aquellos tratamientos de datos que incorporen partes de inteligencia artificial que desarrollan soluciones a un problema concreto y acotado, no interviene o refiere al desarrollo de la inteligencia artificial de forma genérica como tecnología ni a los procesos de investigación implicados en la misma.

La guía está dirigida a responsables de sistemas y desarrolladores que incorporen o den soporte, respectivamente, a elementos de inteligencia artificial en sus programa o tratamientos de datos, ya que estos elementos podrían estar tratando datos personales en distintas fases o etapas del ciclo de vida del sistema y, por consiguiente, tendrían que cumplir con las obligaciones del RGPD. Además, se repasan las relaciones que podrían establecerse entre el responsable del tratamiento de datos personales y terceros que podrían estar interesados en desarrollar IA con dichos datos.

En la guía se recogen las condiciones que deben cumplir estas tecnologías para garantizar y demostrar que el tratamiento efectuado se adecua al RGPD. Entre estas condiciones se plantean aspectos como la legitimación para el tratamiento de datos, la información procesada y generada, el ejercicio de derechos y la toma de decisiones automatizadas. El documento se centra, también, en aspectos como la exactitud de la información, la minimización de los datos utilizados, la evaluación que el impacto de los resultados de la aplicación de la IA pudiera acarrear y un análisis de la proporcionalidad del tratamiento de datos. Incluso, analiza la posibilidad de que el uso de tecnologías basadas en IA implique transferencias internacionales de datos.

En definitiva, la Agencia pone de manifiesto que la puesta en el mercado de tecnologías que hacen tratamientos de datos en los que se utiliza inteligencia artificial exige que se apliquen garantías de calidad y privacidad, y exige cierto nivel de madurez a los modelos de inteligencia artificial, de forma que se pueda determinar objetivamente la adecuación de los tratamientos y la existencia de medidas para gestionar los riesgos que pudieran generarse.

Saber más

¿Qué es la inteligencia artificial y cómo se usa? Parlamento Europeo. e.digitall.org.es/inteligencia-artificial-uso

Protección de datos de carácter personal. Instituto Nacional de Administración Pública. e.digitall.org.es/proteccion-datos-sede

Big data, privacidad y protección de datos. Agencia Española de Protección de Datos. e-digitall.org.es/big-data

Guía de adaptación al RGPD de productos y servicios de inteligencia artificial. Agencia Española de Protección de Datos. e.digitall.org.es/adecuacion-rgdp

Seguridad

Nivel **C2** 4.2 Protección de los datos personales y la privacidad

Profundización sobre los delitos informáticos

Profundización sobre los delitos informáticos

Los delitos contra los sistemas informáticos o las TIC

Las expresiones "delitos informáticos" o "ciberdelitos" no aparecen como tales en el Código Penal español. Sin embargo, habitualmente se suelen incluir en las mismas las siguientes dos categorías de delitos:

1 | Aquellos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC.
2 | Aquellos en los que la actividad delictiva se sirve de manera determinante de la informática o las TIC como medio.

LOS DELITOS INFORMÁTICOS

En este vídeo se han analizado de manera genérica y sintéticamente los delitos más relevantes que se pueden incluir en ambas categorías y se han expuesto ejemplos de todo ello.

e.digitall.org.es/A4C42C2V07

Como complemento, en este documento se recogerán con más detalle las conductas que pueden incluirse en cada uno de esos delitos mediante la reproducción de los preceptos del Código Penal que las definen o tipifican. Esas definiciones o tipos son esenciales, pues para que una conducta pueda ser castigada tiene que encajar exactamente en ellos. Si falta algún requisito no se podrá sancionar.

NOTA

Si programo un virus y simplemente lo guardo en mi ordenador no hay delito, pues la definición del Código Penal exige que se haga con la intención de facilitar otros delitos.

ATENCIÓN

Para que una conducta pueda sancionarse tiene que encajar exactamente en la definición o tipo que recoja el Código Penal.

En la primera categoría expuesta se pueden incluir los delitos que se enumeran en los siguientes subepígrafes:

Delitos de daños, sabotaje informático y ataques de denegación de servicios

"El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave" (*artículo 264 Código Penal*).

Delitos de acceso sin autorización a datos, programas o sistemas informáticos

"...al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado" (*artículo 197.3 del Código Penal*).

Delitos de descubrimiento y revelación de secretos de empresa archivados en soportes informáticos o electrónicos

"El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197..." (*artículo 278 del Código Penal*).

Delitos contra servicios de radiodifusión o interactivos

"...el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º" (*artículo 286 del Código Penal*).

