DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel B1

ÍNDICE

DigitAll

Seguridad

4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel B1 4.1 Protección de dispositivos

Sesiones y autenticación web

Sesiones y autenticación web

Entender cómo funciona la navegación web es esencial para nuestro día a día en línea. Utilizamos la web para hacer compras, gestiones, buscar información o para ver una película. Para ayudarnos a proteger nuestras cuentas en los servicios de la web, veremos a continuación **cómo funciona la autenticación web y las sesiones**.

Servidores y navegadores

Como hemos aprendido en niveles anteriores, la navegación web usa los servidores y los navegadores para funcionar. La mayoría de los servicios a los que accedemos, en lugar de ser páginas web estáticas, ofrecen ciertas funcionalidades. Estos servicios se conocen como aplicaciones web.

Tanto las páginas web estáticas como las aplicaciones web usan **direcciones web** o URLs, que se traducen en direcciones IP a través del DNS. Así, nuestro navegador puede acceder a los recursos alojados en el servidor. Cada imagen, página o documento alojado en el servidor, tiene una URL diferente. Nuestro navegador, **hace una solicitud por cada uno de los contenidos, a través del protocolo HTTP**.

NAVEGACIÓN WEB SEGURA

La navegación web forma parte de nuestro día a día. Este vídeo nos explica qué es una URL y cómo funciona la comunicación entre servidor y navegador.

e.digitall.org.es/A4C41A1V06

Introducción a las sesiones web

Hay ciertos casos en el que el servidor **tiene que conocer nuestra identidad para ofrecernos contenido personalizado o al que sólo tenemos acceso nosotros**. Por ejemplo, los mensajes privados de una red social. En este caso, la aplicación web de la red social, debe autenticarnos cuando entremos en nuestra cuenta.

Las sesiones web se usan para identificar con nosotros cada una de las peticiones HTTP del navegador. Una vez hemos accedido a nuestra cuenta en la aplicación, el servidor **nos otorga un identificador de sesión**. En cada petición que el navegador haga al servidor, incluirá este identificador, para hacer saber que somos nosotros y que ya hemos verificado nuestra identidad al entrar en la cuenta.

El **identificador de sesión** se guarda en las **cookies de sesión**, un pequeño fichero que guarda el navegador durante la navegación. Cuando el servidor recibe una petición HTTP, el

COOKIES, SESIONES Y PRIVACIDAD EN LA WEB

Las sesiones web se usan para autorizar las peticiones web. Las cookies de sesión mantienen esta información. Sin embargo, existen otras cookies que pueden afectar a nuestra privacidad.

e.digitall.org.es/A4C41C1V09

navegador consulta la cookie y envía el identificador en la petición. De esta forma, como hemos accedido a nuestra cuenta y el servidor nos ha asignado un identificador, sólo se muestran nuestros mensajes privados, y no los de otra persona. **La autorización se produce cuando el navegador elige qué contenido mostrarnos acorde a este identificador de sesión**.

Las cookies suelen tener diferentes periodos de caducidad, igual que las sesiones web. Esto se define en el momento que nos autenticamos y el servidor nos asigna el identificador. Si un atacante nos roba nuestro identificador de sesión, podría hacerse pasar por nosotros. Sin embargo, si el periodo de caducidad es corto, esto evita que el atacante pueda mantener acceso por un periodo largo.

Registro, autenticación y sesiones

Para utilizar los servicios web con una cuenta, lo primero que hacemos es registrarnos en el servicio. Además del nombre de usuario y datos necesarios del propio registro, es en este momento en el que configuramos el método de autenticación. En la mayoría de las aplicaciones web, el método por defecto es una contraseña.

En este punto, es importante recordar que **la autenticación no es lo mismo que la autorización**. La autenticación verifica la identidad del usuario, usando algún método como una contraseña. Por otro lado, la autorización permite o deniega el acceso a algún recurso acorde a algún criterio, como la identidad de un usuario a través del identificador de sesión. La primera vez que usamos un servicio, hacemos lo siguiente:

1 | Registro

- Para crear una cuenta, ingresamos los datos necesarios.
- Establecemos el **método de autenticación**, normalmente una contraseña.

2 | Autenticación

- Para acceder a la cuenta, nos identificamos.
- La aplicación web verifica nuestra identidad **autenticándonos** con el método elegido durante el registro.
- El servidor instala **una cookie de sesión** en nuestro navegador.

¿ERES QUIEN DICES SER? INTRODUCCIÓN A LA AUTENTICACIÓN

La autenticación es el proceso de verificar la identidad. Para hacer esto en el mundo digital, existen varios métodos, todos basado en alguno de los tres tipos principales: algo que soy, algo que se o algo que tengo.

e.digitall.org.es/A4C41A2V06

3 | Acceso a los recursos web

- Una vez hemos entrado en nuestra cuenta, consultamos la información privada. Por ejemplo, nuestros mensajes de una red social.
- Para acceder a los mensajes, el navegador **envía la petición con la cookie de sesión.**
- El servidor nos identifica y **autoriza** la petición de acceso al recurso privado: nuestros mensajes de la red social.

4 | Cerrar sesión

- El servidor olvida el identificador y el navegador lo elimina.
- Al hacer las peticiones, el servidor deniega el acceso y nos obliga a volver a autenticarnos.

Este proceso es común a la mayoría de las aplicaciones web. Sin embargo, hay casos concretos en cada una de ellas. La diferencia principal es el método de autenticación empleado.

Como recordarás, lo más seguro es usar más de un método de autenticación. Muchos servicios permiten usar **autenticación multifactor** (MFA) o un **segundo factor de autenticación** (2FA). Por ejemplo, junto a la contraseña, podemos usar códigos TOTP con un generador de códigos en una aplicación, o una llave de seguridad. De esta forma, si un atacante consigue nuestra contraseña, también tendría que conseguir acceso al segundo factor de autenticación.

Por último, si perdemos acceso a la cuenta, lo más habitual es que el servicio nos permita **recuperar la cuenta** enviando un correo electrónico a la dirección que hayamos registrado. Otra opción común es descargar unos códigos de un solo uso, conocidos como **códigos de recuperación**.

⚠ ATENCIÓN

¡Mantén tu cuenta de correo electrónico protegida! Si un atacante se hace con ella, podría utilizar la funcionalidad de recuperación de la cuenta para obtener acceso a otros servicios.

AUTENTICACIÓN BASADA EN TOKENS: ALGO QUE TENGO

La autenticación multifactor puede basarse en algo que poseemos físicamente, un token. Ejemplo de esto son las llaves de seguridad, los códigos TOTP o los códigos SMS. Todos ellos permiten mejorar la seguridad de nuestras cuentas cuando se usan conjuntamente con otro método.

e.digitall.org.es/A4C41C1V07

Seguridad

Nivel B1 4.1 Protección de dispositivos

Cyber Kill Chain

Cyber Kill Chain

En la actualidad, los ciberataques son cada vez más comunes y sofisticados. Para poder defendernos eficazmente contra ellos, es fundamental comprender el proceso que los atacantes utilizan para comprometer los sistemas. En este documento, se explicará en detalle el concepto Cyber Kill Chain, y analizaremos un ataque de ejemplo para mostrar cómo se aplican las diferentes fases.

En 2020, la empresa SolarWinds sufrió un ciberataque altamente sofisticado que permitió a los atacantes acceder a los sistemas de miles de organizaciones, incluyendo agencias gubernamentales y grandes empresas en todo el mundo. El ataque se llevó a cabo siguiendo las siete fases de la Cyber Kill Chain.

Fases del Cyber Kill Chain

El Cyber Kill Chain tiene siete fases diferentes. Las primeras fases corresponden con la preparación del atacante, y las últimas con la explotación y objetivo final del ataque.

> ***Saber más***
>
> Puedes encontrar información del Cyber Kill chain y sus aplicaciones en diferentes organismos especializados en ciberseguridad. Por ejemplo, en el INCIBE: *e.digitall.org.es/fases-ciberataque*

1 | Reconocimiento

La primera fase busca estudiar el objetivo del ataque. En el ejemplo, los atacantes comenzaron investigando a SolarWinds y sus clientes. Utilizaron técnicas de búsqueda en línea para identificar posibles vulnerabilidades y objetivos, y recopilaron información sobre los sistemas y la red de SolarWinds.

2 | Preparación

A continuación, se crean las armas o malware necesario para el ataque. En el ejemplo, los atacantes crearon un malware personalizado llamado SUNBURST que fue integrado en una actualización de software de SolarWinds. El objetivo de esta actualización era distribuirla a los clientes de SolarWinds y permitir a los atacantes obtener acceso no autorizado a sus sistemas.

3 | Entrega

Una vez creada el arma, es el momento de buscar el vector de ataque y hacer la entrega del malware. En el ejemplo, los atacantes utilizaron una técnica llamada "supply chain attack" para distribuir el malware creado por ellos. En lugar de atacar directamente a las víctimas, los atacantes comprometieron un proveedor de software de confianza (en este caso, SolarWinds) y distribuyeron el malware a través de sus actualizaciones de software.

4 | Explotación

Las vulnerabilidades encontradas en la primera fase por los atacantes son explotadas en esta fase. En el ejemplo, una vez que el malware se instaló en los sistemas de los clientes de SolarWinds, los atacantes comenzaron a explotar las vulnerabilidades en los sistemas para obtener control total. Utilizaron técnicas de engaño para obtener información de inicio de sesión y credenciales de los empleados y utilizaron herramientas de penetración para acceder a la red interna.

LOS SISTEMAS INFORMÁTICOS NO SON PERFECTOS: VULNERABILIDADES

Las vulnerabilidades son fallos de los sistemas informáticos que pueden ser explotadas por los atacantes. Cuando una vulnerabilidad se descubre, se denomina 0-day. Para arreglarlas, los fabricantes diseñan parches y los aplican en forma de actualizaciones.

e.digitall.org.es/A4C41B1V04

5 | Comando y control

Cuando ya se ha obtenido acceso al sistema víctima, los atacantes no pierden el control de su arma. En esta fase, se comunican con la víctima infectada usando servidores conocidos como "Command & Control" (C2). En este ejemplo, los atacantes instalaron herramientas adicionales para mantener el acceso a largo plazo y control sobre los sistemas comprometidos. También utilizaron técnicas de evasión para ocultar su actividad y evitar ser detectados por los sistemas de seguridad.

