DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel C1

ÍNDICE

DigitAll

Seguridad

4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel C1 4.1 Protección de dispositivos

Estándares de seguridad en la empresa

Estándares de seguridad en la empresa

Estándares de seguridad

Un estándar de seguridad es un conjunto de normas y mejores prácticas establecidas para garantizar la seguridad y protección de los sistemas, datos, infraestructuras o procesos. Estos estándares se desarrollan con el objetivo de mitigar los riesgos y amenazas que podrían comprometer la integridad, confidencialidad y disponibilidad de la información.

Los estándares de seguridad pueden abarcar diferentes áreas, como la seguridad informática, la seguridad de la información, la seguridad de redes, la seguridad física y la seguridad en el desarrollo de software. Estos estándares definen los requisitos técnicos, controles, políticas y procedimientos que deben implementarse para asegurar que los sistemas y datos estén protegidos de manera efectiva.

> ***Saber más***
>
> Cumplir con los estándares de seguridad adecuados ayuda a garantizar la confianza de los usuarios, clientes y socios comerciales, y reduce los riesgos asociados con incidentes de seguridad, como el acceso no autorizado, el robo de datos o las interrupciones del sistema.

Existen numerosos estándares de seguridad en el mundo por lo que hablar de cuáles o cuántos son resulta muy complicado, pero sí podemos afirmar que los más conocidos o extendidos son los siguientes:

- **ISO/IEC Familia 27K** (*e.digitall.org.es/iso*): estándar internacional para la gestión de la seguridad de la información.
- **NIST SP 800** (*e.digitall.org.es/sp-800*): marco de seguridad desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST).
- **PCI DSS** (*e.digitall.org.es/pci*): estándar de seguridad de datos para la industria de tarjetas de pago.
- **HIPAA** (*e.digitall.org.es/hipaa*): Ley de Portabilidad y Responsabilidad de Seguro Médico en los Estados Unidos, que establece requisitos de seguridad y privacidad de la información médica.

- **GDPR** (*e.digitall.org.es/gdpr*): Reglamento General de Protección de Datos de la Unión Europea, que establece normas de protección de datos y privacidad para los ciudadanos de la UE.
- **CIS Controls** (*e.digitall.org.es/cis*): conjunto de controles de seguridad desarrollados por el Centro de Seguridad de Internet (CIS) para ayudar a proteger los sistemas de información.

La forma de demostrar el cumplimiento de estándares de seguridad radica en la obtención de una certificación donde se evalúa y certifica que se cumple dicho estándar. Es importante resaltar que no todos los estándares son susceptibles de ser certificados.

El proceso de certificación de seguridad generalmente implica las siguientes etapas:

1 | **Evaluación inicial:** se realiza una evaluación exhaustiva de la organización, sistema o proceso de seguridad para determinar si ya se cumple con los estándares y requisitos establecidos.

2 | **Implementación de controles:** si se identifican deficiencias o áreas de mejora durante la evaluación inicial, la organización debe implementar controles y medidas de seguridad adicionales para cumplir con los requisitos.

3 | **Auditoría:** un auditor externo o un organismo de certificación independiente realiza una revisión detallada y exhaustiva del sistema de seguridad para verificar el cumplimiento de los estándares y criterios establecidos.

4 | **Emisión de certificación:** si la organización o sistema cumple con éxito los requisitos de seguridad, se emite una certificación oficial que valida que se ha cumplido con los estándares de seguridad establecidos.

A continuación, se revisan algunos de estos estándares por ser los más extendidos.

ISO/IEC Familia ISO27k

La familia ISO 27k, también conocida como la serie ISO/IEC 27000, se refiere a un conjunto de estándares internacionales que abordan la gestión de la seguridad de la información. Estos estándares son desarrollados por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) con el objetivo de establecer un marco de buenas prácticas para la seguridad de la información en organizaciones de cualquier tamaño y sector.

La serie ISO/IEC 27000 proporciona directrices y recomendaciones para la gestión de la seguridad de la información, y está compuesta por varios estándares interrelacionados, siendo los más conocidos:

- **ISO/IEC 27001:** Es el estándar principal de la familia y especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización.
- **ISO/IEC 27002:** Proporciona un conjunto de controles y buenas prácticas de seguridad de la información que pueden ser utilizados para implementar los requisitos del SGSI descritos en el ISO/IEC 27001.
- **ISO/IEC 27005:** Se centra en la gestión de riesgos de seguridad de la información, proporcionando pautas para identificar y evaluar los riesgos, así como para seleccionar e implementar controles de seguridad adecuados.

Además de estos, existen otros estándares dentro de la familia ISO 27k que cubren temas específicos, como la gestión de incidentes de seguridad, la continuidad del negocio, la auditoría de seguridad de la información, entre otros.

NIST SP 800

El estándar NIST SP 800 se refiere a la serie de publicaciones del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos relacionadas con la seguridad de la información y la ciberseguridad. El NIST SP 800 (Special Publication 800) proporciona directrices, recomendaciones y mejores prácticas para diversos aspectos de la seguridad de la información y la gestión de riesgos.

El NIST SP 800 se compone de múltiples publicaciones, cada una de las cuales se centra en un área específica de la seguridad y la ciberseguridad.

El NIST es ampliamente reconocido como una autoridad en materia de estándares de seguridad y ciberseguridad, y sus publicaciones son ampliamente utilizadas por organizaciones e industrias para fortalecer su postura de seguridad y gestionar los riesgos relacionados con la información y los sistemas.

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) es un estándar de seguridad de datos para la industria de tarjetas de pago. Fue desarrollado por el Consejo de Normas de Seguridad de la PCI (PCI SSC), que es un organismo formado por las principales compañías de tarjetas de crédito y débito, como Visa, Mastercard, American Express, Discover y JCB.

El objetivo del estándar PCI DSS es proteger la información confidencial de los titulares de tarjetas de pago, como los números de tarjeta, mediante la promoción de prácticas de seguridad en las organizaciones que manejan, procesan o almacenan esta información. PCI DSS establece un conjunto de requisitos técnicos y operativos que deben cumplir los comerciantes, procesadores de pagos, emisores de tarjetas y otros actores involucrados en las transacciones con tarjetas de pago.

El cumplimiento del PCI DSS es requerido por los proveedores de servicios de pago y las redes de tarjetas de crédito para garantizar la seguridad de las transacciones con tarjetas de pago. Las organizaciones que manejan tarjetas de pago deben someterse a auditorías periódicas para demostrar el cumplimiento del estándar.

Seguridad

Nivel C1 4.1 Protección de dispositivos

Protección frente ataques a redes

Protección frente ataques a redes

La **protección de las redes de comunicaciones es una parte fundamental de la seguridad informática**. Esto tiene especial relevancia en las redes empresariales, donde se albergan servicios críticos para un negocio, se llevan a cabo multitud de operaciones diarias y se comparte información confidencial.

Los ataques que hemos visto en vídeos de este nivel representan una amenaza constante, para interrumpir o comprometer la comunicación y el flujo de datos.

ATAQUES MÁS COMUNES A LAS REDES

Tanto en redes domésticas como en redes empresariales, existen ataques comunes pero efectivos que amenazan la seguridad de estas. DHCP e IP Spoofing, Man in the Middle o las denegaciones de servicio son algunos de ellos.

e.digitall.org.es/A4C41C1V03

A continuación, **se abordarán las medidas de protección necesarias para mitigar los ataques específicos**, como el DHCP spoofing, IP spoofing, Man in the Middle (MitM) y la denegación de servicio (DoS). Esto es una guía de buenas prácticas, aunque para más detalle de configuración se deberán consultar los manuales específicos de cada dispositivo de red.

DHCP Spoofing

Los ataques **DHCP Spoofing** se utilizan para hacerse pasar por un servidor DHCP legítimo en una red y **tomar el control de la configuración de los dispositivos de la red comprometida**. De esta forma, se podría modificar la puerta de enlace predeterminada y redirigir el tráfico de los dispositivos comprometidos a través del ordenador del atacante, permitiendo la intercepción o inspección de las comunicaciones.

Cuando un dispositivo se conecta a una red, solicita la configuración a cualquier servidor DHCP que pueda responder. Por eso, si el servidor DHCP falso del atacante responde más rápido que el legítimo, el dispositivo obtendrá la configuración errónea. Para prevenir este tipo de ataques existen algunas recomendaciones clave:

1 | Conectar correctamente los routers a la red

- Si se conecta un router a la red utilizando el puerto erróneo y la configuración por defecto, puede que responda a peticiones DHCP y desconfigure los dispositivos de la red.
- Por lo general, no se debe permitir el uso de routers no configurados por el administrador de la red, ya que pueden ser una amenaza para la misma.

2 | Supervisar el tráfico DHCP con DHCP Snooping

- Para evitar un posible ataque de DHCP Spoofing, los dispositivos empresariales de red como switches disponen del mecanismo de DHCP Snooping.
- Este mecanismo permite escanear por paquetes DHCP no autorizados. De esta forma, sólo se autorizarán respuestas DHCP desde el servidor legítimo de la empresa, mitigando los ataques que provienen de usuarios conectados a la red.

IP Spoofing

De forma similar, los ataques de **IP Spoofing** buscan **suplantar la identidad de un dispositivo legítimo de la red**. Es decir, se intenta suplantar la dirección de red de servidores importantes, de un usuario, o incluso la del router. Este ataque hace posible otros muchos que se basan en esta suplantación de identidad. Para mitigar el ataque, existen algunas medidas fundamentales:

3 | Configurar Dynamic ARP Inspection (DAI)

- Para evitar la suplantación de dirección IP asociando una dirección física falsa, se puede activar la inspección del protocolo ARP con DAI.
- Esto mitiga ataques ARP Spoofing que permitirían a un atacante hacerse pasar por una IP que no le corresponde.

4 | Configurar reglas de acceso mediante un firewall

- Como se ha visto en este nivel, la configuración de red con firewalls y la segmentación de red son mecanismos útiles para evitar muchos ataques.

CONTROLANDO LAS CONEXIONES: INTRODUCCIÓN A LOS FIREWALLS

Los firewalls o cortafuegos en una red permiten el filtrado y bloqueo de tráfico de red mediante listas de control de acceso o reglas. Dependiendo del tipo de firewall, se pueden bloquear paquetes de red atendiendo a diferentes características de la comunicación, como la dirección IP o el puerto

e.digitall.org.es/A4C41C1V05

- El filtrado con firewall y el bloqueo de peticiones de IPs que no pertenecen a una red, mitiga ataques de suplantación de IP de forma remota.