Los delitos en los que la actividad delictiva se sirve de la informática o TIC

Delitos de estafa

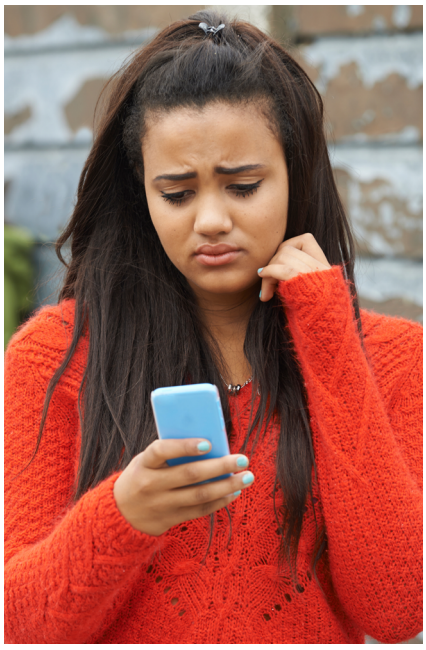
"1.[...] a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."

"2. [...] a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo". (*artículo 249 del Código Penal*).

Delitos de acoso y corrupción de menores/personas discapacitadas; o relativos a pornografía infantil/ personas discapacitadas

"El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 (realización actos de carácter sexual) y 189 (pornografía)..." (*artículo 183 del Código Penal*).



Delitos de hostigamiento

"1. ... el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de esta forma, altere el normal desarrollo de su vida cotidiana: [...]

2ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación…

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella. […]

5. El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación, …" (*artículo 172 ter del Código Penal*).

Delitos contra la propiedad intelectual

"…quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios" (*artículo 270 del Código Penal*).

Saber más

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
e.digitall.org.es/boe-25444

Ministerio del Interior. Informe sobre la Cibercriminalidad en España 2021.
e.digitall.org.es/estadisticas

DigitAll

Seguridad

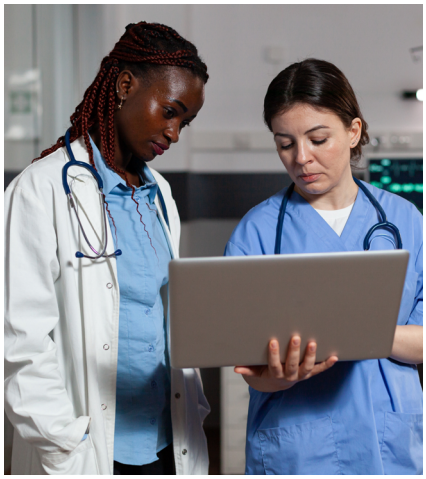
4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel **C2** 4.3 Protección de la salud y el bienestar

Recopilación de fuentes fiables de salud en Internet

Recopilación de fuentes fiables de salud en internet



Recopilación de fuentes fiables en internet

En este documento presentaremos una serie de recursos en los que consultar fuentes fiables en internet para temas relacionados con la salud. Por ello, hemos seleccionado una serie de recursos, que pueden ser de utilidad, y, sobre todo, para que lo puedas tomar como referencia para seleccionar otras posibles fuentes.

Medline

MedlinePlus es un servicio informativo en línea de salud para pacientes, familiares y amigos. Tiene por objetivo brindar información de calidad sobre la salud y el bienestar, ofreciendo datos fiables y fáciles de entender.

La información de esta fuente de salud procede de la Biblioteca Nacional de Medicina de EE. UU (NLM), la biblioteca médica más grande del mundo, que forma parte de los Institutos Nacionales de la Salud de EE. UU. (NIH).

A la página se puede acceder de forma gratuita desde cualquier dispositivo y en los idiomas de inglés y español.

Salupedia

Salupedia es una enciclopedia médica online que recupera, clasifica y ordena la información sanitaria contenida en Internet que este respaldada por profesionales del sector.

Se basa en las publicaciones que realizan los profesionales del sector recomendándole a los pacientes, familiares y ciudadanos, contenidos de salud ya existentes en la red.

De esta manera, el ciudadano encuentra un lugar donde acceder a información confiable recomendada por profesionales; y el profesional, a su vez, dispone de un lugar de confianza donde dirigirse a sus pacientes cuando quiere prescribir información.

Agencia Española de Medicamentos y Productos Sanitarios

La Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) es una agencia estatal adscrita al Ministerio de Sanidad.

Tiene por objetivo garantizar a la sociedad la calidad, seguridad, eficacia y correcta información de los medicamentos y productos sanitarios, desde su investigación hasta su utilización.

