DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel A2

ÍNDICE

DigitAll

Seguridad

4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel A2 4.1 Protección de dispositivos

OSINT: La información de fuentes abiertas

OSINT: la información de fuentes abiertas

A lo largo de nuestra vida digital generamos gran cantidad de datos, muchos de ellos personales, de todo tipo, como fotos, vídeos, texto, audios, ubicaciones, etc. Mucha de esta información permanece pública al alcance de cualquiera con una conexión a Internet. Para proteger nuestra privacidad, es importante ser consciente en todo momento de la información que publicamos en las redes, así como de aquella que esté disponible sobre nosotros a través de otras fuentes.

En esta sección se va a explicar cómo se puede hacer uso de la información pública de las personas para llevar a cabo investigaciones. A las técnicas y procedimientos de recuperar datos públicos y conseguir transformarlos en información relevante se le conoce como OSINT.

¿Qué es OSINT?

La **inteligencia de código abierto o Open Source Intelligence (OSINT)** es un método de recopilación de información en el que se utiliza información disponible públicamente para extraer datos útiles y relevantes que puedan ser utilizados en la toma de decisiones informadas.

Las **fuentes de información** para OSINT pueden ser **diversas**, como medios de comunicación, redes sociales, foros, blogs, sitios web gubernamentales, bases de datos públicas, entre otros. La información recopilada mediante OSINT se utiliza en distintos ámbitos, como la seguridad nacional, la investigación criminal, la gestión de riesgos, la inteligencia empresarial y muchas otras áreas.

La popularidad de OSINT ha aumentado significativamente en los últimos años debido a la **accesibilidad y la abundancia de información disponible públicamente**. Además, el desarrollo de tecnologías y herramientas específicas para la recopilación, análisis y visualización de datos ha facilitado el uso de esta técnica en diversas áreas.

El objetivo principal de OSINT es proporcionar una visión clara y objetiva de la información disponible al público para ayudar en la toma de decisiones informadas. Al utilizar la información disponible públicamente, OSINT puede proporcionar una visión única y más completa de un tema en particular que de otro modo sería difícil de obtener.

En resumen, OSINT es una técnica efectiva y ampliamente utilizada para recopilar información relevante, útil y disponible públicamente para tomar decisiones informadas. Esta técnica se ha vuelto cada vez más importante y popular debido a la accesibilidad de la información y al desarrollo de tecnologías y herramientas específicas.

Proceso OSINT

El proceso de OSINT es el conjunto de pasos que se deben seguir para llevar a cabo una investigación efectiva utilizando fuentes de información públicas. El proceso puede variar según el tipo de investigación que se esté realizando y las herramientas que se utilicen, pero generalmente se compone de los siguientes pasos:

1 | Planificación
Este es el primer paso del proceso y se enfoca en establecer los objetivos de la investigación, definir el alcance de la misma y determinar las fuentes de información que se utilizarán. Es importante establecer un plan para la investigación para mantenerse enfocado en el objetivo final y para asegurarse de no perder tiempo o recursos en información irrelevante.

2 | Recopilación
En este paso, se recopila la información de las fuentes identificadas en la fase de planificación. Es importante tener en cuenta que no toda la información disponible es relevante o precisa, por lo que se debe realizar una evaluación crítica de la información recopilada.

3 | Análisis
Una vez que se recopila la información, se debe analizar y evaluar para determinar su relevancia y utilidad en el contexto de la investigación. Es importante utilizar herramientas y técnicas de análisis para procesar grandes cantidades de información de manera eficiente y efectiva.

4 | Interpretación
En este paso, se interpretan los resultados del análisis para obtener una comprensión clara de la información y cómo se relaciona con los objetivos de la investigación. La interpretación puede requerir la validación de la información y la identificación de patrones y relaciones relevantes.

5 | Presentación
La presentación es el último paso del proceso y se enfoca en la comunicación de los resultados de la investigación a las partes interesadas. Es importante presentar la información de manera clara y concisa, utilizando visualizaciones de datos y otros medios para facilitar la comprensión.

Cabe destacar que las fases del proceso OSINT no tienen por qué ser llevadas a cabo de forma lineal. De hecho, en la mayoría de investigaciones se suele volver a fases anteriores una vez se descubre alguna información interesante que cambia el rumbo de los hechos.

En resumen, el proceso de OSINT implica planificar, recopilar, analizar, interpretar y presentar información pública para obtener conocimientos y tomar decisiones informadas. Cada paso del proceso es importante y se debe realizar con cuidado para garantizar que la información recopilada y analizada sea relevante y precisa en el contexto de la investigación.

Fuentes de información

Las fuentes de información de OSINT pueden variar ampliamente, desde redes sociales y bases de datos públicas hasta sitios web gubernamentales y medios de comunicación. Además, es fundamental asegurarse de que la información obtenida sea legal y ética. Algunas de las fuentes de información más comunes utilizadas en OSINT son:

1 | Redes sociales
Las redes sociales son una de las fuentes más utilizadas y accesibles de OSINT. Plataformas como Facebook, Twitter, Instagram y LinkedIn permiten a los usuarios compartir información personal, opiniones y lugares que visitan. Además, estas plataformas también brindan información valiosa sobre la red de contactos de un individuo, como

amigos, familiares, colegas y contactos profesionales. Algunos ejemplos de información que se puede encontrar en las redes sociales son: fotografías, ubicaciones, gustos y preferencias personales, publicaciones sobre opiniones, entre otros.

2 | Bases de datos públicas

Las bases de datos públicas son una fuente importante de información para OSINT. Algunas de las bases de datos más utilizadas incluyen registros de propiedad, registros de empresas, registros judiciales y registros de vehículos. Por ejemplo, una persona que busca comprar una casa puede utilizar una base de datos de registros de propiedad para obtener información sobre el historial de la propiedad, su valor actual y su ubicación.

3 | Sitios web gubernamentales

Los sitios web gubernamentales son una fuente confiable de información sobre políticas públicas, informes gubernamentales y estadísticas. Por ejemplo, un estudiante que busca información sobre la población y la economía de su país puede visitar un sitio web gubernamental para obtener datos actualizados y confiables.

4 | Medios de comunicación

Los medios de comunicación, tanto tradicionales como en línea, pueden proporcionar información actualizada sobre eventos y noticias relevantes. Los periódicos, las revistas, los canales de televisión y los sitios web de noticias son algunas de las fuentes más utilizadas para obtener información sobre eventos actuales. Por ejemplo, una persona que busca información sobre el clima y las condiciones del tráfico puede consultar el sitio web de noticias local.

Toda la información que se encuentra pública en Internet puede suponer un problema de privacidad importante para las personas. Por el simple uso de los servicios de la red, como la navegación Web o las redes sociales, estamos dejando una huella digital que es muy difícil de ocultar o modificar. En este sentido los datos personales tienen una gran relevancia, y existe legislación que protege su utilización e intercambio de forma segura, como el Reglamento General de Protección de Datos (RGPD). Si quieres saber más sobre este tema puedes ver el vídeo:

PRIVACIDAD, HUELLA DIGITAL Y REPUTACIÓN ONLINE

En este vídeo se resalta la importancia de la información que existe en Internet sobre un usuario, a través de su huella digital, destacando el uso de las redes sociales y la reputación online.

e.digitall.org.es/A4C41A2D02

NOTA

Cualquier persona con acceso a Internet podría acceder a la información que se encuentra publicada en la parte abierta de la red. Es importante por tanto **ser conscientes de toda la información que subimos a las redes**, como fotografías, vídeos, mensajes... por que gran parte de ella puede llegar a contener datos relevantes. Esta información podría ser utilizada por un atacante para crear engaños más creíbles o realizar suplantación de identidad.