Man in the Middle (MitM)

Por otro lado, los taques **Man in the Middle (MitM)** son un concepto genérico que agrupa a amenazas en las cuales **el atacante se sitúa en medio de la comunicación**, con el objetivo de interceptar, inspeccionar o manipular la comunicación. Para evitar este tipo de ataques, es importante evitar la suplantación IP, ARP y DHCP, como se ha comentado antes. Además, hay medidas que ayudan a mitigar los ataques MitM:

5 | Diseñar una topología de red segura y segmentada

- Mantener una red segmentada permite establecer reglas que separan las distintas partes de una red corporativa. Por ejemplo, estableciendo zonas privadas, públicas y desmilitarizadas (DMZ).
- De esta forma, se evita que un atacante conectado a una red más fácilmente accesible tenga acceso a la red de servidores o de administración.

6 | Cifrar y autenticar las comunicaciones

- El cifrado de la información en tránsito mitiga las inspecciones de tráfico y mantiene la información confidencial.
- Usar sistemas de cifrado como TLS permite autenticar a las partes y transmitir la información cifrada entre ambas, evitando manipulaciones.

TOPOLOGÍA SEGURA DE RED

La segmentación de una red y su organización permiten establecer controles de acceso más eficientes. Además, la separación en zonas de dispositivos críticos, dispositivos públicos y los de los usuarios utilizando redes virtuales o VLANs son algunas de las prácticas para establecer un diseño de red más seguro.

e.digitall.org.es/A4C41C1V04

Denegación de Servicio (DoS)

Por último, las **denegaciones de servicio** son ataques menos sofisticados pero muy destructivos, que **afectan a la disponibilidad de la red de comunicaciones** y, por tanto, de la información. Este tipo de ataques pretenden neutralizar y paralizar las comunicaciones para impedir el acceso a los sistemas de información con el objetivo de afectar al proceso de negocio de una empresa.

Existen diferentes tipos de ataques de *Denial of Service (DoS)*, por lo que deben tenerse en cuenta medidas de seguridad de diferente índole, como:

7 | Mantener los dispositivos de red y de usuarios actualizados

- Existe malware como el ransomware u otro tipo de gusanos que pueden distribuirse por la red y afectar a la disponibilidad de la información.
- El malware se aprovecha de las vulnerabilidades existentes en el software, por lo que mantener a los equipos actualizados mitiga este tipo de amenazas.

8 | Instalar sistemas de detección y prevención de intrusiones

- Los IDS e IPS son sistemas que permiten monitorizar la red, detectar e incluso bloquear ataques conocidos como las denegaciones de servicio.
- Instalar y mantener actualizados estos mecanismos ayuda a prevenir DoS bloqueando la comunicación y la saturación de los sistemas.

9 | Diseñar sistemas redundantes y mantener copias de seguridad

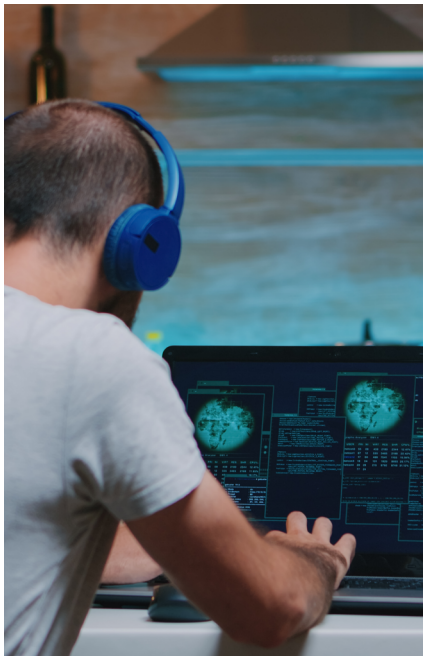
- Las denegaciones de servicio impiden el acceso a sistemas, saturándolos o haciendo inaccesible la información que albergan.
- Para evitar la pérdida de servicio o la pérdida de información, se deben mantener copias de seguridad de la información y sistemas redundantes. En caso de fallo o saturación, se redirigirá a usuarios al sistema redundante, o se reestablecerá la copia de seguridad de la información.

Como hemos visto, existen multitud de medidas que pueden aplicarse para mitigar los ataques más comunes a las redes. La seguridad es un proceso, por lo que estas contramedidas se deben ir aplicando gradualmente, manteniendo actualizadas las soluciones y revisando su correcto funcionamiento de forma periódica.

SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

Los sistemas de detección y prevención de intrusiones permiten monitorizar el tráfico de red para detectar ataques conocidos o incluso desconocidos. Los IPS permiten, además, bloquear la comunicación si se detecta algún tipo de ataque, como una denegación de servicio.

e.digitall.org.es/A4C41C2V08

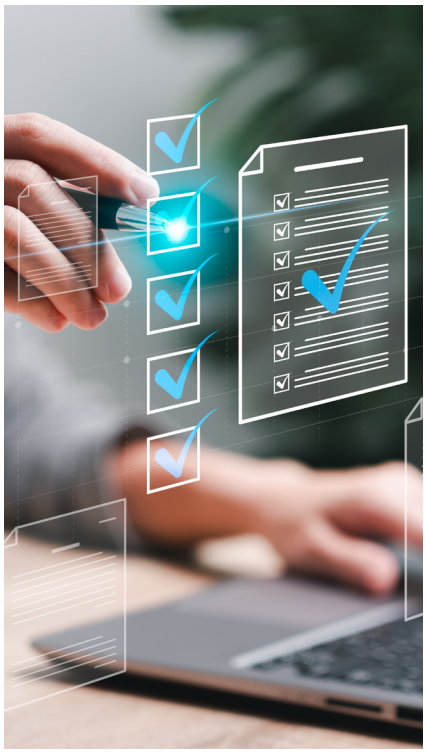


Seguridad

Nivel C1 4.1 Protección de dispositivos

Certificados digitales

Certificados digitales



En la era digital, donde la seguridad de la información es primordial, los certificados digitales desempeñan un papel fundamental en la autenticación y en la protección de la integridad de los datos. Los certificados digitales son documentos electrónicos que contienen información criptográfica, permitiendo la verificación de la identidad de una entidad en entornos digitales. En este artículo, exploraremos los formatos de certificados digitales más comunes, la información que almacenan y las diversas aplicaciones en las que se utilizan.

Concepto y Funcionamiento de los Certificados Digitales

¿Qué es un Certificado Digital y cómo funciona?

Como hemos visto, un certificado digital es un archivo electrónico que se utiliza para asociar una identidad digital a una entidad o persona física. Es emitido por una Autoridad de Certificación (CA, por sus siglas en inglés) confiable y es utilizado para establecer la identidad y confiabilidad en entornos digitales.

Los certificados digitales utilizan criptografía de clave pública para garantizar la autenticidad de la entidad a la que se asocian. El certificado contiene la clave pública de la entidad y está firmado digitalmente por la CA emisora. Cuando un usuario o sistema necesita verificar la identidad de una entidad, verifica la firma digital del certificado utilizando la clave pública de la CA.

Tipos de Certificados Digitales y sus aplicaciones

- **Certificados emitidos por autoridades – formato X.509:** el formato X.509 es uno de los más utilizados para certificados digitales. Es ampliamente reconocido y es compatible con una amplia variedad de aplicaciones y protocolos de seguridad. Los certificados en formato X.509 contienen información como el nombre del titular, el período de validez, la clave pública, el nombre de la CA emisora y su firma digital.

  - Un ejemplo de este tipo de certificados son los certificados de persona física emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT). Para solicitarlos, sólo es necesario utilizar un navegador web compatible y seguir el procedimiento de su página web.
  - Una vez obtenido este certificado, se instalará en el navegador que hayamos usado. Podemos hacer una copia de este certificado desde la configuración del navegador, exportándolo a un archivo protegido por contraseña, para que pueda importarse en otros navegadores o dispositivos.

- **Certificados personales generados por uno mismo para el cifrado de correo - protocolo PGP/GPG:** Pretty Good Privacy (PGP) y GNU Privacy Guard (GPG) son protocolos de criptografía que utilizan formatos de certificados propios. Estos certificados son populares en el ámbito de la seguridad de correo electrónico y permiten la autenticación y el cifrado de mensajes.
  - Para poder generarlos y utilizarlos, es necesario tener instalado software como Kleopatra y OpenPGP. Existen diversos clientes de correo electrónico, como Thunderbird, que permiten cifrar y firmar correos electrónicos usando PGP/GPG.
- **Certificados de correo electrónico - protocolo S/MIME:** el estándar S/MIME (Secure/Multipurpose Internet Mail Extensions) utiliza certificados digitales para proporcionar seguridad y autenticación en el correo electrónico. Los certificados S/MIME se basan en el formato X.509 y se utilizan para firmar y cifrar mensajes de correo electrónico.
  - Existen algunos certificados X.509 que permiten su uso para cifrar correos electrónicos. Usando clientes de correo como Outlook o Thunderbird, es posible cifrar y firmar correos electrónicos con certificados compatibles.

Información Almacenada en los Certificados Digitales

- **Identidad del Titular**
  Uno de los componentes clave de un certificado digital es la información de identidad del titular. Esto puede incluir el nombre, la dirección de correo electrónico, la organización o empresa asociada y otros datos relevantes para verificar la identidad de la entidad.
- **Clave Pública**
  Los certificados digitales también almacenan la clave pública correspondiente a la entidad a la que se asocian. La clave pública se utiliza para verificar la autenticidad y establecer una comunicación segura con la entidad en cuestión.
- **Firma Digital de la CA**
  Para garantizar la integridad del certificado, la CA emisora firma digitalmente el certificado utilizando su clave privada. Esta firma permite a los usuarios y sistemas verificar que el certificado no ha sido alterado y que proviene de una fuente confiable.

Aplicaciones de los Certificados Digitales

Autenticación en Sitios Web

Los certificados digitales desempeñan un papel fundamental en la autenticación de sitios web a través del protocolo HTTPS. Los certificados SSL/TLS (Secure Sockets Layer/Transport Layer Security) permiten establecer conexiones seguras y autenticar la identidad de un sitio web, proporcionando confianza a los usuarios y protegiendo la información transmitida. Cuando un usuario intenta acceder a un sitio web seguro, su navegador solicita al servidor que presente un certificado válido. El navegador verifica la autenticidad del certificado y si coincide con el dominio al que se accede. Si el certificado es válido y confiable, se establece una conexión segura y se muestra un indicador visual, como un candado, para indicar al usuario que la conexión es segura.