6 | Acción sobre los objetivos
Finalmente, se ejecuta el ataque acorde al objetivo principal de los atacantes. En el ejemplo, el objetivo final de los atacantes era la extracción de información confidencial. Una vez que tuvieron acceso a los sistemas comprometidos, los atacantes descargaron y extrajeron datos sensibles, incluyendo información gubernamental y empresarial altamente confidencial.

Para qué se utiliza Cyber Kill Chain

El ciberataque a SolarWinds fue un ejemplo muy sofisticado de un ataque cibernético que sigue las fases de la Cyber Kill Chain. El ataque subraya la importancia de mantener una postura de seguridad sólida y estar alerta ante posibles amenazas en línea. Además, también resalta la importancia de fortalecer la cadena de suministro y la necesidad de realizar controles rigurosos en todos los proveedores de software y servicios para mitigar los riesgos de los ciberataques.

El concepto de Cyber Kill Chain es un marco útil para entender cómo los atacantes pueden comprometer sistemas y qué medidas podemos tomar para defendernos. Es importante tener en cuenta que cada ataque es único y las diferentes fases pueden ser más o menos relevantes dependiendo de la situación. Al comprender cómo funciona el Cyber Kill Chain, podemos mejorar nuestra postura de seguridad en línea y estar mejor preparados para detectar y responder a posibles ciberataques.

Seguridad

Nivel B1 4.1 Protección de dispositivos

Los algoritmos en las redes sociales

Los algoritmos en las redes sociales

En la era digital, las redes sociales han transformado la forma en que nos relacionamos, comunicamos y consumimos información. Detrás de esta revolución tecnológica se encuentran los algoritmos: sistemas inteligentes que procesan y analizan enormes cantidades de datos para ofrecernos contenido personalizado.

Sin embargo, el impacto de estos algoritmos en los usuarios y en la gestión de la información **plantea desafíos y preocupaciones en términos de privacidad, sesgos y manipulación**.

Ya hemos visto algunos de los problemas con la privacidad y la gestión de la información en redes sociales, como son la huella digital, la reputación, y el acceso a la información de las fuentes abiertas (OSINT). A continuación, se explicarán los algoritmos en las redes sociales, su influencia en los usuarios y cómo estos algoritmos gestionan la información.

OSINT: LA INFORMACIÓN DE FUENTES ABIERTAS

Documento referenciado: ***A4C41A2D01***

PRIVACIDAD, HUELLA DIGITAL Y REPUTACIÓN ONLINE

Documento referenciado: ***A4C41A2D02***

La influencia de los algoritmos en los usuarios

En el contexto de las redes sociales, los algoritmos son un aspecto clave para gestionar la gran cantidad de información que el usuario puede ver. Estos algoritmos tienen la capacidad de personalizar el contenido que se muestra a cada usuario, adaptándolo a sus intereses y preferencias.

Sin embargo, esta personalización, puede llevar a la formación de **burbujas de información**, donde los usuarios son expuestos únicamente a información y opiniones similares a las suyas. Las burbujas de información pueden fomentar la polarización y limitar la diversidad de perspectivas.

Saber más

La influencia de los algoritmos y los sesgos de información en las redes sociales son un tema que está en debate público. El documental ***El dilema de las redes sociales*** (*thesocialdilemma.com*) muestra el impacto de estos sesgos de información en la sociedad.

Una de las mayores representaciones del poder de los algoritmos y de la segmentación de la información es la manipulación de masas o las campañas políticas altamente personalizadas. **El caso de *Cambridge Analytica* es posiblemente el más conocido, en el contexto de las elecciones presidenciales de Estados Unidos en 2016**. Esta empresa, dedicada a las campañas políticas, tuvo acceso a datos recopilados por Facebook sin el consentimiento adecuado. Gracias a esta información, utilizó perfiles psicológicos detallados para dirigir información sesgada y de campaña política de forma muy personalizada.

Este incidente generó gran controversia en relación con la privacidad de los datos en las redes sociales y planteó preocupaciones sobre la manipulación de la información y los sesgos algorítmicos.

Saber más

El documental *El Gran Hackeo*, de Jehane Noujaim y Karim Amer (estrenado en 2019) trata el caso de Facebook con Cambridge Analytica.

Cómo las redes sociales gestionan la información

La influencia de los algoritmos es posible debido a la gran cantidad de datos que los algoritmos recopilan sobre los usuarios. Esto es debido al **modelo de negocio de las redes sociales**, cuyos clientes son las empresas publicitarias, y el producto es la propia plataforma de publicidad dirigida: la red social.

Entre otra, la información recopilada sobre los usuarios puede ser:

- **Datos demográficos:** los algoritmos pueden tener acceso a información como edad, género, ubicación geográfica, idioma y ocupación del usuario.
- **Comportamiento en la red social:** los algoritmos registran la actividad del usuario en la plataforma, como los perfiles que se visitan, las publicaciones que se hacen clic, los "me gusta" que se dan y los comentarios que se realizan.
- **Interacciones sociales:** los algoritmos analizan las conexiones sociales del usuario, como sus amigos, seguidores y personas con las que interactúa con mayor frecuencia.
- **Historial de navegación:** en algunos casos, los algoritmos pueden rastrear el historial de navegación del usuario dentro y fuera de la plataforma de redes sociales, usando cookies de terceros, por ejemplo.
- **Datos de dispositivos:** los algoritmos también pueden recopilar información sobre el dispositivo que se utiliza para acceder a la plataforma, como el tipo de dispositivo, el sistema operativo y la resolución de pantalla.

Es muy importante tener en cuenta toda la información que las redes sociales son capaces de recopilar sobre los usuarios, y ser conscientes de ello. Debemos limitar qué compartimos en las redes sociales, cómo las usamos y revisar periódicamente las configuraciones de privacidad, ya que son la clave para hacer un buen uso de éstas y minimizar la capacidad de influencia de los algoritmos.

Seguridad

Nivel B1 4.1 Protección de dispositivos

Metodologías de gestión de riesgos

Metodologías de gestión de riesgos

Metodologías de gestión de riesgos

Características principales

Para ayudarnos a guiar el proceso de gestión de riesgos con mayores garantías de alcanzar los objetivos deseados aparecen distintas metodologías.

NOTA

Metodología de gestión de riesgos: conjunto de procesos y técnicas utilizadas para identificar, evaluar y mitigar los riesgos que puedan afectar a una organización o proyecto.

Saber más

La metodología de gestión de riesgos es esencial para garantizar la continuidad de la operación de la organización y maximizar la probabilidad de éxito y de consecución de sus objetivos

GESTIÓN DE RIESGOS: ACTIVO, PROBABILIDAD E IMPACTO

La gestión de riesgos es el proceso de identificar, analizar y evaluar los riesgos potenciales que pueden afectar a una organización e implementar las medidas preventivas y de mitigación oportunas.

e.digitall.org.es/A4C41B1V02

Todas las metodologías de gestión de riesgos deberían incluir además de las fases ya comentadas (identificación, valoración y priorización de los riesgos) las de: planificación e implementación de la respuesta, monitorización continua de la evolución de los riesgos y reporte de estos a todas las personas interesadas.

Hay que tener en cuenta que existen distintas metodologías de gestión de riesgos y cada una de ellas puede ser más adecuada para ciertas industrias o para distintas tipologías de riesgos como pueden ser riesgos financieros, operacionales, estratégicos, legales, etc.

Dado que la temática relacionada con esta formación es la seguridad de la información se van a revisar las siguientes metodologías que se utilizan en este marco:

- ***ISO 27005*** (*e.digitall.org.es/iso27005*)
- ***Magerit*** (*e.digitall.org.es/magerit*)
- ***OCTAVE*** (*e.digitall.org.es/octave*)
- ***NIST SP 800-30*** (*e.digitall.org.es/nistsp800-30*)
- ***FAIR*** (*fairinstitute.org/learn-fair*)

ISO 27005

La ISO 27005 es una norma internacional desarrollada por la Organización Internacional de Normalización (ISO) revisada por última vez en el año 2018.

Las principales características de la ISO 27005 son su enfoque basado en el riesgo, su adaptabilidad a diferentes tipos de organizaciones, su estructura clara y fácil de seguir, y su capacidad para integrarse con otras normas de seguridad de la información como la ISO 27001.

Incluye diferentes herramientas como las matrices de riesgo, las listas de control, las entrevistas con expertos y los análisis estadísticos.

Magerit

MAGERITv3 es una metodología que se utiliza en España desarrollada por el antiguo Consejo Superior de Administración Electrónica de España.

Como puntos fuertes de la metodología MAGERIT podemos destacar su catálogo de elementos que marca pautas con respecto a tipos de activos, dimensiones de valoración, criterios de valoración, amenazas típicas y salvaguardas. Se debería destacar también su guía de técnicas que proporcionan una orientación de cómo llevar a cabo proyectos de análisis y gestión de riesgos.

Octave

Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología del Software Engineering Institute (SEI) de la Universidad Carnegie Mellon. La última versión disponible es Octave Allegro, que se lanzó en 2012.

Los puntos fuertes de la metodología Octave incluyen un enfoque centrado en los procesos de negocio de la organización y como la información se utiliza en ellos, un proceso estructurado, un enfoque colaborativo de equipo y un alto grado de personalización.

Existen herramientas especializadas para facilitar el proceso de gestión de riesgos, como el software OCTAVE Allegro desarrollado por el SEI.

NIST SP 800-30

El NIST SP 800-30 es una guía desarrollada por el National Institute of Standards and Technology (NIST) de Estados Unidos, siendo la última revisión de septiembre de 2021.

Las características fundamentales o puntos fuertes del NIST SP 800-30 son su estructura, de 4 fases (preparación, evaluación, mitigación y comunicación), su adaptabilidad a las necesidades específicas de cualquier organización y su origen basándose en estándares y mejores prácticas de la industria.

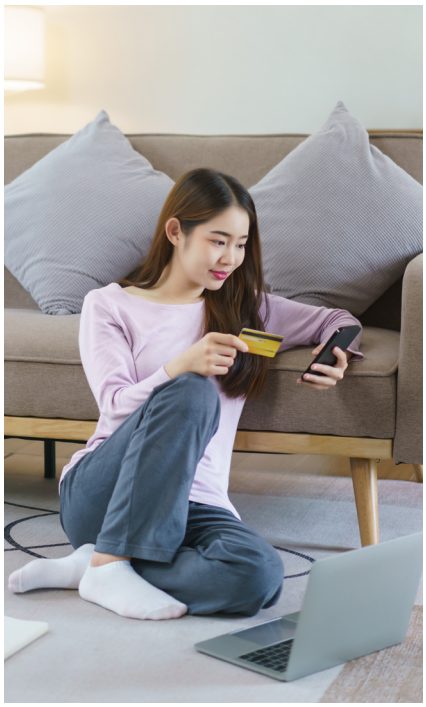
Es importante destacar que el NIST SP 800-30 es una guía de gestión de riesgos y no prescribe herramientas específicas para su implementación.