Herramientas

Existen numerosas herramientas OSINT disponibles, y estas se pueden categorizar en diferentes áreas según su funcionalidad. Aquí p se presentan algunas de las herramientas más populares:

- **Motores de búsqueda.**
  Los motores de búsqueda son una de las herramientas más utilizadas en OSINT. Google es uno de los motores de búsqueda más populares y se utiliza para encontrar información en línea. Otros motores de búsqueda populares son Bing, Yahoo!, y DuckDuckGo. Además, existen motores de búsqueda especializados en la búsqueda de información en redes sociales, como Social Catfish y PeekYou.
- **Herramientas de monitorización de redes sociales**
  Estas herramientas se utilizan para monitorizar y recopilar información de diferentes plataformas de redes sociales. Algunas herramientas populares son Hootsuite, TweetDeck, y Meltwater.
- **Herramientas de análisis de imágenes**
  Estas herramientas se utilizan para analizar y extraer información de imágenes. Algunas herramientas populares son Google Images, TinEye, y Yandex Images.

- **Herramientas de análisis de metadatos**
  Los metadatos son información oculta en archivos digitales, como imágenes y documentos. Las herramientas de análisis de metadatos se utilizan para extraer esta información. Algunas herramientas populares son ExifTool y Metagoofil.
- **Herramientas de análisis de datos en la web**
  Estas herramientas se utilizan para extraer y analizar datos de la web, incluyendo sitios web y redes sociales. Algunas herramientas populares son Import.io, Scrapy, y BeautifulSoup.
- **Herramientas de análisis de correo electrónico**
  Estas herramientas se utilizan para analizar correos electrónicos, incluyendo la información de la cabecera y el contenido. Algunas herramientas populares son MxToolbox y Email Header Analyzer.
- **Herramientas de análisis de nombres de dominio**
  Estas herramientas se utilizan para analizar nombres de dominio, incluyendo información de registro, dirección IP y ubicación geográfica. Algunas herramientas populares son DomainTools y Whois.

Es importante tener en cuenta que estas herramientas solo son útiles si se utilizan adecuadamente. Para obtener los mejores resultados, es importante tener una comprensión sólida de la fuente de información que se está analizando y de las técnicas y metodologías de OSINT.

Caso de uso: Google Dorks

Google Dorks son comandos de búsqueda avanzados que permiten a los usuarios realizar búsquedas más precisas y detalladas en Google. En lugar de simplemente buscar palabras clave, los usuarios pueden utilizar Google Dorks para filtrar resultados de búsqueda utilizando parámetros específicos.

¿Por qué son útiles los Google Dorks? Los Google Dorks son útiles porque permiten a los usuarios encontrar información específica y detallada en línea. Los Google Dorks se utilizan comúnmente en OSINT para buscar información sobre una persona, organización o tema específico en línea.

A continuación, se presentan algunos ejemplos de comandos de Google Dorks útiles para usuarios no avanzados:

- **site:** este comando permite a los usuarios buscar en un sitio web específico. Por ejemplo, "site:nytimes.com coronavirus" buscará resultados en el sitio web del New York Times que incluyan la palabra "coronavirus".
- **filetype:** este comando permite a los usuarios buscar un tipo de archivo específico, como PDF o DOCX. Por ejemplo, "filetype:pdf hackeo informático" buscará resultados que contengan la frase "hackeo informático" en archivos PDF.
- **intext:** este comando permite a los usuarios buscar palabras o frases específicas dentro del contenido de una página web. Por ejemplo, "intext:password seguridad" buscará resultados que contengan la palabra "seguridad" y la palabra "contraseña".
- **inurl:** este comando permite a los usuarios buscar una URL específica o una parte de la URL. Por ejemplo, "inurl:seguridad informática" buscará resultados que contengan la frase "seguridad informática" en la URL.
- **intitle:** este comando permite a los usuarios buscar una página web por título. Por ejemplo, "intitle:seguridad informática" buscará resultados que contengan la frase "seguridad informática" en el título de la página.

Si queremos encontrar ejemplos reales de este tipo de comandos para encontrar información concreta, podemos utilizar la base de datos de Exploit Database llamada Google Hacking Database. Esta página permite encontrar multitud de Google Dorks concretos que nos permiten visualizar su aplicación real en el campo de la seguridad informática, así como recuperar cierta información que de primeras podría pasar inadvertida. Este tipo de recursos nos permiten entender la relevancia y el potencial de las técnicas de OSINT a la hora de realizar una investigación con fuentes abiertas.

NOTA

Es importante tener en cuenta que, aunque los Google Dorks pueden ser útiles, también pueden presentar riesgos de seguridad y privacidad si se utilizan incorrectamente. Por lo tanto, es importante utilizarlos con precaución y siempre tener en cuenta la legalidad y ética del uso de la información encontrada.

Comunidad OSINT

Trace Labs es una comunidad de OSINT dedicada a buscar personas desaparecidas utilizando técnicas de investigación y tecnología avanzada. Han tenido muchos casos de éxito en la búsqueda de personas desaparecidas, pero uno de los más destacados es el caso de "Mary".

En el caso de Mary, una mujer desapareció sin dejar rastro en 2019 en el estado de Nueva York, Estados Unidos. La policía local había intentado localizarla sin éxito durante meses, por lo que la familia de Mary recurrió a Trace Labs para obtener ayuda. La comunidad Trace Labs comenzó a trabajar en el caso y utilizó diversas técnicas de OSINT para buscar información sobre Mary en línea. Algunos de los métodos que utilizaron incluyeron la búsqueda de información en redes sociales, la investigación de registros públicos y la revisión de cámaras de seguridad.

Finalmente, el equipo de Trace Labs encontró información importante que llevó a la ubicación de Mary. La información incluía un registro de cámara de seguridad que mostraba a Mary en un área cercana a un lago, lo que llevó a la policía a buscar en esa zona. Mary fue encontrada con vida y fue devuelta a su familia.

Este caso demuestra el poder de OSINT y la capacidad de la comunidad Trace Labs para trabajar en conjunto para ayudar a las familias a encontrar a sus seres queridos desaparecidos. Trace Labs ha llevado a cabo muchos otros casos de éxito similares y continúa trabajando para ayudar a encontrar a personas desaparecidas en todo el mundo.

A nivel investigación existen también diferentes eventos en los que diversos profesionales del sector de la seguridad, en este caso especializados en OSINT, exponen sus investigaciones y herramientas propias. Algunos ejemplos pueden ser el **Osintomático Conference** o **IntelCon**.

Seguridad

Nivel A2 4.1 Protección de dispositivos

Privacidad, huella digital y reputación online

Privacidad, huella digital y reputación online

El uso de Internet y la publicación de información sobre nosotros, hace que creemos una identidad digital. Esta identidad puede reflejar a la que asociamos al mundo real, pero a diferencia de ésta, la identidad digital está formada por información de fácil acceso por cualquiera.

En esta sección, aprenderemos cómo funcionan los motores de búsqueda como Google o Bing, y qué información forma nuestra huella digital. Es importante conocerla y hacer un análisis consciente de qué implicaciones puede tener para nosotros.

Identidad y huella digital

La identidad digital es aquella que se conforma a partir de la huella digital de un usuario en Internet. Es decir, toda aquella información que está disponible públicamente, y que se puede asociar a una identidad, conforma la identidad digital.

Redes Sociales

Utilizamos redes sociales a diario, pero mucha gente no es consciente de lo que está compartiendo en ellas. Cuando hacemos uso de nuestros perfiles en redes sociales, debemos ser muy cuidadosos a la hora de compartir nuestra información y pensar en los riesgos que nos puede ocasionar.

Muchas veces compartimos demasiados detalles día a día en las redes sociales, incluso hay cierta información que debemos proporcionar de forma obligatoria si queremos hacer uso de ella, normalmente información personal. Esto no debería preocuparnos, siempre que los datos no sean accesibles por terceras personas.

⚠ ATENCIÓN

La información personal, datos personales o información personalmente identificable es aquella que permite identificar a un individuo. Por ejemplo, el DNI, lugar de residencia, estado civil o nacionalidad.