Firmas Digitales

Los certificados digitales también se utilizan para la firma digital de documentos electrónicos. Al firmar un documento digitalmente con un certificado válido, se puede verificar la integridad del documento y la identidad del firmante, lo que es esencial en entornos legales y empresariales. La firma digital utiliza criptografía de clave pública para crear una huella digital única del documento. Esta huella digital se adjunta al documento y se puede verificar utilizando la clave pública del certificado asociado. Si el documento ha sido alterado de alguna manera, la verificación de la firma digital fallará, lo que garantiza la integridad del contenido. Además, la firma digital está vinculada a la identidad del firmante, lo que proporciona una mayor confianza y autenticidad.

Cifrado de Correo Electrónico

Mediante el uso de certificados S/MIME, es posible cifrar y firmar mensajes de correo electrónico para garantizar su confidencialidad y autenticidad. Esto protege la privacidad de las comunicaciones y evita que los mensajes sean interceptados o alterados. Cuando un usuario envía un correo electrónico cifrado con S/MIME, el mensaje se encripta utilizando la clave pública del destinatario, lo que asegura que solo el destinatario pueda descifrar y leer el contenido. Además, al firmar digitalmente el mensaje con el certificado del remitente, se verifica la autenticidad del remitente y se asegura que el contenido del mensaje no haya sido alterado en tránsito.

Conclusión

En resumen, los certificados digitales son una pieza fundamental en la seguridad y autenticación de entornos digitales. Al utilizar criptografía de clave pública y formatos como X.509, PGP/GPG y S/MIME, los certificados digitales permiten verificar la identidad de las entidades, proteger la integridad de la información y establecer comunicaciones seguras. Desde la autenticación en sitios web hasta la firma digital y el cifrado de correo electrónico, los certificados digitales son herramientas versátiles y esenciales para garantizar la confianza y seguridad en la era digital.

Seguridad

Nivel C1 4.1 Protección de dispositivos

Infraestructura de clave pública (PKI)

Infraestructura de clave pública (PKI)

La Infraestructura de Clave Pública (PKI, por sus siglas en inglés) es un sistema vital para la seguridad de la información.

A través de la PKI, se establece una infraestructura de confianza que permite la autenticación, integridad y confidencialidad de las comunicaciones digitales.

La PKI se basa en el uso de certificados digitales emitidos por una Autoridad de Certificación (CA). Estos certificados contienen claves públicas utilizadas para verificar la identidad de los participantes y cifrar la información. Como hemos visto antes, los certificados digitales desempeñan un papel fundamental en aplicaciones como el cifrado de correo electrónico, la firma digital y la protección de las conexiones seguras en línea.

CERTIFICADOS DIGITALES

Documento referenciado: ***A4C41C1D03***

Es necesario comprender bien cómo funciona la PKI y aplicar sus principios en la práctica, para aprovechar sus ventajas y llevar a la práctica el uso de los certificados digitales.

Autoridades de Certificación

Las **Autoridades de Certificación** (CAs, por sus siglas en inglés) son componentes esenciales dentro de la PKI. Son entidades de confianza encargadas de emitir y gestionar los certificados digitales.

A nivel técnico, las CAs utilizan sus claves privadas para firmar los certificados digitales que emiten. De esta forma, cuando se validan las firmas de los certificados digitales, se hace con la clave pública de la Autoridad de Certificación.

Tomemos como ejemplo un usuario que firma un documento PDF con un certificado digital, expedido por la Fábrica Nacional de Moneda y Timbre (FNMT) como Autoridad Certificadora. Cuando se valide la firma usando las claves públicas, se puede utilizar el servicio VALIDe de la FNMT, que verificará usando sus claves de Autoridad Certificadora para autenticar el certificado

con el que se han expedido. De esta forma, se puede identificar que esa firma corresponde a una persona física concreta: el usuario que ha firmado el documento.

Saber más

El servicio VALIDe (*valide.redsara.es/valide*) permite validar la firma de documentos firmados con certificados expedidos por todos los prestadores que se encuentran inscritos en el registro de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de Información del Ministerio de Industria, Turismo y Comercio de autoridades.

Estructura de una PKI

FUNDAMENTOS TÉCNICOS DE LA FIRMA DIGITAL

e.digitall.org.es/A4C41C1V08

Los certificados digitales son normalmente firmados por una autoridad certificadora de último nivel. Una PKI es una estructura jerárquica con varios niveles.

En la cima de esta estructura, están las CAs raíz, en las cuales se deposita máxima confianza. Estas CAs raíz son encargadas de firmar los certificados de otras CAs, debajo en esa jerarquía de confianza. Así, estas últimas CAs firman a su vez los certificados de los usuarios.

De esta forma, se permite una mejor gestión de claves asimétricas y de la confianza en éstas. Las claves privadas de las CAs deben estar muy bien protegidas, ya que son las que firman los certificados. Cuanto más arriba en la cadena del PKI, más confianza depositamos en la CA y, por tanto, en su gestión de claves. Si una CA intermedia es comprometida, entonces sólo aquellos certificados que haya firmado ésta deben ser revocados, es decir, invalidados.

Las estructuras PKI nos permiten crear una cadena de confianza y gestionar de forma más eficiente los certificados, garantizando su validez y fiabilidad. De esta forma, se pueden usar con validez legal y estar respaldados por gobiernos y estados.

DigitAll

Seguridad

4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel **C1** 4.2 Protección de los datos personales y la privacidad

Mejora de la privacidad en las compras y pagos online

Mejora de la privacidad en las compras y pagos online

Web de compras

Gracias a Internet y a su uso generalizado, la sociedad actual ha ido evolucionando hacia un entorno digital con una alta interacción entre personas y servicios. Uno de los servicios que se ha digitalizado y que ha tenido una gran acogida es el mercado de compraventa de productos y servicios. Ya no es necesario ajustarse a compras en los establecimientos cercanos, sino que puedes adquirir el producto o el servicio que deseas casi en cualquier lugar del mundo.

Miles de empresas se han lanzado a ofertar productos y servicios a través de sus webs. La forma de compra es sencilla y consta de unos pasos que se describen a continuación.

Procedimiento habitual de compra online de un producto:

1 | **El usuario accede a la web de la empresa.**
2 | **El usuario busca el producto que desea.**
3 | **El usuario lo añade a su carrito de la compra.**
4 | **El usuario proporciona los datos de entrega.**
5 | **El usuario proporciona los datos de facturación.**
6 | **El usuario realizar el pago.**
7 | **La empresa recibe el pago.**
8 | **La empresa empaqueta el producto.**
9 | **La empresa entrega el paquete con el producto a un operador logístico.**
10 | **El operador logístico se encarga de hacer llegar el producto al usuario.**

Este mecanismo requiere un cierto grado de confianza entre el usuario, la empresa y el operador logístico: el usuario se arriesga dando su dinero a una empresa que debe enviarle el producto, la empresa se arriesga a que la transferencia de dinero del usuario no se haga realmente y la empresa logística a que el producto no sea recogido por el usuario final y que tenga que correr con los gastos de devolución a la empresa vendedora.

La empresa logística es un actor importante en esta transacción, pero su riesgo es menor, puesto que suelen

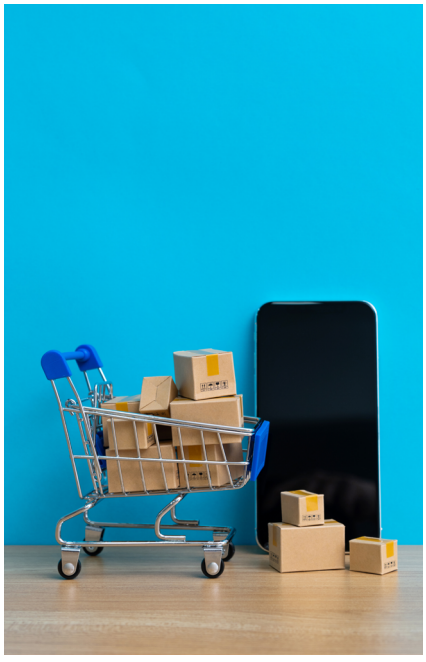
contratar seguros que cubren estos gastos y como suelen hacer un número elevado de entregas desde los mismos proveedores, pueden esperar a tener que realizar un nuevo trayecto a la empresa para realizar la devolución y minimizar los costes de trayectos.

Por tanto, son los usuarios y las empresas vendedoras los que deben tener una seguridad de que no van a ser engañados. Nos vamos a centrar en los usuarios y vamos a ver algunas ideas básicas que deben seguirse para incrementar la seguridad y su privacidad en las compras online.

Confianza en la web de compras

Para poder mantener una alta privacidad, lo primero que debe comprobar un usuario es que la web en la que pretende hacer la compra es de confianza: no le daremos nuestros datos personales a nadie en quién no confiemos. En la vida real, las personas suelen preferir comprar los productos en tiendas de empresas conocidas antes que a un desconocido por la calle. Esto se aplica igual cuando realizamos compras por Internet. Debemos conocer la web en la que compramos y debemos confiar en que la empresa que la gestiona tiene una buena reputación.

Hay miles, millones de webs en Internet. La gran mayoría son de empresas que desean realizar ventas reales, ganándose un beneficio en dicho intercambio. Sin embargo, esa minoría de webs fraudulentas que solo desean engañarnos para obtener nuestro dinero y nuestros datos personales son las que debemos detectar y rechazar.



Si compramos en webs de empresas conocidas y con buena reputación como Amazon, El Corte Inglés, Carrefour, MediaMarkt, etc. tenemos el respaldo de grandes compañías con muchos años de experiencia y que tienen un gran prestigio. Todos estos indicadores muestran que podemos tener un nivel alto de confianza en estas webs y es fiable darle nuestros datos personales, ya que darán un uso legítimo a dichos datos.

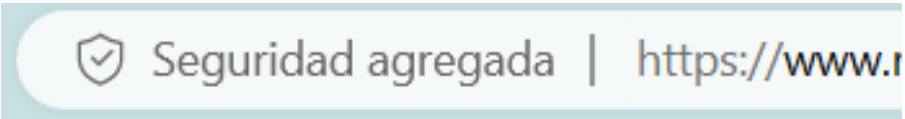
Si la web de compra no es de una empresa conocida, podemos hacer una búsqueda de reseñas de otros usuarios. Es preferible que las opiniones no sean de la propia web, puesto que podrían haberse puesto únicamente aquellas que sean favorables a la empresa o incluso que sean inventadas.

Hay algunos consejos que se pueden seguir para tener indicios de si una web es fraudulenta:

- Está mal traducida.
- Tiene un exceso de publicidad o de ventanas emergentes de productos "extraños" o poco relevantes en relación con la compra que se pretende realizar.
- El aspecto general es poco profesional.
- Los títulos de las secciones no coinciden con el contenido mostrado.
- Los precios son excesivamente baratos sin ofrecer motivos que lo justifiquen claramente (por ejemplo, son baratos porque son productos de segunda mano, devoluciones, descatalogados, etc.)