FAIR

FAIR (Factor Analysis of Information Risk) es un modelo desarrollado por el Open Group en 2006. La revisión actual es la 3.0 publicada en Abril de 2019.

Es un modelo cuantitativo que utiliza técnicas de análisis de datos y estadística para medir la probabilidad y el impacto financiero de un riesgo de seguridad de la información. FAIR se basa en un enfoque bottom-up, que permite una evaluación precisa y objetiva del riesgo a nivel de activos de información específicos. Es importante destacar que se integra fácilmente con otras metodologías y marcos de ciberseguridad, como NIST o ISO.

Para implementar FAIR, existen diversas herramientas que permiten realizar la evaluación cuantitativa de los riesgos de seguridad de la información, tales como RiskLens, FAIR-U y Open Fair.



PILAR

Se dedica un apartado especial a la herramienta ***Plataforma Integrada de Análisis y Gestión de Riesgos (PILAR)*** (*e.digitall.org.es/pilar*) desarrollada por el Centro Criptológico Nacional (CCN).

Es una herramienta gratuita y de acceso restringido, cuya utilización está sujeta a la previa solicitud y autorización por parte del CCN-CERT.

PILAR está diseñada para ayudar a las organizaciones a identificar, evaluar y gestionar los riesgos de seguridad de la información de manera efectiva, siguiendo tanto la metodología MAGERIT como la metodología ISO. Entre las principales características de esta herramienta se encuentran su capacidad para realizar evaluaciones de riesgos tanto cualitativas como cuantitativas, su flexibilidad para adaptarse a diferentes tipos de organizaciones y su capacidad para generar informes detallados de los resultados de las evaluaciones.

Esta herramienta es una de las más utilizadas en España para la gestión de riesgos de seguridad de la información y es ampliamente reconocida por su fiabilidad y precisión en la evaluación de riesgos.

DigitAll

Seguridad

4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel B1 4.2 Protección de los datos personales y la privacidad

Ataques a la privacidad: Phising

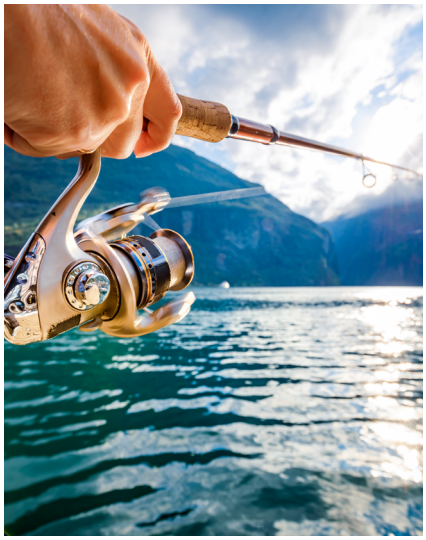
Ataques a la privacidad: Phishing y Smishing

Quizás, una de las principales amenazas a la identidad digital es una de las modalidades de ciberataque conocido como "Phishing". El objetivo de los ciberdelincuentes es conseguir nuestros datos personales y bancarios, para suplantar nuestra identidad digital. De esta forma pueden robar nuestro dinero, o influir en como los demás nos ven publicando comentarios en nuestro nombre. Este tipo de ataque no es nuevo, lleva produciéndose desde hace mucho tiempo. Sin embargo, con las nuevas tecnologías digitales, ha incrementado enormemente su número de víctimas y las formas de realizarse.

En este documento se va a explicar en qué consiste el ataque Phishing, qué modalidades puede presentar, cómo podemos identificar que estamos siendo atacados y cómo podemos protegernos.

¿Qué significa Phishing?

En el diccionario de la Real Academia Española de la Lengua no se encuentra una definición del término Phishing. Sin embargo, es comúnmente aceptado que se refiere al conjunto de técnicas o métodos empleados por los delincuentes utilizando el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial. El objetivo final es utilizar esta información privada para suplantar la identidad digital de la víctima con fines maliciosos.

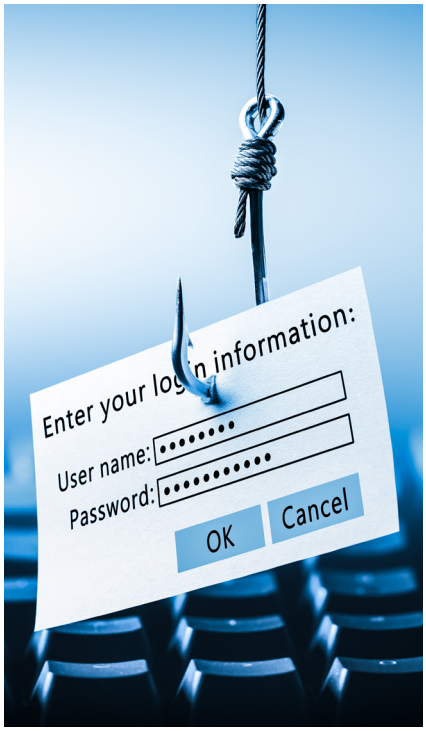


El término Phishing hace referencia a la actividad de pescar ("fishing" en inglés).

La información que estos delincuentes intentan conseguir puede ser muy variada, por ejemplo, el nombre de nuestros hijos, nuestro número de la seguridad social o datos bancarios como el número de nuestra tarjeta de crédito. El problema es que muchas veces es difícil saber el efecto malicioso que puede producir que un determinado dato personal sea conocido.

El término Phishing se origina a partir de la palabra inglesa "fishing", que significa pescar. El término se usa como una metáfora del acto de utilizar un cebo para conseguir que un pez (la víctima) pique el anzuelo y sea pescado. De forma similar, a los delincuentes que utilizan este tipo de ataque se les denominan "phishers".

Funcionamiento del Phishing



Quizás, la mejor forma de prevenir este tipo de ataque sea conocer cómo funciona. Independientemente de la técnica concreta utilizada, los ataques Phishing siguen un mismo patrón:

1 | El atacante inicia una comunicación con la víctima, suplantando la identidad de alguna organización o persona de confianza para esta víctima. Por ejemplo, su banco, la agencia tributaria, un amigo, etc.

2 | En dicha comunicación, el atacante proporciona un cebo. Por ejemplo, "debes actualizar la información de la tarjeta xxxxx ", "tienes una multa pendiente de pagar de tu coche con matrícula yyyyy" o "te ha tocado un premio".

3 | La víctima pica el cebo y proporciona alguna información confidencial confiada en que está haciendo lo correcto. Por ejemplo, da una contraseña, un número de cuenta, etc.

En la época anterior a Internet, las formas de iniciar la comunicación eran principalmente una llamada telefónica, una carta o una visita a nuestro domicilio. Sin embargo, hoy en día, en la era digital, las formas en que los atacantes pueden iniciar esta comunicación pueden ser muy variadas. Quizás las más conocidas son un correo electrónico o un mensaje de texto en el móvil.

Los atacantes utilizan técnicas conocidas como Ingeniería Social, que son el conjunto de técnicas que emplean los ciberdelincuentes para ganarse la confianza del usuario y de esta forma para confeccionar un cebo atractivo para su víctima (*e.digitall.org.es/ingenierial-social*). En más veces de las deseables, será la propia víctima la que facilite todo lo necesario para confeccionar este atractivo cebo ya que ella misma ha publicado demasiada información privada, por ejemplo, en los estados de una red social.

Saber más

Se recomienda visionar el vídeo (*e.digitall.org.es/experimento-social*) para hacerse una idea de la cantidad de información privada que se publicita en Internet y que los "phishers" pueden utilizar para confeccionar cebos atractivos.

Efectos del Phishing

Ser víctima de Phishing puede tener efectos desastrosos. Un atacante que pudiera hacerse con la contraseña para acceder al banco de la víctima podría ordenar transferencias. Si la contraseña es del perfil de la víctima en una red social podría afectar a su identidad digital haciendo comentarios para desacreditarla o incluso servir como base para atacar a una segunda víctima.

AUTENTICACIÓN MULTIFACTOR

Existen técnicas como la identificación multifactor que permiten protegerse incluso si se es víctima de un robo de contraseña.

e.digitall.org.es/A4C41A2V07

Si la víctima es una empresa o entidad pública, los efectos del Phishing pueden ser aún más desastrosos, ya que puede provocar una fuga masiva de datos privados tanto de los empleados como de los clientes o usuarios. En muchas ocasiones, la situación es aún peor porque no se hace público el ataque sufrido y esto imposibilita a las posibles víctimas colaterales el poder adoptar medidas para protegerse como, por ejemplo, cambiar su contraseña.

AUTENTICACIÓN: GESTIÓN DE CONTRASEÑAS

Para evitar el problema de ser víctima colateral en un ataque a una empresa o entidad, se recomienda utilizar una contraseña segura distinta para cada empresa o entidad donde se esté registrado.

e.digitall.org.es/A4C41B1V08

Tipos de phishing digital

Como ya se ha comentado, el Phishing es una técnica utilizada antes de que existiera Internet. Con la llegada Internet y las tecnologías digitales, han aparecido nuevas modalidades Phishing que utilizan estas tecnologías.

Este documento se centra en las modalidades de Phishing que utiliza alguna tecnología digital y que sen denominan de forma genérica como Phishing digital.

Phishing usando el correo electrónico

Quizás sea la modalidad de Phishing digital más común. Se utiliza los mensajes de correo electrónico para entregar el cebo a las víctimas. Estos mensajes suelen contener enlaces que llevan hasta sitios web maliciosos o archivos adjuntos infectados con programas malignos (conocidos como "malware").

Debido a que el coste de enviar un correo electrónico es con frecuencia cero, lo más común es que se utilice un mismo mensaje que se envía de forma masiva a miles de usuarios. Aquí el cebo suele ser burdo pero la esperanza del atacante es que piquen un pequeño porcentaje de víctimas.