Hay cierta información que no deberíamos hacer pública en la red. Es decir, es recomendable que pensemos dos veces antes de publicar:

- **Datos personales:** como nombre y apellidos completo, teléfono, DNI, e-mail … ¡A través de ellos podemos ser identificados!
- **Planes y vacaciones:** pueden saber cuándo no estamos en casa para intentar entrar a robar.
- **Ubicación actual:** permiten saber nuestras rutinas diarias, nuestro domicilio y trabajo.
- **Información bancaria:** pueden robarnos o hacer cargos fraudulentos en nuestras cuentas.
- **Información sobre menores:** pueden herir su sensibilidad en el futuro, o acabar en malas manos.

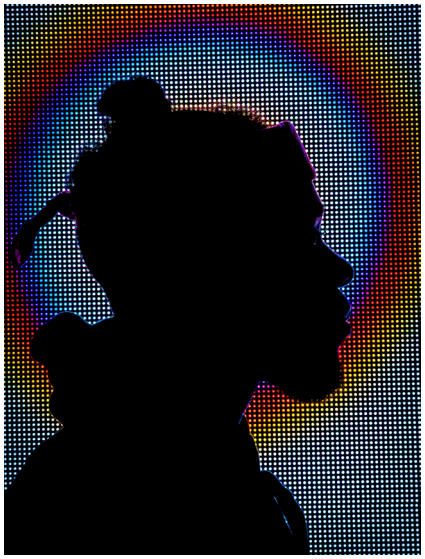
NOTA

Debes revisar las opciones de seguridad y privacidad de tus redes sociales. Las opciones de configuración más comunes suelen estar bajo un apartado en ajustes llamado "privacidad y seguridad". Aquí, puedes ocultar información para que no se muestre de forma pública, y gestionar lo que compartes y tu exposición en la red.

Reputación online

Además de la información anterior, debemos pensar dos veces también cuando publicamos comportamientos inapropiados o alguna opinión personal. Todo ello forma parte de nuestra reputación online. Concretamente, la huella digital que formamos creará nuestra identidad digital, que puede corresponder en mayor o menor medida con nuestra identidad real.

Existen cierto tipo de publicaciones que pueden afectarnos negativamente. Cuando publicamos algo, dejamos de tener control sobre esa información.



Las publicaciones que pueden afectar a nuestra **reputación online** son muchas, como, por ejemplo:

- **Publicaciones ofensivas o comentarios negativos:** insultar o amenazar a través de redes puede ser delito y realizar publicaciones ofensivas puede volverse en nuestra contra.
- **Ciberacoso:** burlas, insultos o humillaciones a una persona. Si eres víctima o un testigo, debes denunciarlo.

- **Quejas laborales:** muchas empresas revisan las redes sociales de sus trabajadores con el objetivo de evitar que compartan contenido inapropiado, o incluso durante procesos de selección.
- **Fotos y vídeos inapropiados:** si subes una fotografía a una red social, pierdes el control sobre ella. Además, fotografías que puedan comprometernos, pueden llegar a manos de terceras personas para chantajear o perjudicarnos.
- **Propagación de noticias falsas o "fake news":** no debemos creer todo lo que vemos por redes sociales o Internet.

Antes de publicar una noticia, es recomendable comprobar sus fuentes. Compartir un bulo o estafa, puede afectar muy negativamente a tu reputación online.

Los motores de búsqueda

Google, Bing, DuckDuckGo y Ecosia son motores de búsqueda en Internet. Nos permiten buscar información accesible de forma pública buscando a través de palabras clave o consultas. Aunque suena complejo, estamos muy acostumbrados a utilizarlos en nuestro día a día, respondiéndonos a dudas con una gran cantidad de enlaces o referencias a contenido en la web.

Sin embargo, **los motores de búsqueda también pueden incluir contenido como perfiles de redes sociales, imágenes, noticias o información general sobre nosotros**. Por eso, es importante entender su funcionamiento y cómo gestionar la información sobre nosotros en la red, accesible a través estos motores de búsqueda.

¿Cómo funcionan?

El objetivo principal de los motores de búsqueda es **ayudar a los usuarios a encontrar información relevante y útil en Internet**. Para lograr esto, los motores de búsqueda recopilan, organizan y presentan la información disponible en la web de manera eficiente y efectiva, con el fin de proporcionar a los usuarios los resultados más relevantes para su consulta.

Algunos buscadores también tienen como objetivo mejorar la experiencia del usuario, proporcionando resultados de búsqueda precisos y actualizados en formato fácil de usar y accesible.

> **NOTA**
>
> En este contexto, han surgido inteligencias artificiales conversacionales como ChatGPT, de OpenAI. Estos sistemas han sido entrenados con una gran cantidad de información en la web y son capaces de responder a preguntas complejas, a diferencia de los buscadores que sólo nos proporcionan referencias a la información.

Para que los buscadores puedan ofrecer al usuario la información relevante tras una consulta, deben haber rastreado la web previamente. Durante el proceso de rastreo de la web o ***web crawling***, los buscadores ordenan la información en una lista. Esto es conocido como "**indexación de contenidos**". Es decir, los buscadores exploran la web y procesan el contenido de ésta para incluirla en la lista de páginas web conocidas.

Esta lista o índice es el que el motor de búsqueda consulta cuando el usuario escribe en la barra de búsqueda o consulta. De esta forma, si hay algún contenido que se acaba de publicar en Internet en los últimos minutos, lo más probable es que el buscador no lo muestre, porque aún no estará "indexado".

Para detectar qué información ha "indexado" sobre nosotros un determinado motor de búsqueda, es recomendable practicar el "ego surfing". Esto consiste en buscar nuestro propio nombre o información personal en motores de búsqueda como Google, Bing o Yahoo. Es decir, buscar información sobre uno mismo en la web, y así analizar nuestra reputación en línea o nuestra huella digital.

El posicionamiento SEO

El *Search Engine Optimisation* (SEO) es un conjunto de técnicas que utilizan los creadores de contenidos, organizaciones y empresas para **conseguir que algún contenido aparezca entre los primeros resultados de los motores de búsqueda cuando el usuario realiza determinadas consultas**. Por ejemplo, un concesionario de coches en Barcelona estará interesado en tener su página web en el primer puesto cuando el usuario busque "venta de coches en Barcelona".

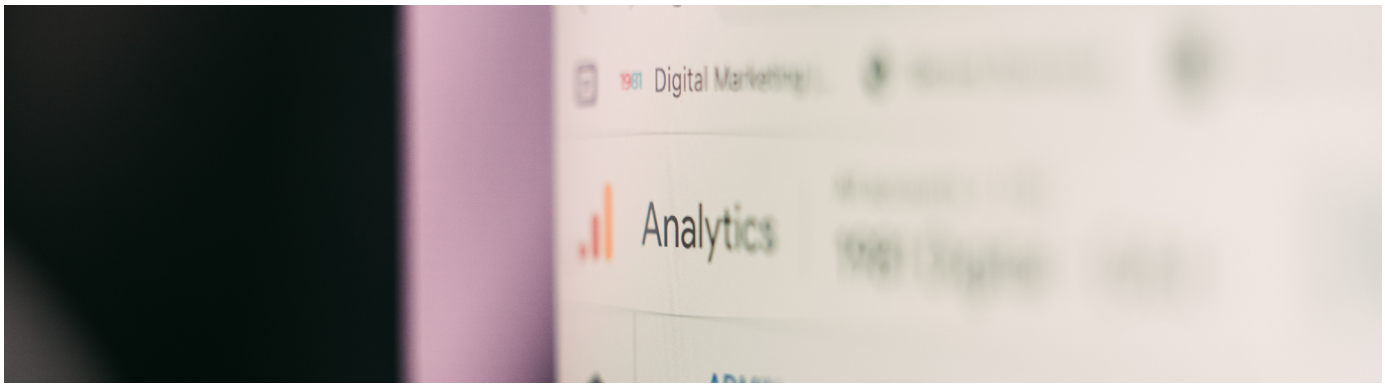
Sin embargo, las técnicas SEO se pueden utilizar para realizar ataques como el **envenenamiento SEO**, que buscan introducir información falsa con algún propósito malicioso. Algunos ejemplos son realizar estafas o minar la reputación de una persona u organización.