Cifrado de la web de compras

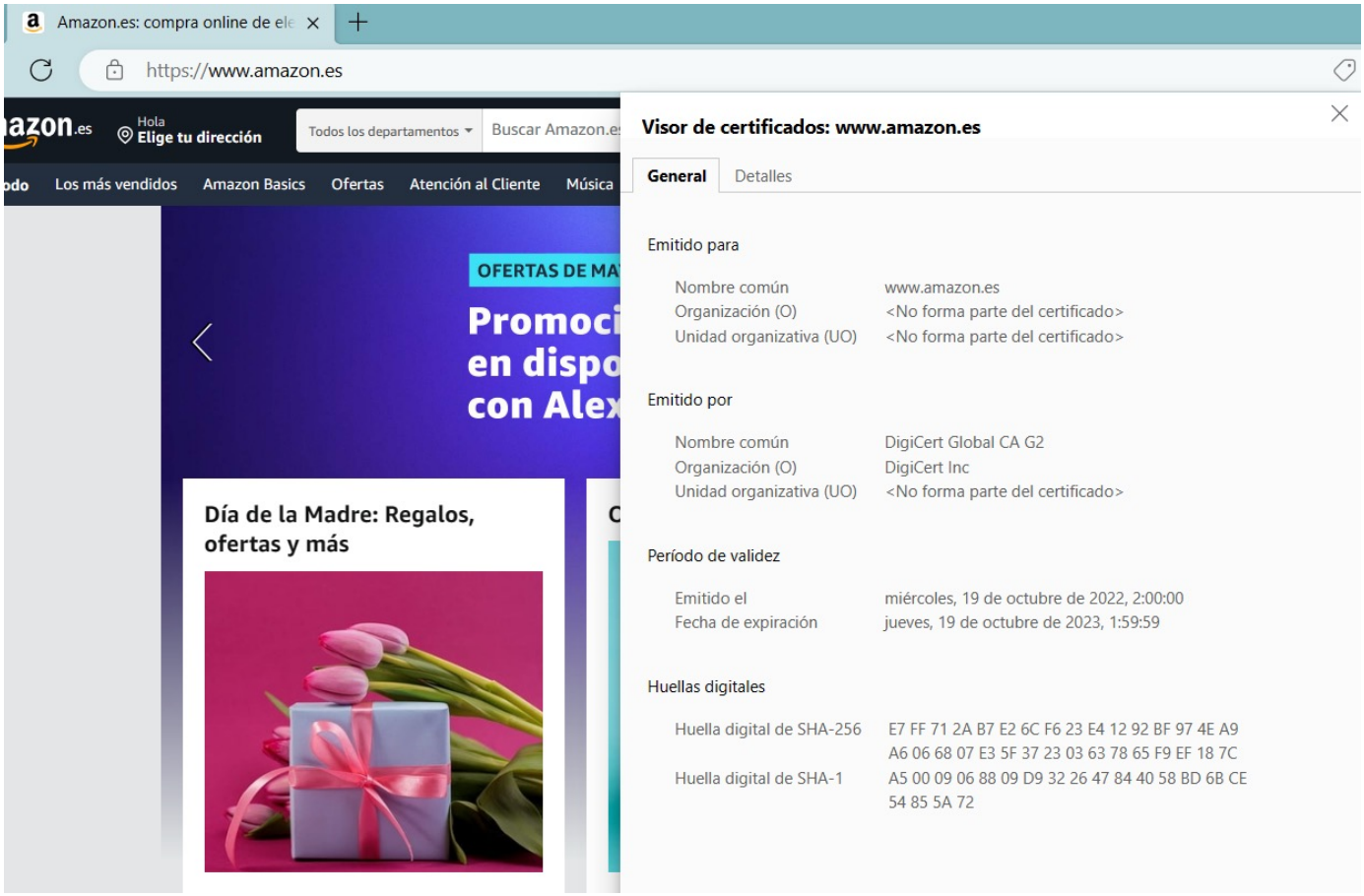
Antes de proporcionar ningún dato personal a una web en la que quieres hacer una compra debes fijarte si la conexión es segura. Para ello tienes que comprobar si la conexión que haces con el navegador está cifrada. Las conexiones seguras se realizan utilizando el protocolo seguro **https**.



Detalle del navegador con conexión con protocolo **https** y símbolo de Seguridad.

Las páginas web que no tienen protocolos seguros **https** podrían ser páginas legítimas, pero su inseguridad podría hacer que nuestros datos pudieran ser capturados por cualquier atacante.

Además, el protocolo **https** permite saber quién ha generado el certificado de identidad. Este **certificado SSL** es el que se usa para establecer la conexión segura entre nuestro navegador y la web de compra de la empresa. Así, revisando el certificado podemos asegurarnos que la web coincide con el nombre certificado y que la organización certificadora es fiable.



Detalle del certificado digital de www.amazon.es.

Otros estándares de seguridad

Aunque el uso del protocolo **https** es el principal estándar de seguridad, existen otros estándares en los que debemos fijarnos para tener una mayor confianza en la web de compras.

Las empresas que gestionan de manera segura tus datos privados siguiendo unos requisitos muy estrictos obtienen la certificación **ISO 27001**. Por tanto, aquellas empresas que tengan dicha certificación han demostrado que tienen un procedimiento muy seguro que garantiza la privacidad de nuestros datos personales.

Ejemplo de web de empresa certificada con ISO/IEC 27001 y otros certificados.

Existen empresas en Internet dedicadas a analizar la privacidad de las páginas web de las empresas y otorgarles sellos de fiabilidad. Uno de los sellos de privacidad más conocidos es TRUSTe®. Tenerlo incrementa la seguridad de los usuarios en como esa web maneja la privacidad de los datos, lo que la hace mucho más confiable.

Logo del sello TRUSTe® de garantía de seguridad y privacidad de empresas y webs.

Políticas de privacidad, entrega y métodos de compra

Una vez el usuario ha podido establecer un nivel de confianza en la web, se puede pasar a un segundo nivel, en el que el usuario debe evaluar si la empresa va a utilizar sus datos personales de la manera que él desea y si existen métodos de compra que le interesen y le garanticen el nivel de privacidad que desea.

Políticas de privacidad

Antes de proporcionar nuestros datos personales a una web, debemos informarnos para qué quieren los datos. Por ejemplo, ¿realmente es necesario que una web sepa nuestra dirección del trabajo si lo que queremos hacer es una compra personal?

O bien, ¿van a guardar nuestros datos en los servidores de la empresa o los van a ceder a terceras empresas para que nos manden mensajes?

Si la empresa es de la Unión Europea deberá cumplir determinadas normativas, como el Reglamento General de Protección de Datos (RGPD, o en inglés, GPRD). Si la web está localizada fuera de la Unión Europea, habrá que revisar la normativa del país en la que se ubica para saber qué derecho tenemos sobre los datos personales que cedemos.

Otras políticas de compras

Además de la privacidad, los usuarios debemos revisar otras políticas que tenga la tienda y que pueden influir mucho la compra de nuestro producto. Por ejemplo, ¿qué garantía tiene el producto? ¿Dónde se aplica la garantía? ¿Quién se encarga de los gastos de transporte? ¿Se incluyen los costes de aduanas si es una venta internacional? ¿Cuánto tiempo se puede retrasar el envío antes de poder reclamar? En caso de reclamación legal, ¿a qué legislación y tribunal se acoge el usuario?

En general, los usuarios deben tener en cuenta los siguientes aspectos para realizar su compra:

- **Formas de envío:** tipo de transporte, embalaje, lugar de entrega, etc.
- **Garantía:** tipo de garantía (reposición completa, arreglo sin franquicia, arreglo con franquicia, bono de recompra, etc.) y tiempo para aplicarla.
- **Desistimiento de compra:** durante cuánto tiempo podemos rechazar la compra, coste del desistimiento, etc.
- **Reclamaciones:** tiempo de reclamación, lugar y modo de reclamación.
- **Transporte:** costes, plazos, tasas adicionales.
- **Servicios adicionales:** seguros de reparación, de transporte, actualizaciones, postventa, etc.

El análisis de estos apartados puede hacer aparecer precios ocultos que no se muestren en el precio inicial del producto.

Métodos de entrega

Existen múltiples formatos para realizar las entregas. Cada uno de ellos tiene un procedimiento diferente, con costes distintos y también con implicaciones de privacidad de los datos diferentes, en cada caso.

En cuanto a la entrega suele haber tres tipos:

- **Entrega en domicilio:** la empresa logística entrega el producto en el domicilio (o donde le indique el cliente). Para ello, necesita muchos datos personales, desde nombre, apellidos, DNI y dirección del domicilio. Es el mecanismo con un menor nivel de privacidad.
- **Entrega en Correos o en una tienda asociada:** el producto se deposita en la oficina de Correos o en una tienda asociada, y el usuario va a dichos lugares y recoge su producto. La empresa debe conocer datos personales del cliente, para poder autorizar la recogida, pero no debe saber el domicilio u otro dato personal.
- **Entrega en un punto de recogida:** el producto se entrega en un casillero seguro y el usuario puede abrirlo con una combinación única y recoger su producto. En este caso, la empresa no tiene ningún dato personal de ubicación ni de domicilio. Es el tipo de entrega con un mayor nivel de privacidad.

Métodos de pago

Nuestros datos bancarios es uno de los datos personales más críticos en cuanto a privacidad. Por tanto, debemos prestar atención particular a los métodos de pago.

Con respecto a estos, existen varias opciones:

- **Transferencia bancaria:** es el mecanismo que tiene un nivel de privacidad más bajo, puesto que es necesario proporcionar un código de cuenta bancario completo, con la inseguridad que ello puede acarrear de cargos indebidos.
- **Pago con tarjeta de crédito:** el cliente proporciona los datos de su tarjeta de crédito y a través de una pasarela segura se realiza el cargo en la tarjeta. En determinadas entidades bancarias puedes activar un segundo nivel de

seguridad teniendo que hacer una autorización de dicho cargo a través de aplicaciones bancarias. Esto proporciona un nivel adicional de seguridad, ya que no pueden hacer cargos adicionales sin la autorización del cliente.