En su web ofrece información sobre medicamentos, productos sanitarios, cosméticos, productos de cuidado personal y biocidas, promoviendo el conocimiento científico-técnico.

Sociedad Española de Medicina de Familia y Comunitaria

Es una sociedad científica médica, sin ánimo de lucro, que vela por el adecuado desarrollo de la Medicina familiar y comunitaria (MFyC) en España. Actualmente es la sociedad científica más grande del país.

La semFYC está integrada por las 17 Sociedades de Medicina de Familia y Comunitaria que existen en España y reúne a más de 20.000 socios especialistas en la medicina de familia.

A través de su página web se puede realizar una búsqueda de filtrado por diversas competencias clínicas (ecografía, cardiovascular, dermatología, infecciones...), se pueden encontrar diversas publicaciones científicas y de salud, eventos del sector y otros temas de actualidad sobre medicina.

Sociedad Española de Médicos de Atención Primaria

La Sociedad Española de Médicos de Atención Primaria (SEMERGEN) ha creado una web cuyo objetivo es informar y formar al paciente, con criterios médicos adecuados, consensuados y documentados, sobre diversos temas del ámbito de la medicina y salud.

La web, llamada Pacientes Semergen, surge para hacer frente al exceso de información médica al alcance de cualquier internauta, la cual puede suponer un importe riesgo para la salud de la población.

Dentro de ella se puede encontrar una sección de preguntas y respuestas, en la que se recibe respuesta directa de los profesionales, un apartado de enfermedades frecuentes, además de diversas noticias de actualidad relacionadas con la salud.

PiCuida

PiCuida es la Red de Cuidados de Andalucía, creada por la Estrategia de Cuidados de Andalucía (Servicio Andaluz de Salud). En su web oficial se puede encontrar información científica y médica sobre diversos temas de la salud.

La plataforma cuenta con una biblioteca de búsqueda donde se puede buscar la palabra clave que se quiera, o bien elegir una categoría ya predeterminada del sector (atención a la infancia, cuidados y salud mental, ética y cuidados, preguntas clínicas...).

Saber más

La página web oficial de la Organización Mundial de la Salud (OMS) cuenta con un buscador alfabético donde se pueden buscar diversas enfermedades o patologías por su letra inicial. Además, dispone de un apartado de publicaciones, comunicados o artículos relacionados con el tema de la salud.

who.int/es

Recomendaciones para reconocer una página fiable

Internet nos da acceso a multitud de fuentes de información relacionadas con diversas temáticas como la salud. Sin embargo, tal y como se abordó en el vídeo 03 de este nivel no todas las páginas web sobre salud a las que podemos acceder son fiables. La selección y recopilación de la información fiable sobre salud en internet es importante para evitar ciertos problemas en nuestra salud mental. Pero ¿qué pautas podemos seguir para reconocer una página fiable? A continuación, se muestran algunos de los principios básicos a seguir para distinguir estas páginas.

NOTA

La fiabilidad de la información en internet hace referencia a la probabilidad de que la información que se adjunta en esa página web sea válida y de calidad, basándose en fuentes científicas principalmente. Para más información puedes revisar el vídeo: ***Fiabilidad de la información de salud en Internet***.

FIABILIDAD DE LA INFORMACIÓN DE SALUD EN INTERNET

e.digitall.org.es/A4C43C2V03

Patrocinador/a del sitio web

Además de conocer la información relevante sobre el autor/a que escribe la información a la que tenemos acceso. También, es necesario conocer quién patrocina esta página web. Por lo que, la URL de esta página nos puede ofrecer información útil en este sentido. Así, por ejemplo: .gov (indica las agencias del gobierno), .edu (identifica las entidades educativas), .org (define las organizaciones sin ánimo de lucro) y .com (indica las páginas web con fines comerciales).

Política de privacidad

Todas las páginas web deberían presentar una política de privacidad. En este sentido, muchas de las páginas web que podemos visitar, hacen uso de "cookies", las cuales pueden alterar la privacidad de los visitantes en estas páginas. Para evitarlo, se puede optar por desactivar el uso de las "cookies" a través del navegador de internet.

Protección de nuestra información sobre salud en internet

Es importante saber cómo se va a recopilar esta información. La mayoría de los sitios web seguros suelen presentar un "http" con una "s" al final. De hecho, en muchas páginas suelen pedir un usuario y contraseña.

Recuerda que algunas pautas relacionadas con este tema son: hacer uso de una contraseña segura, utilizar factores de autenticación, no comparta información privada sobre su salud en una red wifi de uso público.