Es importante conocer el funcionamiento de los buscadores y del posicionamiento SEO para que juegue a nuestro favor. Nuestra reputación online y la huella digital forman nuestra identidad en Internet.

Por eso, es importante favorecer que se posicione bien la información que nos interese promocionar, y vigilar si aparece alguna información personal cierta o falsa que nos pueda perjudicar. En este sentido, recuerda que las técnicas OSINT permiten a atacantes aprovecharse de los motores de búsqueda y obtener información sobre nosotros. Para evitarlo, podemos eliminar el contenido y/o solicitar a los motores de búsqueda que no lo incluyan en la lista o índice.

OSINT: LA INFORMACIÓN DE FUENTES ABIERTAS

Documento referenciado: ***A4C41A2D01***



DigitAll

Seguridad

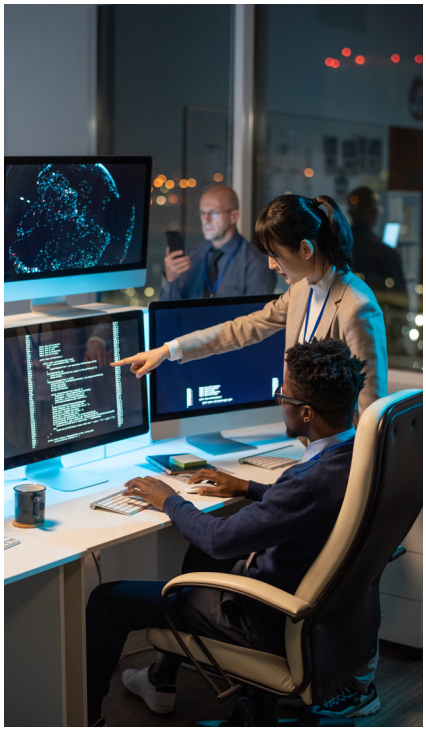
4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel A2 4.2 Protección de los datos personales y la privacidad

Políticas de seguridad. Información privada

Políticas de seguridad. Información privada



Introducción

Las políticas de seguridad en el ámbito de la informática contemplan los procedimientos y normas que permiten garantizar la confidencialidad, integridad y disponibilidad de la información. Estos procedimientos y normativa afectan a cualquier mecanismo o modo de acceso a los sistemas y dispositivos tanto donde se almacena la información como desde donde se pueda tener acceso a la misma.
Las políticas de seguridad afectan tanto a seguridad física, mediante sistemas mecánicos, como a la seguridad lógica, mediante sistemas electrónicos con acceso directo o a través de redes de comunicaciones. Los procedimientos básicos de seguridad se establecen en la Norma internacional ISO 27000 (establecidas por la Organización Internacional de Estándares), y las que se derivan de ella, que aborda todos los aspectos relacionados con la Seguridad de la Información, y se desarrollarán de forma resumida en este documento. Esta norma está desarrollada en cooperación con la Comisión Electrotécnica Internacional (IEC - International Electrotechnical Commission) por lo que se denomina también como ISO/IEC 27000.

Las políticas de seguridad se establecen, entre otras, para mantener la protección de la información privada de los usuarios en el acceso y utilización de los sistemas, de cualquier tipo y a cualquier nivel. Entendiendo, por tanto, la información privada como aquella que corresponde a la privacidad del individuo y que hay que proteger, tanto la correspondiente a los datos privados (nombre y apellidos, domicilio, DNI, teléfono, email, actividades que realiza, amigos, comentarios, etc.) como la relativa a la propia identidad del individuo en los sistemas computadores donde trabaja o que visita.

Políticas de seguridad

Las políticas de seguridad en los sistemas de información deben contemplar tanto la seguridad física, identificando los procedimientos a establecer respecto a restricciones en el acceso a los sistemas, puertas de seguridad con acceso restringido, protección contra incendios, refrigeración, diseño y estructura eficientes de las infraestructuras, etc.; como la seguridad lógica, todos los requisitos para la seguridad de los sistemas de información, en cuanto al acceso, procesamiento y ataques a través de cualquier mecanismo o dispositivo electrónico o informático. Además, entre las directrices que establece la normativa, figuran normas sobre aspectos administrativos que abarcan desde la asignación de responsabilidades hasta la seguridad de los contratos con terceros y el acceso a la información por parte de éstos.

Las normas y estándares son disposiciones que se emplean en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con los requisitos de calidad del cliente y con los objetivos previstos. En este sentido, y en relación con el aspecto particular que nos atañe, la norma ISO 27000 y sus derivadas, normas surgidas a partir de la norma matriz, tratan la seguridad de los sistemas de información en todos sus aspectos.

POLÍTICAS DE SEGURIDAD. ACCESO A SISTEMAS Y DISPOSITIVOS

Generalidades en políticas de seguridad de los sistemas de información (seguridad mecánica, acceso directo, acceso a través de redes).

e.digitall.org.es/A4C42A2V06

Norma ISO 27000. Seguridad de la información

La serie ISO 27000 es la que aglomera todas las normativas en materia de seguridad de la información. Las normas más importantes de esta familia, para establecer una implementación efectiva de la seguridad de la información a través de un Sistema de Gestión de Seguridad de la Información (SGSI) centrado en la prevención de riesgos, son las normas ISO 27001 e ISO 27002. A través de esta normativa,

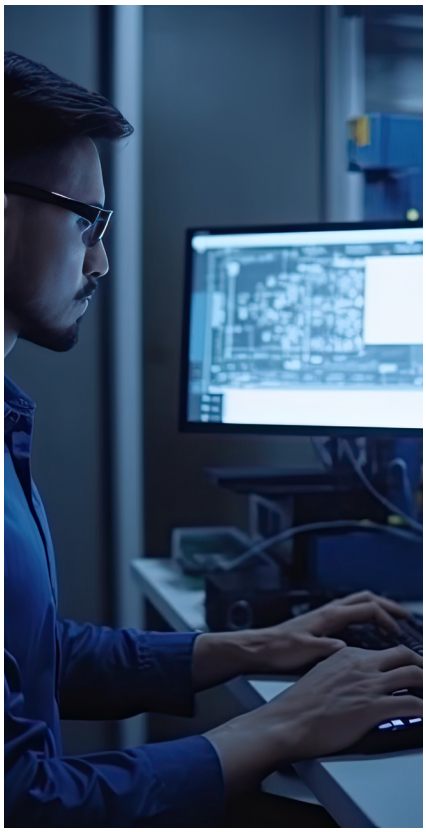
se indican las medidas orientadas a proteger la información, indistintamente del formato de la misma (almacenada electrónicamente, transmitida por correo o por medios electrónicos, impresa en papel, mostrada en video o hablada en conversación), contra cualquier amenaza, de forma que garanticemos en todo momento la Confidencialidad, Integridad y Disponibilidad de la Información.

Esta normativa dispone de un reconocimiento internacional y que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La norma ISO/IEC 27001 ayuda a proteger la empresa, institución o negocio, su reputación y añade valor extra a cualquier transacción; protege los registros personales y la información sensible; reduce los riesgos de ser hackeado o atacado por agentes maliciosos; e, inspira confianza en la organización que la establece.

La norma ISO/IEC 27002:2022, tratada como un código de buenas prácticas ha sido renovada a un conjunto de controles de seguridad que permiten verificar la implantación de la norma 27001.