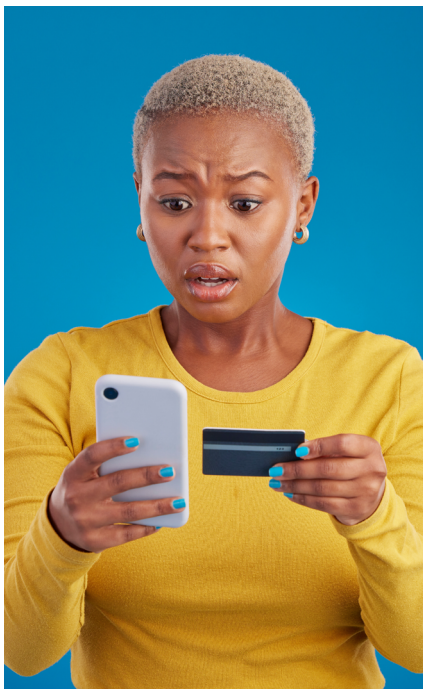
Otras veces el ataque es más especializado aprovechando alguna campaña publicitada de una empresa, o algún mensaje reciente enviado a todos sus clientes. En este caso se envía una copia modificada del anterior mensaje con enlaces maliciosos. En esta modalidad es más difícil detectar que se trata de un ataque.

Phishing usando la Web

En esta modalidad el atacante crea una copia exacta de un sitio Web. De esta forma, la víctima cuando accede a la copia maliciosa se confía y proporciona la información privada que el atacante desea, normalmente, la contraseña para autenticarse.

Otra técnica que pueden usar los delincuentes es inyectar código malicioso en un sitio web. De esta forma, la víctima al acceder al sitio web legítimo, al estar modificado por los atacantes, de nuevo puede proporcionar la información privada sin saberlo. Un ejemplo reciente han sido las ventanas emergentes para introducir las credenciales de inicio de sesión.

También es conocida otra técnica donde los atacantes crean páginas Web donde publicitan productos a muy bajo costo. Esto puede provocar que los buscadores web dirijan a las potenciales víctimas hacia esas páginas donde, como es lógico, deberán proporcionar mucha información confidencial para realizar la supuesta compra. Ejemplos han sido páginas de falsos bancos publicitando préstamos con bajo interés o tarjetas de crédito sin comisiones.



Vishing

En esta modalidad, el atacante utiliza una llamada telefónica. El término Vishing proviene de contraer los términos “voice phishing”. En este tipo de ataque, el delincuente suele camuflarse como trabajador de alguna empresa o entidad de prestigio. No es raro que incluso haya estudiado los perfiles de las redes sociales de sus víctimas para proporcionar información supuestamente privada durante la llamada. Esto hace que la víctima baje su estado de alerta y se confíe. A continuación, el delincuente solicitará la información privada que realmente desea.

Smishing

En esta modalidad el atacante utiliza un mensaje SMS. El término “smishing” proviene de la contracción de los términos “sms phishing”. Esta modalidad de ataque es similar a la que usa correo electrónico. Normalmente, la víctima recibe un mensaje de texto donde se le pide que pulse sobre un enlace o descargue una aplicación. Sin embargo, al hacerlo se le engaña para que descargue en su teléfono una app maliciosa que puede captar su información personal y enviarla al atacante. De nuevo es muy común que estos tipos de ataques coincidan con campañas generales como por ejemplo las campañas para realizar la declaración de la renta de las personas físicas a la Agencia Tributaria.

Phishing usando las redes sociales

En esta modalidad, los delincuentes utilizan toda la información privada que se publica en las redes sociales para intentar secuestrar el perfil de la víctima y forzarla a enviar enlaces maliciosos a sus amigos. De esta forma los amigos se convierten en víctimas a su vez. Otros delincuentes crean perfiles falsos simulando ser otras personas y los utilizan para engañar a sus víctimas intentando influir en ellas.

Principales recomendaciones para prevenir ser víctima de Phishing

Ahora que se han mostrado las principales modalidades de Phishing digital, es hora de dar algunas pautas para prevenirlo.

Pautas para prevenir ser víctima de Phishing.

1 | **Busque formación.** Es lo que está haciendo al leer este documento. La ***Oficina de Seguridad del Internauta*** (*incibe.es/ciudadania*) es una buena fuente para ampliar su formación y estar al día de las últimas estafas conocidas.

2 | **Tenga su software actualizado.** Un elemento clave es utilizar herramientas actualizadas a su última versión, en especial, el navegador web. Los navegadores web modernos tiene tecnologías capaces de detectar y prevenir muchas de las técnicas que utilizan los delincuentes para robar información privada.

3 | **Sea descreído.** Es mejor pecar por prudente ante cualquier correo electrónico. Con los enlaces, confirme que le conectan con los sitios web que dice el texto. Una técnica es leer siempre los correos en modo texto plano. De esta forma verá las direcciones reales de los enlaces o si hay enlaces "camuflados" en imágenes o logos. Si hay aplicaciones piense primero si verdaderamente es necesario descargarlas. Además, como regla general nunca instale aplicaciones que no sean oficiales en el sistema operativo que use: Google Play, Microsoft store, Apple Store, etc.

4 | **Confirme antes de actuar.** Hoy en día la mayoría de las empresas nunca solicitan a sus clientes información privada mediante correo electrónico o llamadas telefónicas. Si fuera el caso, borre el mensaje o cuelgue y confirme usted mismo con la empresa si esa solicitud es real. Por ejemplo, en vez de pulsar sobre el enlace de un correo electrónico para conectarse a su banco, inicie la conexión directamente usando el navegador introduciendo usted mismo la dirección web. Si es una llamada, llame usted a su banco preguntando si es real la campaña por la que ha sido llamado.

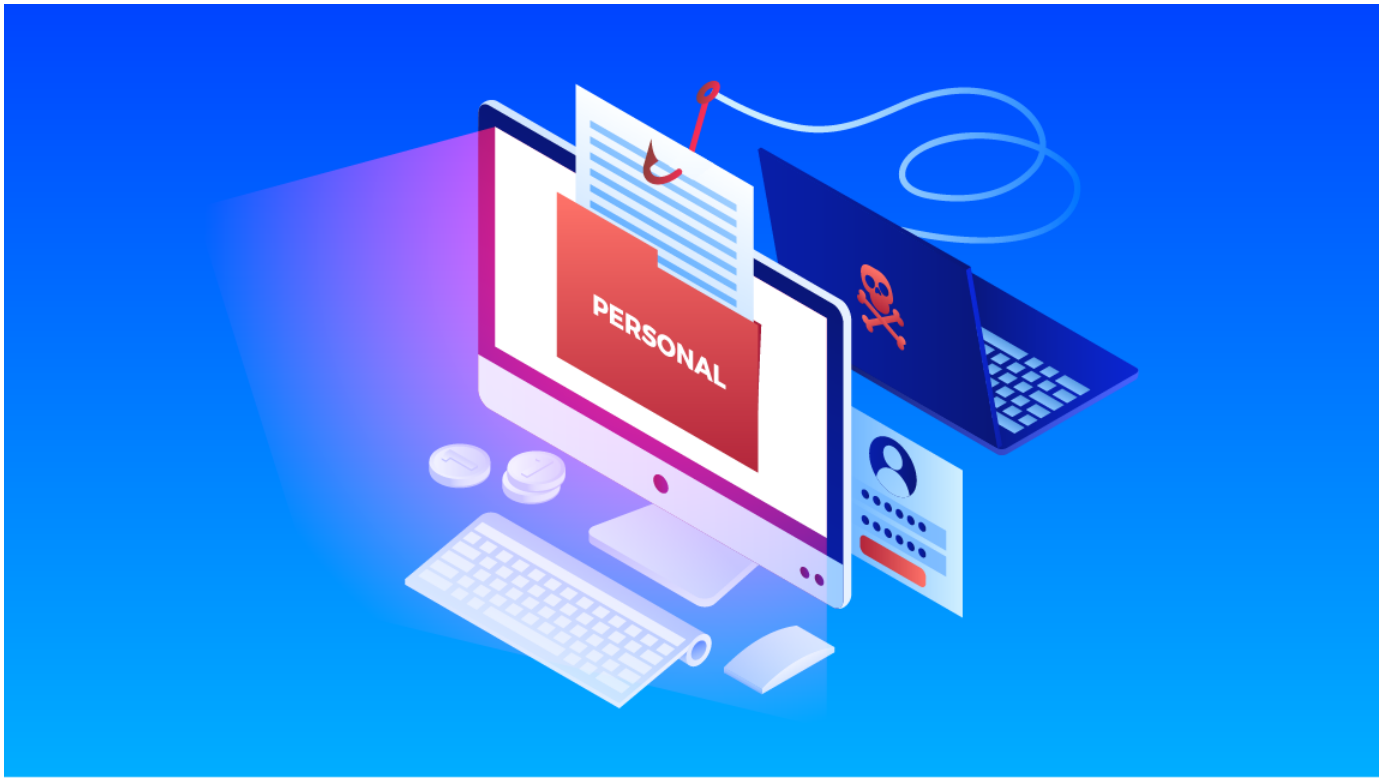
5 | Utilice un gestor de contraseñas. Si una empresa sufre una brecha de seguridad, es posible que sus clientes queden indefensos si utilizan por ejemplo una misma contraseña basada en alguno de los datos personales que han quedado comprometidos, por ejemplo, la fecha de nacimiento. Lo recomendable es usar una contraseña fuerte diferente en cada sitio web en el que estemos registrados. Para gestionar todas las contraseñas usaremos un gestor de contraseñas. La mayoría de los navegadores Web modernos incorporan un gestor de contraseñas, aunque también existe software especializado para ello.

Saber más

Oficina de Seguridad del Internauta. *incibe.es/ciudadania*

Experimento social - los riesgos de nuestros datos personales en internet. *youtu.be/3S7qFGVfsqM*

Ingeniería Social. *incibe.es/aprendeciberseguridad/ingenieria-social*



Seguridad

Nivel B1 4.2 Protección de los datos personales y la privacidad

FAQs sobre un uso adecuado de los datos personales en ámbitos concretos

FAQs sobre un uso adecuado de los datos personales en ámbitos concretos

¿Es posible un consentimiento tácito para el tratamiento de datos personales?

No. El Reglamento General de Protección de Datos exige que el consentimiento siempre sea expreso. No constituye consentimiento el silencio, las casillas ya marcadas o la inacción. Ese Reglamento exige que el consentimiento se formule "mediante un acto afirmativo claro que refleje una manifestación de voluntad libre".