- **Pago con monedero electrónico/tarjeta de prepago:** el procedimiento de pago es igual al de pago con tarjeta, pero la que se usa es una tarjeta en la que se carga el coste que se desea pagar. De esta manera, en el peor de los casos, el atacante solo habría dispuesto del efectivo que hay en dicha tarjeta sin posibilidad de hacer cargos adicionales. Es un nivel de privacidad superior puesto que no se da una tarjeta asociada a la cuenta bancaria del usuario.
- **Pago a través de PayPal, Google Pay, o similar:** la empresa PayPal (Apple, Google u otras similares) realiza un pago en tu nombre, cargándole el coste al usuario en su cuenta corriente o en una tarjeta bancaria que previamente habrá registrado. Es uno de los sistemas más seguros, porque el usuario no tiene que proporcionar datos bancarios a la tienda, lo que implica una mayor privacidad.
- **Pago contrarrembolso:** el usuario paga al transportista al recoger el producto. Suele tener un cierto sobrecoste para cubrir el seguro del transporte. Es uno de los métodos con mayor privacidad, puesto que solo se proporciona el lugar de entrega y el nombre del usuario.

Privacidad en la compra

Al realizar compras por Internet podemos estar dejando rastros a posibles atacantes que puedan aprovechar para invadir nuestra privacidad. Es conveniente conocer diferentes opciones para evitar, o al menos, limitar el ataque a nuestra privacidad.

Registro de usuario en la web

Es habitual que todas las tiendas electrónicas nos soliciten un registro en su sistema. Gracias a dicho registro podemos recuperar pedidos, continuar con el proceso de compra, incorporar tarjetas bancarias para acelerar el mecanismo de pago, etc.

Estas ventajas, sin embargo, puede que no sean interesantes si se va a realizar una compra única y puntual en una determinada web. Le proporcionamos muchos datos personales, con la pérdida de privacidad que ello conlleva. Habrá determinados datos que tendremos que proporcionar para hacer la compra según el procedimiento de entrega y el método de pago que escojamos.

Existen algunas tiendas que permiten realizar compras como **invitados**, sin necesidad de realizar un registro, pidiendo los datos personales exclusivamente necesarios para realizar la compra. Pero la gran mayoría de webs exigen el registro para realizar una compra y en muchos casos, solicitan un email.

En estos casos, para evitar tener que darles nuestro email personal, podemos crear otros emails secundarios que usemos únicamente para realizar compras. De tal manera, que separamos nuestro email personal del email de compras. Si por algún motivo hubiera un fallo de seguridad en la web de compras o se produjera un hackeo, no estaríamos dando acceso a nuestro email personal.

COMPARTIENDO DATOS EN LA RED Y REDES SOCIALES (INFORMACIÓN, FORMULARIOS, ARCHIVOS, FOTOS, ETC.)

Ver diferentes formas de compartir información en la red.

e.digitall.org.es/A4C42C1V07

Otra opción es el uso de alias de email. Se crean diferentes alias de la misma dirección de email original, de tal forma, que un correo electrónico enviado al alias se recibe en la carpeta de correo de la dirección de email original. Se suelen agregar filtros de recepción, que conforme se reciba un email de un alias se envíe a una subcarpeta. En este caso, igual que en el anterior, un atacante no tendría acceso al correo principal y las contramedidas se podrían implementar fácilmente, simplemente anulando dicho alias.

Finalmente, hay servidores de email que permiten agregar a nuestro correo principal etiquetas, alterando el identificador del email, pero entregando el correo en la misma carpeta del email original. Esto es posible hacerlo con Gmail.

Saber más

Gmail es capaz de crear direcciones email añadiendo el símbolo + detrás del nombre de usuario y antes de @gmail.com. Todos los emails llegarán a la misma bandeja de entrada del usuario, pero mediante un filtro de etiqueta, se podrá gestionar mejor los correos electrónicos que se proporcionen a las webs.

Por ejemplo, para el usuario maria@gmail.com puedes crear emails adicionales:

maria+webCompra@gmail.com
maria+amazon@gmail.com
maria+spam@gmail.com

Todos los emails llegarán a la carpeta de entrada de maria@gmail.com pero cada uno con una etiqueta diferente.

Dispositivos seguros

El proceso de compra por Internet comienza por la navegación hasta encontrar el producto que deseas en una web. A partir de ahí, como hemos visto, se produce todo el procedimiento de compra digital. Por lo tanto, el uso de un dispositivo informático para navegar es imprescindible.

Hay múltiples dispositivos que pueden utilizarse para navegar por Internet: smartphones, tablets, ordenadores portátiles, ordenadores de sobremesa, etc. Todos ellos requieren un navegador para explorar las páginas web de las tiendas donde realizar las compras: Chrome, Firefox, Edge, etc.

La principal recomendación es que utilices un dispositivo personal y no compartido con ninguna otra persona. Si el dispositivo está compartido, es posible que se dejen archivos después de la navegación y la compra, que podrían explorarse por otros usuarios con la consecuente brecha de privacidad.

Si se utiliza un dispositivo compartido, se recomienda que cada usuario tenga su perfil propio protegido con contraseña, sin que el resto de usuarios tenga posibilidad de acceder a dicho perfil.

Si no es posible tener un perfil propio protegido por contraseña, se recomienda utilizar el modo incógnito o de navegación privada de los navegadores, para que al finalizar la sesión todos los ficheros creados por el propio navegador se eliminen.

Navegación en redes seguras

Las webs pueden ser muy seguras y garantizar una alta privacidad, pero si estás usando una red inalámbrica que no es segura, estás dejando que cualquier atacante pueda ver lo que estás haciendo.

El primer consejo es no utilizar redes públicas. Tampoco son seguras las redes WiFi que ofrecen gratis los establecimientos, cafeterías u otros comercios. Estas utilizan redes con seguridad, pero que se expone públicamente la clave, de tal manera que cualquiera puede conocerla y acceder a dicha red.

Mejor usar nuestra red propia con seguridad y control de acceso, para garantizar que no hay atacantes en dicha red que puedan espiarnos.

Sin embargo, si no podemos utilizar nuestra propia red, tenemos algunas opciones para evitar el problema de utilizar una red WiFi que podría no ser segura.

1 | **Crear una WiFi a partir de los datos de tu teléfono móvil:** utilizando tu smartphone puedes crear una red WiFi con una clave que sólo tú sepas y utilizar el propio smartphone para acceder a Internet, garantizándote que ningún otro dispositivo estará utilizando dicha WiFi.

2 | **Utilizar una VPN:** las Redes Privadas Virtuales (VPN, por sus siglas en inglés) permiten crear una conexión segura dentro de una red pública mediante una conexión encriptada con un servidor remoto que se encargará de tramitar las peticiones que hagamos.

Saber más

Métodos de pago y su seguridad. *e.digitall.org.es/pago-seguridad*

Métodos de pago seguro. *e.digitall.org.es/metodos-pago*

Detecta si una página es fiable para comprar o es una estafa. *e.digitall.org.es/detectar-estafas*

TRUSTe® Privacy Certification. *e.digitall.org.es/truste*

DigitAll

Seguridad

4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel C1 4.3 Protección de la salud y el bienestar

Guía visual sobre el bloqueo de usuario y mensajes. Enfoque desde la salud

Guía visual sobre el bloqueo de usuario y mensajes. Enfoque desde la salud

En el presente documento se mostrará una guía visual para bloquear usuarios y mensajes que no queremos recibir. De esta forma, se presentan los bloqueos en los dispositivos móviles y también en las redes sociales.

Bloqueo de usuarios y mensajes en la red

Los ordenadores y dispositivos móviles proporcionan un acceso rápido y sencillo a múltiples formas de comunicación como llamadas, mensajes o redes sociales. Esto ha supuesto innumerables ventajas a la hora de relacionarse, pero también ha provocado algunos peligros como el ciberacoso o el flaming. En uno de los vídeos de este nivel se han explicado dichos conceptos y se han proporcionado una serie de pautas para detectarlos y protegerse.

CIBERACOSO Y FLAMING: ¿CÓMO DETECTARLOS Y PROTEGERSE?

En este vídeo se profundiza en los conceptos de ciberacoso y flaming. Así mismo, se proporcionan varios métodos para evitar dichas situaciones y detectar las mismas.

e.digitall.org.es/A4C43C1V02

Este documento se centra en la propia configuración de los dispositivos tecnológicos y de las redes sociales. En concreto, presenta diferentes posibilidades de bloqueo de usuarios y mensajes en la red.

NOTA

La llegada de los ordenadores a los hogares, el acceso a dispositivos móviles asequibles y la propagación de Internet han provocado un profundo cambio en el modo en que las personas se relacionan.

Hoy en día, prácticamente todo el mundo dispone de un móvil con acceso a Internet. Esto posibilita múltiples formas de comunicación: llamadas, videollamadas, mensajes de texto o interacción en redes sociales.

Las ventajas son claras. Actualmente, es posible realizar una llamada desde prácticamente cualquier lugar, captar una foto

de la actividad que se está realizando y enviarla al instante o debatir sobre un evento en tiempo real.
Sin embargo, este tipo de comunicaciones pueden conllevar ciertos peligros como el ciberacoso o el flaming. Algunos de estos peligros también pueden suceder en el mundo real, sin embargo, el que suceda a través de un medio digital podría tener una mayor repercusión sobre ciertos tipos de acoso, debido a la facilidad con la que se puede difundir un mensaje.

Este tipo de situaciones pueden provocar un enorme sufrimiento a la víctima, lo cual podría derivar en una afección sobre su salud mental.

En una situación así, además de poner lo sucedido en conocimiento de las autoridades y de valorar el acudir a un especialista en salud mental, es posible tomar medidas en los dispositivos tecnológicos y redes sociales. En las siguientes subsecciones se explicarán diferentes maneras de bloquear a un determinado usuario en la red, así como a limitar la recepción de llamadas y mensajes en los dispositivos móviles.

Bloqueo de llamadas y mensajes en dispositivos móviles

Una de las formas más habituales de acoso mediante el uso de dispositivos tecnológicos es el acoso telefónico. Este tipo de acoso implica la realización de llamadas o el envío de mensajes de texto de forma insistente y reiterada. Además, en muchas ocasiones estas llamadas incluyen amenazas o insultos. Todo ello puede conllevar a una situación de temor, ansiedad o estrés para la víctima, causándole importantes implicaciones sobre su salud mental.

Saber más

El acoso telefónico es un tipo de acoso, y como tal, es un delito recogido en el Código Penal Español. El artículo 172 ter. establece lo siguiente:

Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses 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.

e.digitall.org.es/acoso-telefonico

Ante una situación de acoso telefónico, además de ponerlo en conocimiento de las autoridades, es posible tomar medidas a través del menú de configuración del dispositivo móvil.

Hoy en día prácticamente todos los equipos, independientemente de la marca o modelo, cuentan opciones para bloquear números de teléfono. Esto permite impedir las llamadas o mensajes provenientes de un número determinado.