Saber más

Existen diversas listas de verificaciones que nos pueden ayudar a conocer si una página web es fiable o no. A continuación, se muestran algunas de las preguntas que uno/a debería hacerse a sí mismo para el uso de páginas web sobre salud:

- ¿Pertenece esta página web a alguna organización, entidad o gobierno? ¿Quién es el autor que redacta esta información sobre la salud?
- ¿Se refleja el objetivo de esta página web? ¿Para qué fue creada esta página web?
- ¿Por qué fue creado el sitio web? ¿Está clara la misión o el objetivo del patrocinador del sitio web?
- ¿La página web presenta algún contacto o persona y/o grupo de referencia?
- ¿Cuándo fue la última actualización de esta página web?
- ¿La información sobre su privacidad está protegida?
- ¿Esta página recoge información sobre curas milagrosas?

Ejemplos de páginas de salud no fiables

Tras observar diferentes puntos relevantes para conocer la fiabilidad de una página web sobre salud, se muestran algunos ejemplos de páginas web ligadas a la salud no fiables.

- Blogs y páginas relacionadas con temas de nutrición, ofreciendo dietas y fármacos para combatir contra la obesidad, que finalmente no son milagrosas y pueden provocar un efecto negativo en el estado de salud. Además, este tipo de páginas no suelen presentar el autor/a de su contenido.
- Páginas web relacionadas con la salud de la mujer. Estas páginas contienen remedios y algunas consideraciones a tener en cuenta en ciertos momentos vitales de la mujer. Además, también, se realizan venta de productos. En general, estas páginas suelen ser administradas por personas sin formación médica.

Saber más

- *medlineplus.gov/spanish*
- *who.int/es*
- *salupedia.org*
- *aemps.gob.es*
- *semfyc.es/medicos*
- *pacientessemergen.es*
- *picuida.es*
- *e.digitall.org.es/informacion-salud*
- *e.digitall.org.es/bulos-salud*

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel C2 4.4 Protección del medio ambiente

ODS y Tecnologías Digitales

ODS y Tecnologías Digitales

Introducción

En este documento se van a tratar de forma más detallada los conceptos que se han incluido en los videos del nivel C1 y C2 ODSs y Tecnologías digitales (I y II).

ODSS Y TECNOLOGÍAS DIGITALES (I)

Situación actual de las problemáticas y desafíos relacionados con la tecnología digital para el cumplimiento de los ODS.

e.digitall.org.es/A4C44C1V05

ODSS Y TECNOLOGÍAS DIGITALES (II)

Potenciales aplicaciones de la tecnología digital para el cumplimiento de los ODS.

e.digitall.org.es/A4C44C2V05

Su finalidad es la de ampliar información sobre los Objetivos de Desarrollo Sostenible (ODS), aprobados en 2015 por los Estados Miembros de las Naciones Unidas.

Este documento se va a centrar, especialmente, en dar a conocer la importancia de los ODS, cuál es su cometido y por qué persiguen retos que tienen, y van a tener, repercusión mundial para el Planeta, las Personas, la Prosperidad, la Paz y las Alianzas internacionales.

Vamos a ver que la *Agenda 2030 para el Desarrollo Sostenible*, adoptada por la Asamblea General de la ONU (2015), es el plan de acción que guía los programas de implementación de las metas que persiguen los 17 ODS: se trata de 169 metas interrelacionadas que se encaminan hacia la optimización (sostenibilidad) de las esferas económica, social y ambiental, poniéndose como fecha de consecución el año 2030.

El compromiso de los países con los ODS marca un antes y un después en la apuesta internacional y la movilización de recursos para lograr los mayores desafíos del mundo actual: desde la erradicación del hambre, la pobreza o la desigualdad social, hasta el acceso universal a la sanidad, la educación, el trabajo decente y el acceso generacional a los recursos naturales.

Además, se aporta información para comprender cómo estos desafíos únicamente podrán ser alcanzados si el progreso se fundamenta en la economía circular, es decir, que se lleva a cabo en paralelo a la protección ambiental y social, el consumo sostenible de recursos naturales y la adecuada gestión y reciclaje de los residuos generados.

En definitiva, comprenderemos cómo los ODS muestran que la *Economía* y la *Sociedad* deben contemplarse como partes necesariamente dependientes de la sostenibilidad de la *Biosfera* de nuestro planeta.

También entenderemos la importancia de aplicar los principios de sostenibilidad en la fabricación de la tecnología digital como única vía para que verdaderamente supongan una herramienta esencial en el proceso de digitalización sostenible.