¿Puede un menor de edad dar su consentimiento para que sus datos sean tratados por Facebook, Tik-tok, Twitter, etc.?

Ese tratamiento únicamente podrá fundarse en el consentimiento del menor cuando sea mayor de 14 años. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

¿Se pueden enviar los resultados académicos a los padres o tutores sin el consentimiento de los menores?

Sí. En este caso el tratamiento que realiza la institución educativa es necesario para la satisfacción de un interés legítimo de un tercero, los padres o tutores. Ese interés legítimo deriva de la patria potestad. Debe tenerse en cuenta que el artículo 154 del Código Civil impone a los padres/tutores el deber de educar y procurar una formación integral a sus hijos e hijas no emancipados.

¿Responder a las preguntas en una entrevista de trabajo equivale a un consentimiento para el tratamiento?

No. Es habitual que durante una entrevista de trabajo, la persona candidata responda a numerosas preguntas que contienen datos de carácter personal (su opinión de un asunto, sus aficiones, sus perspectivas de futuro, su situación familiar, etc.). La respuesta a esas preguntas no equivale a un consentimiento para el tratamiento de esos datos personales.

Además, el hecho de someter a la persona candidata a preguntas familiares y personales totalmente ajenas al trabajo que se va a desempeñar supone una conducta contraria a los deberes de minimización de datos y limitación de la finalidad.

NOTA

Constituye infracción administrativa muy grave «Solicitar datos de carácter personal en los procesos de selección…, que constituyan discriminaciones para el acceso al empleo por motivos de sexo, origen, incluido el racial o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación e identidad sexual, expresión de género, características sexuales, afiliación sindical, condición social y lengua dentro del Estado» [*art. 16.1.c) Texto refundido de la Ley de Infracciones y Sanciones en el Orden Social*].

¿Puede el empleador acceder a la información médica del trabajador obtenida por los servicios de prevención?

No. La Ley de Prevención de Riesgos Laborales obliga al empresario a garantizar a sus trabajadores una vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. La regla general es que esta vigilancia solo puede llevarse a cabo cuando el trabajador presta su consentimiento. El acceso a esa información médica de carácter personal y especialmente protegida se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud. No puede facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

El empresario solo será informado de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo.

¿Es legal recibir llamadas publicitarias?

Depende. Conforme a la Ley General de Telecomunicaciones se pueden distinguir dos supuestos:

- Las **llamadas automáticas**, es decir, en las que no existe una intervención humana, requieren consentimiento previo e informado por parte del abonado para que se realicen.

- Las **llamadas en las que interviene una persona** son legales, a menos que el abonado haya manifestado su oposición a su recepción.

PROTECCIÓN DE DATOS Y ÁMBITOS PARTICULARES

Se expuso cómo protegerte de la publicidad no deseada

e.digitall.org.es/A4C42C1V08

¿Se pueden tomar imágenes o grabar vídeos en eventos escolares?

Siguiendo las directrices de la Agencia Española de Protección de Datos, cuando se trate de eventos organizados por el centro escolar hay que distinguir:

a) Si el evento responde al ejercicio de la función educativa del centro (por ej., una función de teatro programada en la asignatura de literatura), la utilización de los datos se entendería amparada en la Ley Orgánica de Educación. Por tanto, no es necesario el consentimiento.

b) Si se trata de un evento al margen de la función educativa que cumple el centro escolar (por ej., una fiesta de navidad o de disfraces):

- Si es el centro escolar el que procede a la grabación de las imágenes deberá informar a los interesados, los propios menores si tienen más de 14 años y, si fueran más pequeños, a sus padres o tutores, de la finalidad de la grabación de las imágenes y de la difusión que de ellas se pretende hacer (si van a ser publicadas en páginas web, en redes sociales, ...) y solicitar su consentimiento.

- Si la toma de imágenes se realiza por los familiares de los alumnos y su uso es exclusivamente personal o doméstico, estaría fuera del ámbito de aplicación del Reglamento General de Protección de datos.
  No obstante, la divulgación fuera de ese ámbito de imágenes de personas sin su consentimiento a terceros, por ejemplo, la publicación de las imágenes en redes sociales "en abierto", constituye un tratamiento de datos que sí necesitaría del consentimiento de los afectados, pues en ese caso le sería de aplicación la legislación de protección de datos.

¿Puede un centro de educación infantil instalar un sistema de videovigilancia en las aulas?

No. Según el informe 475/2014 de la Agencia Española de Protección de Datos, la instalación de un sistema de videovigilancia para controlar al personal laboral es desproporcionada, pues esto puede conseguirse mediante mecanismos menos agresivos y/o intrusivos. En definitiva, se estaría vulnerando el principio de minimización de datos. A estos efectos sería indiferente que existiera el consentimiento de los padres (por las imágenes de sus hijos) e incluso del propio personal laboral.

Sí podría instalarse dicho sistema ante una situación concreta de incumplimientos laborales muy graves u otra finalidad que hiciera proporcional su uso.

¿Puede un órgano administrativo publicar un acto administrativo (por ej., listado de admitidos a un concurso-oposición) donde aparezca el DNI completo?

No. La Ley Orgánica de Protección de Datos personales y garantía de los derechos digitales, establece que cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

¿Cómo se eliminan fotos y vídeos de internet con nuestra imagen?

La imagen es un dato personal, ya se incluya en una foto o en un vídeo. Es habitual la presencia de fotos y vídeos en internet sin que exista una causa de legitimación para ese tratamiento. En estos supuestos, para conseguir esa eliminación se debe ejercer el derecho de supresión ante el responsable del tratamiento.

Los prestadores de servicios en internet más populares disponen de mecanismos propios para ejercer este derecho:

Facebook:

- A través del servicio de Ayuda: *e.digitall.org.es/ayuda-facebook*
- También a través del enlace Denunciar, que aparece situado en la mayoría de los contenidos publicados

Google:

- Formulario de solicitud de retirada de contenido: *e.digitall.org.es/contenido-google*

Youtube:

- A través del enlace Denunciar, que aparece debajo del vídeo.
- Existen otras opciones de denuncia para reflejar de forma más precisa el problema: *e.digitall.org.es/denuncia-youtube*

Twitter:

- En esta página se recoge la información y vínculos: *e.digitall.org.es/denuncia-x*
- También se puede denunciar directamente desde un Tweet, Lista o un perfil.

Instagram:

- En este link se encuentra la información correspondiente: *e.digitall.org.es/ayuda-instagram*

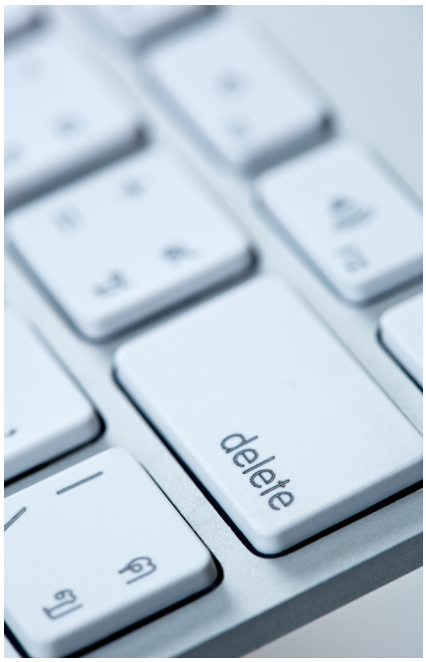
TikTok:

- En esta página se facilita información y links según el problema: *e.digitall.org.es/ayuda-tiktok*

Todas estas empresas y cualquier otra deben resolver sobre la solicitud de supresión en el plazo máximo de un mes a contar desde la recepción. Transcurrido ese plazo sin que de forma expresa respondan a la petición o si el interesado considera que esa respuesta es insatisfactoria, se puede interponer la correspondiente reclamación ante la Agencia Española de Protección de Datos, a través de su sede electrónica: *e.digitall.org.es/sede-electronica*

Esa reclamación se debe acompañar la documentación acreditativa de haber solicitado la supresión ante la entidad de que se trate.

¿Cómo se eliminan de internet contenidos sensibles?



La Agencia Española de Protección de Datos tiene un Canal Prioritario para la atención de situaciones excepcionalmente delicadas, cuando los contenidos (fotografías o vídeos) tengan carácter sexual o muestren actos de agresión y se estén poniendo en alto riesgo los derechos y libertades de los afectados. A ese canal se accede a través de la sede electrónica de la Agencia: *e.digitall.org.es/sede-electronica*

La información que se facilite se analizará de forma prioritaria y, en su caso, la Agencia Española de Protección de Datos ordenará la retirada del contenido al prestador del servicio o plataforma donde se esté difundiendo. Además, si hay indicios de delito, lo pondrá en conocimiento de la Fiscalía.

DigitAll

Seguridad

4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel B1 4.3 Protección de la salud y el bienestar

Guía visual para utilizar el control de tiempo de los dispositivos

Guía visual para utilizar el control de tiempo de los dispositivos

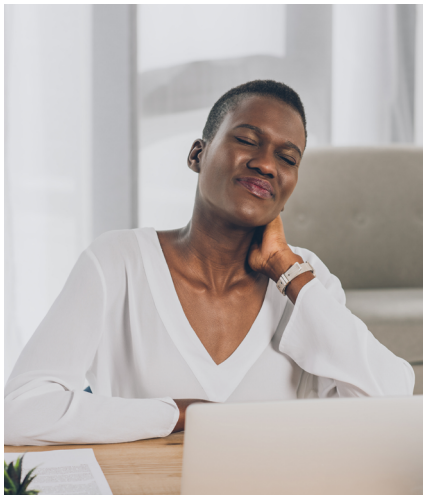
En el presente documento se mostrará una guia visual para utilizar el control del tiempo de los dispositivos comenzando con una introducción sobre el uso abusivo de los dispositivos, seguido de la necesidad de controlar el tiempo y la repercusión sobre la salud y se mostrarán diferentes métodos para el control del tiempo.

El uso abusivo de los dispositivos

Los dispositivos electrónicos como los móviles, tablets y ordenadores ocupan cada vez más un lugar muy importante en la vida diaria de la gente. Hoy en día, casi todo el mundo dispone de ellos y los usa con regularidad, tanto en un ámbito laboral como lúdico, familiar, entre otros.