Indicaciones de las normas 27001 y 27002

A grandes rasgos, esta normativa establece los protocolos a implementar para la seguridad y fiabilidad de los sistemas. En concreto, esta norma identifica los protocolos o procedimientos a establecer tanto respecto a la seguridad física de los sistemas, como respecto a la seguridad lógica, de acceso a través de mecanismos electrónicos o informáticos, procesamiento de la información o ataques a los sistemas de información. Se incluyen aquí los procedimientos a seguir para la protección contra código malicioso, las copias de seguridad, la seguridad en las redes o el intercambio de información y la gestión de servicios con terceros. Recomendaciones sobre la notificación de eventos y puntos débiles de seguridad, y los procedimientos y responsabilidades para la gestión de incidentes y mejoras de seguridad de la información. También se incluyen protocolos relativos a recursos humanos y aspectos administrativos o de organización que abarcan desde la asignación de responsabilidades para el acceso a la información hasta la seguridad de los contratos con terceros y el acceso a la información por parte de éstos.



En concreto, algunas de estas normas se refieren a:

- **Restricciones mecánicas en el acceso a los sistemas.** Es necesario proteger los servidores que mantienen la información para evitar el acceso físico no autorizado a las instalaciones. Los equipos donde se procesa y almacena la información deben estar en áreas seguras y protegidas dentro de un perímetro definido con controles para saber quién accede a ellos.
- **Protección contra incendios y otras catástrofes.** Además de la normativa existente sobre la protección contra incendios de edificios, instalaciones industriales y entornos naturales, existe una normativa específica para la protección contra incendios muy estricta para evitar que la información sufra daños o pueda perderse, especialmente en centros de procesamiento de datos donde se almacena nuestra información. El hardware existente en estos centros emite casi el 100% de la energía utilizada en forma de calor y un aumento excesivo de la temperatura podría dañar los sistemas por lo que la refrigeración es fundamental (se establece una densa red de detectores y un sistema de detección temprana de incendios). En muchos casos, se hace obligatorio disponer de réplicas sincronizadas del sistema de información, en lugares lejanos entre sí, de tal modo que, si un sistema falla o cae, por incendio o incluso por catástrofe natural, el servicio continúe para el usuario final.
- **Diseño y estructura eficientes de las infraestructuras y refrigeración.** Habitualmente, en las distintas organizaciones, instituciones o empresas, los sistemas de información se ubican en centros de procesamiento de datos que mantienen los servicios y sistemas de información activos. Estos centros de proceso de datos deben disponer de unas infraestructuras que les permitan, de una forma organizada y estructurada dar servicio tanto interno como a usuarios externos a la misma.

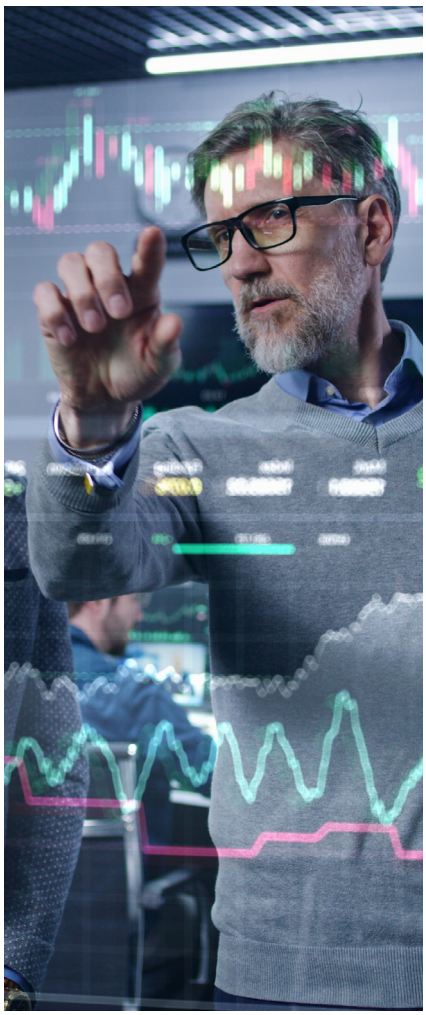
  La normativa establece los requisitos en cuanto al diseño de soportes y canales para las vías de comunicación y conexionado, disponiendo de un sistema de cableado estructurado y a prueba de fallos que permita la ampliación sencilla a elevadas necesidades de

Sistema de identificación para acceso a los sistemas informáticos.

Diseño de un centro de procesamiento de datos, conexionado y racks.

transmisión; sistemas de alimentación eléctrica segura y SAI (sistema de alimentación ininterrumpida), en caso de que falle el suministro eléctrico principal, las baterías del sistema SAI toman el relevo temporalmente; despliegue de racks de servidores en la zona interior del centro de proceso de datos, de este modo se facilita la configuración, enlazado y posible sustitución de elementos en el sistema de información.

- **Recursos humanos.**
  La norma, y sus actualizaciones, tratan aspectos sobre la contratación de personal, los procesos disciplinarios, el cese de relación laboral o el cambio de puesto de trabajo, como la suspensión de las credenciales de acceso. Indica de forma concisa las actuaciones sobre política de control de acceso, gestión de accesos de usuarios, o los accesos a la red, sistema operativo y aplicaciones; incluyendo el manejo de ordenadores portátiles y teletrabajo.
- **Seguridad y controles criptográficos.**
  Los ataques contra la seguridad de la información hacen que la normativa sobre la seguridad de la información sea cada día más actual y permiten asignar la importancia necesaria a los controles sobre la seguridad de los sistemas. Así, se ha de garantizar que la información y las instalaciones de procesamiento de información se encuentran protegidas contra el código malicioso. Para ello, en primer lugar, se debe disponer de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo. Además, los controles criptográficos pretenden la protección de la información en caso de que un intruso pueda tener acceso físico a la información, se establece un sistema de cifrado para mantener la confidencialidad e integridad de la información.



Norma ISO 27002. Controles de verificación seguridad de la información.

La normativa presentada en la ISO 27002 se plantea como un inventario de buenas prácticas sobre controles de seguridad de la información. La norma ofrece una serie de controles que se utilizan como guía de implementación para lograr los objetivos de la seguridad de la información que se establecen en las normas anteriores.

Los parámetros de control que incorpora esta norma afectan, por tanto, a las políticas de seguridad de la información, a la organización de dicha seguridad y los recursos empleados, controles de acceso y seguridad física del entorno, criptografía y seguridad de las comunicaciones y operaciones, y gestión de activos, entre otros.

Normas ISO 27017 y 27018. Sistemas de información en la nube (cloud). Protección de datos personales.

La norma ISO 27017 establece los controles de seguridad de la información para servicios en la nube, entendiendo por tales los que se realizan a través de internet, es decir, aquellos que ofrecen aplicaciones que no están instaladas en el propio ordenador. Para ello el servidor de dichas aplicaciones o programas debe ser accesible desde cualquier dispositivo conectado a internet y debe disponer de garantías de seguridad y capacidad de almacenamiento suficientes para cualquier usuario. Esta norma dispone de una guía de controles adicionales a los establecidos en la ISO 27002, específicos para la nube.

Mientras, la norma ISO 270018 indica las pautas para la protección de información de identificación personal en la nube. Para trabajar con estas aplicaciones es necesario identificarse, siendo muy rigurosos los requisitos de seguridad necesarios a la hora de realizar dicha identificación personal. Esta norma establece los objetivos de control, pautas y controles que implementan la protección de información de identificación personal de acuerdo con la normativa vigente sobre los principios de privacidad existentes para los sistemas de computación en la nube.

Norma ISO 27799. Gestión de la seguridad de la información en sanidad.

Se trata de una norma internacional que indica la mejor manera de proteger los datos personales de salud. Entre otras, establece controles de acceso a datos con indicación de acceso privilegiado; gestión criptográfica de datos confidenciales, con protección de las claves de cifrado; y, registro de la utilización de los datos de usuarios, protegiendo los mismos de alteraciones y accesos no autorizados.

Información privada

En los sistemas de información, especialmente en la navegación por internet y accesos en la nube, es necesario mantener la protección de la información privada de los usuarios, en el acceso y en la utilización de los mismos. La información privada es la que corresponde a la privacidad del individuo, tanto los datos privados como la relativa a la identidad digital del individuo.