NOTA

A veces, la situación de acoso no proviene de una persona en particular, sino de una compañía que está intentando captar clientes. Además de las recomendaciones ya indicadas, existe una opción muy interesante denominada Lista Robinson. Se trata de un servicio para evitar recibir publicidad de entidades o empresas a las que no se le haya dado un consentimiento expreso para ello.

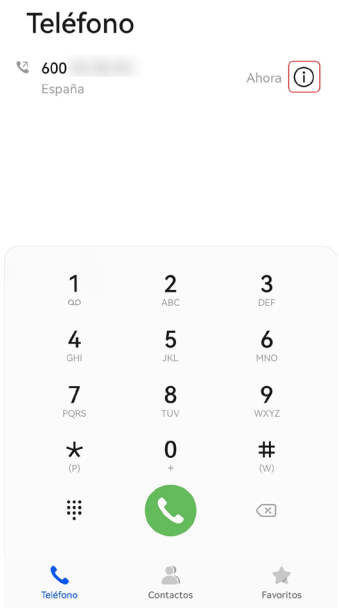
listarobinson.es

A continuación, se va a indicar como bloquear un número de teléfono en un dispositivo Android. No obstante, el procedimiento es muy similar en terminales iOS.

- La manera más sencilla de bloquear un número es abriendo la aplicación **Teléfono**. Habitualmente, al realizar dicha acción ya se visualiza el historial de llamadas, en caso contrario, habrá que seleccionar la opción **Recientes o Historial de llamadas**, en función del dispositivo.

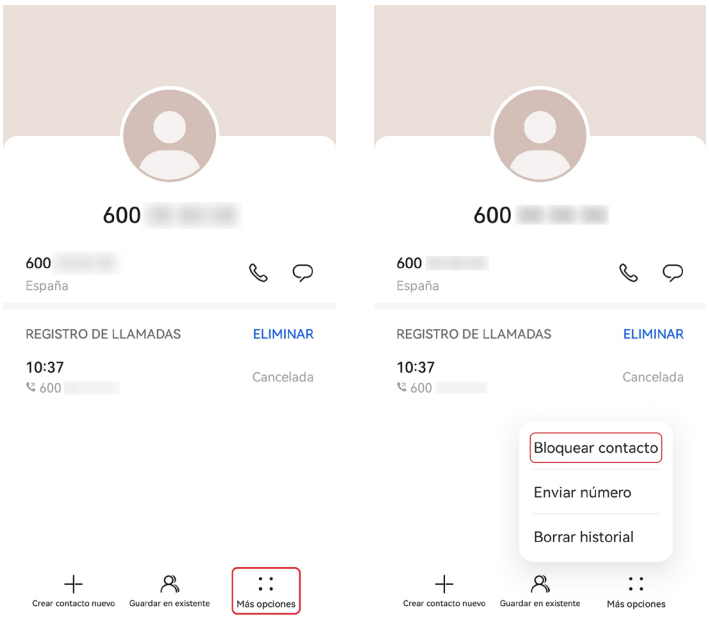
Fuente: Autoría propia.

- Una vez se visualizan las últimas llamadas recibidas, simplemente hay que localizar el número que se desea bloquear y presionar el icono ⓘ



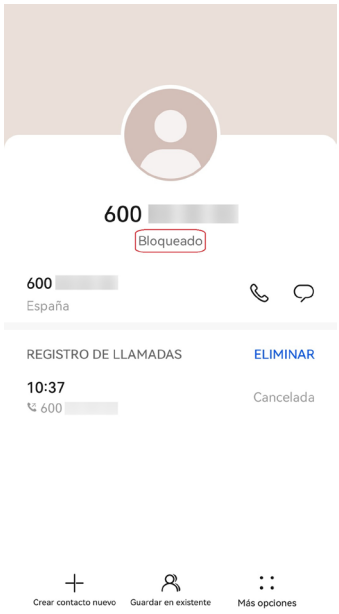
Fuente: Autoría propia.

- A continuación, hay que seleccionar el icono correspondiente a **Opciones** y hacer clic en **Bloquear contacto**.



Fuente: Autoría propia.

- De este modo, el número quedará bloqueado y no se recibirán llamadas ni mensajes que provengan de este.



Fuente: Autoría propia.

Si el número que se desea bloquear se encuentra guardado como contacto en la agenda del dispositivo, el procedimiento es prácticamente igual. Simplemente hay que abrir la aplicación **Contactos**, seleccionar el contacto que se quiere bloquear, y realizar el proceso explicado anteriormente.

Saber más

Además de permitir bloquear un número concreto, los dispositivos permiten configurar filtros para bloquear números desconocidos, es decir, todo aquel que no se encuentre guardado como contacto en el terminal. Así mismo, también es posible bloquear cualquier llamada que no esté identificada, esto es, que oculte el número de teléfono.

Enlace web Android: *e.digitall.org.es/bloquear-telefono-android*
Enlace web iOS: *e.digitall.org.es/bloquear-telefono-ios*

Bloqueo de usuarios y mensajes en redes sociales

El uso de redes sociales ha aumentado en gran medida en los últimos años, convirtiéndose en una de las principales maneras de comunicarse entre las personas. Esto también ha supuesto que sean utilizadas como un medio de ciberacoso. Algunas de las posibles formas de acoso están relacionadas con el envío reiterado de mensajes, imágenes o vídeos hirientes, o que supongan una amenaza, con la difusión de mentiras o con el envío de mensajes suplantando la identidad de la víctima.

Saber más

Unicef dispone en su web de un completo documento en el que dan respuesta a algunas de las preguntas más frecuentes sobre el ciberacoso y en el que también se ofrecen varios consejos acerca de la manera de hacerle frente.

e.digitall.org.es/ciberacoso

Entre las redes sociales más utilizadas en el mundo destacan Facebook, YouTube, WhatsApp o Instagram. A través de todas ellas pueden producirse situaciones de ciberacoso, por ello es importante conocer que opciones ofrecen respecto al bloqueo de usuarios y mensajes.

A nivel general, bloquear a un usuario implica el no recibir mensajes, ni ningún tipo de contenido procedente del mismo. Por otra parte, el usuario bloqueado no podrá visualizar el contenido de la otra persona, ni interactuar con la misma, entre otras acciones.

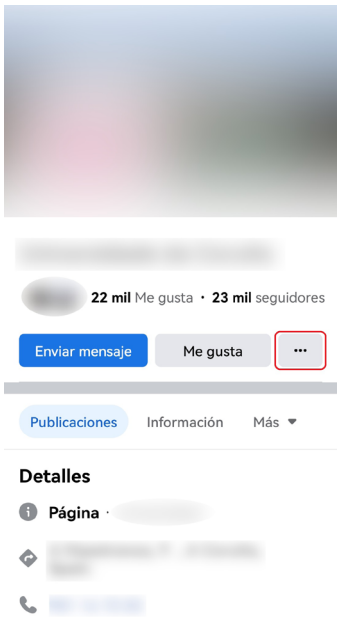
A continuación, se va a explicar cómo bloquear a un usuario en las redes sociales mencionadas. En cualquier caso, habitualmente toda red social cuenta con opciones de bloqueo.

Facebook

Si se bloquea el perfil de alguien en Facebook, este no podrá etiquetar a la persona que ha realizado el bloqueo ni consultar sus publicaciones, entre otras acciones.

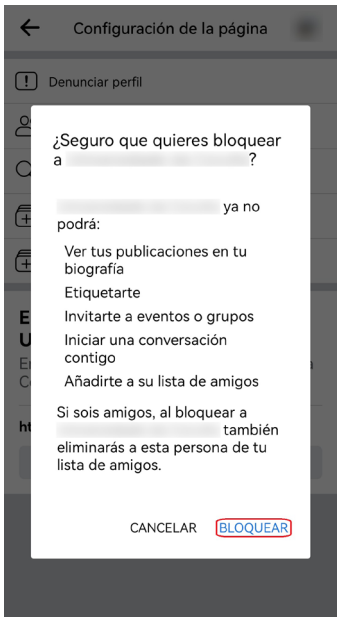
Para bloquear un perfil en Facebook hay que seguir los siguientes pasos:

1 | Buscar el perfil de la persona que se desea bloquear y hacer clic en el icono ···



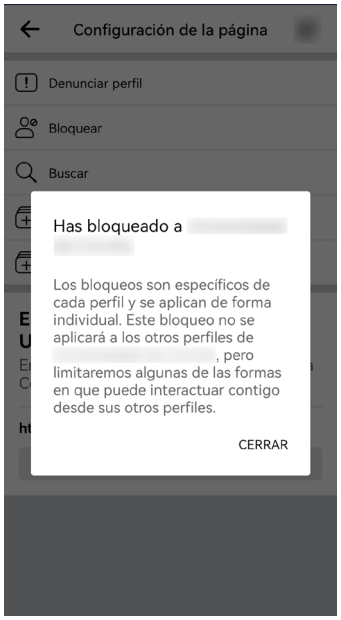
Fuente: Autoría propia.

2 | A continuación, un mensaje emergente mostrará las acciones que no podrá realizar el perfil una vez este bloqueado. Para continuar con el proceso, simplemente hay que hacer clic en **Bloquear**.



Fuente: Autoría propia.

3 | Finalmente, un mensaje informará de que el perfil ha sido bloqueado correctamente.

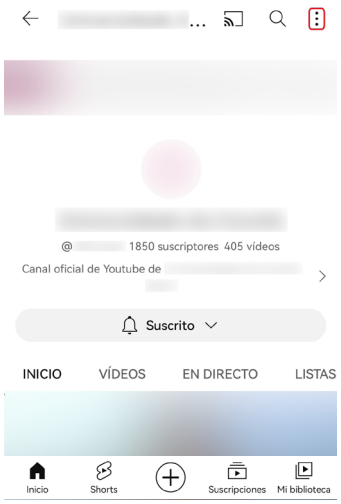


Fuente: Autoría propia.