Aunque estas nuevas tecnologías han supuesto un gran avance en diversos ámbitos y nos han facilitado la vida para bien, hay que tener en cuenta que también pueden tener un impacto negativo sobre nuestra salud física y mental. Hacer un uso desmesurado de las mismas puede ocasionar en los usuarios altos grados de adicción y dependencia.

Además de la adicción, este uso abusivo de las tecnologías puede causar consecuencias físicas, emocionales o sociales a la persona que hace uso de ellos. Las consecuencias más comunes suelen el insomnio, la ansiedad, el estrés, la depresión, la irritabilidad y/o los dolores articulares o musculares, entre otros.

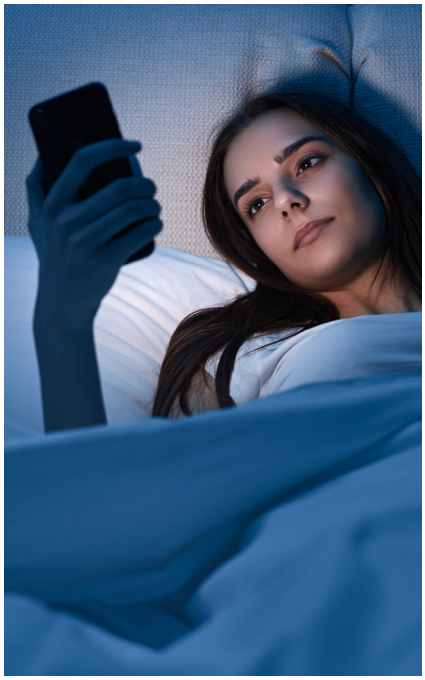


NOTA

En la página web de Kapersky han publicado un artículo muy interesante sobre cómo el uso de dispositivos electrónicos influye en la salud de los usuarios. Se centra en diferentes problemas como los musculoesqueléticos, psicológicos, la fatiga visual, influencia negativa a la hora de dormir...

Efectos de la tecnología en la salud (e.digitall.org.es/kapersky)

La necesidad de controlar el tiempo



Para evitar la dependencia de la que hablamos anteriormente, hay que aprender a desconectarse y a tener un control consciente del tiempo que se pasa haciendo uso de los dispositivos.

Es por esto que es altamente recomendable limitar el uso de los dispositivos electrónicos al mínimo tiempo posible y siempre y cuando sea estrictamente necesario. Para llevar a cabo este control existen una serie de aplicaciones y funcionalidades que permiten cronometrar el tiempo dedicado al uso de la tecnología a lo largo del día.

Además de esto, existen una serie de recomendaciones más sencillas que también pueden ayudar a controlar y limitar mejor el uso desmesurado:

No mirar el teléfono móvil u otros dispositivos antes de irse a dormir ni tampoco nada más levantarse, pues repetir con frecuencia estas acciones hace que se convierta en una rutina, lo que lleva a estar más horas con los dispositivos. Además, puede repercutir de forma negativa en el descanso y en el estado de ánimo del usuario.

Saber más

Usar durante mucho tiempo los dispositivos electrónicos antes de irse a dormir afectará a la glándula pineal, la cual es parte del cerebro que se encarga de producir melatonina, la hormona que regula el ciclo de nuestro sueño. Revisar constantemente el móvil antes de irnos a descansar nos hará perder horas de sueño. Para ello, lo ideal será dejar el móvil media hora antes, y alejarlo de nuestra cama, para que nos cueste un poco más el hecho de volver a cogerlo.

Dejar los dispositivos en un cuarto diferente al del usuario, lo que limitará el acceso directo y propiciará que se centre en otras tareas que tenga delante. Del mismo modo que el ejemplo anterior, el usuario no podrá ver notificaciones, lo que hará que no esté sujeto a tantos estímulos auditivos ni visuales.

Métodos para control del tiempo

En lo relativo a las aplicaciones y funcionalidades de control tiempo dedicado al uso de la tecnología que nombramos en el apartado anterior, destacan:

Alarmas y cronómetro

Hacer uso de las alarmas o del cronómetro de los móviles, tablets o wearables servirá para ser conscientes del tiempo que se dedica al uso de la tecnología. Estas avisan del tiempo que se está usando o no el dispositivo, además, el cronómetro permite calcular el tiempo con mayor exactitud.

Por lo general, la mayor parte de dispositivos móviles cuentan con una app propia de Reloj. Para acceder a la misma y activar una alarma se debe:

1 | Abrir la app de Reloj del teléfono.
2 | En la parte inferior, presionar Alarma.
3 | Elegir una alarma.
- Para agregar una alarma, presionar Agregar.

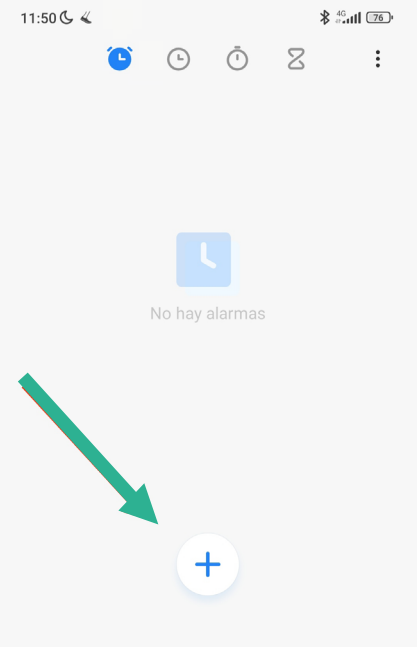
4 | Establecer la hora de la alarma.
- **En el reloj analógico:** deslizar la aguja hasta la hora que se desee. luego, hacer lo mismo para encontrar los minutos que se quiera.
- **En el reloj digital:** ingresar la hora y los minutos que se desee.
- **En el formato de 12 horas:** presionar A.M. o P.M.

5 | Presionar Aceptar.

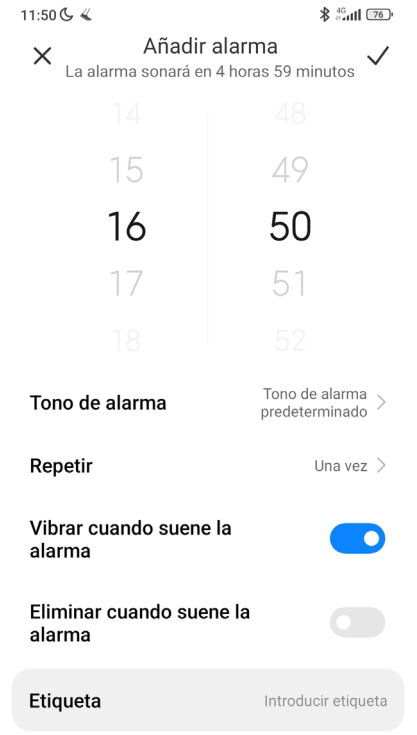
En caso de que querer anular dicha alarma:

1 | Abrir la app de Reloj del teléfono.
2 | En la parte inferior, presionar Alarma.
3 | En la alarma correspondiente, presionar la flecha hacia abajo.
- **Cancelar:** si se desea cancelar una alarma programada para sonar en las próximas 2 horas, presionar Descartar.
- **Borrar:** para quitar la alarma de forma permanente, presionar Borrar.

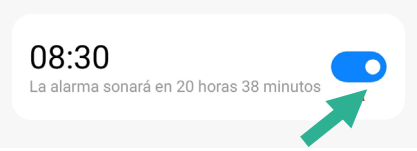
En otros casos la alarma aparece con un botón al lado, lo que le permite activarla y desactivarla directamente sin necesidad de seguir todo el paso 3.



Fuente: autoría propia.



Fuente: autoría propia.



Fuente: autoría propia.

Modo avión

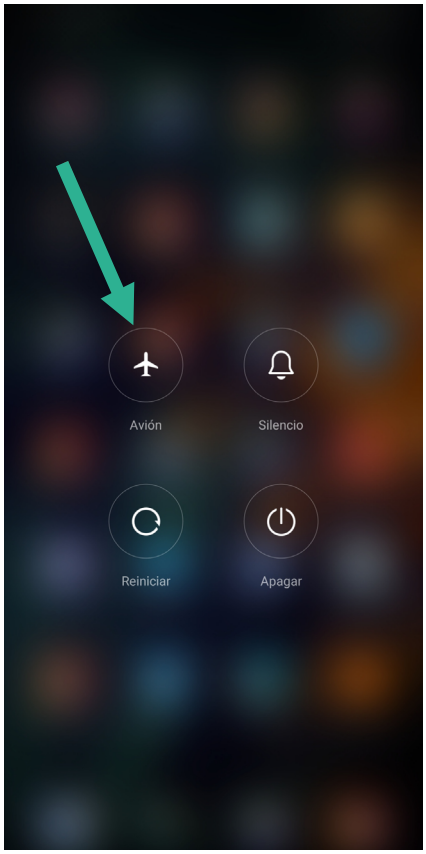
Usar el modo avión del teléfono o tablet para intentar limitar el tiempo de uso, o mismo apagarlo durante un tiempo. El modo avión impide que el dispositivo reciba notificaciones o llamadas, por lo que el usuario no estará tan pendiente de estos estímulos y le ayudará a desconectar.

Para acceder al modo avión de un dispositivo móvil se puede hacer de tres modos:

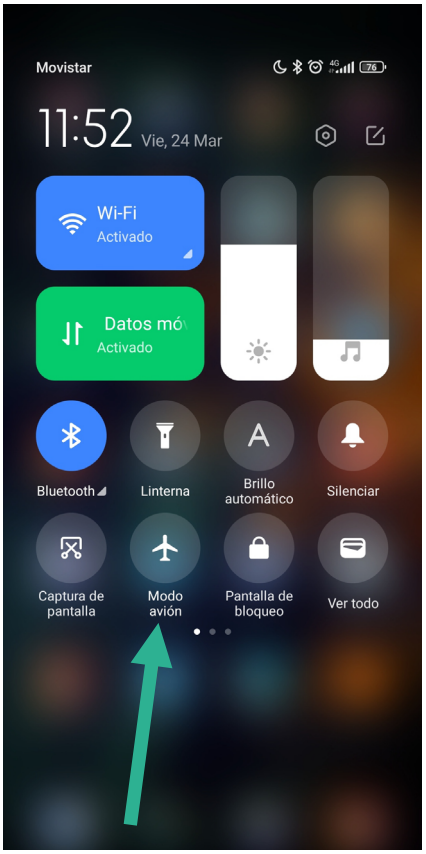
1 | Manteniendo pulsado el botón de apagado del dispositivo, lo que hará que aparezca la opción de modo avión. Ahí se puede activar y desactivar.