POLÍTICA DE PRIVACIDAD EN INTERNET Y EN LAS APLICACIONES

Importancia de la política de privacidad. Contenido de un documento de política de privacidad).

e.digitall.org.es/A4C42A1V07

Contemplando la importancia de la privacidad de la información y de la identidad del individuo, se establecen unas políticas de privacidad que todos los sistemas que visitamos o en los que trabajamos deben satisfacer. Es necesario demandar una aceptación expresa al usuario de que acepta las condiciones establecidas en dichas políticas, especialmente en aquellos sitios donde nuestros datos son solicitados. El documento con la política de privacidad se debe mostrar en el primer nivel de información previo a la recopilación de datos de los usuarios. Además, para cada formulario debe figurar quién es el responsable de los datos, la finalidad de la recogida de los mismos, la legitimación, dónde se van a almacenar y los derechos que tienen los usuarios. En la política de privacidad deben figurar:

- La normativa y legislación de aplicación.
- Cómo se introducen los datos por parte de los usuarios.
- Para qué se van a utilizar los datos.
- Porqué deben introducir los datos y qué ocurrirá si no lo hacen.
- Qué datos son necesarios para comunicarse con la página web o aplicación.
- Compromiso de confidencialidad.
- Compromiso de no compartir los datos con terceros.

- Compromiso de no enviar publicidad sin su consentimiento.
- Información relativa al derecho a cancelación, rectificación, portabilidad o limitación de tratamiento de los datos.

La política de privacidad evita que terceros utilicen nuestros datos personales si así lo indicamos expresamente.

Norma ISO 29100. Protección de datos y privacidad en la nube.

Este estándar internacional proporciona un marco de referencia de alto nivel para la protección de información de identificación personal (PII), con el objetivo de ayudar a las organizaciones a definir los mecanismos de protección relacionados a la privacidad de datos. En concreto, la norma especifica una terminología común en lo relativo a privacidad; define los actores y sus roles en cuanto al procesamiento de información de identificación personal; indica las recomendaciones y consideraciones a contemplar para salvaguardar la privacidad; y, establece los principios de privacidad relativos a las tecnologías de la información y las comunicaciones.

DigitAll

Seguridad

4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel A2 4.3 Protección de la salud y el bienestar

Signos y síntomas asociadas a la salud digital. Casos típicos

Signos y síntomas asociadas a la salud digital. Casos típicos

El presente documento te aproximará al concepto de salud digital y casos típicos, junto con los principales signos y síntomas más típicos asociados a la salud digital desde una perspectiva biopsicosocial, es decir, la implicación a nivel físico, psicológico y social, correspondiéndose con el concepto de salud definido por la Organización Mundial de la Salud.

Casos típicos de salud digital

El concepto salud digital abarca el impacto que tiene el uso y empleo de las Tecnologías de la Información y las Comunicaciones (TIC) sobre la salud y el bienestar de las personas. A continuación, se mostrarán diferentes situaciones típicas en las que podría considerarse que disfrutas de una buena salud digital:

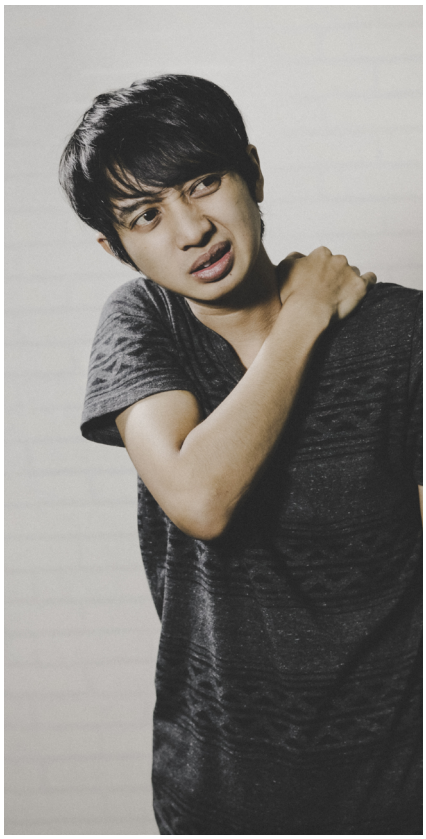
- Respetas los tiempos de dedicación a la tecnología, buscando un equilibrio en el uso de la tecnología e intentando en la medida de lo posible dedicar el mínimo tiempo indispensable a su uso. En caso de hacer uso prolongado, respetas e incluyes pausas intercaladas en el tiempo.
- Eres consciente del tiempo que le dedicas al uso de la tecnología y en ocasiones hasta llegas a cronometrar cuánto tiempo exacto estás dedicando. Periódicamente, revisas las estadísticas de tu teléfono móvil para ver en qué aplicaciones pasas más tiempo.
- Eres consciente de que un uso abusivo y descontrolado de los dispositivos electrónicos puede llevarte a una adicción digital. Sabes que mantenerte informado/a sobre este tipo de adicción te ayudará a llevar un mejor control sobre el uso de la tecnología y a prever sus efectos.
- Mantienes una postura corporal correcta y adecuada cuando haces uso del teléfono móvil, del ordenador, de la Tablet o de cualquier otro dispositivo. Además, no haces movimientos repetitivos y excesivos de las manos cuando utilizas los dispositivos.

- Mantienes una vida social activa aparte de hacer uso de la tecnología, sin estar aislado o aislada del mundo real.

Signos y síntomas asociados a la salud digital a nivel físico

El uso desmedido de los aparatos o dispositivos tecnológicos, como permanecer mucho tiempo delante de una pantalla, puede afectar a nuestra salud física. Deberías tener cuidado si identificas algunos de los siguientes casos relacionados con el uso indebido de la tecnología de los que podrías no ser consciente:

- Sientes que ves borroso o que tienes la vista cansada después de haber estado muchas horas observando la pantalla de un dispositivo tecnológico. Incluso, en ocasiones, puedes llegar a ver doble o a ver las líneas torcidas. Pueden ser signos o síntomas que debes consultar con tu médico de cabecera.
- Tu espalda, hombros, cuello, o mismo tus extremidades se notan agarrotadas (pudiendo llegar a experimentar dolor) tras permanecer mucho tiempo sentado haciendo uso de las nuevas tecnologías. Es posible que a altura de la pantalla o del dispositivo del que haces uso, te esté provocando que fuerces una postura inadecuada. Todos estos signos prolongados en el tiempo pueden dar lugar a lesiones cronificadas.
- Tu cuello y tus manos se presentan entumecidos o con un ligero malestar tras el uso constante de dispositivos móviles, como el teléfono, o por el uso repetitivo de las teclas del ordenador, que mantenido en el tiempo puede derivar en situaciones más graves.
- Si te duele la cabeza más de lo habitual, puede estar relacionado con haber permanecido mucho tiempo observando fijamente una pantalla.
- Si te duele la cabeza más de lo habitual, puede estar relacionado con haber permanecido mucho tiempo observando fijamente una pantalla.



Signos y síntomas asociados a la salud digital a nivel psicológico

La tecnología y en especial diversas redes sociales como Instagram o Facebook pueden provocar problemas a nivel psicológico debido a diversos factores. Por ello, en este punto se van a tratar aspectos que nos pueden ayudar a identificar algunos problemas que nos provoca la tecnología a nivel psicológico.

- El desarrollo de ansiedad provocado por el miedo a perder o no saber dónde se encuentra nuestro dispositivo electrónico.
- Dejar de realizar las actividades de la vida diaria que no conllevan el uso de la tecnología debido a la existencia de dependencia digital.
- Sentir que tus emociones varían en función del uso de la tecnología. Por un lado, el hecho de no tener acceso a los dispositivos tecnológicos te provoca un sentimiento de tristeza e irritabilidad. Por otro, sientes felicidad debido a la compra o al uso de un nuevo dispositivo tecnológico.
- Tienes una sensación de soledad cuando no tienes tu dispositivo cerca. Sientes la necesidad de interactuar con las personas mediante la tecnología, incrementando en este sentido la dependencia de estos dispositivos.
- No eres capaz de hacer un uso controlado de tu dispositivo, redes sociales o diversas aplicaciones durante un período de tiempo. Esto altera tus hábitos y rutinas yprovoca una reducción de tus horas de sueño.
- Disocias tu imagen corporal debido al uso excesivo de filtros de redes sociales como Instagram o Snapchat para manipular tu imagen, o bien, no te identificas con alguna parte de tu cuerpo real provocando alteraciones de autopercepción estéticas.