YouTube

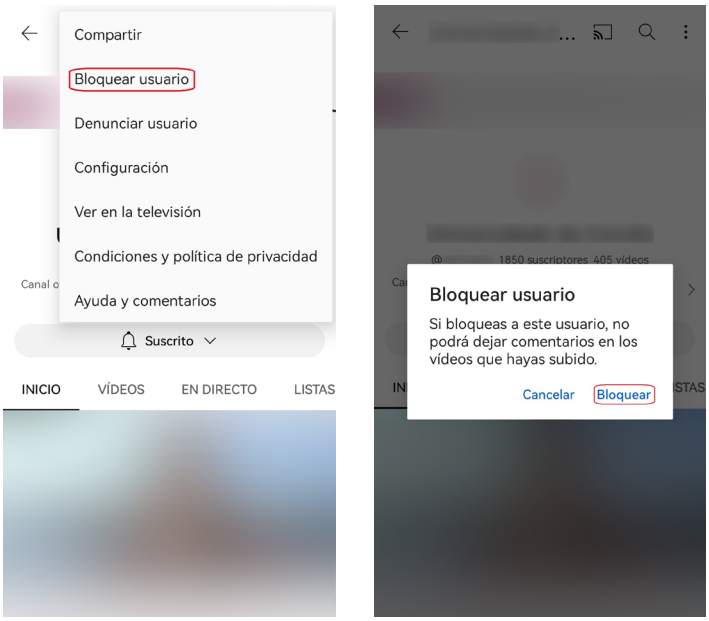
YouTube es una plataforma en la cual los usuarios pueden compartir sus vídeos. Por lo tanto, su objetivo principal no es el envío de mensajes. Sin embargo, sí es posible dejar comentarios en los vídeos, lo cual podría suponer un medio para publicar mensajes que buscan molestar o acosar al autor de la publicación o al resto de usuarios.

1 | Localizar el canal del usuario que se desea bloquear y seleccionar el icono ⋮



Fuente: Autoría propia.

2 | Hacer clic en la opción **Bloquear usuario** y confirmar la acción. A partir de ese momento, el usuario bloqueado no podrá dejar comentarios en los vídeos de la persona que ha solicitado el bloqueo.



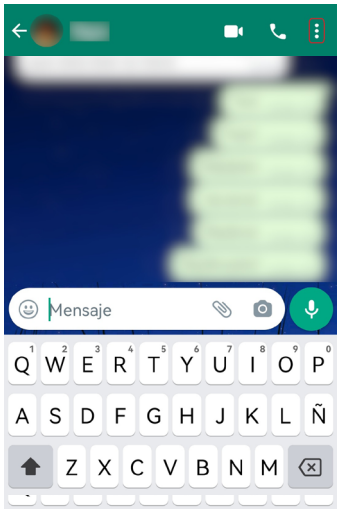
Fuente: Autoría propia.

WhatsApp

WhatsApp es sin duda una de las principales plataformas para comunicarse en la red y, por lo tanto, hace que sea uno de los principales medios presentes en situaciones de ciberacoso.

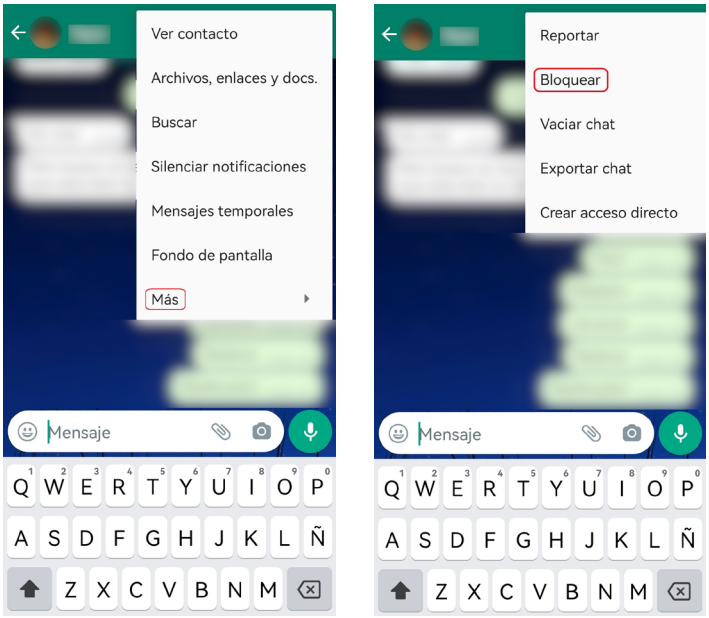
El procedimiento para bloquear a un contacto en WhatsApp es el siguiente:

1 | Abrir el chat con el contacto y seleccionar ⋮



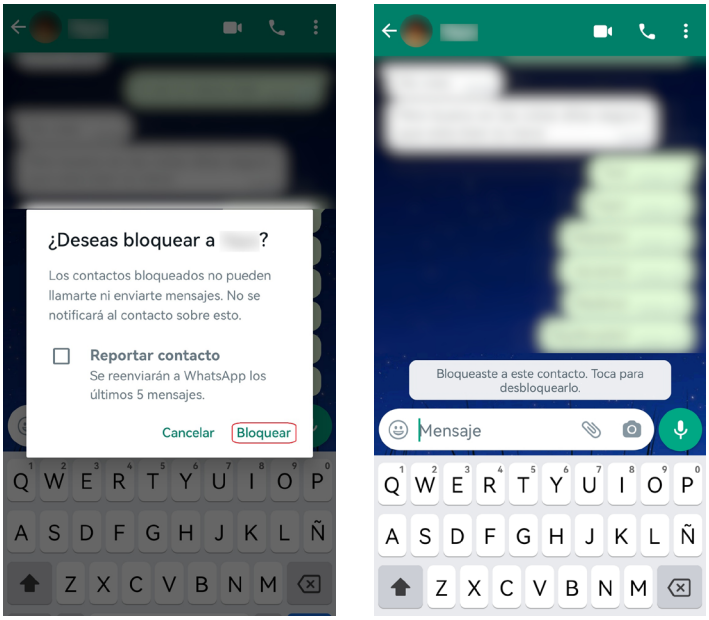
Fuente: Autoría propia.

2 | En el menú emergente hacer clic en **Más** y, posteriormente, en **Bloquear**.



Fuente: Autoría propia.

3 | Confirmar la acción.

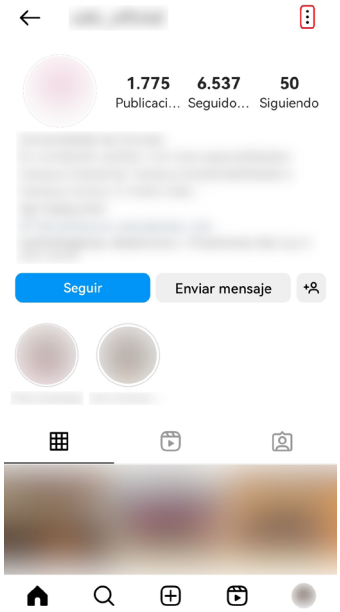


Fuente: Autoría propia.

Instagram

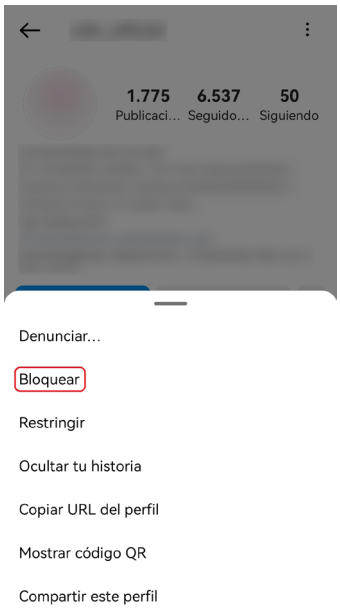
Instagram es otra de las redes sociales más utilizadas en el mundo. Los pasos a seguir para bloquear a un perfil de esta red son muy similares al resto de plataformas vistas. A continuación, se detalla el proceso a realizar:

1 | Localizar el perfil del usuario y seleccionar ⋮



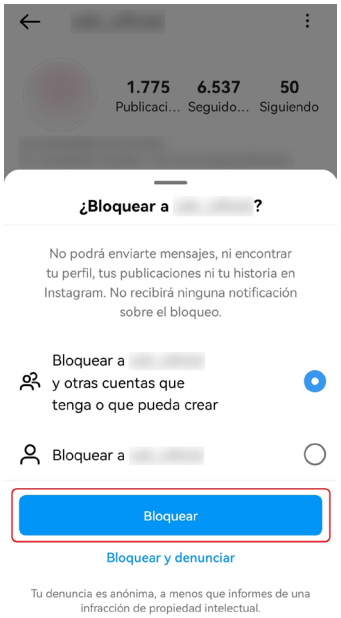
Fuente: Autoría propia.

2 | Hacer clic en la opción **Bloquear**.



Fuente: Autoría propia.

3 | Seleccionar si se desea bloquear todos los perfiles pertenecientes al usuario o que pueda crear en el futuro, o bloquear únicamente el perfil seleccionado. Por último, hacer clic en **Bloquear**.



Fuente: Autoría propia.

NOTA

La mayoría de las redes sociales, además de permitir bloquear usuarios, también suelen contar con la opción de denunciar al mismo en la plataforma. De este modo, los administradores de la red social investigarán lo sucedido y podrían tomar medidas como la suspensión de la cuenta denunciada, entre otras acciones.

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel C1 4.4 Protección del medio ambiente

Big Data y Tecnologías digitales para la sostenibilidad ambiental

Big Data y tecnologías digitales para la sostenibilidad ambiental

En este documento vamos a desarrollar el glosario de términos y ampliar conceptos relacionados con las aplicaciones de las tecnologías digitales y el big data en referencia a la eficiencia energética y sostenibilidad que se han incluido en los vídeos del nivel.

Como hemos visto en el **vídeo A4C44C1V02 *"Tecnologías digitales, Big Data y Sostenibilidad Ambiental"*** relacionado con el big data en este nivel, titulado también "Tecnologías digitales, big data y sostenibilidad ambiental" actualmente nos enfrentamos a retos muy importantes relacionados con la situación ambiental del planeta. Retos que nos afectan en todos los aspectos de nuestra vida diaria y que hemos de modificar para poder adaptarnos a los cambios venideros.

TECNOLOGÍAS DIGITALES, BIG DATA Y SOSTENIBILIDAD AMBIENTAL

Aplicaciones ambientales del análisis del flujo de datos provenientes del empleo masivo de las tecnologías digitales que contribuyen a mejorar la eficiencia energética y apostar por la sostenibilidad.

e.digitall.org.es/A4C44C1V02

Para ello, los gobiernos y empresas privadas, conscientes del momento decisivo en el que nos encontramos, han comenzado a desarrollar políticas para hacer frente a dichos retos y proteger y conservar los recursos naturales manteniendo el respeto por el medioambiente. Para el desarrollo de estas políticas, utilizan los resultados del uso de herramientas tan eficaces como el análisis del big data, que se ha convertido en una herramienta fundamental para la toma de decisiones, analizando el éxito o fracaso de medidas o conociendo la opinión de la población.

Cada día se generan en todo el mundo millones de datos digitales que, o bien la administración, o bien las empresas almacenan para su posterior uso.