2 | Accediendo al apartado de ajustes del dispositivo. Por lo general suele estar entre las primeras opciones de la lista, con un botón de apagado y encendido al lado.

3 | A través de la barra de notificaciones del dispositivo. Basta con bajar dicha barra desde la parte superior del dispositivo. También suele aparecer entre las primeras opciones, y se puede activar y desactivar.



Fuente: autoría propia.



Fuente: autoría propia.

Bienestar digital de Android

Es una aplicación nativa implementada en Android 9 que permite monitorizar el tiempo que se está usando cada app y también permite poner límites al tiempo que se pasa en un web o en una app concreta.

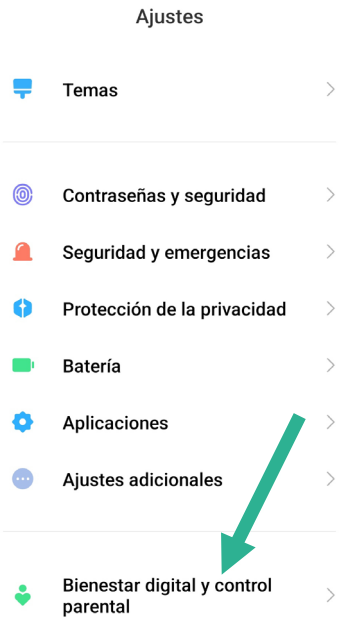
Otros fabricantes como Huawei tienen también sus propias aplicaciones de Bienestar Digital implementadas en sus dispositivos. En estos casos, pueden usar el mismo nombre u otros diferentes, como el Equilibrio digital de Huawei. Cada una de estas opciones tiene su propia interfaz y controles diferentes.

En el caso de dispositivos Android, para acceder al apartado de Bienestar Digital se debe:

1 | Entrar en la opción de ajustes del dispositivo móvil.

2 | Seleccionar la opción de Bienestar Digital y Control Parental. En otros casos, tal como se mencionó con anterioridad, podría aparecer otro nombre como Equilibrio Digital.

3 | Una vez dentro se podrá ver un gráfico con el tiempo que se ha utilizado el dispositivo en general (tiempo de uso); también se mostrará la aplicación que se ha usado más durante ese tiempo. Debajo se podrá ver un contador con el número de desbloqueos del dispositivo y la cantidad de notificaciones que se han recibido durante todo el día.



Fuente: autoría propia.

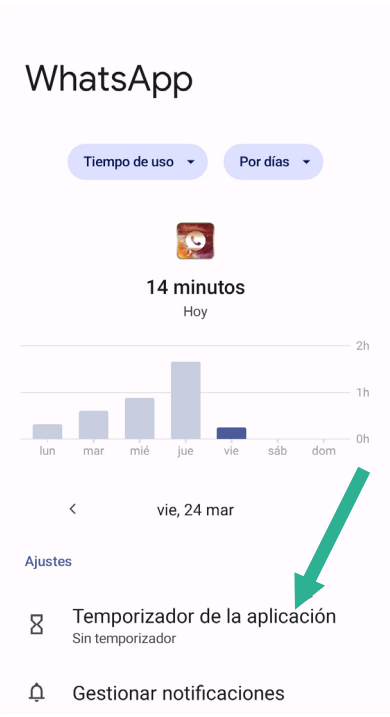
Fuente: autoría propia.

4 | Si se pulsa sobre la cantidad de minutos que se ha estado mirando el móvil, en la pantalla aparecerá una lista del tiempo de uso del dispositivo junto a las apps que se han usado, se podrán ver todas las aplicaciones que se abrieron y durante cuánto tiempo. También se puede observar un gráfico comparativo con los datos de toda la semana, pudiendo consultar otros días pasados.

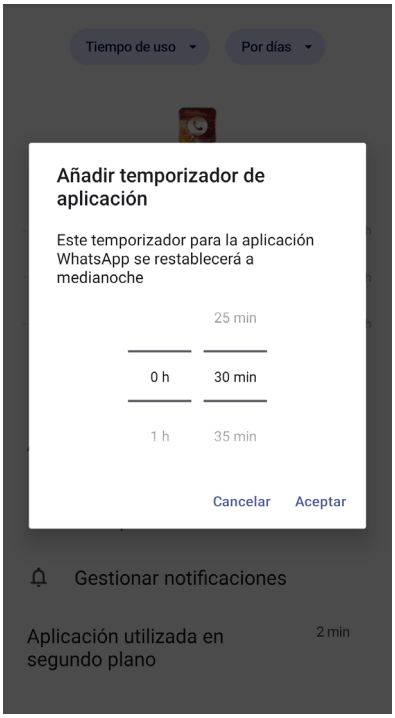
5 | Si se pulsa sobre una de las aplicaciones de la lista anterior, aparecerá una pantalla casi idéntica, pero con los datos únicos de esa aplicación concreta. Así se puede saber cuánto se utiliza cada app día a día. Debajo se encuentran las opciones para ir a la configuración de notificaciones y el temporizador de la aplicación.

6 | Si se pulsa en la opción Temporizador de la aplicación, se podrá establecer el tiempo máximo que Android permitirá usar una app en concreto. Así, si se quiere limitar el uso de las apps, cuando se llegue al tiempo establecido, Android bloqueará la app.

Fuente: autoría propia.



Fuente: autoría propia.



Fuente: autoría propia.

NOTA

Una vez se supera alguno de los límites establecidos la aplicación en cuestión aparece sombreada en la pantalla principal. Y si decides acceder aparece un cartel que te recuerda el bloqueo establecido, aunque siempre tienes la opción de ignorarlo

Saber más

DEPENDENCIA, USO Y ABUSO DE LOS DISPOSITIVOS TECNOLÓGICOS - Psicóloga Gloria Martínez Ayala. *https://psicologagloriamartinezayala.es/dependencia-uso-y-abuso-de-los-dispositivos-tecnologicos/*

¿Qué es el modo avión y como activarlo/desactivarlo en Android? *https://androidspain.es/modo-avion/*

Cómo establecer, cancelar o posponer alarmas - Ayuda de Android. *https://support.google.com/android/answer/2840926?hl=es-419#zippy=%2Cc%C3%B3mo-establecer-la-hora-de-la-alarma*

Tiempo de uso en Android: cómo saber cuánto tiempo pasas en el móvil y qué apps usas más. *https://www.xataka.com/basics/tiempo-uso-android-como-saber-cuanto-tiempo-pasas-movil-que-apps-usas*

Efectos de la tecnología en la salud. *https://www.kaspersky.es/resource-center/preemptive-safety/impacts-of-technology-on-health*

Bienestar digital en móviles : ¿cómo funciona el Tiempo de uso en iPhone y iPad? | Blog Educación y Bienestar digital. *https://gaptain.com/blog/bienestar-digital-en-moviles-como-funciona-el-tiempo-de-uso-en-iphone-y-ipad/*

Por qué no deberías estar con el móvil antes de dormir. *https://www.movilzona.es/noticias/problemas/utilizar-movil-antes-dormir/*

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel B1 4.4 Protección del medio ambiente

Hábitos de consumo “e-corresponsable” de tecnología

Hábitos de consumo "e-corresponsable" de tecnología

Introducción. El concepto "e-corresponsable"

En este documento se presenta un breve marco conceptual en torno al término "e-corresponsable", que hace referencia a la necesidad de asumir responsabilidades sobre las acciones que el consumo de tecnología digital pueda tener a nivel social y ambiental. Desde esa perspectiva, el concepto integra tres vertientes.

En primer lugar, la ambiental ("eco-responsable"), con relación a los impactos sobre el entorno natural de los procesos ligados a la producción, comercialización, mantenimiento y desecho de los dispositivos tecnológicos y las infraestructuras que le dan soporte. Estos impactos han sido descritos en videos y documentos anteriores, por ejemplo, los videos del nivel A1 "**Procesos de fabricación de recursos tecnológicos**" y "**Materias primas para el desarrollo de la tecnología**"; el video del nivel A2 "**El consumo energético de los dispositivos tecnológicos (la huella de tu email)**"; o el documento del nivel A2 "**Impactos ambientales de la tecnología**".

Por tanto, en este texto nos centraremos en las acciones propositivas de diseño, producción, comercialización y consumo que puedan abrir camino hacia vías de actuación menos impactantes con el entorno.

Por otro lado, la vertiente social debe considerarse también como eje central del concepto. Ser "corresponsable" implica entender nuestro papel como elementos interrelacionados dentro de una sociedad, en la que las acciones individuales pueden tener repercusiones tanto para el entorno como para otras personas. Por tanto, esta perspectiva debe ser tenida en cuenta para reflexionar sobre nuestros comportamientos individuales, pero también para plantear intervenciones colectivas de incidencia política.

El tercer eje del concepto hace referencia a la relevancia del sector tecnológico a nivel económico y social en nuestras sociedades contemporáneas, de ahí la importancia de tener en cuenta la "e" de electrónico en el concepto "e-corresponsable".

PROCESOS DE FABRICACIÓN DE RECURSOS TECNOLÓGICOS
e.digitall.org.es/A4C44A1V03

MATERIAS PRIMAS PARA EL DESARROLLO DE LA TECNOLOGÍA
e.digitall.org.esA4C44A1V05

EL CONSUMO ENERGÉTICO DE LOS DISPOSITIVOS TECNOLÓGICOS (LA HUELLA DE TU EMAIL)
e.digitall.org.es/A4C44A2V03

IMPACTOS AMBIENTALES DE LA TECNOLOGÍA
Documento referenciado: ***A4C44A2D01***

⚠ ATENCIÓN

En suma, debemos ser responsables y corresponsables tanto ambiental como socialmente a la hora de ejercer nuestro papel como personas consumidoras y usuarias de tecnología, tanto a nivel individual como colectivamente.

La eco-responsabilidad en el sector empresarial

La toma de decisiones para adquirir hábitos social y ambientalmente responsables en el consumo y uso de tecnología digital no debe recaer solamente en las personas usuarias o consumidoras de bienes y servicios tecnológicos. Al contrario, buena parte de esa responsabilidad debe enfocarse tanto en las instituciones encargadas de la legislación específica como en las empresas del sector de la tecnología digital.