Signos y síntomas asociados a la salud digital a nivel social

La utilización excesiva o descontrolada de dispositivos tecnológicos puede afectar a la manera en la que nos relacionamos con otras personas. Así, el uso inadecuado de dispositivos tan habituales en nuestro día a día como el móvil, el ordenador o una consola pueden modificar la manera y la frecuencia con la que nos relacionamos con nuestra familia, amigos, compañeros de trabajo y, en general, con el resto de la sociedad.

Hay algunos signos y síntomas que pueden indicarnos que el uso de un determinado dispositivo está afectándonos a nivel social. Su identificación puede ayudarnos a modificar nuestro comportamiento en una etapa inicial, evitando consecuencias mayores en nuestra vida. A continuación, se nombran algunos de los signos y síntomas más comunes:

- Disminuir la frecuencia habitual con la que nos reunimos con nuestra familia o amigos y preferir invertir este tiempo en el uso de los dispositivos tecnológicos.
- Abandonar o reducir actividades deportivas o de ocio que solías hacer en tu día a día.
- Primar las comunicaciones en línea sobre la presencialidad, es decir, optas por hablar por llamada, videollamada, WhatsApp, entre otras opciones, antes que quedar presencialmente con las personas de tu entorno. Por comodidad puede ser una opción óptima, pero prolongado en el tiempo puede aislarnos del mundo real.

ATENCIÓN

El cambio en el modo de relacionarnos no es un suceso inmediato, sino que es un proceso progresivo, condicionado por la persona en particular y por como gestione el uso de los diferentes dispositivos tecnológicos.

NOTA

Tras la pandemia, en ocasiones tendemos a utilizar las ventajas de las TIC, en el sentido de que mantenemos reuniones virtuales, videollamadas, entre otros, mientras que, lo recomendable, en la medida de lo posible, es mantener la presencialidad y el contacto físico con los demás. Los índices de soledad han aumentado en la población, siendo los más afectados los jóvenes y las personas mayores, aumentando a su vez, los suicidios en la población, y por ende, realzando los problemas de salud mental

Saber más

Organización Mundial de la Salud. Recomendaciones sobre intervenciones digitales para fortalecer los sistemas de salud.

e.digitall.org.es/directriz-oms

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel A2 4.4 Protección del medio ambiente

Impactos ambientales de la tecnología

Impactos ambientales de la tecnología

Introducción

Tal y como hemos visto en los diferentes videos de este nivel, especialmente en el video 3 "***El consumo energético de los dispositivos tecnológicos (la huella de tu email)***" y el video 5 "***¿Usamos de manera eficiente y sostenible la tecnología?***", cada vez está más claro que el aumento constante del uso de la tecnología digital hace mella en la salud del planeta. Según se señala en los videos y se detalla en un informe de Greenpeace en 2017, la huella energética del sector de las tecnologías digitales se correspondía aproximadamente con un 7% del consumo total de la electricidad mundial (Greenpeace, 2017). Es una cuestión cada vez más preocupante, teniendo en cuenta el contexto post-pandemia y el escenario actual de transición energética global.

EL CONSUMO ENERGÉTICO DE LOS DISPOSITIVOS TECNOLÓGICOS (LA HUELLA DE TU EMAIL)

e.digitall.org.esA4C44A2V03

¿USAMOS DE MANERA EFICIENTE Y SOSTENIBLE LA TECNOLOGÍA?

e.digitall.org.es/A4C44A2V05

El citado informe pone el foco en el consumo creciente de productos digitales, tanto el hardware como el software, y en los materiales y la energía que se necesitan para su producción y uso.

Otra de las cuestiones más preocupantes es la de los residuos tecnológicos, que están en continuo crecimiento y que se relacionan con el fenómeno de las obsolescencias, ya sean la programada, la percibida o la de especulación

⚠ ATENCIÓN

Por ejemplo, si nos centramos en los teléfonos móviles, los expertos advierten que su ciclo de vida es demasiado corto, ya que hay cálculos que muestran que cada dos años el 40% de las personas usuarias cambia de teléfono, mientras que casi el 60% han cambiado de teléfono más de ocho veces a lo largo de su vida (ONTSI, 2021).

Por tanto, aunque los impactos ambientales asociados a las tecnologías digitales son múltiples, podemos dividirlos en tres grandes bloques: impactos asociados a la extracción de materiales y el proceso de producción de dispositivos; consumo de energía del sector de las tecnologías digitales; y generación de residuos electrónicos. Ya que el consumo de energía de la tecnología digital se analizó en el nivel anterior, en este documento nos centraremos en los otros dos bloques mencionados.

Impactos de la extracción de materiales para la tecnología digital

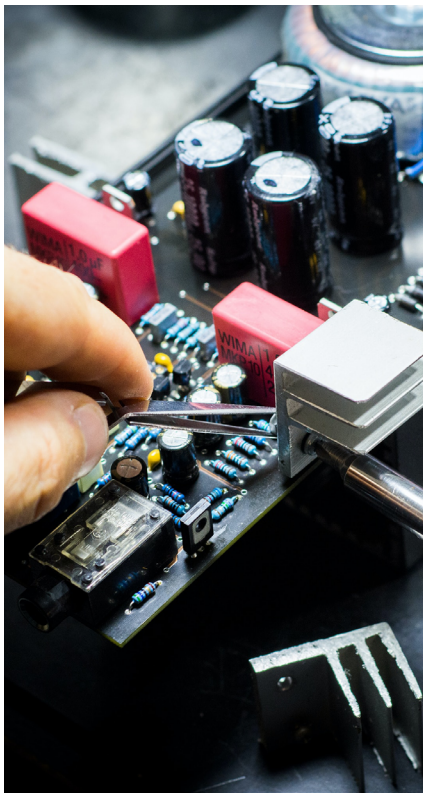
Como ya vimos en el nivel anterior, especialmente en el video 3 "***Procesos de fabricación de recursos tecnológicos***", la mayoría de los elementos necesarios para la fabricación de dispositivos digitales como los teléfonos móviles, pero también los ordenadores personales o las tablets, deben extraerse a través de actividades mineras.

PROCESOS DE FABRICACIÓN DE RECURSOS TECNOLÓGICOS

e.digitall.org.es/A4C44A1V03

Podemos clasificar las actividades mineras dentro de distintos tipos según diferentes criterios. Si atendemos a su volumen de extracción podemos hablar de minería a gran escala, mediana y pequeña minería, e incluso de minería artesanal. También las podemos clasificar según el tipo de extracción, distinguiéndose así entre la minería de interior o subterránea, y la minería a cielo abierto.

Tradicionalmente se ha utilizado de manera mayoritaria la minería en galería o en pequeñas zanjas para extraer carbón y otros materiales, e incluso hoy día se sigue utilizando la minería artesanal para extraer oro y otros minerales en pequeñas cantidades. Pero la minería a cielo abierto se está convirtiendo en la fórmula preferida en la actualidad para la extracción de materiales de todo tipo, y especialmente los necesarios para el desarrollo de la tecnología digital.



Los proyectos extractivos de minería a gran escala a cielo abierto son muy comunes para explotar yacimientos de cobre o litio. Estos son esenciales para la industria digital, pero también para los yacimientos polimetálicos, que contienen diversos minerales en distintas concentraciones.