Acabaremos por mostrar la contribución de la digitalización sostenible en la implementación de los ODS: tengamos en cuenta que tecnología digital está presente en todas y cada una de las actividades industriales, empresariales, administrativas y personales de la sociedad del siglo XXI.

La *Tarta de Boda* de los ODS

A lo largo de la serie de videos hemos podido conocer que la tecnología digital nos ha abierto paso hacia un nuevo estilo de vida fundamentado en la transformación digital en constante evolución. Sin duda, que la innovación digital al servicio de la sociedad facilita nuestro sistema de vida. Pero, también es bien cierto que su uso en la transformación digital está suponiendo una enorme demanda de dispositivos digitales cuya fabricación, uso y consumo está teniendo un impacto ambiental que está poniendo en riesgo las reservas naturales del mundo.

Debemos ser conscientes de ambos panoramas:

- Por un lado, el beneficio de la transformación digital para contribuir en la sostenibilidad de nuestro progreso.
- Por otro lado, del impacto ambiental asociado a la transformación digital.

Y, efectivamente, consecuente con esta supuesta incompatibilidad entre la sostenibilidad y la insostenibilidad

del progreso humano y sus recursos actuales, entre otras, la transformación digital, la *Agenda 2030 para el Desarrollo Sostenible* (2015) establece una serie de *Objetivos* encaminados a mejorar nuestro sistema de vida actual y el de las generaciones futuras.

Los Objetivos de Desarrollo Sostenible (ODS) se establecen para guiar el progreso de la humanidad considerando que debe ser integrador, inclusivo y universalmente justo y equitativo. Para ello, los países de la ONU se comprometieron a que, antes de 2030, nuestra sociedad habrá prosperado en bienestar y calidad de vida, pero sin descuidar su obligación de hacerlo ambiental y económicamente sostenible.

Los ODS apuestan por desafíos a nivel mundial que hay que entender en contexto. La implicación para contribuir a la consecución de los ODS recae tanto en las instituciones públicas, el ámbito político y el tejido productivo industrial y empresarial como en todos y cada uno de nosotros y nosotras.

Era preciso dar a conocer los ODS en términos que nos permitan entender su esencialidad y la importancia de la implicación a todos los niveles sociales, económicos y ambientales. Debíamos contar con una forma de "mirar" los ODS en los que se evidenciara dónde encaja nuestra sociedad, o sea, dónde encajamos como individuos y consumidores, y nuestra forma de vida.

Para ello, el Centro de Resiliencia de la Universidad de Estocolmo presentó en 2016 una nueva forma de observar los ODS, a la que denominó "la tarta de boda de los ODS" (2016).

Fue presentada en *Stockholm EAT Food Forum* de 2016 para hacer ver la importancia de la alimentación como uno de los retos más trascendentales de los desafíos mundiales de salud y sostenibilidad a los que se enfrenta el mundo.

Esta ilustración muestra cómo la **Economía** y la **Sociedad** deben contemplarse como partes necesariamente dependientes de la sostenibilidad de la **Biosfera** de nuestro planeta. Representa una visión novedosa, alejándose del actual enfoque sectorial donde el desarrollo social, económico y ecológico se ven como partes separadas.

La base de esta tarta muestra los ODS más medioambientales, es decir, los que sostienen al resto de los ODS para que la tarta no se venga abajo. Nada tendríamos sin disponer de Agua limpia y Saneamiento (ODS 6), Vida submarina (ODS 14), Acción por el Clima (ODS 13) y Vida de los Ecosistemas Terrestres (ODS 15).

El primer piso de la tarta incluye los ODS que dan sentido a nuestra vida: las personas y la sociedad. La humanidad será justa cuando se ponga Fin a la Pobreza (ODS 1), consigamos el Hambre Cero (ODS 2), tengamos acceso universal a Salud y Bienestar (ODS 3), a Educación de Calidad (ODS 4), a Energía asequible y no contaminante (ODS 7) y vivamos en Ciudades y Comunidades Sostenibles (ODS 11), todo ello en un entorno en el que se haya obtenido la total Igualdad de Género (ODS 5).

¿Y dónde está la economía? Para ello se reserva el tercer piso de la tarta ya que con la economía están vinculados el Trabajo decente y el Crecimiento económico (ODS 8), la Industria, Innovación e Infraestructura (ODS 9), la Producción y Consumo responsables (ODS 12) y en el que la Reducción de las Desigualdades (ODS 10) sea una realidad.

Alcanzar la consecución de todos estos ODS sólo será posible con la implicación y acción efectiva internacional, por los que las Alianzas para lograr los ODS (ODS 17) se instauran como el objetivo coordinador que sujeta y asegura todos estos desafíos.