Como ya vimos en documentos anteriores, ya hay en marcha diversas iniciativas institucionales que ponen el foco en la necesidad de diseña los productos y dispositivos tecnológicos teniendo en cuenta los posibles impactos ambientales y sociales de su ciclo de vida completo, por ejemplo, la propuesta del Parlamento Europeo que promueve el derecho a reparar (Parlamento Europeo, 2022).

NOTA

Otras iniciativas a destacar serían las distintas metas relacionadas con la contribución a la transición ecológica de los dispositivos digitales incluidas en las metas de la Comisión Europea (2021).

Estas disposiciones implican que cada vez más empresas de distintos ámbitos y sectores busquen implicarse en las propuestas de eco-responsabilidad en sus actividades. Según un informe de la Cámara Oficial de Comercio de España en Bélgica y Luxemburgo (2022), cada vez más empresas europeas se están implicando en la transformación de procesos productivos y comerciales en una apuesta por la eco-responsabilidad. Esta apuesta obedece, principalmente, a **cuatro razones**:

1 | **Imagen**. Las personas consumidoras hoy día prestan cada vez más atención a los detalles sobre el origen y procesos productivos de lo que compran y es más probable que compren sus productos o servicios si saben que su empresa se preocupa por su impacto en el medio ambiente y la sociedad.

2 | **Ahorro.** La aplicación de acciones concretas busca que la sostenibilidad ambiental de los procesos, como reducción, reciclaje, reutilización o gestión del consumo energético, por ejemplo, puede permitir ahorrar dinero a medio, e incluso a corto plazo.

3 | **Criterios de evaluación.** Los enfoques que buscan optimizar el uso de la energía y reducir el impacto ambiental y la sostenibilidad en general, son ahora criterios importantes en la evaluación y calificación de las empresas. Muchos inversores, como el banco HSBC, por ejemplo, ahora sólo financian proyectos con un rigor en la evaluación del impacto social y ambiental demostrado.

4 | **Captación de talento.** Debido a la creciente concienciación ambiental en ciertos sectores sociales y formativos, muchos futuros empleados son más propensos a trabajar en empresas con una sólida reputación social y ambiental. En otras palabras: para ser un imán de nuevos talentos, hay que ser verde.

Pero, ¿cómo puede transformar una empresa su funcionamiento en eco-responsable? Más allá de planes concretos de sostenibilidad o gestión ambiental como los basados en las normas ISO 14000, que aseguran ciertos estándares ambientales que pueden ser constatados en procesos de certificación, hay algunos sencillos pasos concretos que cualquier compañía puede poner en marcha de forma autónoma para promover procesos eco-responsables de producción y comercialización.

Más allá de los consabidos procesos de **reducción en el uso de materiales; separación y reciclaje de residuos; reutilización de recursos y gestión del gasto de agua y energía**, hay otros consejos interesantes para fomentar la eco-responsabilidad de los procesos productivos empresariales.

En primer lugar, se debe fomentar **el consumo de energía procedente de fuentes renovables**, como paneles solares, viento, biogás o energía geotérmica. En la actualidad, en el marco de la promoción de la Agenda 2030, en el contexto europeo se pueden encontrar multitud de subvenciones y ayudas institucionales para promover la transición energética, y el sector empresarial debe ser clave en la misma.

Por otro lado, la **movilidad** es otro eje clave a trabajar. Precisamente la tecnología digital permite introducir jornadas de teletrabajo que no sólo ahorrarán tiempo en términos de desplazamientos, sino que también reducirán el impacto ambiental.

A un nivel más concreto y casi anecdótico, hay iniciativas "micro" que pueden ayudar a fomentar la sostenibilidad en las instalaciones y además promover la seguridad y salud laboral, como el uso de plantas verdes para limpiar el aire de los centros de trabajo. En efecto, hay plantas que pueden absorber ciertas sustancias nocivas para la salud (por ejemplo, el benceno y el tricloroetileno).

Por último, se deben destacar los **incentivos fiscales** como herramienta clave para promover la eco-responsabilidad empresarial. Por ejemplo, podemos destacar aquí la iniciativa del **"eco-cheque"** que se ha puesto en marcha en Bélgica. El eco-cheque se define como un cheque para la compra de productos y servicios respetuosos con el medio ambiente que una empresa entrega a sus empleados.

Además de una ventaja económica y fiscal concreta, es una oportunidad para adaptar ligeramente su patrón de consumo hacia formas más sostenibles. El eco-cheque permite darse cuenta de que la forma de consumir puede tener un impacto sobre las opciones de: movilidad, las actividades de ocio sostenibles, la reutilización, el reciclaje, la prevención de residuos o la compra de productos locales y circuitos cortos de comercialización.

Por tanto, las opciones de consumo eco-responsable no sólo deben partir de iniciativas individuales, sino que pueden y deben estar favorecidas y fomentadas por apuestas institucionales y corporativas, como hemos visto con los ejemplos anteriores.

El eco-diseño como elemento central del consumo eco-responsable

El **eco-diseño** es uno de los conceptos clave para concretar el cambio de nuestro modelo de producción y consumo hacia otros menos impactantes a nivel ambiental y social, en la línea de las propuestas afines a la economía circular. A un nivel básico, el eco-diseño consiste en incluir la sostenibilidad ambiental como un criterio fundamental en la fase de diseño de productos y sistemas, como pueda ser la funcionalidad, la seguridad o la ergonomía. El objetivo último del eco-diseño es reducir el impacto ambiental del producto o servicio.

NOTA

El concepto ganó popularidad a finales de la década de 1970, principalmente a partir de la publicación de Victor Papanek "Diseñar para un mundo real" (Papanek, 1977). En la actualidad, el concepto ha ganado relevancia hasta el punto de generar la directiva europea de eco-diseño (2005/32/EC).

Esta directiva fue actualizada en el año 2009 (2009/125/EC), y su objetivo principal es definir un marco que establece los requisitos fundamentales de diseño ecológico para los productos que utilizan energía y pueden generar impacto ambiental. Si bien dicha directiva fue considerada como un elemento consultivo y casi accesoria durante la década anterior, en el marco de la Agenda 2030 y el **Plan de Acción para la Economía Circular 2020** presentado por la UE dentro del Pacto Verde Europeo, el concepto de eco-diseño se ha convertido en un elemento central.

Tomando como referencia la normativa anterior y el trabajo de diversos grupos de investigación, como puede ser *Institut de Ciència i Tecnologia Ambientals* (ICTA) de la Universidad Autónoma de Barcelona, se pueden destacar diversas iniciativas de desarrollo de productos basados en el eco-diseño en distintos sectores como pueden ser el mobiliario o el de los envases (González-García et al., 2011; Sanyé-Mengual et al., 2014).

En esta línea, existen múltiples herramientas cualitativas y cuantitativas para analizar el perfil ambiental del producto y establecer las consideraciones ambientales. Cada una de estas herramientas será apropiada para unas aplicaciones y circunstancias concretas ya que difieren en complejidad y coste. Entre las metodologías que se pueden aplicar para el ecodiseño de productos/servicios se pueden mencionar las siguientes: Análisis de Ciclo de Vida (ACV), Huella Ecológica, Huella de Carbono, Intensidad Material por Unidad de Servicio, Evaluación del Cambio de Diseño, Demanda Acumulada de Energía, Listas de Comprobación, Matrices de Análisis de Aspectos Ambientales o Valorización de la Estrategia Ambiental de Producto (Cámara de Comercio, 2023).

Como ya hemos visto en videos y documentos anteriores, el sector de la tecnología digital debe transformarse hacia modos de producción y consumo más sostenibles ambiental y socialmente, y las propuestas y estrategias centradas en el fomento de la reparabilidad, el reciclaje, la reutilización o el alargamiento de la vida útil, todas vinculadas al eco-diseño, pueden resultar fundamentales en dicha transformación.

⚠ ATENCIÓN

Teniendo en cuenta todo lo anterior, queda claro que el eco-diseño puede y debe ser una estrategia central en el proceso de transformación hacia modelos de economía circular que minimicen los impactos sociales y ambientales de nuestros hábitos de producción y consumo y por supuesto, el sector de la tecnología digital debe erigirse en punta de lanza de dicho proceso.

Como conclusión, en este documento señalamos la importancia de que la transformación de hábitos de consumo de tecnología hacia un modelo "e-corresponsable" no recaiga únicamente en las personas consumidoras, sino que tanto las instituciones como las empresas y compañías implicadas en el sector promuevan los cambios necesarios a través de estrategias como el eco-diseño.

Saber más

Cámara de Comercio (2023) Ecodiseño: Diseño de Productos-Servicios Sostenibles. *https://www.camara.es/innovacion-y-competitividad/como-innovar/diseno-sostenible*

DIRECTIVA 2009/125/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO (2009) de 21 de octubre de 2009 por la que se instaura un marco para el establecimiento de requisitos de diseño ecológico aplicables a los productos relacionados con la energía. *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0125&from=LV*

Comisión Europea (2021). La Década Digital de Europa: metas digitales para 2030. *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es*

González-García, Sara, Carles M. Gasol, Raúl García Lozano, M Teresa Moreira, Xavier Gabarrell, Joan Rieradevall i Pons, Gumersindo Feijoo (2014) Assessing the global warming potential of wooden products from the furniture sector to improve their ecodesign, Science of The Total Environment, Volumes 410–411. *https://www.sciencedirect.com/science/article/abs/pii/S004896971101093X*

Papanek, Victor (1977) Diseñar para el mundo real. *https://www.academia.edu/28853738/Dise%C3%B1ar_para_el_mundo_real_Victor_Papanek_pdf*

Parlamento Europeo (2022). Derecho a reparar: el PE quiere productos más duraderos y fáciles de reparar. *https://www.europarl.europa.eu/news/es/press-room/20220401IPR26537/derecho-a-reparar-el-pe-quiere-productos-mas-duraderos-y-faciles-de-reparar*

Sanyé-Mengual, E., Lozano, R.G., Oliver-Solà, J.,Gasol, C.M., Rieradevall, J. (2014) Eco-design andproduct carbon footprint use in the packagingsector, In: Subramanian, S.M.: Assessment ofcarbon footprint in different industrial sectors,Vol. 1, EcoProduction 2014, Springer, Singapore,pp. 221-245. *https://www.researchgate.net/publication/276266546_Eco-Design_and_Product_Carbon_Footprint_Use_in_the_Packaging_Sector*

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

El material del proyecto DigitAll se distribuye bajo licencia CC BY-NC-SA 4.0. Puede obtener los detalles de la licencia completa en: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es