ATENCIÓN

La variedad de estos datos es tan amplia que abarcan desde todos los aspectos de la actividad humana hasta los registros naturales que se dan en todas las áreas del planeta. Esta acumulación, procesamiento, estudio y empleo de datos a gran escala se denomina Big Data. Cuando se utilizan estos datos para la gestión ambiental y el desarrollo sostenible, se habla entonces de Sustainable Data o Datos sostenibles.

Origen del Big Data

TECNOLOGÍAS DIGITALES, BIG DATA Y SOSTENIBILIDAD AMBIENTAL

e.digitall.org.es/A4C44C1V02

Como se comenta en el vídeo ***"Tecnologías digitales, Big Data y Sostenibilidad Ambiental"*** de este nivel, al hablar del big data surgen varias preguntas como ¿qué es?, ¿cómo se origina? y ¿para qué sirve?

Big Data ¿qué es?

El big data son muchísimos datos recogidos en "bruto" que se procesan con programas informáticos específicos para obtener información que pueda ayudar a sectores concretos.

Big Data ¿cómo se origina?

Esta cantidad de información puede ser recopilada de diversas formas. Pueden ser imágenes de satélites, estaciones meteorológicas, dispositivos móviles, sensores de temperatura, sensores de humedad, sensores de luminosidad o incluso se pueden obtener de redes sociales (Facebook, Instagram, Tik Tok…) o bases de datos públicas. Podríamos resumir que las principales fuentes de big data son:

1 | **Producidos por personas.** Una gran fuente de información de primera mano y que se considera de muy buena calidad, son las redes sociales. Estas redes recopilan datos, opiniones, reacciones a contenidos e incluso imágenes de los propios usuarios sobre aspectos que puedan interesar a gobiernos y empresas. Por ejemplo, mandar un email, escribir un comentario en Facebook, contestar a una encuesta telefónica, meter información en una hoja de cálculo, responder a un WhatsApp, coger los datos de contacto de un cliente, hacer clic en un enlace de Internet… Infinidad de acciones que realizamos en el día a día suponen una fuente de datos inmensa.

NOTA

Un ejemplo de la envergadura del big data son los datos que se generan de las redes sociales por parte de los usuarios: Google procesa más de 3,5 mil millones de consultas de búsqueda todos los días, cada día se cargan 350 millones de fotos en Facebook, todos los días se envían 306,4 mil millones de correos electrónicos y se realizan 5 millones de Tweets.

2 | Generados por el intercambio de información entre máquinas. Además de la interconexión entre personas, las máquinas también están interconectadas y comparten datos directamente, en lo que se conoce como M2M, que viene del inglés «machine to machine». Así, sistemas de control de temperatura, parquímetros, sistemas de riego automático de jardines, GPS de vehículos y teléfonos móviles, máquinas expendedoras de todo tipo situadas en centros públicos y privados, o contadores de electricidad de las viviendas, entre otros muchos sistemas controlados por máquinas, se comunican a través de dispositivos con otros sistemas, a los que transmiten los datos que van recogiendo. Todos ellos utilizan métodos de comunicación para llevar a cabo la interconexión como Wifi, ADSL, fibra óptica o Bluetooth.

3 | Biométricas. Son datos que provienen de sensores de uso en la vida diaria para acceso a recintos o que llevamos puestos (del inglés *weareables*), algunos ejemplos son sensores de huellas dactilares de teléfono móviles, escáneres de retina, lectores de ADN, sensores de reconocimiento facial o reconocimiento de voz, pulseras de actividad, pulsómetros, etc. Su uso está muy extendido en materia de seguridad en todas sus variantes (privada, corporativa, militar, policíaca, de servicios de inteligencia, etc.) y también en la tecnología deportiva y médica.

4 | Marketing web. El aumento del comercio electrónico y los portales de venta online hace que nuestros movimientos en la Red estén sujetos a todo tipo de mediciones que tienen como objeto estudios de marketing y análisis de comportamiento. Por ejemplo, cuando se realizan mapas de calor basados en el rastreo del movimiento del cursor por parte de los usuarios de una web, en la detección de la posición de la página, o en el seguimiento de desplazamiento vertical a lo largo de esta. Con esos datos se llega a conclusiones tales como qué partes de una página atraen más al usuario, o qué productos son los que más le interesan (serán aquellos donde se sitúen los productos sobre los que hace clic o en qué zona de esta pasa más tiempo).

5 | Transacciones de datos. De la misma forma que ha aumentado el comercio electrónico, los traspasos de dinero de una cuenta bancaria a otra, la reserva de un billete de avión o añadir un artículo a un carrito de compra virtual de un portal de comercio electrónico, serían algunos ejemplos.

Big Data ¿para qué sirve?

Una de las preguntas que más se hace hoy en día, sobre todo teniendo en cuenta que para el público en general este concepto es bastante novedoso, es la utilidad o los beneficios que aporta el big data. Existen muchas utilidades y beneficios, entre las que destacan:

1 | Reducir los costes de producción y optimizar recursos. Las grandes tecnologías de datos y el análisis basado en la nube aportan importantes ventajas en términos de costes cuando se trata de almacenar grandes cantidades de datos e identificar maneras más eficientes de gestionar recursos para dedicarlos a las actividades que darán mejor rendimiento o beneficio, ya sea económico, social o tecnológico.

2 | Detectar el comportamiento fraudulento u opiniones sobre acciones realizadas. Cuando los gobiernos o empresas toman medidas o lanzan productos, utilizan el big data para sondear el resultado de dichas acciones. Dichos datos analizados y estructurados dan mucha información para modificar, mejorar o cancelar la continuación de esas acciones.

3 | Tomar decisiones inteligentes y disminuir el tiempo de ellas. La velocidad del análisis, mezclada con la capacidad de examinar nuevas fuentes de datos, hace que las organizaciones puedan tomar decisiones basadas en lo que han aprendido.

4 | Determinar las causas de origen de fallos, problemas y defectos casi en tiempo real.

5 | Desarrollar nuevos productos. Con la capacidad de evaluar las necesidades de los clientes y su satisfacción, viene el poder de darles lo que quieren. Esto significa que es posible crear nuevos ítems para dar respuesta a esos requerimientos.

6 | Optimizar las ofertas. El big data permite predecir cómo se comportarán los compradores en el futuro en función de sus comportamientos anteriores, por lo que se pueden establecer ofertas de un modo fundamentado y ahorrar dinero.

7 | Generar cupones para los clientes en el punto de venta basados en sus hábitos de compra.

8 | Tener un mayor conocimiento del mercado.

9 | Seguimiento de la competencia. Los macrodatos proporcionan una mayor comprensión de la competencia y anticiparse a ella.

10 | Información en tiempo real. La información anticuada no tiene valor aplicable en el presente y menos en el futuro, por eso la recopilación de datos de manera diaria que proporciona esta tecnología permite disponer de un feedback casi en el momento.

Tipos de Big Data

Estructurados

Cualquier dato que se pueda almacenar, acceder y procesar en formato fijo recibe el nombre de dato «estructurado». Son los que tradicionalmente se han usado en el tratamiento de datos. Sus características principales son que se pueden almacenar en tablas y tienen una clara definición de longitud y formato.

Entre ellos, se encuentran los números, cadenas de caracteres y las fechas. Aunque haya otros tipos de datos que contengan más información, no significa que estos no tengan importancia. No obstante, hoy en día, existen problemas con respecto al tamaño de dichos datos ya que crecen en gran medida, llegando a dimensiones típicas del rango de múltiples zettabytes.

No estructurados

Son cualquier dato de forma desconocida o cuya estructura se clasifica como un dato no estructurado. Además, de ser enormes en tamaño, los datos no estructurados plantean múltiples desafíos con respecto a su procesamiento para derivar valor de ellos.

Se trata de datos en su forma original, tal y como fueron recogidos. No poseen un formato específico que permita almacenarlos de forma tradicional, pues no se puede desglosar la información que facilitan a tipos de datos definidos en longitud y formato. Entre ellos son comunes, por ejemplo, los emails, las presentaciones multimedia como los PowerPoint, documentos de procesadores de textos o los archivos en formato PDF.

Un ejemplo típico de datos no estructurados son las fuentes de datos heterogéneos que contienen una combinación de archivos de texto simples, imágenes, vídeos, entre otros.

En la actualidad, las organizaciones cuentan con una gran cantidad de datos disponibles. Pero, desafortunadamente, no saben cómo derivar valor de ellos porque estos datos se encuentran en su forma cruda o formato no estructurado.

Semiestructurados

Los datos semiestructurados pueden contener ambos tipos de datos. Suelen tener un formato que se puede definir, pero el usuario no lo puede comprender fácilmente y requiere el uso de reglas complejas que ayuden a determinar cómo leer cada pieza de la información. Un ejemplo de un dato semiestructurado es un dato representado en un archivo XML.

Siguen una especie de estructura, pero esta no es lo suficientemente regular como para gestionarla como datos estructurados. Posee ciertos patrones comunes que los describen y dan información sobre las relaciones entre los mismos. Como ejemplo, el HTML, lenguaje para la elaboración de páginas web, donde su sistema de etiquetas permite detectar esas pautas comunes.

Ejemplos de uso

Además de los ejemplos mostrados en el vídeo **A4C44C1V02** ***"Tecnologías digitales, Big Data y Sostenibilidad Ambiental"*** sobre este tema, existen muchos más ejemplos de uso del big data para la sostenibilidad, como por ejemplo el proyecto de la compañía leonardo (*leonardo.com*). Esta compañía está desarrollando diferentes proyectos basados en el big data utilizando información de satélites.

TECNOLOGÍAS DIGITALES, BIG DATA Y SOSTENIBILIDAD AMBIENTAL

e.digitall.org.es/A4C44C1V02

Entre varios proyectos, destacan el uso de imágenes satelitales que procesan con potentes algoritmos para ayudar a alcanzar los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de la ONU, como la gestión sostenible del suelo, los recursos hídricos, los bosques y las ciudades. Los satélites hacen una contribución muy importante ya que, a través de un único punto de observación, ofrecen una medida de las variables y fenómenos que queremos observar, es decir, globales, objetivas y trasladables de un punto a otro del planeta, para correlacionarlos con indicadores de sostenibilidad.

Saber más

- e.digitall.org.es/sustainable-data
- e.digitall.org.es/un-bigdata
- e.digitall.org.es/master-bigdata
- e.digitall.org.es/data-catalog
- e.digitall.org.es/fao
- e.digitall.org.es/bigdata-analysis
- lifeunderyourfeet.org
- e.digitall.org.es/bangladesh
- e.digitall.org.es/postgrado-bigdata
- e.digitall.org.es/youtube-bigdata

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