Las 5P de los ODS para la Acción Digital

Como ya hemos visto, los ODS apuestan por retos sumamente importantes para nuestros valores vitales ya que se centran en la protección de nuestro *Planeta*, las *Personas* y su *Prosperidad*, al tiempo que velan por la universalización al amparo de la *Paz* para todos a través de *Alianzas* internacionales.

Aunque no corresponde exactamente con sus términos en idioma español, estos retos se han dado a conocer como las 5P de la Agenda 2030 por su terminología en inglés: *Planet* (Planeta), *People* (Personas), *Prosperity* (Prosperidad), *Peace* (Paz)y *Partnership* (Alianzas).

Veamos por qué y su relación con la Acción Digital. Empecemos por distinguir los ODS que se engloban en cada una de estas P:

- **Personas (*People*):** fácilmente identificamos cuáles son los ODS enfocados directamente en las personas. Son ODS 1 Fin de la Pobreza, ODS 2 Hambre Cero, ODS 3 Salud y Bienestar, ODS 4 Educación de Calidad y ODS 5 Igualdad de Género.
- **Planeta (*Planet*):** la protección ambiental se convierte en la base de nuestra propia existencia y nada será posible sin la consecución de los ODS relacionados con ello: ODS 6 Agua limpia y Saneamiento, ODS 12 Producción y Consumo responsables, ODS 13 Acción por el Clima, ODS 14 Vida Submarina y ODS 15 Vida de Ecosistemas Terrestres.
- **Prosperidad (*Prosperity*):** debemos aspirar a vivir con armonía con lo que la naturaleza nos ofrece con la finalidad de ser coherentes con los ODS 7 Energía asequible y no contaminante, ODS 8 Trabajo decente y crecimiento

económico, ODS 9 Industria, innovación e infraestructuras, ODS 10 Reducción de desigualdades y ODS 11 Ciudades y comunidades sostenibles.

- **Paz (*Peace*):** no cabe duda de que los conflictos, las guerras, la inseguridad, las instituciones débiles y las desigualdades y la injusticia social constituyen una de las peores amenazas para el avance hacia un desarrollo sostenible y para mejorar esta situación se persiguen las metas del ODS 16 Paz, Justicia e Instituciones sólidas.
- **Alianzas (*Partnership*):** el ODS 17 Alianzas para lograr los ODS fomenta las relaciones de cooperación entre líderes mundiales con la finalidad de proveer financiación y acción coordinada a nivel internacional.

Recordemos que por digitalización sostenible entendemos el proceso por el cual las sociedades se digitalizan protegiendo el medio ambiente, la economía circular y el bienestar de las personas. Únicamente, leyendo esta definición podemos ver fácilmente alguna interrelación con las 5P pero veamos algunos ejemplos.

Empecemos por el impacto ambiental de la tecnología digital. Como ya hemos visto en los videos, cualquier actividad que realicemos en el entorno digital genera impactos, ya sea por emisiones de gases de efecto invernadero, ya sea por el uso de recursos naturales imprescindibles en la fabricación de dispositivos digitales y la infraestructura para su funcionamiento. A esto hay que sumar tanto el consumo energético que necesita todo el proceso, así como la ingente cantidad de residuos que generamos y que deben ser debidamente gestionados para reducir e impedir consecuencias negativas para nuestra seguridad y la de nuestro planeta.

La *contaminación digital* incide directamente en los ODS tanto dificultando su consecución como favoreciéndola. En cuanto al tema que nos ocupa, los ODS establecen metas que llaman la atención sobre cualquier tipo de impacto negativo, entre los que está la contaminación digital, e instan a ponerles freno y atención constante para su prevención, minimización y, al ser posible, evitación.

Ya en 2010, el investigador Jonathan Koomey, indicó que se debería hacer frente para que la tendencia al alza de gasto energético de los dispositivos digitales fuese cada vez más eficiente (ley de Koomey, 2010), mejorando los procesos para una producción e infraestructuras digitales sostenibles, incluyendo la optimización de software, hardware, redes de acceso y centros de datos.

En la transición ecológica fundamentada en la coherencia con los ODS, la tecnología digital no es sólo una necesidad operativa, sino que, además, hoy día es la herramienta por excelencia que está permitiendo llevar a cabo una transformación digital sostenible. La Estrategia Digital de la UE (2021), con el documento "*Brújula Digital 2030: el enfoque de Europa para el Decenio Digital*", marca la visión y objetivos concretos para ello: Ciudadanos con capacidades digitales (Plan Nacional de Competencias Digitales. DigitAll), Digitalización de los servicios públicos, Infraestructuras digitales seguras y sostenibles y Transformación digital de las empresas.