NOTA

La minería a cielo abierto es comparativamente menos costosa, tanto en infraestructura como en mano de obra, debido a la gran cantidad de superficie que se puede explotar en un mismo proyecto. Pero, precisamente por eso, presenta muchos más impactos ambientales y sociales para el entorno explotado y las comunidades que lo habitan.

Entre los **impactos ambientales de la minería a cielo abierto**, podemos destacar los siguientes:

1. **Contaminación atmosférica.** Se producen impactos en la atmósfera debidos a las voladuras empleadas para la apertura del tajo, y el arranque de material, generando ruido intenso y emitiendo grandes cantidades de polvo al aire.

2. **Impactos sobre el terreno**. Principalmente la deforestación, erosión, modificación del relieve y la morfología local por los movimientos de tierra, además de acumulaciones de material de desecho.

3. **Contaminación del suelo.** En los suelos se alteran diversas propiedades físicas y químicas, e incluso puede suponer la inutilización absoluta de estos para otros usos como la agricultura.

4. **Contaminación de las aguas superficiales y daños a acuíferos.** Puede haber afectaciones en los cursos de los ríos y acuíferos, además de la contaminación por metales pesados y variaciones de pH de las aguas subterráneas.

5. **Impactos sobre la flora y fauna.** Además de las alternaciones directas sobre el terreno que eliminan la flora superficial y desplazan a la fauna, se producen cambios en el hábitat y contaminación de fuentes de agua que pueden afectar a las poblaciones.

6. **Contaminación visual.** El impacto visual generado por la alteración de la morfología del terreno, así como de los enormes huecos o cráteres que se generan durante la explotación minera.

7. **Conflictos entre comunidades y empresas de minería,** debidos al uso indebido de las tierras y amenaza a los modos tradicionales de subsistencia.

A otra escala, las disputas por el control de los recursos naturales para el desarrollo de la tecnología digital generan conflictos de mayor calado e intensidad, definidos por factores geopolíticos y estratégicos que serán analizados en siguientes niveles.

Residuos electrónicos y tecnológicos

Los aparatos eléctricos y electrónicos necesarios para el desarrollo de la tecnología digital suelen ser productos muy complejos que normalmente contienen piezas y componentes de diverso tipo, que van desde el plástico, madera o metal; hasta los componentes de las tarjetas de circuitos impresos o las pantallas de cristal líquido, sin olvidar los cables, pilas, baterías, o cartuchos de impresión (Miteco, 2022).

ATENCIÓN

Según estimaciones del Foro Económico Mundial y la OIT, cada año desde 2018 se generan más de 50 millones de toneladas de residuos de aparatos electrónicos y eléctricos (RAEE), y es una cifra que va en aumento (World Economic Forum, 2019).

De esa cantidad, sólo se recicla formalmente menos de un 20%, mientras que el resto es depositado en vertederos donde estos residuos son abandonados generando distintos tipos de impactos al entorno; o en los que millones de personas trabajan informalmente para recolectar, reciclar y desechar los residuos electrónicos, y gran parte de este trabajo es realizado en condiciones nocivas tanto para la salud como para el ambiente (OIT, 2019).

Gran parte de esos residuos que acaban en vertederos no controlados provienen de países del Norte donde deberían ser sometidos a procesos de reciclaje formales. Sin embargo, terminan en países donde la regulación ambiental es menos estricta, a pesar de que existe un acuerdo internacional, la Convención de Basilea de Naciones Unidas, que regula el tránsito de desechos peligrosos entre países y prohíbe el llamado "*dumping* ecológico".

Pero esta Convención no es efectiva y los residuos tecnológicos siguen inundando países como Ghana, Nigeria o India. El informe Agujeros en la economía circular: Fugas en los residuos electrónicos de Europa, redactado por la BAN (Basel Action Network), denuncia que al menos 10 países europeos, entre los que se encuentra España, exportaron de forma ilegal más de 350.000 toneladas de residuos de RAEE en 2017.

NOTA

El mismo informe además detalla cómo cada persona en Europa genera 17,7 kg de RAEE al año, por los 20 kg. de cada estadounidense, mientras en África la media es de 1,7 kg. por persona.

Como veremos en próximos niveles, el correcto reciclaje de estos residuos, así como el fomento de la reducción del consumo y reutilización de los dispositivos ya en uso, puede llevarnos a paliar la problemática actual. Los materiales valorizables que contienen suponen un recurso que no debe ni puede perderse. Por ejemplo, reciclar de manera correcta y responsable los teléfonos móviles que se desechan cada año, permitiría recuperar grandes cantidades de cobre, de oro o de litio, por poner ejemplos de materiales que requieren de procesos extractivos que generan grandes impactos ambientales y pueden desencadenar conflictos de diverso tipo.

No obstante, estos aparatos o equipos también contienen sustancias peligrosas que, si bien son necesarias para garantizar su funcionalidad, pueden generar contaminación ambiental y daños para la salud humana si, una vez convertidos en residuos, los aparatos no se gestionan y tratan adecuadamente.

Por ejemplo, muchos aparatos o dispositivos pueden contener cadmio, mercurio, plomo, arsénico, fósforo, que son elementos con alta capacidad contaminante. Es por eso por lo que todas las etapas de la gestión de los RAEE, incluyendo recogida, almacenamiento, transporte y tratamiento deben hacerse en unas condiciones seguras y que eviten manipulaciones o roturas que puedan liberar este tipo de sustancias peligrosas al ambiente o exponer a los trabajadores que están en contacto con estos residuos, durante su tratamiento (Miteco, 2019).

El problema principal es que los productos electrónicos no están diseñados en la actualidad para que se puedan actualizar o tener una vida larga, con lo que se agrava la problemática de generación de residuos. Ante esta situación, como ya vimos en el nivel anterior, el informe “La Década Digital de Europa: metas digitales para 2030” de la Comisión Europea propone que los usuarios tengan acceso al conocimiento sobre el impacto medioambiental de sus dispositivos y de las opciones de minimizar los mismos.

Ante esta situación, parece claro que la gestión responsable de RAEE es de vital importancia para alcanzar los Objetivos de Desarrollo Sostenible. Tratarlos correctamente ayudaría a mejorar la salud y el bienestar de las personas y del entorno, además de contribuir a una transformación del modelo de producción y consumo hacia alternativas más sostenibles.

Pero, por supuesto, esta cuestión no es solo responsabilidad de las personas consumidoras de tecnología digital. Es necesario poner el foco en procesos colectivos, y promover la colaboración entre las multinacionales, las pequeñas y medianas empresas (PYME), los emprendedores, las universidades, los sindicatos, la sociedad civil y las asociaciones empresariales con el fin de crear las vías necesarias para alcanzar progresivamente una economía circular de la electrónica donde se limite el despilfarro de recursos y materiales, se reduzca el impacto ambiental y se creen empleos decentes para millones de personas (OIT, 2019).

Saber más

Comisión Europea (2021). *La Década Digital de Europa: metas digitales para 2030*.
e.digitall.org.es/metas-2030

Greenpeace (2017). *Clicking Clean*.
e.digitall.org.es/clicking-ckean

Lillo (2010). *Impactos de la minería en el medio natural*.
e.digitall.org.es/impactos-minería

Miteco (2019). *Aparatos eléctricos y electrónicos*.
e.digitall.org.es/miteco

National Geographic (2022). *Tierras raras*.
e.digitall.org.es/tierras-raras

Observatorio Nacional de Tecnología y Sociedad (ONTSI, 2021). *Tendencias en el uso de dispositivos tecnológicos*.
e.digitall.org.es/tendencias-uso-dispositivos

Organización Internacional del Trabajo (2019). *50 millones de toneladas de residuos electrónicos se desechan cada año*.
e.digitall.org.es/residuos-tecnologicos

Parlamento Europeo (2022). *Derecho a reparar: el PE quiere productos más duraderos y fáciles de reparar*.
e.digitall.org.es/derecho-reparar

World Economic Forum (2019). *A New Circular Vision for Electronics*.
e.digitall.org.es/vision-electronics

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