En la *Brújula Digital 2030* se destaca que los dispositivos digitales deben favorecer la sostenibilidad y transición ecológica, haciendo hincapié en los derechos y principios digitales, como vía para contribuir a los ODS con la implicación y apoyo social, institucional y empresarial. Es una ambición declarada para "*aplicar políticas digitales que capaciten a las personas y las empresas para aprovechar un futuro digital centrado en el ser humano, sostenible y más próspero*" (UE, 2021).

Por su parte, el Pacto Mundial de la ONU (2019) expone que la tecnología digital ofrece un gran potencial para acelerar el cumplimiento de los ODS y reducir sus procesos de implementación. Por ejemplo, promover el acceso a la información de calidad, el análisis y la recolección de datos a gran escala (Big data) tiene impacto positivo en todos los ODS, entre otros ámbitos para ayudar a acercar los servicios sociales de educación, salud, alimentación, empleo, igualdad de oportunidades, etc., así como la toma de decisiones en temas ambientales o económicos.

La digitalización empresarial e industrial hace posible tanto la optimización sostenible de sus procesos como nuevas formas de negocio que aprovechan su potencial para mejorar su impacto positivo reduciendo su huella ambiental, como el

comercio electrónico, la optimización de labores agrícolas o sistemas de salud, entre otros.

Por ende, los dispositivos electrónicos cada vez más eficientes y sostenibles se conciben como impulsores de la Acción Digital para la consecución de los ODS de la Agenda 2030 y la transformación digital para "*lograr un sociedad más sana y ecológica*" (UE, 2021).

Saber más

Parlamento Europeo (2021). Bruselas, 9.3.2021 COM(2021) 118. Estrategia Digital de la UE (2021), *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital*. e.digitall.org.es/brujula-digital

Pacto Mundial Red Española (2019). *Siete formas en las que la tecnología puede contribuir a los ODS*. e.digitall.org.es/pacto-mundial

The SDGs wedding cake. Stockholm Resilience Centre. Stockholm University (2016). e.digitall.org.es/tarta-boda

Asamblea General de la ONU (2015). *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*. e.digitall.org.es/onu-agenda2030

Materiales de comunicación de los ODS de la ONU (2015). e.digitall.org.es/materiales-ods

Koomey, J. et all. (2010) *Implications of Historical Trends in the Electrical Efficiency of Computing*. DOI:10.1109/MAHC.2010.28. Corpus ID: 8305701. e.digitall.org.es/koomey

Otros recursos:

- Stockholm EAT Food Forum (2016). e.digitall.org.es/2016-eat
- e.digitall.org.es/tarta-bbva
- e.digitall.org.es/5p

DigitAll

Formación en
Competencias
Digitales

https://www.digitall.org.es/

DigitAll

Coordinación General

Universidad de Castilla-La Mancha
Carlos González Morcillo
Francisco Parreño Torres

Coordinadores de área

Área 1. Búsqueda y gestión de información y datos

Universidad de Zaragoza
Francisco Javier Fabra Caro

Área 2. Comunicación y colaboración

Universidad de Sevilla
Francisco Javier Fabra Caro
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Julio Cabero Almenara
María Ángeles Borrueco Rosa

Área 3. Creación de contenidos digitales

Universidad de Castilla-La Mancha
David Vallejo Fernández
Javier Alonso Albusac Jiménez
José Jesús Castro Sánchez

Área 4. Seguridad

Universidade da Coruña
Ana M. Peña Cabanas
José Antonio García Naya
Manuel García Torre

Área 5. Resolución de problemas

UNED
Jesús González Boticario

Coordinadores de nivel

Nivel A1

Universidad de Zaragoza
Ana Lucía Esteban Sánchez
Francisco Javier Fabra Caro

Nivel A2

Universidad de Córdoba
Juan Antonio Romero del Castillo
Sebastián Rubio García

Nivel B1

Universidad de Sevilla
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Montserrat Argandoña Bertran

Nivel B2

Universidad de Castilla-La Mancha
María del Carmen Carrión Espinosa
Rafael Casado González
Víctor Manuel Ruiz Penichet

Nivel C1

UNED
Antonio Galisteo del Valle

Nivel C2

UNED
Antonio Galisteo del Valle

Maquetación

Universidad de Salamanca
Fernando De la Prieta Pintado
Pilar Vega Pérez
Sara Alejandra Labrador Martín

Creadores de contenido

Área 1. Búsqueda y gestión de información y datos

1.1 Navegar, buscar y filtrar datos, información y contenidos digitales

Universidad de Huelva
Ana Duarte Hueros (coord.)
Arantxa Vizcaíno Verdú
Carmen González Castillo
Dieter R. Fuentes Cancell
Elisabetta Brandi
José Antonio Alfonso Sánchez
José Ignacio Aguaded
Mónica Bonilla del Río
Odiel Estrada Molina
Tomás de J. Mateo Sanguino (coord.)

1.2 Evaluar datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Ana María López Torres
Francisco Javier Fabra Caro
José Antonio Simón Lázaro
Laura Bordonaba Plou
María Sol Arqued Ribes
Raquel Trillo Lado

1.3 Gestión de datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Francisco Javier Fabra Caro
Gregorio de Miguel Casado
Sergio Ilarri Artigas

Área 2. Comunicación y colaboración

2.1 Interactuar a través de tecnología digitales

Iseazy

2.2 Compartir a través de tecnologías digitales

Universidad de Sevilla
Alién García Hernández
Daniel Agüera García
Jonatan Castaño Muñoz
José Candón Mena
José Luis Guisado Lizar

2.3 Participación ciudadana a través de las tecnologías digitales

Universidad de Sevilla
Ana Mancera Rueda
Félix Biscarri Triviño
Francisco de Asís Gómez Rodríguez
Jorge Ruiz Morales
José Manuel Sánchez García
Juan Pablo Mora Gutiérrez
Manuel Ortigueira Sánchez
Raúl Gómez Bizcocho

2.4 Colaboración a través de las tecnologías digitales

Universidad de Sevilla
Belén Vega Márquez
David Vila Viñas
Francisco de Asís Gómez Rodríguez
Julio Barroso Osuna
María Puig Gutiérrez
Miguel Ángel Olivero González
Óscar Manuel Gallego Pérez
Paula Marcelo Martínez

2.5 Comportamiento en la red

Universidad de Sevilla
Ana Mancera Rueda
Eva Mateos Núñez
Juan Pablo Mora Gutiérrez
Óscar Manuel Gallego Pérez

2.6 Gestión de la identidad digital

Iseazy

Área 3. Creación de contenidos digitales

3.1 Desarrollo de contenidos

Universidad de Castilla-La Mancha
Carlos Alberto Castillo Sarmiento
Diego Cordero Contreras
Inmaculada Ballesteros Yáñez
José Ramón Rodríguez Rodríguez
Rubén Grande Muñoz

3.2 Integración y reelaboración de contenido digital

Universidad de Castilla-La Mancha
José Ángel Martín Baos
Julio Alberto López Gómez
Ricardo García Ródenas

3.3 Derechos de autor (copyright) y licencias de propiedad intelectual

Universidad de Castilla-La Mancha
Gabriela Raquel Gallicchio Platino
Gerardo Alain Marquet García

3.4 Programación

Universidad de Castilla-La Mancha
Carmen Lacave Rodero
David Vallejo Fernández
Javier Alonso Albusac Jiménez
Jesús Serrano Guerrero
Santiago Sánchez Sobrino
Vanesa Herrera Tirado

Área 4. Seguridad

4.1 Protección de dispositivos

Universidade da Coruña
Antonio Daniel López Rivas
José Manuel Vázquez Naya
Martiño Rivera Dourado
Rubén Pérez Jove

4.2 Protección de datos personales y privacidad

Universidad de Córdoba
Aida Gema de Haro García
Ezequiel Herruzo Gómez
Francisco José Madrid Cuevas
José Manuel Palomares Muñoz
Juan Antonio Romero del Castillo
Manuel Izquierdo Carrasco

4.3 Protección de la salud y del bienestar

Universidade da Coruña
Javier Pereira Loureiro
Laura Nieto Riveiro
Laura Rodríguez Gesto
Manuel Lagos Rodríguez
María Betania Groba González
María del Carmen Miranda Duro
Nereida María Canosa Domínguez
Patricia Concheiro Moscoso
Thais Pousada García

4.4 Protección medioambiental

Universidad de Córdoba
Alberto Membrillo del Pozo
Alicia Jurado López
Luis Sánchez Vázquez
María Victoria Gil Cerezo

Área 5. Resolución de problemas

5.1 Resolución de problemas técnicos

Iseazy

5.2 Identificación de necesidades y respuestas tecnológicas

Iseazy

5.3 Uso creativo de la tecnología digital

Iseazy

5.4 Identificar lagunas en las competencias digitales

Iseazy

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia