Co-funded by the
Erasmus+ Programme
of the European Union

Erasmus+

CREW

**Creativity, Resilience,
Empowerment for Work**

IO1 CURSO DE FORMACIÓN EN ALFABETIZACIÓN DIGITAL

Austrian Association of Inclusive Society
M&M profuture training
TATICS HUMAN EVOLUTION
ENOROSCONSULTING Ltd
KOKKALIS FOUNDATION
VERSLI MAMA

Tabla de Contenidos

Co-funded by the Erasmus+ Programme of the European Union

Table of Contents

Co-funded by the Erasmus+ Programme of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Objetivos y finalidad del IO1

Internet se convirtió en una mercancía en el siglo XXI, casi lo mismo que el aceite, los cereales, o el azúcar. Es el ingrediente principal para que existan servicios en muchos sectores, como finanzas, salud, marketing, entretenimiento, educación. Internet es una especie de materia prima o un marco en sí mismo, que se emplea como material de construcción para una variedad de otros servicios y ecosistemas, que evolucionan a su alrededor.

A medida que las herramientas digitales y en línea evolucionan rápidamente, se fusionan y producen una gama aún más amplia de servicios y productos innovadores, mientras que los dispositivos utilizados en las actividades personales y públicas cotidianas se vuelven más rápidos, ampliamente adoptados y conectados; las habilidades de alfabetización digital se vuelven esenciales en la construcción de carreras y competencia exitosa en un mercado laboral. El desarrollo constante de habilidades, la participación significativa y decidida en el mundo digital, la capacidad de consumir, evaluar y crear la información a través de Internet, al mismo tiempo que te mantienes segura/o y resistente frente a la información falsa y de baja calidad ... todo ello no es de menor importancia.

Las personas altamente capacitadas y versátiles, capaces de adaptarse rápidamente a las condiciones cambiantes, especialmente en un mundo digitalizado, son las más valoradas por los empleados. Poder usar un teclado y un ratón, poseer un cierto grado de conocimiento ya no se considera una ventaja, se requiere que las personas tengan una gama muy amplia de habilidades digitales básicas y especializadas, así como la capacidad de adquirir habilidades nuevas a un ritmo muy rápido.

Por lo tanto, el objetivo de este curso es ayudar a ampliar las habilidades básicas que ya poseen las personas que mejoran sus habilidades generales de alfabetización digital y empoderarlas para un mayor desarrollo, al tiempo que ayudar a las personas con menos habilidades técnicas a combatir su ansiedad en la mejora de las habilidades digitales. Este curso está dirigido a estudiantes adultos menos competentes, ayudándolos a involucrarse más en la sociedad y el mercado laboral, así como a educadoras y educadores, organizaciones, e instituciones que organizan cursos de aprendizaje, involucrados en la enseñanza y formación de alfabetización digital y temas relacionados, que pueden beneficiarse utilizando nuestros cursos con fines educativos.

1 MODULO

Co-funded by the Erasmus+ Programme of the European Union

CREW
Creativity, Resilience and Empowerment for Work

TEORÍA Y METODOLOGÍA DE LA ALFABETIZACIÓN DIGITAL

1.1 INFORMATION ACQUISITION

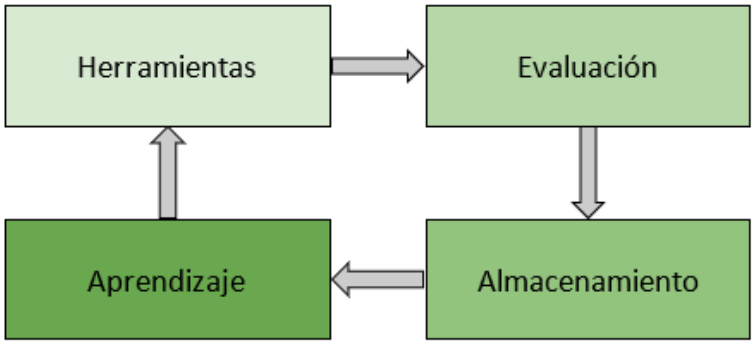
Aunque el término de "adquisición de información" no es algo nuevo, crea nuevas percepciones en un mundo tan vastamente conectado a principios de la tercera década del siglo XXI. La Asociación Estadounidense de Bibliotecas (ALA, 1989) define la alfabetización informacional como la capacidad de determinar qué información se necesita, comprender cómo se prepara la información, encontrar las mejores fuentes de información para una necesidad determinada, identificar esas fuentes, evaluar las fuentes analíticamente y compartir esa información.

Más de tres décadas de explicación de la alfabetización informacional pasan una prueba del tiempo para definir bastante bien lo que puede ser la adquisición de información desde una perspectiva de alfabetización digital. Sin embargo, el flujo de información de fácil acceso, que cambia rápidamente y a menudo involuntariamente en un mundo digitalizado hace que la adquisición de información sea muy diferente debido a la magnitud enormemente diferente de la información disponible en Internet.

Nos atenemos a lo básico y hacemos hincapié en los siguientes pilares principales de lo que es la adquisición de información en el ámbito de la alfabetización digital:

1. Es poder utilizar correctamente las herramientas en línea para adquirir información.
2. Evaluar críticamente la información y filtrar la que provenga de fuentes de información irrelevantes de baja calidad.
3. Ser capaz de almacenar y gestionar de forma segura la información adquirida.
4. Adquirir los nuevos conocimientos y ser capaz de desarrollar continuamente nuevas habilidades y seguir aprendiendo sin parar para adquirir más información y de mejor calidad.

Figura 1. Una ilustración del ciclo continuo de adquisición de información y mejora de la calidad.



Las herramientas básicas para adquirir la información digitalizada suelen ser bastante conocidas y populares:

- Google y otros motores de búsqueda.
- Wikipedia.
- Youtube y otros servicios de video.
- Redes sociales: Facebook, Twitter, Linkedin.
- Portales de noticias, foros, directorios de Internet.

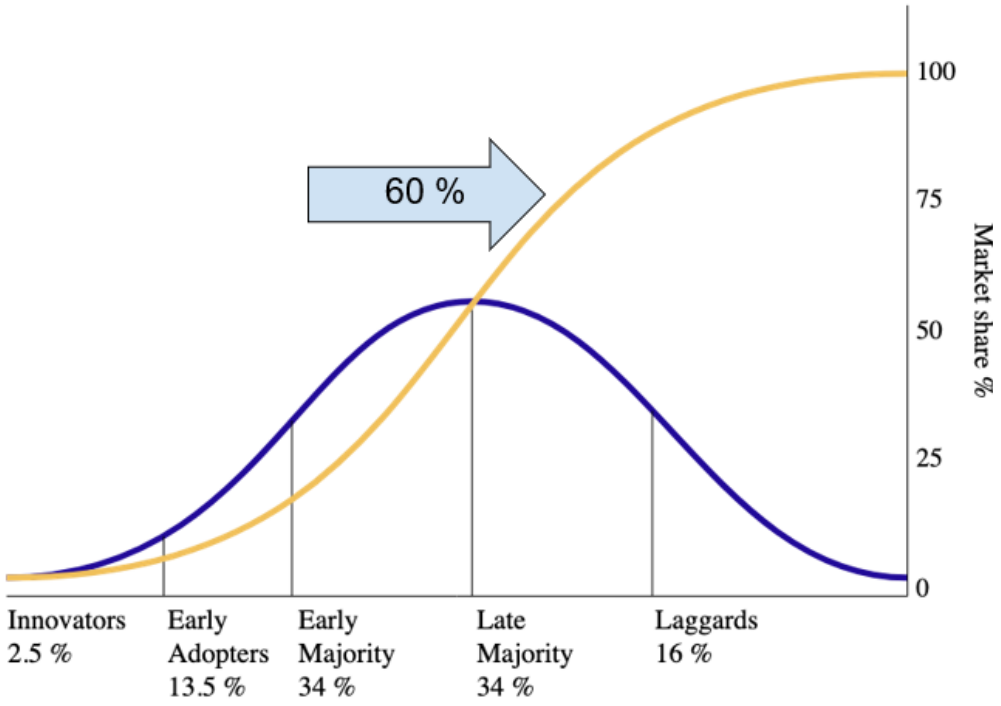
El almacenamiento de información es un tema bastante técnico, por lo cual, cubriremos temas como: seguridad, confiabilidad y mejores prácticas o temas relacionados para el almacenamiento de información en capítulos posteriores.

La parte de evaluación es crucial para desarrollar las habilidades digitales necesarias; por lo tanto, profundizaremos en este tema en el próximo capítulo.

¿Cuál es el grado de adopción real de Internet en este momento?

Según el modelo de difusión de innovaciones de Everett Rogers, que se puede utilizar para describir bien la evolución y adopción de cualquier tecnología, todavía nos queda un largo camino para que Internet se adopte en todo el mundo.

Figura 2. Adopción de Internet basada en una penetración de Internet del[1] 60% en 2021 [fuente: Statista.com]



A pesar de la adopción desigual de Internet en todo el mundo, todavía podemos considerar que las herramientas digitales y la conexión a Internet son el principal factor positivo para difundir las ideas, educar a las personas, luchar contra la pobreza y el desempleo.

Co-funded by the
Erasmus+ Programme
of the European Union

1.2 EVALUACIÓN DE LA INFORMACIÓN

¿Por qué necesitamos evaluar la información?

Una vez que haya encontrado información que coincida con el tema y los requisitos de su investigación, debe analizar o evaluar estas fuentes de información. La evaluación de la información anima a pensar críticamente sobre la confiabilidad, validez, precisión, autoridad, oportunidad, punto de vista, o sesgo de las fuentes de información.

El hecho de que un libro, artículo, o sitio web coincida con sus criterios de búsqueda y, por lo tanto, parezca, literalmente, relevante para su investigación; no significa que sea necesariamente una fuente de información confiable. Es importante recordar que las fuentes de información que componen las colecciones impresas y electrónicas de la Biblioteca ya han sido evaluadas para su inclusión entre los recursos de la Biblioteca. Sin embargo, esto no significa necesariamente que estas fuentes sean relevantes para su investigación.

Esto no se aplica necesariamente a las fuentes de información en la Web para el público en general. Muchos de nosotros con cuentas de Internet / Web somos posibles editores de sitios web; la mayor parte de este contenido se publica sin revisión editorial. Piénsalo. Hay muchos recursos disponibles para ayudar en la evaluación de las páginas web.

La forma más sencilla de evaluar la información es hacerse las preguntas adecuadas. ¿Qué criterios debería utilizar para juzgar las fuentes de información?

1. Inicialmente, observar el autor, el título, el editor y la fecha de publicación. Esta información se puede encontrar en la cita bibliográfica y se puede determinar incluso antes de tener el artículo físico en la mano.
2. A continuación, observar el contenido, p. Ej. audiencia destinataria, objetividad de la redacción, cobertura, estilo de redacción y, si están disponibles, reseñas de evaluación.

Por ejemplo, se deben hacer las siguientes preguntas para evaluar paso a paso la calidad de la información:

¿Quién es la autora / el autor (puede ser un individuo u organización) y / o editor?

1. ¿Cuáles son las credenciales y la afiliación o patrocinio de cualquier persona u organización nombrada?
2. ¿Qué tan objetivos, confiables y autorizados son?
3. ¿Han escrito otros artículos o libros?
4. ¿Se enumeran autores y autoras con la información de contacto (dirección postal, correo electrónico)?
5. ¿Ha publicado la editora o editor otros trabajos?
6. ¿Se especializan en publicar ciertos temas o campos?
7. ¿Es la editora una erudita (prensa universitaria, asociaciones académicas)? ¿Comercial? ¿Agencia del gobierno? ¿Prensa de "autobombo"?

¿Qué se puede decir sobre el contenido, contexto, estilo, estructura, integridad y precisión de la información proporcionada por la fuente?

1. ¿Se ofrecen conclusiones? Si es así, ¿en base a qué evidencia y respaldado por qué documentación primaria y secundaria?
2. ¿Qué implica el contenido?
3. ¿Están representadas las diversas perspectivas?
4. ¿El contenido es relevante para sus necesidades de información?
5.

¿Cuándo se publicó la información?

1. La fecha de publicación generalmente se encuentra en la página del título o en el reverso de la página del título (fecha de copyright).
2. ¿La información proporcionada por la fuente está en su forma original o ha sido revisada para reflejar cambios en el conocimiento?
3. ¿Es esta información oportuna y se actualiza periódicamente?

¿Dónde más se puede encontrar la información proporcionada por la fuente?

1. 1. ¿Es esta información auténtica?
2. 2. ¿Esta información es única o se ha copiado?
3. 3. ¿Por qué se publicó la información proporcionada por la fuente?

¿Cuál es el contexto en torno a esta información?

1. . ¿Cuáles son las perspectivas, opiniones, suposiciones y sesgos de quien sea responsable de esta información?
2. ¿Quién es el público objetivo?
3. ¿Se vende algo?

Una introducción adecuada a la evaluación de la información es crucial para lograr los resultados deseables para la mejora de las habilidades de alfabetización digital, especialmente mientras se proporciona a las y los alumnos las direcciones y pautas para su superación personal y el autoaprendizaje mediante la práctica.

1.3. LA CREACIÓN DE INFORMACIÓN DIGITAL COMO PROCESO DE APRENDIZAJE

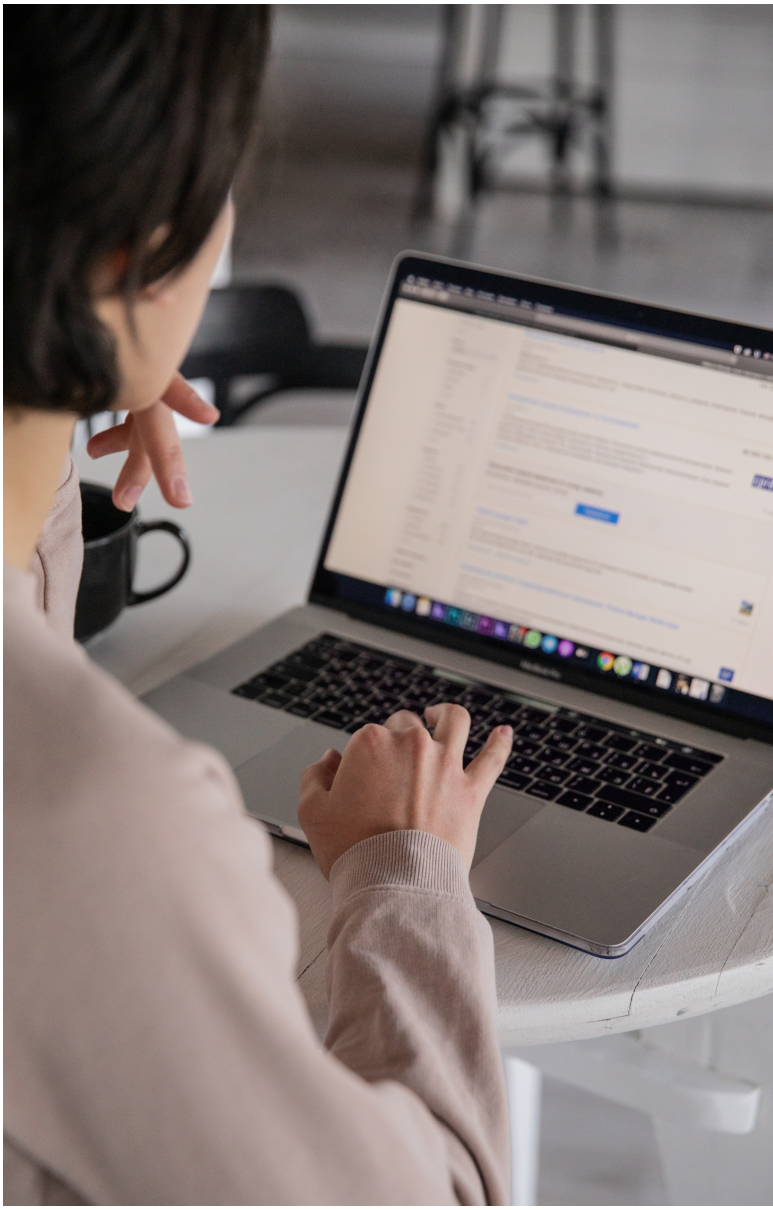
La información en cualquier formato se produce para transmitir un mensaje y se comparte a través de un método de entrega y distribución seleccionado. Los procesos iterativos de investigar, crear, revisar y compartir la información varían; por lo tanto, todo el proceso en sí es una gran parte del proceso de aprendizaje constante mientras la información se crea, consume y distribuye.

El aprendizaje práctico como enfoque de la educación es muy adecuado para la mejora de las habilidades de alfabetización digital, porque existe una gama muy amplia de herramientas y software disponibles, listos para ser utilizados por estudiantes de cualquier nivel de habilidad con el fin de lograr objetivos específicos, entregables y propósitos de aprendizaje. Las herramientas e instrumentos existentes en el mundo digital están disponibles en cualquier país, son compatibles con la mayoría de idiomas y son muy baratas o totalmente gratuitas. Esto hace que la adquisición de habilidades digitales esté disponible y sea relativamente fácil para cualquiera. Para afinar el proceso educativo, las y los educadores deben elegir el medio adecuado para impartir su formación.

Tomando la construcción de sitios web como un ejemplo de enfoque práctico, para poder construir un sitio web, una persona debe tener conocimientos básicos y habilidades de uso de la computadora, lo que la ayudaría a encontrar las instrucciones y requisitos necesarios para la construcción del sitio web. Esas habilidades básicas pueden adquirirse antes durante la educación formal, sin embargo, se adquirirán conocimientos más profundos después de completar las tareas prácticas.

La construcción de sitios web es una tarea compleja, que requiere mejorar las habilidades en la búsqueda y evaluación de información, almacenamiento, también creación y distribución, por lo que enfatizamos que este tipo de ejercicio es una forma perfectamente adecuada para la mejora de las habilidades digitales. Si es necesario, los ejercicios de creación de sitios web pueden incluir marketing y comunicación, redacción de artículos de calidad complementados con adiciones interactivas y de medios enriquecidos, investigación sobre el comportamiento y la experiencia de las y los usuarios de Internet, la seguridad y la privacidad y cómo el diseño, la estructura o las funcionalidades de un sitio web pueden ayudar a lograr los mejores resultados.

Las y los estudiantes pueden optar por trabajar en la creación de blogs personales o en la creación de un sitio web de comercio electrónico simple, lo que los obliga a adquirir las habilidades necesarias en áreas como finanzas, creación de identidad digital, precauciones contra delitos cibernéticos, uso de firma electrónica y servicios públicos electrónicos. También deberían empezar a verse a sí mismas como parte de un proceso interminable tanto en la creación de información como en el consumo de información al mismo tiempo, lo que amplía su percepción de la alfabetización digital en su conjunto.



Nuestra recomendación metodológica para la educación en alfabetización digital es utilizar un enfoque práctico de creación de sitios web y ajustar ejercicios particulares en función de las habilidades, motivaciones y expectativas reales de las y los alumnos.

2 MODULO

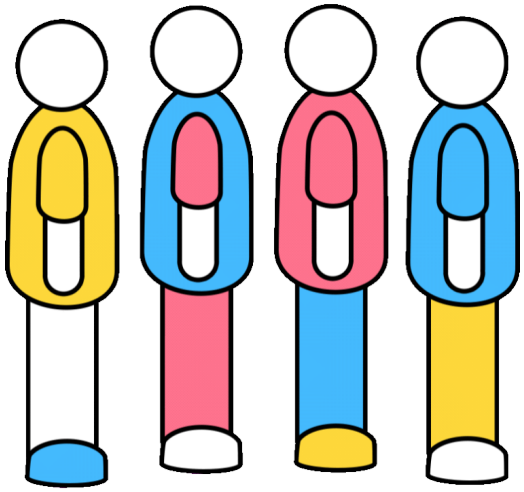
Co-funded by the Erasmus+ Programme of the European Union

CREW
Creativity, Resilience and Empowerment for Work

DESARROLLO DE HABILIDADES PRINCIPALES

2.1. LA ALFABETIZACIÓN DIGITAL COMO ENFOQUE CULTURAL

Estamos viendo un período de desarrollo tecnológico sin precedentes y ampliamente disruptivo. En el corto tiempo transcurrido desde que se creó Internet, mucho ha cambiado, incluido el diseño de las interfaces de las computadoras, la velocidad de procesamiento y la portabilidad de los dispositivos, la accesibilidad de la información y el conocimiento, nuestros métodos de comunicación, el mantenimiento de nuestras relaciones, el comercio, la protección de la privacidad personal, procesos creativos, publicación de contenidos y el surgimiento de nuevas tribus digitales y clanes virtuales (Wheeler, 2009).



Varios artículos publicados recientemente han explorado la noción de "alfabetización digital" y, como era de esperar, hay numerosos puntos de vista. Anderson (2010), por ejemplo, describe las alfabetizaciones digitales como la capacidad de explotar el potencial de las tecnologías informáticas. Las alfabetizaciones, en todas sus formas, son a la vez culturales, sociales y personales (Kress, 2009) y nos permiten interactuar plenamente en culturas específicas. Algunos advierten que sin un nivel adecuado de alfabetización, los medios digitales tienen la capacidad de perjudicar a algunos (van Dijk, 2005), mientras que otros advierten sobre la naturaleza de la web para socavar el conocimiento y la competencia (Carr, 2008; Keen, 2007). Sin embargo, la gran mayoría de los comentaristas elogian el potencial de la web social para liberar la educación y democratizar el aprendizaje, con la salvedad de que se practican las alfabetizaciones digitales. El grupo de trabajo de alfabetización digital de la American Library Association ofrece esta definición: "La alfabetización digital es la capacidad de utilizar las tecnologías de la información y la comunicación para encontrar, evaluar, crear y comunicar información, lo que requiere habilidades tanto cognitivas como técnicas".

El término "alfabetización digital" se ha vuelto tan popular y generalizado en los últimos 10 años que casi se da por sentado. Con diversos grados de complejidad, la expresión “alfabetización digital” ahora se usa para describir nuestros compromisos con las tecnologías digitales, ya que median muchas (si no la mayoría) de nuestras interacciones sociales.

Con esta definición de alfabetización digital de la Asociación Estadounidense de Bibliotecas como guía, es importante entender que incluso las personas nativas digitales que saben cómo enviar un texto y publicar en las redes sociales, no se consideran "alfabetizadas digitalmente" de ninguna manera. Es importante tener en cuenta que el simple hecho de leer en línea o suscribirse a un servicio de libros electrónicos no hace que un/a estudiante tenga conocimientos digitales.

La alfabetización digital en la educación abarca mucho más. Por ejemplo, se deben de tener habilidades específicas al leer texto en línea que puede contener recursos incrustados como hipervínculos, clips de audio, gráficos o tablas que requieren que se hagan elecciones.

La alfabetización digital significa tener las habilidades que se necesita para vivir, aprender y trabajar en una sociedad donde la comunicación y el acceso a la información están aumentando a través de tecnologías digitales como Internet, las redes sociales y los dispositivos móviles.

Desarrollar su pensamiento crítico es esencial cuando una persona se enfrenta a tanta información en diferentes formatos: buscar, cribar, evaluar, aplicar y producir información requieren que se piense críticamente.

La comunicación también es un aspecto clave de la alfabetización digital. Al comunicarse en entornos virtuales, la capacidad de expresar claramente sus ideas, hacer preguntas relevantes, mantener el respeto y generar confianza es tan importante como cuando uno se comunica en persona.

También se necesitan habilidades prácticas en el uso de la tecnología para acceder, administrar, manipular y crear información de una manera ética y sostenible. Es un proceso de aprendizaje continúo debido a las nuevas aplicaciones y actualizaciones constantes, ¡y necesitas mantener tu vida digital actualizada!

La alfabetización digital es realmente importante ahora y será realmente importante en tu futuro profesional. En tu lugar de trabajo, debes interactuar con personas en entornos digitales, utilizar la información de manera adecuada y crear nuevas ideas y productos de forma colaborativa. Por encima de todo, debes mantener tu identidad digital y tu bienestar a medida que el panorama digital continúa cambiando a un ritmo acelerado.

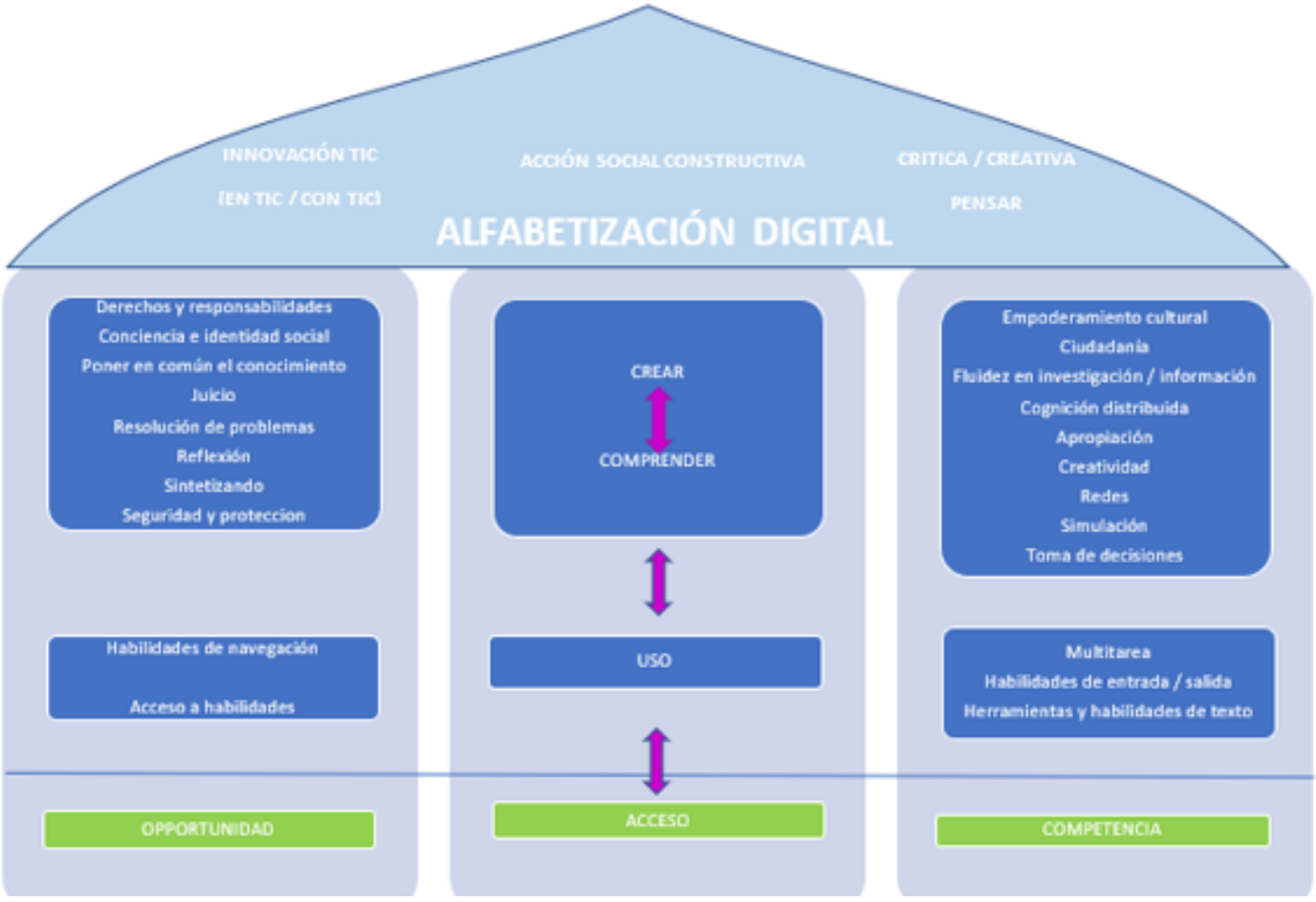
Como se mencionó, las habilidades digitales se desarrollan a lo largo de un continuo y se actualizan constantemente de acuerdo con los cambios en la tecnología. Los marcos de competencias digitales desempeñan un papel fundamental en la captura de la gama de competencias, así como de estos cambios, lo que permite a las personas responsables de la formulación de políticas y a las proveedoras de competencias digitales garantizar que sus programas y planes de estudios de formación sigan siendo relevantes y actualizados. Muchas organizaciones y agencias internacionales han desarrollado marcos de habilidades digitales. Destacamos el trabajo de la Comisión Europea: el Marco de Competencia Digital para Ciudadanos (o “DigComp”) que proporciona un lenguaje común sobre cómo identificar y describir las áreas clave de la competencia digital y, por lo tanto, ofrece una referencia común a nivel europeo.

A nivel mundial, la Sociedad Internacional para la Tecnología en la Educación (ISTE) enmarca sus puntos de referencia para la alfabetización digital en torno a seis estándares: creatividad e innovación, comunicación y colaboración, fluidez en la investigación y la información, pensamiento crítico, resolución de problemas y toma de decisiones, ciudadanía Digital y operaciones y conceptos tecnológicos.

Este modelo muestra los muchos elementos interconectados que caen bajo el paraguas de la alfabetización digital. Existe una progresión lógica desde las habilidades más fundamentales hacia los niveles más altos y más transformadores, pero hacerlo no es necesariamente un proceso secuencial: mucho depende de las necesidades de las y los usuarios individuales.

Figura 3. Modelo de alfabetización digital

Illustración tomada de Report of the Digital Britain Media Literacy Working Group (March 2009), DigEuLit – a European Framework for Digital Literacy (2005), and Jenkins et al., (2006) Confronting the Challenges of Participatory Culture: Media Education for the 21st Century.



¿Qué elementos te hacen una persona digitalmente alfabeta?

La alfabetización digital va más allá de las habilidades funcionales de TIC para describir un conjunto más rico de comportamientos, prácticas e identidades digitales.

Figura 4. El modelo Jisc

El modelo Jisc[que se muestra a continuación ilustra la idea de que el dominio de las TIC (tecnologías de la información y la comunicación) es un elemento central de nuestra alfabetización digital, mientras que otras habilidades se superponen y se basan en esta capacidad, y por encima de todo está nuestra identidad digital y nuestro bienestar.

isc. (2016). Digital capabilities: The six elements.
Extraido de https://www.jisc.ac.uk/rd/projects/building-digital-capability

1. Dominio de las TIC (habilidades funcionales).
2. Alfabetización en información, datos y medios (uso crítico).
3. Creación digital, resolución de problemas e innovación (producción creativa).
4. Comunicación, colaboración y participación digitales (participación).
5. Aprendizaje y desarrollo digitales (desarrollo).
6. Identidad digital y bienestar (autorrealización).

2.2. REDUCIR LA ANSIEDAD MIENTRAS DESARROLLAMOS Y ENSEÑAMOS HABILIDADES DIGITALES

Para algunas personas adultas, incluidas las jóvenes adultas, su uso incompleto de Internet está relacionado con un bajo nivel de alfabetización y aritmética y con la falta de confianza y motivación para aprender nuevas habilidades y aplicarlas en sus vidas. Las habilidades digitales son clave para la inclusión en la sociedad. Adquirir estas habilidades, junto con la confianza y la motivación para usarlas en la vida real, puede ayudar a las personas a tener una vida mejor. Las personas pueden sentirse avergonzadas por no saber cómo usar Internet y la ansiedad causada por el ordenador es una consecuencia de ello. La ansiedad por los ordenadores es un fenómeno que ocurre ampliamente desde su introducción en nuestra vida, lo que demuestra que los usuarios que saben poco acerca de los ordenadores tienen más probabilidades de sentir ansiedad por ellos, pero la ansiedad digital puede reducirse aumentando la capacidad para resolver problemas tecnológicos y digitales. La ansiedad en sí misma se define como un trastorno de salud mental que abarca miedos y preocupaciones "excesivos". Esta discapacidad, a menudo “silenciosa”, puede manifestarse de muchas formas, y la vida diaria no es una excepción.

Los signos comunes de que se puede estar experimentando estrés digital cuando no se está capacitado al comenzar a usar herramientas digitales incluyen los siguientes:

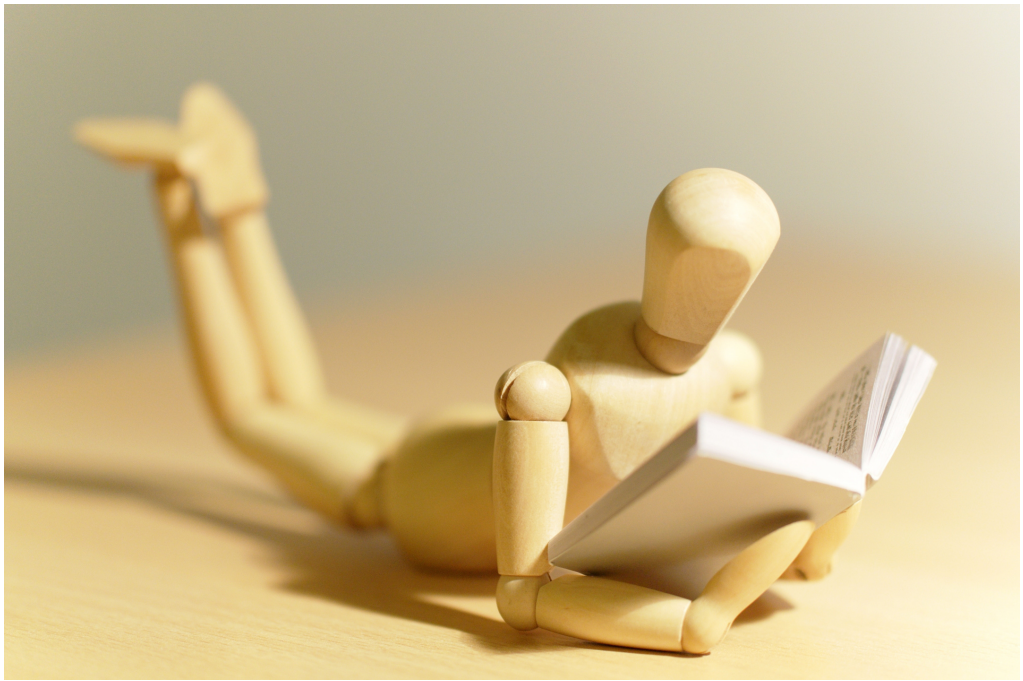
- Ansiedad o ataques de pánico.
- Aislamiento o retraimiento de actividades sociales.
- Mayor secretismo.
-Ira.
- Depresión.
-Bajas calificaciones.
- Rebelión.
- Dolores de estómago, dolores de cabeza u otros dolores generales del cuerpo que no se explican por una afección médica.

El acceso a la tecnología y las habilidades digitales es fundamental para acceder a áreas clave en la escuela y la vida social, pero ¿está la tecnología contribuyendo al aparente crecimiento de los problemas de ansiedad que se observan en el mundo moderno? ¿Qué tienen la tecnología digital y las nuevas tecnologías que nos están causando ansiedad y estresando a tantas personas? La ansiedad causada por las TIC se caracteriza por sentimientos de preocupación y aprensión junto con la tensión física relacionada con el uso actual o futuro de los ordenadores, por ejemplo; el miedo a cometer errores o perder datos. También puede provocar tecnoestrés. En su forma más extrema, la ansiedad causada por las TIC puede convertirse en "tecnofobia", lo que implica resistencia al uso de la tecnología y puede provocar una falta de información sobre tecnología y alfabetización digital.

¿Cómo se puede hacer frente a esta ansiedad informática y digital?

Preparación

Este es el lema de los Boy Scouts por una razón: es un consejo inteligente. Cuando se trata de ordenadores y las habilidades digitales necesarias, muchos de nosotros nos sentimos un poco intimidados, solo queremos aprender los conceptos básicos y lidiar con las cosas técnicas lo menos posible. Si bien esto es comprensible, puede ahorrarse estrés aprendiendo los aspectos básicos de cómo funcionan sus sistemas leyendo los manuales y tal vez uno o dos libros sobre ordenadores, y practicando, practicando y practicando.



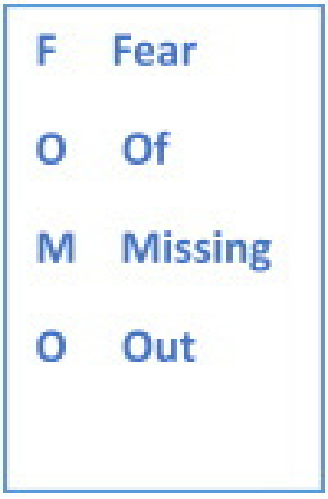
Hacer copias de seguridad a menudo

Si aún no tienes esto incorporado en tu rutina, es vital que comiences a hacer copias de seguridad de tus archivos con regularidad (te recomendamos hacerlo una vez por semana), de modo que, si te encuentras con dificultades importantes, no pierdas gran parte de tu valioso tiempo y trabajo.

FOMO

Pero, ¿qué pasa si no tienes miedo de usar el ordenador, pero necesitas revisar constantemente el correo electrónico y estar activa en las redes sociales y tienes la sensación de que tienes que estar constantemente conectada e interactuando y si no lo estás, estás perdida y sufrirás las consecuencias de ello? ¿Puede ser negativo?

Figura 5. La explicación del miedo a perderse algo



Todos tenemos una relación de amor-odio con el correo electrónico y las redes sociales y a veces, nos quejamos de que recibimos demasiado correo electrónico, pero a la inversa, lo revisamos con demasiada frecuencia por “miedo a perdernos algo” (FOMO). El uso del correo electrónico a menudo se ve agravado por tener múltiples cuentas de correo para cubrir diferentes áreas de tu vida; es decir: negocios, personales, e intereses como clubes deportivos / grupos religiosos, etc. Además, se tiene la necesidad de revisar las redes sociales una y otra vez para no sentirse fuera del circuito. Cuando lo tiene controlado sabes que lo estás haciendo bien, con la finalidad de no sentirte excluido.

¿Cómo manejar tu miedo a perderse algo? “FOMO” es una tortura psicológica inventada por una misma y es un producto de la peor imaginación de nuestra mente.

Aquí hay 4 consejos para mantener su salud mental durante su sensación de FOMO

1. Notificaciones

Se amable contigo misma y apaga todos los anuncios por correo electrónico en tu ordenador portátil y teléfono móvil; no deseas un intermedio continuo. Esto incluye desactivar el molesto número de conteo de correos electrónicos que aparece a menudo en la imagen de tu perfil de correo electrónico. Ver 100 correos electrónicos no leídos solo aumentará tus niveles de estrés y te llevará a echar un vistazo a tus correos electrónicos.

No es necesario que veas todos los correos electrónicos, incluso los de las partes interesadas clave; el correo electrónico no es un mensaje directo y te impide realizar un trabajo en profundidad.

Mientras esté allí, desactiva todas las notificaciones no esenciales, incluidas Facebook, Twitter y WhatsApp; desactivar las notificaciones puede ser increíblemente liberador. Además, puedes mover sus aplicaciones de correo electrónico a la segunda página de su teléfono inteligente.

2. Distancia saludable

.No digas "sí" a los eventos por miedo a perdértelos, y mantén una distancia saludable de las versiones de tus vidas que otras personas han visto. Durante una semana, cuenta la cantidad de tiempo que pasas revisando correos electrónicos, mensajes de texto o redes sociales a diario. ¿Qué otras cosas podrías estar haciendo con ese tiempo? El miedo a perderse algo es real y FOMO puede ser peligroso, pero si sabes qué buscar, FOMO es reversible. Piensa en “JOMO”[1], (“alegría de perderse algo”).
[1] Nota del t. JOMO = Joy of Missing Out

3. Establecer prioridades

Recuerda que la cantidad de información que eres capaz de manejar es limitada y céntrate en las personas y los datos que realmente te interesan o pueden ser de utilidad.

4. Actúa

Si estás conectado/a permanentemente por miedo a lo que te puedas perder, lo que realmente te estás perdiendo es la vida. En lugar de mirar lo que hacen los demás y pasar tu tiempo libre fotografiando, grabando y publicando tus actividades, disfruta de buenas experiencias y compártelas con quienes te importan.

2.3. CONCEPTO DE CONSUMIDOR INTELIGENTE

El rápido desarrollo de tecnología fácil de usar y el acceso inmediato a la información ha hecho que las y los clientes de hoy sean inteligentes y conscientes. Con cada vez más posibilidades disponibles con un toque de la pantalla táctil, el comportamiento y las preferencias del consumidor están en constante cambio.

Cuando escuchas la palabra “consumir”, ¿a dónde va tu mente? Probablemente empiece a pensar en la comida y en lo que come. Para ser justos, no está demasiado lejos. El consumo es más de lo que se lleva a la boca. Es lo que haces con tu dinero y tu tiempo. Tu dinero compra comida, techo, ropa, juegos, automóvil, conocimientos, pensiones, etc. Tu tiempo se dedica a aprender una nueva habilidad o consumir las últimas noticias del día. Lograr este equilibrio entre crear y consumir puede ser complicado. Si se obtiene el equilibrio correcto, se mejora la capacidad financiera.

Las nuevas tecnologías están cambiando la forma en que actúan los consumidores. Gracias a la tecnología, las y los consumidores están cada vez más informados, empoderados y exigentes. Armados con el conocimiento recopilado de una multitud de fuentes, están usando su dinero en los bienes y servicios que valoran. Quieren interactuar de una manera que sea relevante y oportuna: relevante para lo que sea que estén comprando, independientemente de dónde, cuándo y cómo lo estén comprando; y oportuno para satisfacer sus necesidades. En resumen, los consumidores de hoy se están volviendo más inteligentes. Pero, ¿cómo puedes ser una consumidora más inteligente?

Los consumidores de todas las edades y en todas partes del mundo están acudiendo a las redes sociales. Comprender las redes sociales ya no es opcional; es un imperativo para ser un consumidor inteligente. La saturación de los medios debe volverse más activa como consumidores, en parte para administrar el torrente de datos que nos inundan cada día, pero también para emitir juicios informados sobre la importancia de lo que vemos.

¿Cuáles son las mejores formas de combatir las “noticias falsas” y desarrollar habilidades de información digital? La proliferación de noticias falsas en los últimos años se ha visto reflejada en una proliferación de recomendaciones sobre cómo abordarlas. Las habilidades involucradas en la lucha contra la desinformación son, de hecho, las habilidades que necesitas desarrollar. Tu desafío es pensar en cómo los factores externos a la fuente en sí, como la identidad, la audiencia y el propósito de la autora o autor, pueden producir distorsiones sutiles. Por lo tanto, combatir las "noticias falsas" requiere ejercitar tu cerebro de una manera más esforzada, leer no solo con comprensión, sino también con discernimiento, en resumen, aplicar el pensamiento crítico a lo que estás leyendo y comprando.

A continuación, se ofrecen algunas recomendaciones sobre cómo ser un/a consumidora más inteligente en la era digital:

1.Comienza con el conocimiento de que cualquier cosa puede existir, y existe, en línea.

Eso significa que lo real existe junto con lo falso, lo bueno con lo malo, lo legal con lo ilegal y todo lo demás. Internet puede ser una habitación llena de sueños y también es un lugar donde puedes ver la parte más delicada de la bestia social. Puede estar lleno de oportunidades, comodidades y disfrute; también puede ser un lugar desleal que espera engañar, incitar, ser inmoral y degradar. Comprador, cuidado, multiplicado por un millón. Cuanto más identifiques la dualidad de Internet, más obviamente la verás por lo que es y también por todo lo que no es.

2. Haz tu propia investigación.

Cualquiera en línea puede ser técnicamente un 'líder de pensamiento', pero depende de nosotros si decidimos darles a estos individuos concretos el poder suficiente para obtener realmente ese pedestal como el "líder". Todos somos seguidores de “influencers” sociales, personalidades o marcas que queremos imitar; o de aquellas personas a quienes permitimos que influyan en nuestros pensamientos o elecciones de compra. El hecho de que publiquen información en línea no significa que sean una fuente de información válida; esta no es una ecuación 1 = 1. Lo que consumes en línea siempre debe ser cuestionado, investigado y verificado.

3.Considera cómo se utilizan tus datos.

Cuantos más datos facilites en línea, más anuncios dirigidos recibirás. Pero ten en cuenta que, más allá de lo que ofreces, otra información privada se extrae de diferentes fuentes. Por ejemplo, piensa en profundidad antes de permitir que las pruebas en línea accedan a la información de tu perfil, que incluye tu fecha de nacimiento, número de teléfono, ubicación, lista de amigos, lugar de trabajo, etc.

4. Protégete a ti y a tu información.

Compartir, o compartir información en exceso, puede provocar la recepción de anuncios molestos de cosas que parecen importantes o, lo que es peor, puede usarse para manipularlo en la creación de opiniones específicas, gastar dinero o agregar tu nombre como respaldo de cosas que quizás no comprendas o apoyes completamente.

5. Es responsabilidad tuya prestar atención y mantenerte informada/o.

Es fácil querer ignorar lo que está sucediendo o decirse a sí mismo que puede confiar en que los demás se mantendrán al día sobre los cambios en el uso de Internet, las leyes de privacidad y los acuerdos de usuario de la plataforma. Sin embargo, si continúas utilizando las partes valiosas de Internet, debes aceptar que existe un nivel de responsabilidad que posees como compensación por esos beneficios.

Nuestra sociedad moderna se ha vuelto mucho más consciente de los productos y servicios disponibles para comprar, con publicidad y marketing altamente inteligentes que nos convencen de que necesitamos ese anillo de diamantes, el teléfono más moderno, o los juguetes para los programas que nuestras hijas e hijos ven en la televisión. Reconociendo esto, existe un argumento para practicar buenos hábitos.
.

Figura 6. Consumidor/a más inteligente (Fuente: Elaboración propia

2.4. PENSAMIENTO CRÍTICO Y TÉCNICAS DE EVALUACIÓN

El uso de Internet es probablemente una actividad diaria para muchas de vosotras, pero a veces es una segunda naturaleza en que no nos detenemos a pensar en lo que subyace a la información que usamos. Ahora vivimos en una era en la que la información está ampliamente disponible. Siempre que las personas se enfrentan a una pregunta, su respuesta predeterminada es "búscalo en Google" en lugar de buscar una respuesta en una lluvia de ideas. Esto contrasta marcadamente con lo que solía ocurrir en el pasado, en el que los libros eran la principal fuente de información. Hoy en día, tu pensamiento crítico es un factor clave a la hora de analizar la información digital que nos rodea.

Hay muchas definiciones de pensamiento crítico, en su forma más básica, se trata de poder pensar por una misma. Para poder pensar críticamente, necesitas poder:

1. Examinar y evaluar información y argumentos.
2. Ver patrones y conexiones.
3. Identificar y generar información significativa para ser utilizada.

Alguien con habilidades de pensamiento crítico puede:

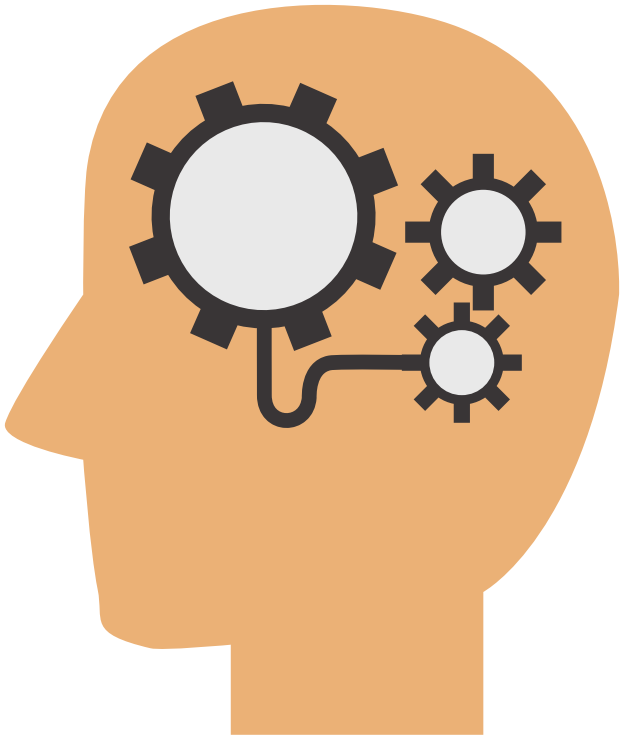
1. Comprender los vínculos entre ideas.
2. Determinar la importancia y relevancia de argumentos e ideas.
3. Reconocer, construir y evaluar argumentos.
4. Identificar inconsistencias y errores en el razonamiento.
5. Abordar los problemas de forma coherente y sistemática.
6. Reflexionar sobre la justificación de sus propios supuestos, creencias y valores.

Figura 7. Habilidades de pensamiento crítico (Fuente: Elaboración propia)

Probablemente ya tengas práctica en el pensamiento crítico en otras áreas de la vida, como decidir qué teléfono, computadora o automóvil comprar, dónde vivir; o incluso qué ponerte en una ocasión particular. En cada situación, probablemente no solo no haces lo que otra persona te dice que hagas, sino que puede que tomes una decisión basada en una variedad de factores. Aplicar una habilidad crítica en tus habilidades digitales significa usar tu capacidad para encontrar, evaluar, administrar, curar, organizar y compartir información digital. Además, se trata de la capacidad de interpretar información digital con fines académicos y profesionales, y de revisar, analizar y "re-presentar" información digital en diferentes escenarios. Un enfoque crítico para evaluar la información en términos de su procedencia, relevancia, valor y credibilidad. Hay que comprender las reglas de derechos de autor/a y alternativas abiertas, por ejemplo, Creative Commons; la capacidad de hacer referencia a obras digitales de manera adecuada en diferentes contextos.

Uno de los elementos más importantes de estar en línea es la capacidad de ser consciente de dónde proviene el contenido y quién lo ha escrito. Deberías poder hacer preguntas que te permitan comprender mejor el contexto.

En relación con tu habilidad crítica, es importante la capacidad de recopilar, administrar, acceder y utilizar datos digitales en hojas de cálculo, bases de datos y otros formatos, e interpretar datos mediante la ejecución de consultas, análisis de datos e informes: tu conocimiento de datos y las prácticas de seguridad personal de datos.



Otro factor es la comprensión de cómo se utilizan los datos en la vida pública y profesional; de directrices legales, éticas y de seguridad en la recopilación y el uso de datos; de la naturaleza de los algoritmos; y de cómo se pueden recopilar y utilizar los datos personales. No es necesario que seas una experta o una profesional de los datos, pero tienes que ser consciente de su existencia y de los peligros que puede ocasionarte su mal uso.

Otro factor importante es tu capacidad para recibir y responder críticamente a mensajes en una variedad de medios digitales (texto, gráficos, video, animación, audio) y para seleccionar, reeditar y reutilizar los medios, dando el debido reconocimiento a los creadores. Un enfoque crítico para evaluar los mensajes de los medios en términos de su procedencia y propósito. Comprensión de los medios digitales como herramienta social, política y educativa, y de la producción de medios digitales como práctica técnica.

Cuando se trata de evaluar contenido digital, hay que buscar el mejor contenido digital disponible. Por ejemplo: deseas evitar el contenido que es simplemente una versión electrónica del libro de texto sin ningún valor agregado. La alfabetización digital consiste en encontrar, evaluar, usar y crear contenido digital de manera significativa y responsable. Requiere habilidades de pensamiento y habilidades técnicas.

Teniendo en cuenta que encontrar contenido digital sobre el empleo de varias estrategias de búsqueda para ayudar a obtener información de calidad, el uso de múltiples motores de búsqueda para desafiar las burbujas de filtro personal usando recursos escritos, visuales y de audio para navegar por la información en una variedad de modos, recolectando una variedad de información que puede luego ser evaluada para cumplir con sus requisitos.

Otro punto importante es que antes de comenzar a buscar contenido digital relevante, debes considerar cuál es la pregunta de consulta que está tratando de responder o el tema cuya información estás explorando que ya contiene el tipo de información que necesita, por ejemplo: una descripción general, análisis / investigación detalladas o estadísticas. También hay que considerar cuánta información necesitas: qué lagunas hay en tu conocimiento.

En la era digital actual, cualquier persona puede distribuir cualquier información en sus sitios web, plataformas de redes sociales y otros foros en línea. Desafortunadamente, aquellos que buscan información paralela no verifican realmente la autenticidad de la información. Como resultado, la propaganda y la información falsa a menudo se interpretan como la verdad, lo que genera problemas en la toma de decisiones. No existe un estándar para verificar la información.

¿Cómo hacer una búsqueda eficaz de contenido digital? Obtén mejores resultados utilizando palabras clave precisas y estrategias de búsqueda. Piensa en palabras clave de tu pregunta de consulta o tema, incluidos sinónimos, diccionarios y un diccionario enciclopédico que sean útiles para compilar una lista de palabras-clave. Mira la pregunta o el tema sobre el que deseas obtener información y elige la fuente más relevante para tu búsqueda, por ejemplo, motores de búsqueda y / o bases de datos en línea, e intenta usar diferentes palabras-clave y técnicas de búsqueda para ampliar o limitar tu búsqueda.

Las técnicas de búsqueda comunes en Internet incluyen:

- **Excluye palabras de tu búsqueda:** Pon “– “delante de una palabra que deseas omitir. Por ejemplo: Jaguar velocidad - coche.
- **Busca una coincidencia exacta** coloca una palabra o frase entre comillas. Por ejemplo, "edificio más alto".
- **Busca dentro de un rango de números** Pon “...” entre dos números. Por ejemplo: cámara 50 € ... 100 €.
- **Combinar búsquedas** coloque "o" entre cada consulta de búsqueda. Por ejemplo, maratón o carrera.
- **Busca un sitio específico** coloca "sitio:" delante de un sitio o dominio. Por ejemplo, sitio: youtube.com o sitio: .gov.
- **Busca sitios relacionados** coloca "relacionado:" delante de una dirección web que ya conoces. Por ejemplo, relacionado: time.com.

La mayor parte de la información que se encuentra en Internet tiene una razón oculta de ser. Las empresas y las escritoras que colocan la información en Internet probablemente intentaban vender algo a los lectores. Otros son propagandistas que buscan influir en el modo de pensar del lector / lectora. El pensamiento crítico nos ayuda a pensar en los problemas y a aplicar la información correcta al desarrollar soluciones. Es importante que la era digital aprenda a diferenciar la información basada en hechos de la falsa. Además, es bueno que la información provenga de diversas fuentes en línea y fuera de línea para que sea precisa y tenga suficientes datos.

Hacer preguntas siempre es una buena idea. Te convertirá en una mejor aprendiz y pensadora. Hacer preguntas críticas significa profundizar en tus preguntas y no solo preguntar quién, qué, cuándo, dónde, por qué y cómo; sino hacer preguntas más descriptivas como "¿Quién se beneficia de esto?" "¿Qué se interpone en el camino de la acción?" "¿Por qué ha sido así durante tanto tiempo?" o "¿Cómo podemos cambiar esto en beneficio nuestro?"

Como dice Jesse R. Sparks:
"Debemos desarrollar las habilidades de alfabetización en información digital necesarias para evaluar la veracidad, relevancia, credibilidad y calidad de los argumentos de la información para aprender, resolver problemas y tomar decisiones de manera efectiva en el mundo actual".

2.5.PERCEPCIÓN CULTURAL Y COMPRENSIÓN SOCIAL

Las tecnologías digitales han transformado profundamente la escena cultural. Esa tecnología se ha infiltrado en nuestras vidas, ahora puede comprar, realizar operaciones bancarias, comunicarse, socializar, navegar y colaborar con personas en su teléfono inteligente o dispositivo. En este sentido, debemos saber que la cultura digital no solo está conectada con la digitalización de términos analógicos, sino que también se refiere a un espacio altamente dinámico en el que conviven modalidades multimedia, "cross media", transmedia, realidad aumentada y realidad virtual. Sin embargo, la escena digital no está exenta de riesgos.
Las nuevas tecnologías han modificado el espacio, el tiempo, las relaciones y los tipos de comunicación que aún continúan conviviendo con los otros campos del conocimiento inherentes a una cultura. Está claro que las nuevas tecnologías implican grandes ventajas en cuanto al acceso a la cultura y también es evidente que en la era digital hay muchas más ofertas culturales de las que los usuarios estaban acostumbrados.

La cultura digital se refiere al conocimiento, las creencias y las prácticas de las personas que interactúan en redes digitales que pueden recrear culturas del mundo tangible o crear nuevas corrientes de pensamiento y prácticas culturales nativas de las redes digitales. La cultura digital es Internet, transhumanismo, inteligencia artificial, ética cibernética, seguridad, privacidad y política. Es piratería, ingeniería social y psicología moderna (Digital Culturist, 2015).

Los teléfonos móviles son muy utilizados tanto por jóvenes como por adultos. Los sitios web como YouTube y Wikipedia son el primer puerto de escala para muchas personas que buscan información sobre un área de interés seleccionada. La televisión, las películas y la música se almacenan y se accede a ellas en computadoras, reproductores MP3 y en línea. Las compras en línea y por banca online se han vuelto más dominantes y los servicios gubernamentales se han basado cada vez más en Internet. El correo electrónico permite la comunicación instantánea entre personas de todo el mundo. Tanto los juegos en línea como fuera de línea ocupan un lugar destacado en la vida de muchas personas y las tecnologías Web 2.0, como los sitios de redes sociales, permiten que las personas colaboren compartiendo y editando contenido en línea.

La sociedad actual, a menudo llamada "la era de la información", está marcada por el rápido desarrollo de los recursos de comunicación e información.

La comprensión cultural y social le proporciona un idioma y un contexto para su alfabetización digital. Ciertamente, el desarrollo de la comprensión cultural y social es fundamental para que las personas puedan contribuir no solo social y culturalmente, sino también política, económica e intelectualmente. Debes darte cuenta de que existen ciertas influencias sociales, culturales e históricas que dan forma a tu comprensión y aprendizaje.

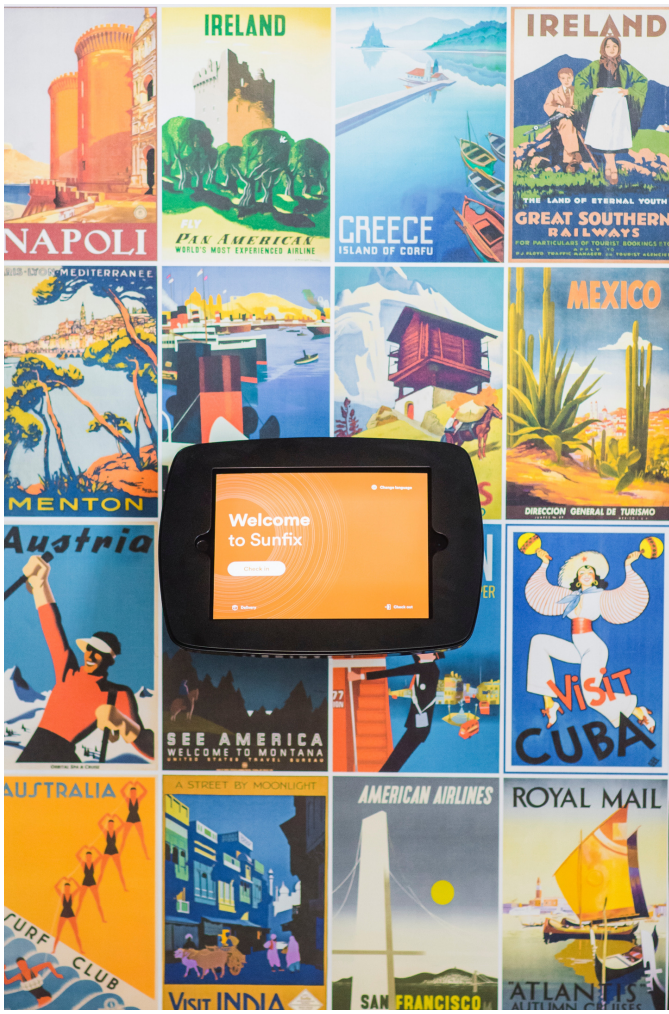
¿Cuánto podría cambiar la cultura cuando ciertas prácticas pasan a desarrollarse en línea? ¿Con qué frecuencia se pueden transportar las creencias y expectativas culturales actuales a otra realidad? Con frecuencia pensamos en la información y la comunicación de una manera técnica e instrumental, como datos y transmisión de datos. Sin embargo, la información y la comunicación también son fenómenos sociales.

La propagación de la tecnología no solo afecta el estatus de clase social, sino la formación, división y aspectos de la clase social que contribuyen a cada grupo. Aún así, muchas personas entienden menos dónde se encuentran dentro de la clase social ya que las culturas digitales confunden los tipos de capital. Esta falta de identificación o comprensión claras no disminuye la importancia de la jerarquía de clases, ya que el espacio digital categoriza el contenido a través de aspectos como los problemas de clase y de los trabajadores, que no se abordan claramente a través de su punto de vista, o por falta de cohesión de clase social digital.

La cultura y la tecnología digitales han formado nuevas formas de ver la clase social teóricamente, incluido el trabajo inmaterial, el trabajo digital, el trabajo informativo y cultural, el "concepto de trabajo libre en las condiciones de la Nueva Economía, así como las ahora famosas nociones de fábrica social" (Qiu, 2018)

La construcción de una cultura global en línea a través de los nuevos medios debe centrarse en cómo los cambios radicales son adoptados por las reglas y principios democráticos. Las tecnologías digitales, principalmente los espacios en línea, te brindan oportunidades para muchas formas nuevas de interacción. Cada vez más, estas interacciones están mediadas por diferentes modos de representación, como imágenes y sonidos. Ser capaz de decodificar estos textos multimodales requiere una comprensión de las prácticas sociales y culturales que rodean su creación.

Diferenciamos épocas culturales según la tecnología de comunicación utilizada. En la cultura oral, la transferencia de conocimientos solo puede ocurrir en la comunicación directa. En la cultura escrita, ciertos tipos de conocimiento o la memoria de una persona en particular podrían conservarse y los mensajes escritos podrían enviarse a través del espacio y registrarse (y conservarse) para el futuro. La cultura de la prensa y la radiodifusión permitió la distribución masiva de mensajes de fuentes centralizadas. Hoy en día podemos referirnos a conceptos como cultura digital, internet y su carácter participativo, convergencia, inteligencia ambiental, etc.



El efecto de las tecnologías de la comunicación en la cultura es importante porque la forma en que las usamos puede producir cambios en la esencia misma de nuestros modelos culturales y de comunicación, pero, aunque las herramientas digitales intensifican sus posibilidades, paradójicamente, el crecimiento exponencial en la oferta de contenido de todo el mundo a veces tiene el efecto contrario: resulta en un exceso que puede desviar su atención.

En base a las ideas presentadas, piensa en:

1. ¿En qué medida las habilidades de las y los ciudadanos digitales continúan mejorando sus estilos y habilidades de comunicación a través de los nuevos medios?

2. ¿Qué tipo de experiencias auténticas en línea se asocian con el desarrollo de estilos y habilidades de comunicación a través de los nuevos medios?

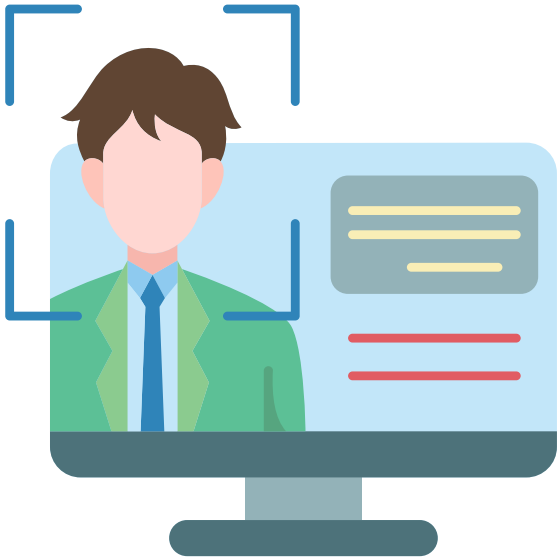
3. ¿Cuáles son los patrones de participación de las y los ciudadanos digitales en los estilos y habilidades de comunicación a través de los nuevos medios?

4. ¿Cuáles son los impactos de los estilos y habilidades de comunicación a través de los nuevos medios de comunicación?

Los individuos pueden convertirse en participantes activos en sus construcciones de conocimiento en lugar de ser receptáculos pasivos. En este entorno constructivista, los ciudadanos digitales pueden trabajar en proyectos globales complejos a través de los nuevos medios.

2.6. CREACIÓN DE IDENTIDAD VIRTUAL; GESTIÓN E IMPLICACIONES

Nuestra identidad es, literalmente, quiénes somos y presentarse en línea mediante un blog personal, una página web o un sitio de redes sociales necesita una selección intencionada de texto, imágenes, gráficos y audio para generar una impresión. Esto no se hace por casualidad. El mundo en línea requiere que las personas se escriban a sí mismas y sus perfiles brindan la oportunidad de crear la impresión deseada a través del lenguaje, las imágenes y los medios.



En la Reunión Anual del Foro Económico Mundial en Davos 2018 se identificaron un conjunto inicial de cinco elementos que una buena identidad debe satisfacer:

1. Adecuada a su propósito. Las buenas identidades digitales ofrecen una manera confiable para que las personas generen confianza en quienes dicen ser, para ejercer sus derechos y libertades y / o demostrar su elegibilidad para acceder a los servicios.
2. Inclusiva. La identidad inclusiva permite a cualquier persona que la necesite establecer y utilizar una identidad digital, libre del riesgo de discriminación por sus datos relacionados con la identidad y sin enfrentarse a procesos de autenticación que la excluyan.
3. Útil. Las identidades digitales útiles ofrecen acceso a una amplia gama de servicios e interacciones útiles y son fáciles de establecer y utilizar.
4. Ofrece opciones. Las personas pueden elegir cuándo pueden ver cómo los sistemas usan sus datos y pueden elegir qué datos comparten para qué interacción, con quién y durante cuánto tiempo.
5. Segura. La seguridad incluye proteger a las personas, las organizaciones, los dispositivos y la infraestructura del robo de identidad, el intercambio de datos no autorizado y las violaciones de los derechos humanos.

Figura 8. . Cinco elementos de buena identidad (Fuente: elaboración propia)

Fuente: Insight Report - Identity in a Digital World A new chapter in the social contract. World Economic Forum (Sep 2018)
http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

ISi buscaras en Google tu nombre, ¿qué encontrarías? Teniendo en cuenta que su identidad en línea no es lo mismo que su identidad en el mundo real porque las características que representa en línea difieren de las características que representa en el mundo físico; es posible que hayas oído hablar de la idea de “huella digital”.

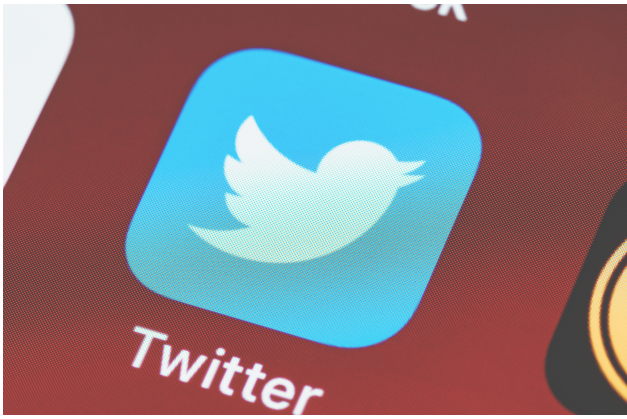
Esto se refiere a los rastros de tu información personal y profesional que quedan en las redes en línea, tanto de forma intencionada como no intencionada. A veces, es posible que escuches consejos sobre no publicar nada que no desees que nadie vea. Eso tiene sentido, pero también piensa en lo que te gustaría que vieran las generaciones futuras.

Publicar material en línea de manera efectiva significa que estás dejando de controlarlo, por lo que debes asegurarte de que no dañará tu reputación o credibilidad. Incluso si luego eliges eliminarlo, no hay garantía de que alguien no lo haya copiado o compartido sin tu conocimiento. Desafortunadamente, hay personas que disfrutan acosando a otros en espacios digitales, o que se aprovecharán de ti si se les da la oportunidad.

¿Qué necesitas saber durante el proceso de creación y protección de tu identidad en línea?

Hay una variedad de formas en las que puedes utilizar las redes sociales en línea cuando busques trabajo, que incluyen

1. Sitios de redes sociales como Facebook, Twitter y LinkedIn.
2. Participar en foros en línea y listas de discusión.
3. Creación de un blog personal.



Al participar en las redes sociales, siempre es prudente presentarse de manera profesional y también es importante proteger tu información personal.

Algunos consejos básicos para recordar cuando estés en línea

1. Internet es un espacio público. Cuando publicas en línea, renuncias a tu derecho a la privacidad.
2. El contenido en línea puede ser permanente, se puede buscar; puede llegar a muchas personas y puede revelar tu ubicación.
3. Al dar información, asegúrate de saber cómo se está utilizando.
4. Proporciona información sensible o confidencial solo a través de sitios web seguros.
5. Utiliza las redes sociales con prudencia; ajusta tu configuración de privacidad a su propio nivel de comodidad.
6. A pesar de todas las precauciones, ¡no tenga miedo de participar y conectarse!

¿Qué pasa con tu identidad profesional?

Las y los empleadores de hoy en día quieren saber a quién han contratado y muchos reclutadores revisan las redes sociales de los empleados potenciales. Los sitios de redes sociales son buenas formas de difundir sus intereses, habilidades y necesidad de trabajo. Según una encuesta de 2017, el 70 por ciento de los empleadores usan las redes sociales para seleccionar a sus candidatos antes de contratarlos. Además, el 69 por ciento de los empleadores utilizan motores de búsqueda en línea como Google, Yahoo y Bing para buscar candidatos. Construye y administra sus perfiles públicos en línea para que los empleadores potenciales encuentren información positiva y profesional sobre ti. Es un aspecto importante cuando estás buscando trabajo.

FFacebook, LinkedIn, Twitter, Pinterest (y cualquier otra comunidad en línea) pueden ser herramientas excelentes para establecer contactos, encontrar recursos y promover intereses personales o profesionales, pero solo si se usan de manera inteligente e intencional. Las primeras impresiones toman forma incluso antes de conocer físicamente a alguien. Al igual que el dicho "Su reputación le precede", tu reputación online hoy a menudo precede a tus reuniones y entrevistas en persona.

Lo que debes de tener en cuenta es que la gestión de la reputación en línea es una de esas cosas que funciona mejor si la implementas antes de que realmente la necesites.

Los 5 mejores consejos y trucos

1. Googleate a ti misma/o. Puede parecer vanidoso; pero, en este caso, estás excusado; necesitas saber qué ven las personas cuando te buscan.

2. Si no lo estás utilizando, elimínalo. Encuentra todos tus perfiles antiguos y cualquier cuenta no utilizada que ya no uses y elimínalas.

3. Recuerda que hay más de una página en Google. Asegúrate de revisar todo lo que puedas en Google en caso de que te pierdas algo.

4. La primavera limpia tu historia. Tomará tiempo, pero revisa tu Twitter / Instagram / Facebook y revisa cada publicación y elimina las que te dan mala imagen.

5. Deshazte de pruebas. Elimina las imágenes que te hagan quedar mal y pídeles a tus amigos que hagan lo mismo.

¿Ahora qué?

Piensa en lo que estás publicando. Has pasado todo ese tiempo limpiando tu huella digital. No deshagas todo ese buen trabajo adoptando viejos hábitos y ten cuidado con el contenido que compartes.

Entrar en bloqueo

Asegúrate de reforzar tu configuración de seguridad en plataformas como Facebook para que solo tus amigos puedan verte.

Ten cuidado al presionar el botón “Agregar”

A todos nos encantan los nuevos amigos de Facebook o los seguidores de Twitter, pero ten cuidado. A veces, no es aconsejable agregar colegas o conferenciantes en las redes sociales. Siempre es una buena idea mantener tu vida privada en privacidad.

Crea contenido excelente

Haz cosas que te den una buena imagen y conviértelas en parte de tu huella digital. Si tu jefe/a se conecta a Facebook, permítele encontrar un álbum de fotos tuyas como voluntaria /o en la comunidad. Si aún no lo usas, LinkedIn es una excelente manera de mostrar todas las cosas excelentes que haces y puede actuar como un CV en línea.

Co-funded by the Erasmus+ Programme of the European Union

HERRAMIENTAS MÁS IMPORTANTES EN LA ALFABETIZACIÓN DIGITAL EN GENERAL

3.1. . HERRAMIENTAS BÁSICAS DE SOFTWARE Y DE COMUNICACIÓN

El software básico y los programas de ordenador que permiten la ejecución de la mayoría de las tareas comunes para los usuarios de ordenadores se pueden dividir en dos grupos: software gratuito y pago. Nos gustaría enfatizar el software libre, sin embargo, los productos pagados y con licencia tienen sus propias ventajas, por ejemplo; soporte y una gama más amplia de herramientas y posibilidades adicionales. La mayoría de los programas de licencia de pago también ofrecen versiones limitadas, pero gratuitas, inusualmente para uso personal.

Para simplificarlo, preparamos una lista de las tareas más comunes que se pueden resolver con software gratuito o de pago. Esta lista también cubre la mayoría de las herramientas que generalmente requieren los empleadores.

También compartimos los enlaces a herramientas alternativas en línea, ya que muchas de las tareas se pueden resolver utilizando soluciones basadas en la nube, especialmente porque la evolución digital se está moviendo rápidamente hacia la computación basada en la nube. Los dispositivos personales se parecen cada vez más a terminales para acceder a máquinas remotas y potentes y mostrar los resultados. Tenga en cuenta que la mayoría de las herramientas y programas tienen sus propias versiones alternativas en los dispositivos de teléfonos inteligentes y están disponibles para descargar en las tiendas de aplicaciones.

Una lista de software básico gratuito y pad

Una tarea o propósito	Gratuito (instalación)	De pago / alternativo (instalación)	Acceso y uso en línea
Acceso a Internet	Chrome, Firefox, Opera	Google News (app)	N/A
Búsqueda de información	Google, Yahoo, Bing, Yandex	Duckduckgo	Quora, Wikipedia
Acceso y creación de cuentas de email	Thunderbird	Microsoft Outlook	Gmail
Colaboración y comunicación	Skype, Telegram, Viber	Slack, Zoom	Trello, Asana
Editar documentos, guardar y visionar PDF	OpenOffice (Writer)	Microsoft Word	Google Docs
Hacer cálculos, dibujar tablas y diagramas	OpenOffice (Calc)	Microsoft Excel	Google Sheets, Infogram.com
Proteger el ordenador de virus	GIMP	Photoshop	Snappa.com, Canva.com
Edición de fotos	VLC	Vimeo.com	Youtube.com
Media Player	Avast, Avira	ESET Antivirus	Eset online scanner
Seguridad y gestión de contraseñas	LastPass (para personas individuales)	1password, Bitwarden	N/A
Herramientas de búsqueda segura (VPN)	Opera built-in VPN	Nord VPN, Express VPN	N/A

Profundizaremos en ciertas herramientas y software básicos en capítulos posteriores.

3.2. LOS MOTORES DE BÚSQUEDA

Un motor de búsqueda es un sitio web a través del cual las y los usuarios pueden buscar contenido en Internet. Los motores de búsqueda permiten a las usuarias buscar contenido en Internet utilizando palabras clave. Cada motor de búsqueda funciona de manera similar.

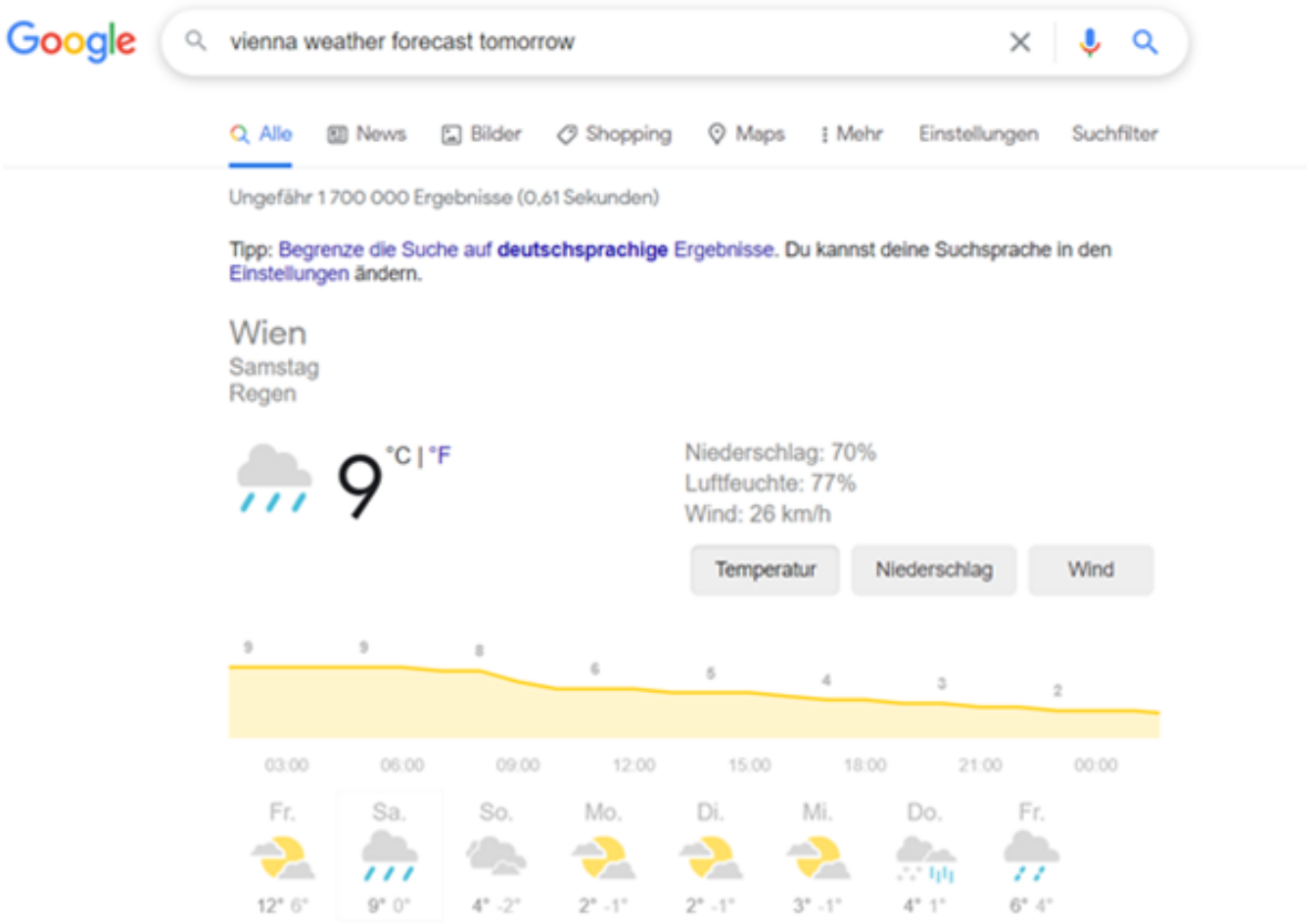
Si vas a la página de inicio de un motor de búsqueda, encontrarás un solo cuadro. Simplemente escribe lo que quieras buscar en ese cuadro. Los motores de búsqueda son una excelente manera de encontrar cosas en la web. Si buscas con cuidado, puedes encontrar información confiable y confiable. Con tal diversidad de contenido y con el enorme volumen de información en Internet, recuperar la información relevante puede resultar particularmente difícil.

Palabras clave en tus criterios de búsqueda

Debes pensar detenidamente sobre las palabras clave que ingresas en tu búsqueda. Deben ser relevantes. Por ejemplo: para saber cuál es el pronóstico del tiempo para mañana, puedes escribir palabras clave como: "Pronóstico del tiempo en Viena para mañana" y aparecerán los resultados de búsqueda más relevantes.

También debes pensar en la cantidad de palabras clave que usas. Si utilizas muy pocas palabras clave, podrías obtener demasiados resultados y no todas serán relevantes. Sin embargo, si usas demasiadas palabras clave, es posible que no obtengas ningún resultado. Para ayudar a que tu búsqueda sea más específica, puedes usar "comillas" alrededor de un conjunto de palabras para encontrar una frase exacta.

Figura 9. . Ejemplo de búsqueda: "Pronóstico del tiempo en Viena mañana" (Fuente: Google)



Si agregas un símbolo menos (-) antes de una palabra, excluirás las páginas que contienen esa palabra. Por ejemplo, "Emperadores romanos-César" buscará páginas con "Romanos" y "emperadores", pero no "César".

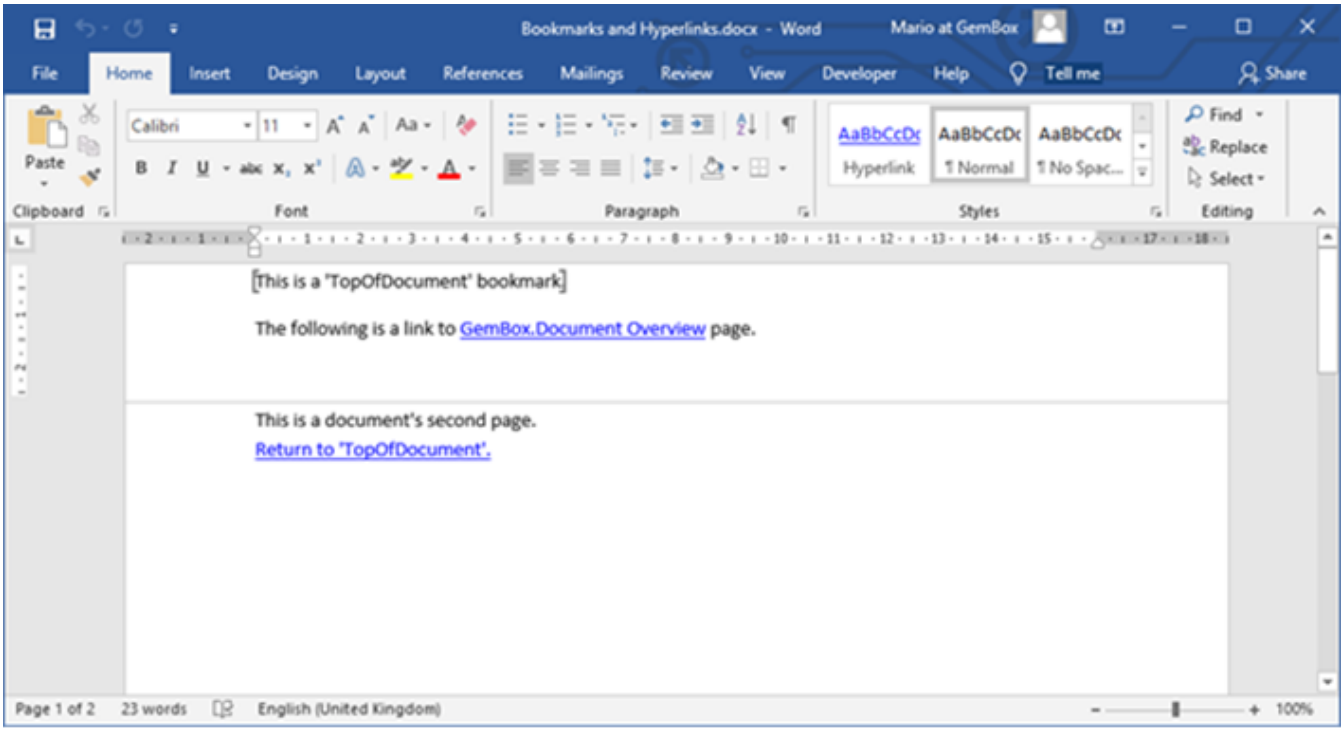
¿Qué es una URL?

Cada sitio web tiene su propia dirección en línea, denominada URL, que significa Localizador de recursos uniforme. Cuando estás viendo una página en la World Wide Web, es la dirección larga que aparece en la barra de direcciones en la parte superior de tu navegador

Existen algunos métodos más diferentes para localizar la información en Internet:

1. Puedes ir directamente a una página web simplemente conociendo su ubicación (por ejemplo: te gustaría visitar el sitio web de la empresa donde estás solicitando trabajo y estás familiarizada con la dirección exacta de su sitio web).
2. El enlace de hipertexto que emana de una página web proporciona asociaciones integradas con las otras páginas que su autor/a considera que proporcionan información relevante.

Figura 10. . Marcadores e hipervínculos. (Fuente: elaboración propia)



Los servicios “Narrowcast ”pueden“ enviarte páginas ”que se ajustan a tu perfil de usuaria/o

Se sabe que Google es el buscador online más famoso del mundo, pero también hay muchas otras opciones disponibles. Además, algunos de estos motores de búsqueda alternativos son inmensamente populares por derecho propio; simplemente no parecen demasiado populares en comparación con Google. Sin embargo, si no estás dispuesto a cambiar la privacidad por conveniencia o tienes necesidades de búsqueda específicas, existen varias alternativas a Google que ofrecen una experiencia de búsqueda más adecuada. Conocer el motor de búsqueda adecuado para realizar tu consulta significa que no gastas tu valioso tiempo navegando en cosas que no necesita. Uno podría perderse fácilmente en el vasto mundo de Internet sin las herramientas adecuadas.

A continuación, te presentamos 15 buscadores para probar como alternativas a Google para obtener mejores resultados de búsqueda.

Motores de búsqueda alternativos más populares

1. https://duckduckgo.com/	6. https://www.aol.com/	11. https://swisscows.com/
2. https://www.bing.com/	7. http://seznam.com/	12. https://startpage.com/
3. https://www.yahoo.com/	8. https://usearch.com/	13. https://www.ecosia.org/
4. https://yandex.com/	9. https://www.yippy.com/	14. https://www.naver.com/
5. https://www.ask.com/	10. https://www.searchencrypt.com/	15. https://www.baidu.com/

3.3. CORREO ELECTRÓNICO

El correo electrónico (o “email”) es un método de intercambio de mensajes ("correo") entre personas que utilizan dispositivos electrónicos. Es como el correo tradicional, pero también tiene algunas diferencias clave.

Por ejemplo: el correo tradicional se envía con el nombre, la calle, la dirección, la ciudad, el estado o provincia y el código postal del destinatario. Los correos electrónicos se envían electrónicamente a través de Internet. Un correo electrónico incluye un nombre de usuaria/o, el símbolo @ (arroba) y el dominio del proveedor de correo electrónico. Los nombres de usuaria/o a menudo incluyen números y versiones abreviadas de un nombre para crear una dirección de correo electrónico única y, por lo general, se verán así: emarosa82@gmail.com

Cuando envías un correo electrónico a alguien, llega casi instantáneamente y espera en la "bandeja de entrada" hasta que su destinataria/o lo lee. Con el correo electrónico, existe la posibilidad de agregar imágenes. Sin embargo, antes de continuar con los detalles, es importante explicar cómo crear una cuenta de correo electrónico.

Para comenzar a enviar correos electrónicos, necesitarás una dirección de correo electrónico que será única para ti. Para obtener esto, deberás registrarte para obtener una cuenta con un proveedor de correo electrónico; puedes elegir entre varios proveedores: Yahoo, Gmail, Hotmail, Outlook, GMX ... Depende de tus preferencias y necesidades con respecto al correo electrónico. Por ejemplo, si necesitas espacio y sencillez, Gmail es muy adecuado. Si solo necesitas un programa de correo electrónico simple para enviar y recibir correos, con pocas funciones, Yahoo puede ser una buena opción. Puede obtener información sobre cada proveedor de servicios escribiendo tu nombre en el cuadro de búsqueda del motor de búsqueda y hacer la comparación.

Dado que Gmail fue el proveedor más popular en 2020, ahora explicaré cómo crear una cuenta de Gmail (tenga en cuenta que esta metodología de creación de un correo electrónico puede aplicarse a casi todos los proveedores de servicios).

Paso 1. Escribe en tu motor de búsqueda www.gmail.com y te llevará a esta página.
Haga clic en "crear cuenta", en la esquina inferior izquierda y aparecerá la siguiente página:

Figura 11.Formulario de inicio de sesión de Google

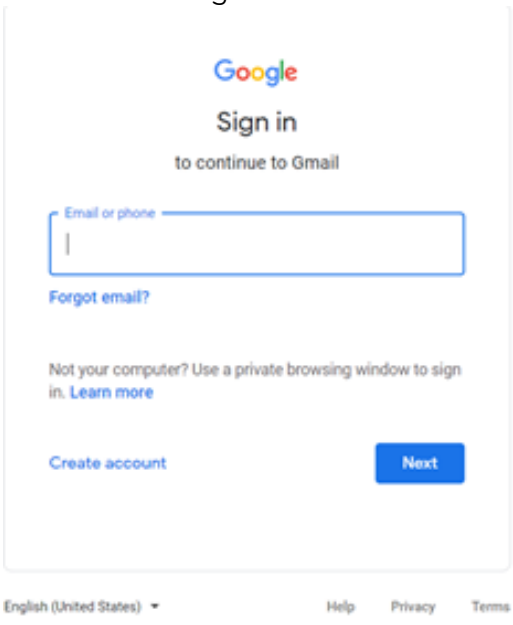
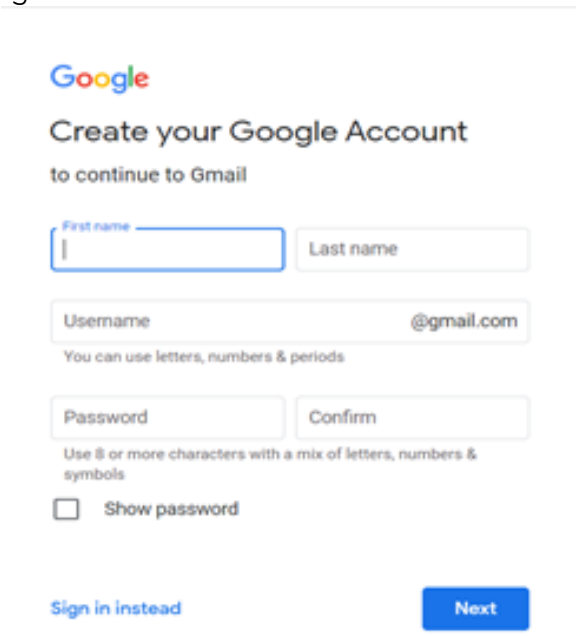
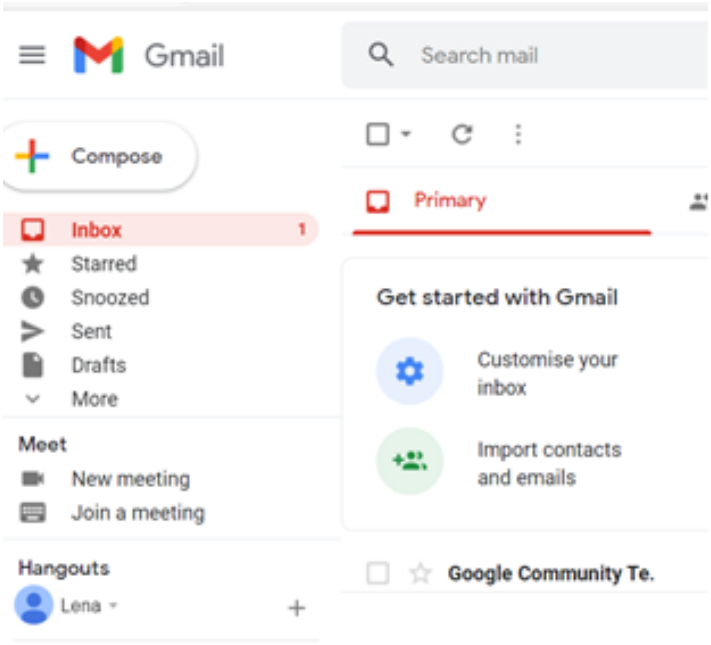


Figura 12. . Formulario de cuenta en creación de Google



Escribe tu nombre, apellido, nombre de usuaria/o y contraseña. Ten cuidado al elegir la contraseña correcta, asegúrate de que no será fácil de adivinar (evita la fecha de tu cumpleaños, por ejemplo, porque tu familia, amigos y conocidos podrían adivinarla fácilmente y acceder a tu correo privado). Puede hacer una combinación de letras, números y signos para crear una contraseña segura y confiable para tu cuenta. Después de crear una cuenta, podrás acceder a la interfaz de Gmail

Figura 13. Página principal de Gmail



Como puede ver, es muy fácil de usar e intuitivo. Si deseas crear un correo electrónico, haz clic en el botón "redactar" y aparecerá una ventana más pequeña en la esquina inferior derecha donde deberás escribir el nombre (dirección de correo electrónico) del destinatario y el asunto de tu correo electrónico. El lugar para el texto está debajo de la fila "asunto".

En la parte inferior de la ventana, verás un botón "enviar", así como el símbolo de "clip de papel" si deseas agregar algunos archivos a tu correo electrónico o "insertar emoji" si deseas agregar caras sonrientes a tu correo electrónico. Cuando hayas redactado tu correo electrónico, haz clic en el botón "enviar" y tu correo electrónico se entregará a la dirección de correo electrónico deseada y se almacenará en los mensajes "enviados".

Si recibes un correo electrónico de alguien, aparecerá en su "bandeja de entrada" como un mensaje no leído en negrita. Los mensajes más importantes pueden estar marcados con una "estrella" y facilitará tu búsqueda mediante la búsqueda en la sección "destacados".

3.4. REDES SOCIALES

Una red social se define como una cadena de individuos y sus conexiones personales. También conocida como comunidad virtual o sitio de perfil, una red social es un sitio web que reúne a las personas para hablar, compartir ideas e intereses o hacer nuevas amistades. Este tipo de colaboración e intercambio se conoce como redes sociales.

Ampliar las conexiones con otras personas es una técnica que se puede utilizar tanto por motivos personales como empresariales. Las aplicaciones de redes sociales hacen uso de las asociaciones entre individuos para facilitar aún más la creación de nuevas conexiones con otras personas. Esto podría usarse para conocer nuevos amigos y conectarse con los antiguos, como lo hace mucha gente en Facebook, o para expandir las conexiones profesionales a través de una red comercial como LinkedIn.

El proceso para crear una nueva cuenta para una red social es diferente para cada red social. En general, visita el sitio web de la red social donde deseas tener una cuenta y buscas el enlace "Registrarse" o "Crear nueva cuenta".
Sigue los pasos de creación de la cuenta para crear tu nueva cuenta.
Es probable que debas proporcionar tu nombre, rango de edad y dirección de correo electrónico como mínimo. Es posible que se requiera información adicional, dependiendo de los requisitos de la red social. Ten cuidado con la configuración de privacidad para restringir cierto contenido solo a amigos y, al mismo tiempo, mantenga una buena imagen pública.

Además, para ser visto por empresas y reclutadores, debe asegurarse de tener un perfil público. Si además usas Facebook como red social para el ocio, puedes cambiar tu configuración de privacidad para restringir ciertos contenidos solo a amigos y al mismo tiempo mantener una buena imagen pública, dependiendo del tipo de trabajo al que aspires.

Los 10 principales sitios de redes sociales que deben interesarte en 2021

Nombre	Enlace	Información
Facebook	www.facebook.com	La red social más popular para configurar un espacio personal y conectarse con amistades, compartir imágenes, compartir películas, etc.
Youtube	www.youtube.com/	Una excelente red para publicar blogs de video o blogs y otros videos divertidos y emocionantes.
Twitter	www.twitter.com	Un medio muy popular para comunicarse (30-65 años), noticias de última hora, digerir contenido pequeño (se permiten 150 caracteres). Usando el hashtag puedes filtrar la información.
Instagram	www.instagram.com	Es otra red social muy utilizada por los aficionados a la fotografía, como actividad de ocio o de trabajo. Para aquellos que buscan trabajo en campos creativos, esta red social es una de las más adecuadas.
Tik tok	www.tiktok.com	TikTok es una especie de karaoke visual, en el que montajes al límite de la ciencia ficción se vuelven al alcance de todos, alcanzables directamente con unos toques en su teléfono móvil. El contenido que funciona mejor en TikTok: contenido de video de formato corto entretenido, interesante, cómico y, a veces, sin sentido, generalmente con la melodía de canciones populares. Piense en contenido de estilo de video musical divertido y pegadizo.

Nombre	Enlace	Información
Snapchat	https://www.snapchat.com	Snapchat sigue siendo una de las aplicaciones más utilizadas entre los menores de 25 años. Si tiene una habilidad especial para crear videos cortos convincentes (generalmente estilo selfie) que pueden entretener y educar a una audiencia joven. Snapchat es una plataforma obvia para que establezca conexiones con sus clientes.
LinkedIn	www.linkedin.com/	Es la red social profesional más famosa. Con "Conexiones" profesionales, busque trabajo en la sección dedicada a las ofertas de trabajo y envíe su solicitud directamente, comparta información pública en su página personal, videos, imágenes o documentos varios como una forma de hacerse notar por las empresas. Tiene muchos grupos de discusión y foros alos que puedes unirte y tener la oportunidad de intercambiar opiniones.
Pinterest	www.pinterest.com	Pinterest se ha convertido en una herramienta de marcadores sociales muy popular para guardar ideas y encontrar inspiración creativa. Se trata de todo, desde cocinar hasta proyectos domésticos de bricolaje, ideas de vacaciones, diseño de interiores, negocios y todo lo demás.
Reddit	www.reddit.com	La comunidad de usuarios registrados (redditors) envía contenido que la comunidad vota a favor. Reddit tiene un subreddit (tablero) para casi todas las categorías.
Google+	https://plus.google.com/collections/featured	Es una red social en la que puedes formar parte de "círculos", es decir, grupos que hablan de un tema determinado y elegir el que te interesa. En tu perfil puedes añadir las direcciones de otras redes sociales en las que estés registrado.

3.5. SOFTWARE DE NEGOCIOS

El software comercial es, en muchos casos, un combustible para el éxito del negocio o una herramienta necesaria para una amplia gama de operaciones comerciales. Por lo tanto, básicamente todos los puestos de la mayoría de las empresas que existen requieren al menos conocimientos básicos y competencia en las herramientas comerciales más utilizadas.

No cubriremos el software básico que cualquier persona alfabetizada digitalmente debe conocer y operar, como ya se explicó en nuestro capítulo anterior. El objetivo de este capítulo es explicar mejor el conjunto genérico de herramientas y agruparlas en las más utilizadas, independientemente de la industria en la que se utiicen.

Vale la pena mencionar que muchos software y herramientas que usan las empresas se instalan en un ordenador como un programa independiente o se puede acceder a ellos a través de herramientas en línea. Dicha industria se está convirtiendo en una industria en constante crecimiento: SaaS. SaaS significa "Servicio como software", y suele ser un acceso de pago a determinados servicios en línea.

El tipo de software y el conjunto de herramientas que utilizan las empresas depende principalmente de la industria en la que operan, el tipo de clientes a los que atienden, ya sea otros negocios o clientes habituales, así como el tamaño de la empresa. Las pequeñas empresas normalmente no dependen mucho de una amplia gama de herramientas que son esenciales para las corporaciones más grandes. Sin embargo, el éxito de cualquier empresa depende mucho de las habilidades y experiencia que posean sus empleados, especialmente en el uso de herramientas digitales.

Lista de herramientas digitales de uso común:

Conferencias remotas	„Zoom“, „Skype“, „Google Hangouts“
Marketing y publicidad	Facebook Ads, Google Local Business and Maps, Google Ads, Linkedin Ads
Envío de correos electrónicos, respuestas automáticas y seguimientos	„Mailchimp“, „MailerLite“, „Woodpecker“
Automatización de marketing y CRM	„Hubspot“, „Salesforce“
Gestión, planificación y eficiencia de proyectos	„Trello“, „TeamGantt“
Colaboración y comunicación	„Slack“, „Microsoft Teams“, „Asana“
Supervisión y optimización del rendimiento del sitio web	„Google Analytics“, „Hotjar“, „Google Optimize“
Cuentas de correo electrónico y muchas de las anteriores	Google Workspace“
Almacenamiento en la nube	„Google“ diskas, „Dropbox“
Flujo de datos, automatización de informes e integración de herramientas	„Zappier“, „Supermetrics“, „Google Data Studio“
Firma electrónica de contratos y documentos	„DocuSign“, „Docobit“
Compartir y transferir archivos	„WeTransfer“
Asistente de escritura	„Grammarly“.

Esta lista no cubre todas las excelentes herramientas que utilizan las empresas en sus actividades diarias, hay muchas más herramientas, dedicadas a más nichos y propósitos únicos para diferentes tipos de negocios.

3.6. DESARROLLO DE SITIOS WEB, BLOGS Y MARKETING.

Los sitios web son sin duda el elemento más importante de Internet, ya que permiten mostrar contenido como textos, imágenes y videos en Internet.

La página central de un sitio web se llama página de inicio o página de inicio / página de índice. Luego, el/la usuario/a profundiza en las subpáginas del sitio.

Una presencia web digital permite que contenido como textos, imágenes y videos se muestren en Internet.

Dependiendo del tamaño del sitio web, las y los visitantes del sitio tienen la oportunidad de acceder a las subpáginas del sitio web.

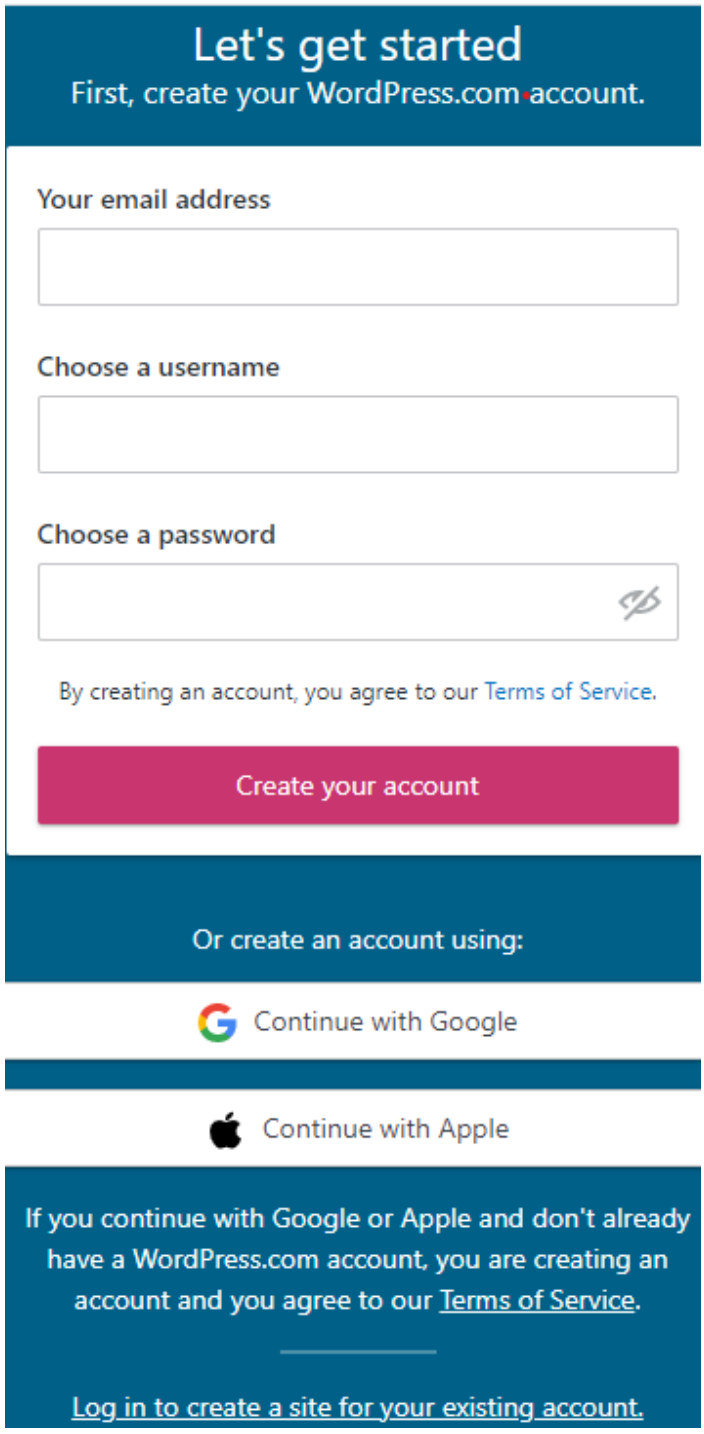
- Los hipervínculos, o simplemente "enlaces", se utilizan para conectar documentos HTML únicos de un sitio web. Los enlaces a subpáginas importantes (por ejemplo: departamentos, categorías de productos o páginas de información representativa) generalmente se combinan en la navegación y se pueden encontrar en el encabezado del sitio web.
- Se muestran en cada subpágina del sitio web y no solo en la página de inicio. La navegación ayuda al usuario / a la usuaria a orientarse y ver una descripción general de la estructura del sitio web.
- También se pueden colocar enlaces a más subpáginas en los elementos de texto e imagen del contenido del sitio web
- El pie de página en la parte inferior de una página a menudo contiene vínculos a más información, como el propietario o propietaria del sitio y el marco legal.

Creando un sitio web gratuito con WORDPRESS

WordPress.com es la primera solución a considerar para crear un sitio web gratuito utilizando el famoso CMS. Esta plataforma te permite crear tu propio sitio web con un dominio de tercer nivel (www.namewebsite.wordpress.com) poniendo a disposición un espacio de almacenamiento de 3 GB.

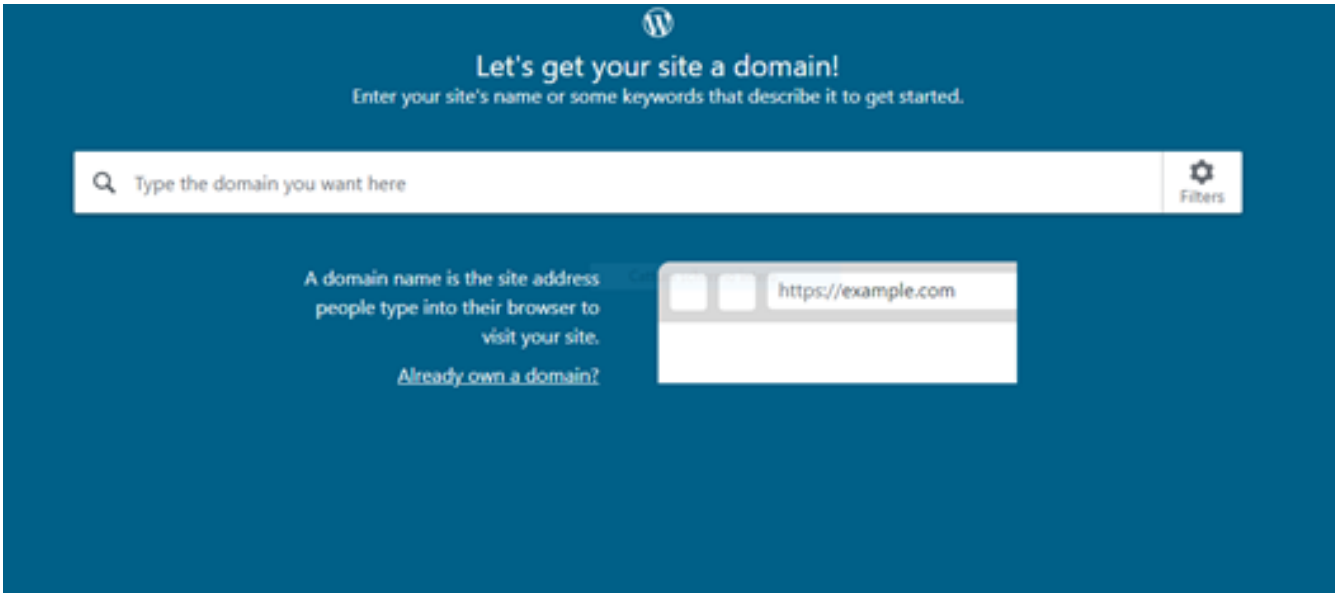
Ve a la página de inicio https://wordpress.com/, haz clic en "Crear su cuenta". Posteriormente, indica en el campo de texto correspondiente la dirección de forma gratuita.

Figura 14. Crear una cuenta de wordpress

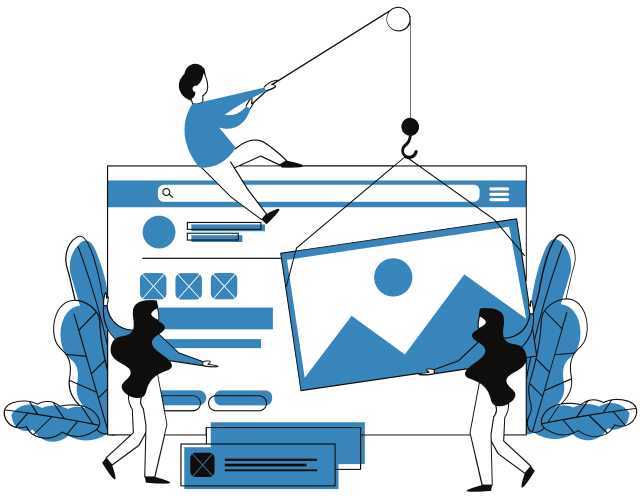


Luego, ingresa el nombre que deseas mostrar en el dominio de tu sitio web en el campo “Ingresa un nombre o palabra clave” y haz clic en el botón “Seleccionar” para la opción “Gratis”. En la nueva página abierta, presiona el botón “Comenzar con gratis”, ingresa los datos requeridos en los campos “Su dirección de correo electrónico”, “Elige un nombre de usuario” y “Elige una contraseña”, haz clic en el botón “Continuar” dos veces seguidas y listo.

Figura 15. Ingresar un nombre de dominio



Ahora, presiona el botón “Ver sitio” para ver tu sitio web creado con WordPress.com. Para agregar nuevas páginas y artículos, haz clic en el botón “Agregar” relacionado con las opciones de “Páginas del sitio” y “Artículos de blog”, mientras seleccionas el elemento “Personalizar” en la barra lateral izquierda, puedes cambiar la apariencia y elegir otro tema gratuito disponible. Selecciona una de las muchas plantillas disponibles: para hacerlo, haz clic en la vista previa de la que te interesa y haz clic en el botón “Aplicar”, para aplicarla directamente al sitio que has creado; o haz clic en el botón “Personalizar” si deseas modificarlo un poco.



Para agregar nuevas páginas o nuevas publicaciones al sitio, en su lugar, haz clic en las palabras “Páginas” o “Publicaciones” (a la izquierda) y haz clic en el botón (+) “Nueva página” o (+) “Nueva publicación” ubicado en la parte superior izquierda. En la pantalla que se abre, puedes crear una nueva página o una nueva publicación escribiendo su título y cuerpo en los campos de texto correspondientes. Usando los botones de la barra de herramientas ubicada en la parte superior, también puedes formatear el texto, insertar enlaces, imágenes, etc. Sin embargo, al hacer clic en los botones “Vista previa” y “Publicar”, puedes obtener una vista previa del contenido y publicarlo.

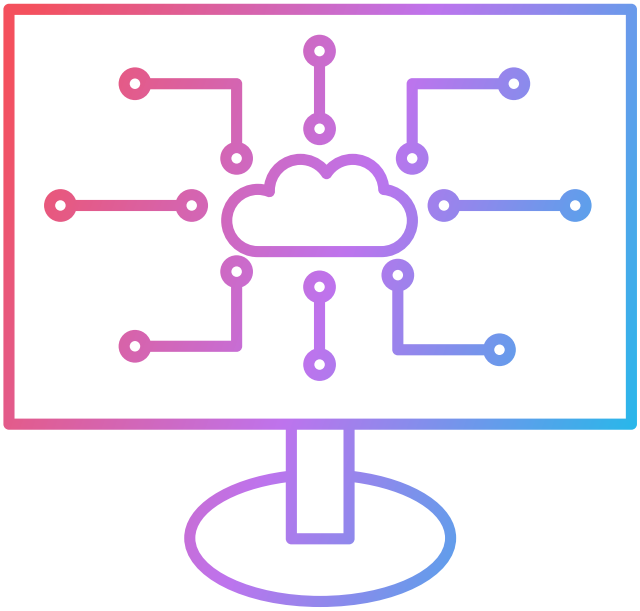
Si bien ejecutar un sitio web a través de la solución de alojamiento de Worpress.com es fácil y conveniente, especialmente para principiantes, a veces es más adecuado elegir un enfoque totalmente personalizable para la creación de un sitio web y alojarlo tú misma/o. Deberías comprar un plan de alojamiento de uno de los muchos proveedores de servicios de alojamiento e instalar Wordpress CMS utilizando una variedad de herramientas proporcionadas por el anfitrión.

Como Wordpress es una plataforma, creada originalmente para bloggers, su popularidad creció hasta convertirse en la opción número uno para todo tipo de desarrolladores de sitios web individuales y también para empresas. Es compatible con una amplia gama de herramientas y complementos, que permiten que Wordpress se adapte al comercio electrónico, foros, subastas o incluso plataformas de redes sociales. Los profesionales de Wordpress lo ven más bien como un núcleo muy bien optimizado para cualquier tipo de desarrollo de proyectos en línea, además, con los componentes originales de Wordpress eliminados.

Existen muchas plataformas CMS alternativas para Wordpress y entre las más populares se encuentran Joomla, Drupal como plataformas CMS, mientras que Wix.com, Shopify.com son plataformas web y paquetes de servicios, dedicados a necesidades particulares, como comercio electrónico y otros.

Figura 16. Algunas de las plataformas y servicios de CMS más populares

Para finalizar, vale la pena enfatizar que un sitio web verdaderamente exitoso suele ser el que proporciona un valor real a los visitantes del sitio web: los usuarios de Internet. Una forma de proporcionar valor puede ser la creación de contenido de calidad al poder escribir artículos e historias interesantes y atractivas, por lo que las habilidades para contar historias son útiles al crear cualquier tipo de contenido en Internet. En el siguiente capítulo preparamos algunos consejos para un narrador exitoso al presentarle qué es la narración personal y estas habilidades pueden ser útiles.



3.7. NARRATIVA PERSONAL

La narrativa es la capacidad de cautivar a alguien o un grupo de personas con una narrativa atractiva que los influencia y los hace sentir como parte de la historia. La gente recuerda las historias mucho mejor que los hechos y las cifras. Es una de las habilidades más importantes que puede aprender a dominar.

Puntos clave:

1. La narración influye en el cambio a nivel de la práctica individual y organizativa.
2. Escuchar historias facilita una mejor atención centrada en la persona y puede conducir a mejores servicios
3. Escuchar historias personales genera una mayor comprensión, empatía y reflexión.
4. La simpatía, la confianza y el cuidado pueden fomentarse en las relaciones entre el médico y el usuario del servicio mediante la narración de historias.
5. La narración personal beneficia al narrador, ya que puede empoderar, fomentar el crecimiento personal y desarrollar la resiliencia.

¿Por qué la narrativa es valiosa para el/la narrador/a?

Reformula la identidad propia y fomenta el desarrollo personal.

La evidencia sugiere que el proceso de narración personal permite que el concepto de uno mismo y la historia de la vida propia se conecten de una manera que facilita un replanteamiento de la identidad y fomenta el crecimiento personal. Al impartir una historia, un individuo expresa los eventos significativos en sus propias palabras y en su propio tiempo, y está capacitado para reflexionar. El proceso permite que surjan una nueva conciencia y nuevos significados del yo.

Es una relación que coproduce significado.

La relación de narración implica una escucha y un compromiso diferentes a los de un intérprete-público o entrevistador-participante. Es una relación que cierra la brecha entre la persona y los que brindan apoyo, por ejemplo, el médico-usuario del servicio.

Promueve la resiliencia.

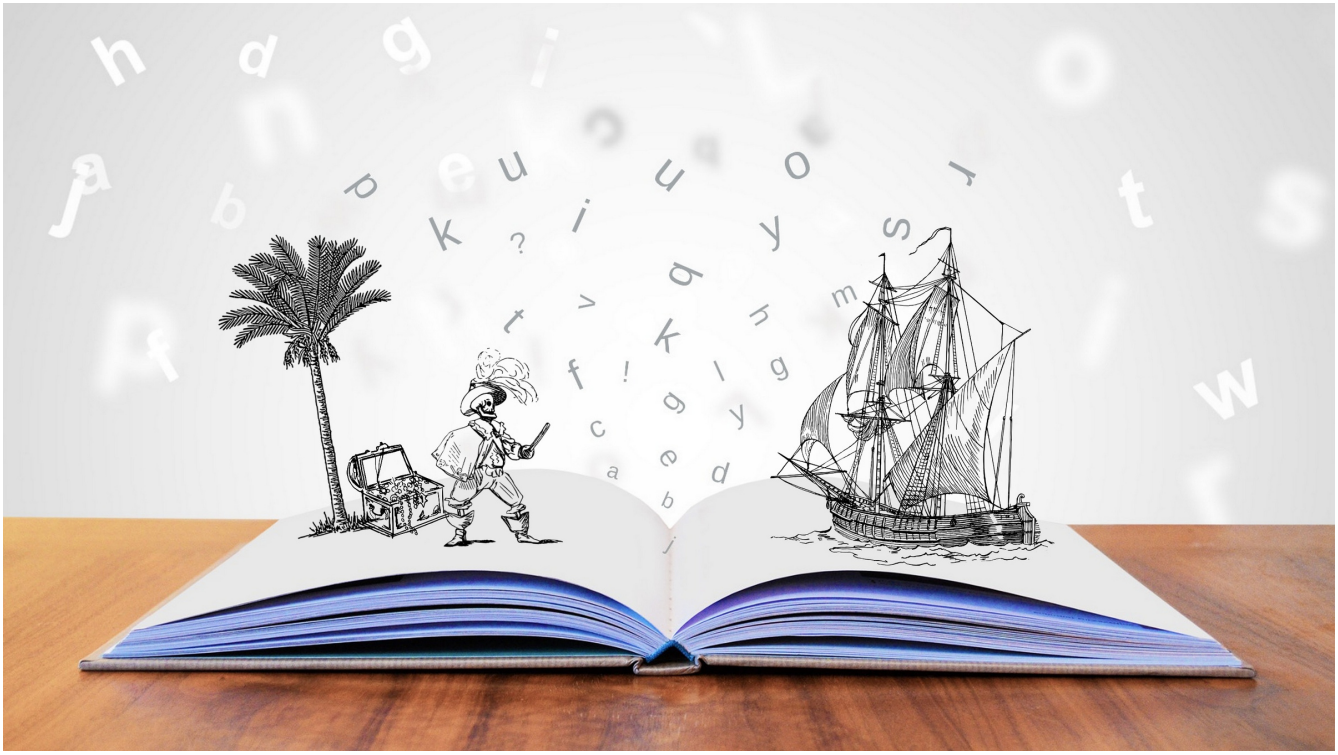
La resiliencia implica la voluntad de convertir las emociones negativas involucradas en eventos perturbadores de la vida, en algo que fortalezca y empodere. La resiliencia se desarrolla mediante un proceso de reflexión sobre los significados, que posibilita la comprensión emocional. El apoyo de las y los compañeros y otras redes, es clave para formar vínculos y sentirse conectado con otras personas. La combinación de estos factores da como resultado una fortaleza en las personas, que se basa en la premisa de que las experiencias de la vida (incluidas las negativas) ofrecen oportunidades para el crecimiento personal.

Es terapéutico

El valor terapéutico de contar una historia a menudo se informa en el trabajo de narración de historias (Hardy, 2007; Scottish Recovery Network, 2012). Si bien a menudo se expresa preocupación por el bienestar de las personas al contar historias y algunos narradores han informado un grado de disgusto al transmitir su historia, se reconoce que, en su mayor parte, los aspectos positivos de contar tu historia superan con creces cualquier angustia emocional encontrada. Es más frecuente que el acto de contar una historia y reflexionar sobre ella tenga un efecto catártico y sea un catalizador de la recuperación.

Técnicas de narración

Los mejores narradores son capaces de realizar elecciones narrativas útiles para hacer avanzar sus historias, para involucrar al público objetivo mediante la difusión de información importante, para mantener la atención. Saben cómo referirse a sus experiencias de vida para dar emoción al texto.
También debes ser capaz de ponerte en contacto íntimo contigo misma/o, hasta el punto de que las palabras y las emociones se conviertan en una sola entidad, capaz de despertar conciencia y reflexiones entre los interlocutores.
Estos últimos representan el target, que es un grupo de clientes potenciales a los que una empresa quiere vender sus productos, servicios o el propio contenido, y tendrá que "enamorarse" de la idea y la historia que se cuenta. El “Storytelling” se puede adaptar a cualquier ámbito que necesite ser apoyado desde un punto de vista comunicativo; una empresa, un producto intelectual o físico, un servicio, una marca, una persona, o un evento.



3.8. FIRMA ELECTRÓNICA Y SERVICIOS ELECTRÓNICOS

Firmas electrónicas

Las firmas electrónicas ofrecen una forma de firmar documentos en el mundo en línea, de forma muy similar a como se firma un documento con un bolígrafo en el mundo real (fuera de línea). En el pasado, solo las firmas escritas a mano eran legalmente válidas. La Directiva sobre un marco comunitario para las firmas electrónicas (Directiva sobre firmas electrónicas), adoptada en 1999, amplió ese reconocimiento a las firmas electrónicas. Un sistema fiable de firmas electrónicas que funcione en todos los países de la UE es vital para el comercio electrónico seguro y la prestación electrónica eficiente de servicios públicos a empresas y ciudadanas/os. La Directiva de firma electrónica estableció el marco legal a nivel europeo para las firmas electrónicas y los servicios de certificación. El objetivo es facilitar el uso de las firmas electrónicas y ayudarlas a ser reconocidas legalmente en los Estados miembros de la UE.

La definición de firmas electrónicas varía según la jurisdicción aplicable. Un denominador común en la mayoría de los países es el nivel de una firma electrónica avanzada (una firma electrónica que cumple con los requisitos establecidos por el reglamento de la UE) que requiere:

1. Autenticidad: el mensaje se origina en el remitente dado, y el remitente puede ser identificado de forma única.
2. Integridad: La manipulación de la firma del documento firmado se puede detectar de inmediato.

Con la invención de la firma del teléfono móvil, se diseñaron herramientas para firmar electrónicamente documentos, facturas y contratos legalmente vinculantes. Es posible agregar una firma electrónica al documento PDF de forma rápida y segura, que es el equivalente legal de una firma manuscrita. La autenticidad de la firma y la autenticidad de los datos transmitidos pueden ser verificadas en cualquier momento por el remitente o el destinatario.

Firma digital

Las firmas digitales presentan implementaciones criptográficas de firmas electrónicas utilizadas como prueba de autenticidad, integridad de los datos y no repudio de las comunicaciones realizadas a través de Internet. Cuando se implementa de acuerdo con los estándares de firma digital, la firma digital debe proporcionar privacidad de extremo a extremo con un proceso de firma fácil de usar y seguro. Las firmas digitales se generan y verifican a través de marcos estandarizados como el Algoritmo de firma digital (DSA

Por lo general, hay tres algoritmos involucrados en el proceso de firma digital:

1. Generación de claves: este algoritmo proporciona una clave privada junto con su clave pública correspondiente.
2. Firma: este algoritmo produce una firma al recibir una clave privada y el mensaje que se está firmando.
3. Verificación: este algoritmo verifica la autenticidad del mensaje verificándolo junto con la firma y la clave pública.

El proceso de firma digital requiere que la firma generada tanto por el mensaje fijo como por la clave privada pueda ser luego autenticada por la clave pública que la acompaña. Usando estos algoritmos criptográficos, la firma de la persona usuaria no se puede replicar sin tener acceso a su clave privada. Por lo general, no se requiere un canal seguro. Al aplicar métodos de criptografía asimétrica, el proceso de firma digital evita varios ataques comunes en los que el atacante intenta obtener acceso a través de los siguientes métodos de ataque.

Firma biométrica

La firma electrónica también puede referirse a formas electrónicas de procesamiento o verificación de identidad mediante el uso de "firmas" biométricas o cualidades de identificación biológica de un individuo. Dichas firmas utilizan el enfoque de adjuntar alguna medida biométrica a un documento como prueba. Las firmas biométricas incluyen huellas dactilares, geometría de la mano (longitud de los dedos y tamaño de la palma), patrones del iris, características de la voz o incluso patrones retinianos. Todos estos se recopilan mediante sensores electrónicos de algún tipo. Debido a que cada una de estas características físicas tiene pretensiones de ser únicas entre los humanos, cada una es hasta cierto punto útil como firma.

Figura 17. aplicación de firma electrónica. (Fuent: https://bit.ly/2ZdPQmX)

Los cinco servicios de firma electrónica más populares:

1. „eSignly“ es una solución de firma electrónica líder para millones de usuarios en todo el mundo por la facilidad que brinda en la firma y administración de documentos. La aplicación ofrece varias funciones como firma en persona, firma programada, autofirmación, administración de equipos, seguridad de primer nivel, integración con aplicaciones de trabajo populares, seguimiento de auditoría, etc

2. „PandaDoc“ está disponible para plataformas móviles Android e iOS. El software en línea es un software de firma electrónica galardonado que tiene una interfaz de usuario fácil de usar.

3. „Adobe Sign“ está disponible en las plataformas móviles iOS y Android. Adobe es un nombre común en el mundo de los gráficos y, como tal, se dice que es uno de los pioneros en servicios de eSign. El software es rico en funciones, lo que le da al usuario el poder de administrar flujos de trabajo continuos desde cualquier ubicación o dispositivo. La aplicación tiene firmas digitales y electrónicas.

4. „SignEasy“ es otro software de firma electrónica compatible con las plataformas Android e iOS. SignEasy no es una aplicación de firmas pesada porque ofrece una interfaz de usuario mínima con la intención de facilitar su uso. La firma con SignEasy permite la firma automática, la firma remota y la firma en persona.

5. „RightSignature“ utiliza las plataformas Android e iOS. Esta aplicación de firma electrónica utiliza la velocidad para impresionar a sus usuarios, ya que los documentos llegan más rápido al enviar y recibir firmas. Con él, puede cargar, formatear y enviar documentos en el menor tiempo posible.

Agregar o eliminar una firma electrónica de Microsoft Word o Adobe

Con una línea de firma electrónica en un documento de Word, puede solicitar información sobre el firmante y proporcionar instrucciones. Cuando se envía una copia electrónica al firmante, esta persona ve la línea de firma y una notificación solicitando su firma. El firmante puede:

1. Escribir una firma.
2. Seleccionar una imagen de una firma entintada.
3. Escribir una firma utilizando la función de entintado en una computadora con pantalla táctil u otro dispositivo.

Cómo crear una línea de firma en Word o Excel (Office 365 o 2019):

1. En el documento, coloca el cursor donde desees una línea de firma.
2. En la pestaña “Insertar” del grupo “Texto”, haz clic en la lista “Línea de firma”. Luego, haz clic en Línea de firma de Microsoft Office.
3. En el cuadro de diálogo “Configuración de la firma”, escribe la información que aparecerá debajo de la línea de la firma:
   - Firmante sugerido: el nombre completo del / de la firmante.
   - Título de firmante sugerido: el título del firmante, si lo hubiera
   - Dirección de correo electrónico del / de la firmante sugerida: la dirección de correo electrónico del firmante, si es necesario.
   - Instrucciones para el firmante: instrucciones para el firmante, como "Antes de firmar el documento, verifique que el contenido sea correcto".
4. Selecciona una o ambas de las siguientes casillas de verificación:
   - Permitir que el firmante agregue comentarios en el cuadro de diálogo “Firmar”: el / la firmante puede escribir el propósito de la firma.
   - Mostrar fecha de firma en la línea de firma: La fecha en que se firmó el documento aparecerá con la firma.

Además, puedes eliminar una firma haciendo clic en la flecha junto a la firma en el “Panel de firmas” y luego haciendo clic en “Eliminar firma”.

Alternativamente, puedes requerir una firma electrónica en un documento PDF. Consulta la siguiente sección para saber cómo utilizar las firmas electrónicas en archivos PDF.

Firmar electrónicamente un archivo PDF

El formato de documento portátil (PDF) de Adobe es un formato común para documentos de diseño fijo. Al igual que Word, Adobe PDF ha agregado una variedad de capacidades desde que se introdujo al mercado en 1993. Ahora es posible firmar electrónicamente un archivo PDF para su autenticación.

Si eres usuaria/o de Windows, probablemente estés familiarizada con los lectores de PDF. Son programas informáticos que te permiten abrir archivos PDF, es decir, archivos con la extensión de archivo .pdf. La opción más popular en estos días es Adobe Acrobat Reader.

Para agregar una firma electrónica a un PDF, sigue estos pasos:

1. Abre el archivo PDF en Adobe Acrobat Reader.
2. Haz clic en “Rellenar” y firmar” en el panel “Herramientas” a la derecha.
3. Haz clic en “Firmar” y luego selecciona “Agregar firma”.
4. Se abrirá una ventana emergente. Selecciona una opción: “Tipo”, “Dibujo”, o “Imagen”.
5. Haz clic en el botón “Aplicar”.
6. Arrastra, cambia el tamaño y coloca la firma dentro de su archivo PDF.

Servicios electrónicos

E-service (o eservice) es un término muy genérico, que generalmente se refiere a 'La prestación de servicios a través de Internet (el prefijo' e 'significa' electrónico ', como ocurre en muchos otros usos). Los servicios electrónicos incluyen todos los servicios y actividades que se crean mediante ordenadores y se ofrecen y ejecutan de forma interactiva a través de medios electrónicos, como Internet.

Los servicios electrónicos pueden ser servicios de información y educación tales como educación electrónica, aprendizaje electrónico, enseñanza electrónica, publicación electrónica, libros electrónicos, revistas electrónicas y catálogos electrónicos, adquisiciones, comercio y servicios de pedidos como: negocios electrónicos, comercio electrónico, adquisiciones electrónicas, efectivo electrónico, tienda electrónica, intermediario electrónico, subastas electrónicas, servicios culturales y administrativos como: cultura electrónica, gobierno electrónico o voto electrónico, mejora del marketing, producto, o cliente; servicios de relaciones, servicios de consultoría electrónica como: consultoría electrónica o asesoramiento electrónico, servicios relacionados con la seguridad (seguridad electrónica), servicios de producción, científicos o logísticos.
Los servicios electrónicos se utilizarán en muchas otras aplicaciones en el futuro.

¿Cómo se utilizan los servicios electrónicos?

Para utilizar los servicios, primero debes registrarte como nueva/o usuaria/o en la parte superior de cualquier página.
1. Seleccionarás el enlace "Registrarse" y completarás los campos obligatorios.
2. Al registrarte, recibirás una confirmación de que te has registrado, lo que permitirá la aplicación de cualquier servicio gubernamental en línea.

3.9. SOFTWARE DE SEGURIDAD

Cualquier dispositivo conectado puede ser una puerta de entrada a una amenaza a la seguridad. La mejor manera de proteger un dispositivo, especialmente uno conectado a Internet, es utilizar un software de seguridad adecuado y actualizado, generalmente conocido como antivirus.

Una capa adicional de seguridad de datos personales y tanto para la información transferida a través de Internet como para el dispositivo mismo, puede ser proporcionada por un conjunto especial de herramientas llamadas VPN, que significan Red Privada Virtual.

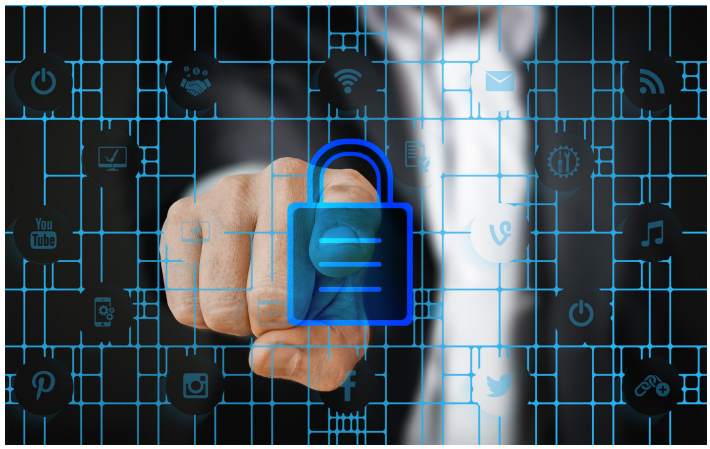
Al navegar o, especialmente, realizar transacciones financieras mientras estás conectada/o a una red WiFi no segura, las personas pueden exponerse a sí mismas y a sus datos confidenciales a una amenaza de seguridad.

Las herramientas y servicios antivirus generalmente proporcionan un conjunto de herramientas que monitorean el tráfico de Internet, escanean los archivos e intentan revelar posibles amenazas de seguridad incluso de virus desconocidos. Dichas herramientas ayudarían a evitar publicidad maliciosa, bloquear sitios web potencialmente dañinos y utilizar otras soluciones para proteger el dispositivo y la información del usuario.

Las herramientas de VPN ayudan a conectarse a Internet a través de un servidor remoto seguro, que oculta la dirección IP original de las y los usuarios, lo que permite a los usuarios cifrar su tráfico y disfrazar su identidad en línea. De esta manera, el anonimato y la seguridad aumentan mientras se navega utilizando puntos de acceso WiFi públicos u otras conexiones de red no seguras.
Algunos programas antivirus también pueden proporcionar un servicio VPN.

Software antivirus más utilizado:

- Avira
- Avats
- McAfee
- ESET
- Bitdefender
- AVG
- Kaspersky
- Microsoft security essentials
- Norton



Herramientas de VPN más utilizadas:

- Nord VPN
- Express VPN
- Surfshark
- Tunnelbear

Co-funded by the
Erasmus+ Programme
of the European Union

3.10. SEGURIDAD Y HARDWARE DE DISPOSITIVOS FÍSICOS

Todas sabemos lo molesto que es perder un teléfono, que te lo roben, o simplemente dejarlo caer al suelo y romper su pantalla a un nivel en el que el dispositivo se vuelve inutilizable. Por lo general, el problema no se considera importante hasta que ocurre. Para evitar todo tipo de daños en un dispositivo.
Hablando de seguridad física, asumimos que cualquier dispositivo podría sufrir daños físicos por caídas, fallas de hardware, daños por agua o podría perderse o ser robado.

Compilamos una lista de formas y soluciones de cómo se pueden evitar las pérdidas mediante el uso de técnicas simples de seguridad de un dispositivo físico:

Contraseña o encriptación

Evita la pérdida de información por intentos de robo. Utiliza una contraseña segura, una huella digital, u otros datos biométricos para proteger el acceso a tu dispositivo, tanto el teléfono móvil como el escritorio. Evita utilizar la misma contraseña en todas partes y bloquear o cifrar archivos importantes con contraseña. Habilita el software de rastreo incorporado o instalado que algunos proveedores brindan para poder rastrear tu dispositivo usando los servicios de ubicación, incluso si está bloqueado cuando se pierde o es robado.

Copia de seguridad

Realiza siempre una copia de seguridad de los archivos importantes, guárdalos en CD o tarjetas de memoria o incluso en un almacenamiento en la nube de terceros.

Sentido común

No tientes a los ladrones con dispositivos móviles desatendidos, especialmente en lugares públicos. No dejes la bolsa de tu ordenador portátil en el automóvil, sin vigilancia en una cafetería, aeropuerto, u otros lugares públicos.

Actualizaciones

Mantén tu software y dispositivos actualizados, instala actualizaciones en el sistema operativo cuando se te solicite.

Actúa con rapidez.

Dependiendo de la situación, si el dispositivo se pierde, no entres en pánico, comienza por cambiar tu contraseña a los sistemas más importantes, informa a tu supervisor o al departamento de TIC si el dispositivo comercial se perdió y si es necesario informa a la policía.

Venta

Si vendes un dispositivo antiguo, un teléfono, una tableta o un ordenador, asegúrate de que toda tu información personal se elimine permanentemente del disco duro o de la memoria del dispositivo. Puedes utilizar un software especial como: Eraser, File shredder, o WipeFile, u otras herramientas similares.

3.11. INTERNET DE LAS COSAS

Básicamente, una vida conectada. La idea de dispositivos interconectados donde los dispositivos son lo suficientemente inteligentes como para compartir información con nosotras, con aplicaciones basadas en la nube y entre sí (de dispositivo a dispositivo).

Los dispositivos inteligentes o "dispositivos conectados", como se les llama comúnmente, están diseñados para capturar y utilizar todos los datos compartidos o utilizados en la vida cotidiana. Y estos dispositivos utilizarán estos datos para interactuar contigo a diario y completar tareas.

El Internet de las cosas (IoT) es un sistema de dispositivos informáticos, máquinas mecánicas y digitales, objetos, animales, o personas interrelacionados que cuentan con identificadores únicos y la capacidad de transferir datos a través de una red sin requerir la interacción por ordenador de persona a persona.

Esta nueva ola de conectividad va más allá de los ordenadores portátiles y los teléfonos inteligentes, se dirige hacia automóviles conectados, hogares inteligentes, dispositivos portátiles conectados, ciudades inteligentes y atención médica conectada.

Estos dispositivos cerrarán la brecha entre el mundo físico y el digital para mejorar la calidad y la productividad de la vida, la sociedad y las industrias. Con IoT poniéndose al día, los hogares inteligentes son la característica más esperada, y las marcas ya están compitiendo con electrodomésticos inteligentes.

Los wearables son otra característica que está en segundo lugar en tendencia en Internet. Con el lanzamiento de Apple Watch y la llegada de más dispositivos, estos dispositivos conectados nos mantendrán enganchados con el mundo interconectado.

10 Aplicaciones de Internet de las cosas (IoT) en el mundo real- explicadas en videos

Aplicación	Explicación	Enlace de vídeo
1. Smart Home	Smart Home se ha convertido en la escalera revolucionaria del éxito en los espacios residenciales y se predice que las casas inteligentes se volverán tan comunes como los teléfonos inteligentes. Se promete que los productos Smart Home ahorrarán tiempo, energía y dinero.	https://youtu.be/NjYTzvAVozo
2. Wearables	Los dispositivos portátiles se instalan con sensores y software que recopilan datos e información sobre las / los usuarios. Posteriormente, estos datos se procesan previamente para extraer información esencial sobre el usuario. Estos dispositivos cubren ampliamente los requisitos de fitness, salud y entretenimiento. El requisito previo de la tecnología de Internet de las cosas para aplicaciones portátiles es ser de gran eficiencia energética o de consumo ultrabajo y de tamaño pequeño.	https://youtu.be/h8-TAqzYrno
3. Coches conectados	La tecnología digital automotriz se ha enfocado en optimizar las funciones internas de los vehículos. Pero ahora, esta atención está creciendo hacia la mejora de la experiencia en el automóvil. Un automóvil conectado es un vehículo que puede optimizar su propio funcionamiento, mantenimiento y comodidad de los pasajeros utilizando sensores a bordo y conectividad a Internet. La mayoría de los grandes fabricantes de automóviles, así como algunas nuevas empresas valientes, están trabajando en soluciones de automóviles conectados. Las principales marcas como Tesla, BMW, Apple, Google están trabajando para traer la próxima revolución en los automóviles	https://youtu.be/0HxZuQ0woLY

Aplicación	Explicación	Enlace de vídeo
4. Internet Industrial	Internet industrial es lo más nuevo en el sector industrial, también denominado Internet industrial de las cosas (IIoT). Está empoderando a la ingeniería industrial con sensores, software y análisis de big data para crear máquinas brillantes. Según Jeff Immelt, director ejecutivo de GE Electric, IIoT es un activo "hermoso, deseable e invertible". La filosofía que impulsa el IIoT es que las máquinas inteligentes son más precisas y consistentes que los humanos en la comunicación a través de datos. Y estos datos pueden ayudar a las empresas a detectar ineficiencias y problemas antes. IIoT tiene un gran potencial para el control de calidad y la sostenibilidad. Las aplicaciones para rastrear mercancías, el intercambio de información en tiempo real sobre el inventario entre proveedores y minoristas y la entrega automatizada aumentarán la eficiencia de la cadena de suministro. Según GE, la mejora de la productividad de la industria generará entre 10 billones y 15 billones de dólares en PIB en todo el mundo durante los próximos 15 años.	https://youtu.be/8NGzrtK7eV0
5. Ciudades inteligentes	La ciudad inteligente es otra poderosa aplicación de IoT que genera curiosidad entre la población mundial. La vigilancia inteligente, el transporte automatizado, los sistemas de gestión de energía más inteligentes, la distribución de agua, la seguridad urbana y el monitoreo ambiental son ejemplos de aplicaciones de Internet de las cosas para ciudades inteligentes. IoT resolverá los principales problemas a que se enfrentan las personas que viven en las ciudades, como la contaminación, la congestión del tráfico y la escasez de suministros de energía, etc. Productos como la comunicación celular habilitada para la basura Smart Belly enviarán alertas a los servicios municipales cuando sea necesario vaciar un contenedor. Mediante la instalación de sensores y el uso de aplicaciones web, los ciudadanos pueden encontrar plazas de aparcamiento gratuitas disponibles en toda la ciudad. Además, los sensores pueden detectar problemas de manipulación del medidor, fallas generales y cualquier problema de instalación en el sistema eléctrico. Para comprender mejor el funcionamiento de las ciudades inteligentes, consulte este video.	https://youtu.be/Br5aJa6MkBc

Aplicación	Explicación	Enlace de vídeo
6. IoT en agricultura	Con el continuo aumento de la población mundial, la demanda de suministro de alimentos aumenta enormemente. Los gobiernos están ayudando a las y los agricultores a utilizar técnicas e investigación avanzadas para aumentar la producción de alimentos. La agricultura inteligente es uno de los campos de más rápido crecimiento en IoT. Las y los agricultores están utilizando información valiosa de los datos para generar un mejor retorno de la inversión. La detección de la humedad y los nutrientes del suelo, el control del uso de agua para el crecimiento de las plantas y la determinación de fertilizantes personalizados son algunos de los usos simples de IoT. Si tienes curiosidad, el video a continuación explica más sobre este concepto. Lee más para conocer lo último sobre IoT en agricultura.	https://youtu.be/q0FnMD2_0Fw
7. Venta minorista inteligente	El potencial de IoT en el sector minorista es enorme. IoT brinda a las / los minoristas la oportunidad de conectarse con los clientes para mejorar la experiencia en la tienda. Los teléfonos inteligentes serán la forma en que los minoristas permanecerán conectados con sus consumidores incluso fuera de la tienda. La interacción a través de teléfonos inteligentes y el uso de la tecnología Beacon puede ayudar a los minoristas a brindar un mejor servicio a sus consumidores. También pueden rastrear los caminos de los consumidores a través de una tienda y mejorar el diseño de la tienda y colocar productos premium en áreas de alto tráfico. Mira este video para descubrir cómo el comercio minorista conectado le facilitará la vida.	https://youtu.be/gUcuqhduWao
8. Compromiso energético	Las redes eléctricas del futuro no solo serán lo suficientemente inteligentes sino también altamente confiables. El concepto de “red inteligente” se está volviendo muy popular en todo el mundo. La idea básica detrás de las redes inteligentes es recopilar datos de forma automatizada y analizar el comportamiento de las y los consumidores y proveedores de electricidad para mejorar la eficiencia y la economía del uso de la electricidad. Las redes inteligentes también podrán detectar fuentes de cortes de energía más rápidamente y en los niveles de hogares individuales, como un panel solar cercano, haciendo posible un sistema de energía distribuida. Aquí hay un video para explicar	https://youtu.be/JwRTpWZReJk

Aplicación	Explicación	Enlace de vídeo
9. "IOT" en atención médica	La atención médica conectada sigue siendo el gigante dormido de las aplicaciones de Internet de las cosas. El concepto de un sistema sanitario conectado y dispositivos médicos inteligentes tiene un enorme potencial no solo para las empresas, sino también para el bienestar de las personas en general. La investigación muestra que IoT en la atención médica será enorme en los próximos años. IoT en el cuidado de la salud tiene como objetivo capacitar a las personas para que vivan una vida más saludable mediante el uso de dispositivos conectados. Los datos recopilados ayudarán en el análisis personalizado de la salud de un individuo y proporcionarán estrategias personalizadas para combatir enfermedades. El video a continuación explica cómo IoT puede revolucionar el tratamiento y la ayuda médica..	https://youtu.be/8AkXW9EPFJg
10. IoT en la avicultura y la agricultura	El monitoreo del ganado consiste en la cría de animales y el ahorro de costos. Mediante el uso de aplicaciones de IoT para recopilar datos sobre la salud y el bienestar del ganado, las y los ganaderos que sepan antes de un animal enfermo pueden retirarlo y ayudar a prevenir una gran cantidad de ganado enfermo. Con la ayuda de los datos recopilados, las y los ganaderos pueden aumentar la producción avícola. Mira este interesante video.	https://youtu.be/eZ2sVriiluU

Co-funded by the Erasmus+ Programme of the European Union

EJEMPLOS, ESTUDIOS DE CASOS Y PRECAUCIONES PARA DESARROLLAR RESILIENCIA

4.1. VIOLACIONES DE PRIVACIDAD Y ROBO DE DATOS

¿Qué es la violación de la privacidad de los datos?

1. Una violación de datos es un incidente en el que se roba o se toma información de un sistema sin el conocimiento o la autorización del propietario del sistema. Una pequeña empresa u organización grande puede sufrir una filtración de datos.
2. Se produce una violación de la privacidad cuando alguien accede a la información sin permiso. Comienza con una brecha de seguridad (penetrar en una red informática protegida) y termina con la exposición o el robo de datos. Esos datos pueden incluir información de identificación personal, como su nombre, dirección, número de seguro social y detalles de la tarjeta de crédito.

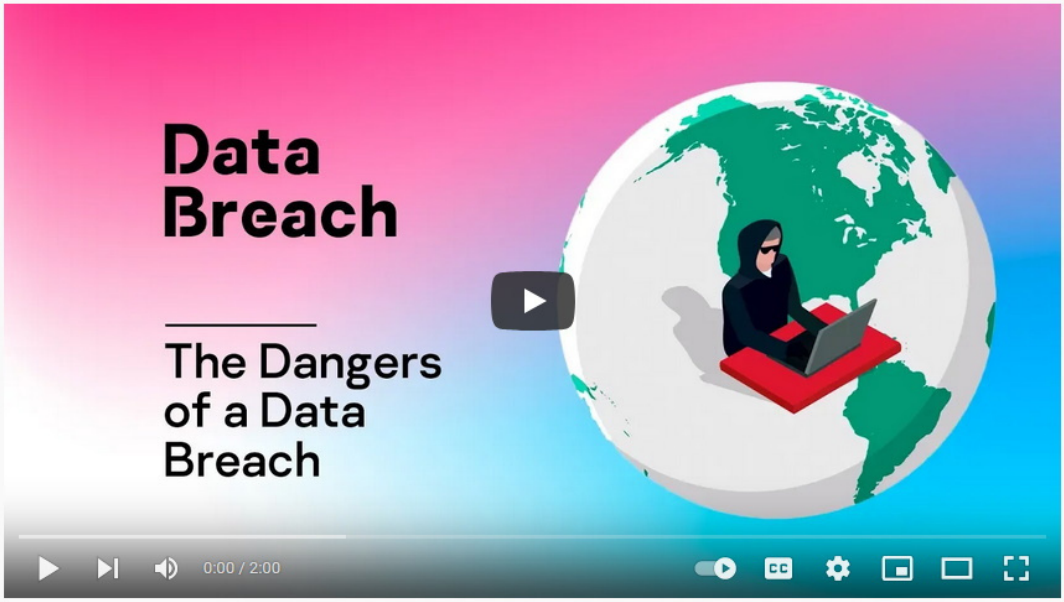
¿Cuáles son tus riesgos de privacidad?

1. La privacidad se relaciona con cualquier derecho que tengas para controlar tu información personal y cómo se utiliza esa información. Tu información está en muchos lugares. Eso incluye agencias gubernamentales, organizaciones de atención médica, instituciones financieras, plataformas de redes sociales, creadores de aplicaciones informáticas y en muchos otros lugares.
2. Tu información tiene valor. Es por eso que los ciberdelincuentes a menudo se dirigen a organizaciones donde pueden recopilar datos personales. Pueden usarlo para cometer delitos como el robo de identidad o venderlo en la web oscura.
3. ¿Alguna otra similitud entre las violaciones de la privacidad y las violaciones de datos? No hay mucho que puedas hacer para prevenirlos. La seguridad de tu información está en manos de otra persona. Aun así, hay cosas que puedes hacer para protegerte.

¿Cómo prevenir una filtración de datos?

1. Crea contraseñas complejas. Usa diferentes contraseñas para cada cuenta y cambia tus contraseñas si una empresa con la que has interactuado recientemente es pirateada.
2. Utiliza la autenticación multifactor cuando esté disponible. Esto permite el acceso solo después de que se presenten dos o más pruebas, generalmente una contraseña y un código que se envía al usuario por teléfono, mensaje de texto o correo electrónico durante el inicio de sesión.
3. Compra con tarjeta de crédito. Es posible que tengas menos responsabilidad por cargos fraudulentos de tarjetas de crédito.
4. Estate atenta/o al fraude. Si recibes un aviso sobre la violación de datos, llama a la empresa para confirmar que es legítimo, utilizando un número que sepas que es válido en lugar de un número que puede aparecer en el aviso.
5. Protégete contra el robo de identidad. A nivel mundial, el 65% de las violaciones de datos resultan en el robo de identidad, lo que lo convierte en el resultado más común.
6. Si te conviertes en víctima de un robo de identidad, comunícalo a cada compañía de tarjetas de crédito para configurar alertas de fraude y congelar tus cuentas. Luego, comunícate con su oficina local del Seguro Social para conocer los próximos pasos.

Video: The Dangers of a Data Breach https://www.youtube.com/watch?v=0kK902-ZvNM



4.2. "HACKING" Y EXTORSIÓN CIBERNÉTICA

La piratería ("Hacking") es un intento de explotar un sistema informático o una red privada dentro de un ordenador. En pocas palabras, es el acceso no autorizado o el control de los sistemas de seguridad de la red informática para algún propósito ilícito.

La extorsión cibernética es un delito en Internet en el que alguien retiene archivos electrónicos o los datos de su empresa como rehenes hasta que se les pague el rescate exigido.

Video: Cyber Extortion https://www.youtube.com/watch?v=UNCBuFJRrYk

El impacto financiero negativo de los ataques cibernéticos puede mitigarse mediante un seguro de riesgo cibernético. Es especialmente relevante para las empresas que tienen una gran granja de TI y/o administran grandes bases de datos personales. Muchas compañías de seguros ofrecen estos servicios en Lituania. La idea principal de dicho seguro es que a medida que las empresas se vuelven cada vez más dependientes de los sistemas de TI y la seguridad de los datos, y a medida que crece la cantidad de delitos en el espacio digital, es posible obtener la propiedad y la responsabilidad civil de la empresa por un cierto prima asegurada.

Las compañías de seguros suelen ofrecer cubrir no solo las pérdidas relacionadas con daños a los activos de la empresa debido a ataques cibernéticos, sino también las pérdidas causadas por la fuga de datos personales de terceros almacenados por la empresa.

El mejor ejemplo de esto es el caso de la compañía lituana de autos compartidos City Bee cuando se secuestraron 110,000 datos de usuarios.
Encuentre más at https://www.euronews.com/2021/02/17/thousands-of-citybee-users-have-their-personal-data-leaked-online.

Más sobre seguros de riesgo cibernético: https://youtu.be/F7mYEm-kx-Q (available only in Lithuanian)

4.3. ROBOS DE IDENTIDAD

El robo de identidad es el delito de obtener información personal o financiera de otra persona para usar su identidad para cometer fraude, como realizar transacciones o compras no autorizadas. El robo de identidad se comete de muchas formas diferentes y sus víctimas suelen sufrir daños en su crédito, finanzas y reputación.

El robo de identidad ocurre cuando alguien roba su información personal y credenciales para cometer fraude. Existen varias formas de robo de identidad, pero la más común es la financiera. La protección contra el robo de identidad es una industria en crecimiento que realiza un seguimiento de los informes crediticios de las personas, la actividad financiera y el uso del número de seguro social.

Video: What is Identity Theft? https://www.youtube.com/watch?v=kDFeSUUwRnA

Tipos de robo de identidad

Robo de identidad financiera: alguien usa la identidad o información de otra persona para obtener crédito, bienes, servicios o beneficios.

Robo de identidad del Seguro Socia si los ladrones de identidad obtienen tu número de Seguro Social, pueden usarlo para solicitar tarjetas de crédito y préstamos.

Robo de identidad médica alguien se hace pasar por otra persona para obtener atención médica gratuita.

Robo de identidad sintético un delincuente combina información real (generalmente robada) y falsa para crear una nueva identidad, que se utiliza para abrir cuentas fraudulentas y realizar compras fraudulentas.

Robo de identidad infantil: alguien usa la identidad de un niño para diversas formas de beneficio personal.

Robo de identidad fiscal alguien usa su información personal, incluido su número de Seguro Social, para presentar una declaración de impuestos estatal o federal falsa a su nombre y cobrar un reembolso.

Robo de identidad criminal un criminal se hace pasar por otra persona durante un arresto para tratar de evitar una citación, evitar el descubrimiento de una orden emitida en su nombre real o evitar un registro de arresto o condena.

Video: Watch Out These 8 Types of Identity Theft -
https://www.youtube.com/watch?v=EZa2um76rFY

Protección contra robo de identidad

Una forma es verificar continuamente la exactitud de los documentos personales y tratar con prontitud cualquier discrepancia. Existen varios servicios de protección contra el robo de identidad que ayudan a las personas a evitar y mitigar los efectos del robo de identidad. Por lo general, estos servicios brindan información que ayuda a las personas a proteger su información personal; monitorear registros públicos y registros privados, como informes de crédito, para alertar a sus clientes de ciertas transacciones y cambios de estado y brindar asistencia a las víctimas para ayudarlas a resolver problemas asociados con el robo de identidad. Algunas agencias gubernamentales y organizaciones sin fines de lucro brindan asistencia similar, generalmente con sitios web que tienen información y herramientas para ayudar a las personas a evitar, remediar e informar incidentes de robo de identidad. Muchos de los mejores servicios de monitoreo de crédito, también brindan herramientas y servicios de protección de identidad.

Para evitar el robo de datos personales, debe:

- Asegurar todos los documentos con información personal, como licencia de conducir, pasaporte, extractos bancarios, facturas de servicios públicos, etc.;
- Destruir documentos antiguos o innecesarios que muestren el nombre, la dirección u otra información personal de una persona

- Supervise su informe de historial crediticio y verifique periódicamente los estados de cuenta de su tarjeta de crédito y cuenta bancaria para ver si se han completado las transacciones;
- Al cambiar el lugar de residencia, informe a su banco, tarjeta de crédito, proveedor de servicios de comunicación móvil, TV/internet y otros proveedores de servicios sobre el cambio de dirección para que los mensajes y cartas con información personal no lleguen a otras personas;
- Recuerde que cuanto menos información proporcione una persona sobre sí misma, menor será el riesgo de que la información caiga en manos equivocadas;
- Cuando compre productos en línea, elija un sitio web seguro que muestre la información de contacto de la empresa, una política de privacidad clara, garantía de bienes y servicios y devoluciones;
- Al elegir un sitio web de comercio por correo electrónico, asegúrese de que aplique el cifrado de los datos enviados (certificado SSL adecuado y válido), y verifique que la dirección del sitio web comience con HTTPS.

4.4. CIBERACOSO

El ciberacoso puede definirse como un acto agresivo, intencionado y repetido realizado por un grupo o individualmente, realizado a través de medios electrónicos como teléfonos móviles o internet, contra una víctima que no puede defenderse fácilmente (Slonje, Smith y Frisén, 2013). El acoso, en general, se separa de otras conductas agresivas en base a dos aspectos; el primero es la repetición, como se menciona en la definición anterior, y el segundo es el desequilibrio de poder.

Por lo general, la intención del perpetrador no es repetir el acto abusivo, pero debido al uso excesivo de la tecnología, esto puede escaparse de su control. Por ejemplo, una imagen con contenido ofensivo puede publicarse en Internet una vez, pero en consecuencia puede ser compartida varias veces por otras personas, no por el autor inicial. De esta manera, la repetición es inevitable y la víctima experimenta muchas veces la vergüenza.

En cuanto al desequilibrio de poder en términos de ciberacoso, no necesariamente se refiere a la “debilidad” física o psicológica, sino también al desconocimiento en las TIC y / o al anonimato que ofrece el ciberespacio (Slonje, Smith y Frisén, 2013). Estudios realizados hasta el momento indican que existe una correlación entre estudiantes con conocimientos avanzados en TIC y actividades realizadas, delincuentes, en línea. En cuanto al anonimato, generalmente la víctima desconoce la identidad del perpetrador y, por lo tanto, es difícil hacerle frente de manera eficiente (Slonje, Smith y Frisén, 2013).

Motivos

Los motivos del ciberacoso se pueden dividir en dos categorías: internos y externos. Los motivos internos incluyen la ira, los celos, la voluntad de venganza o incluso el aburrimiento (Slonje, Smith y Frisén, 2013). Estos también pueden indicar problemas familiares. Además, el comportamiento de ciberacoso puede satisfacer la necesidad de imposición de poder (Nika, Gioldasi y Vitta, 2017).

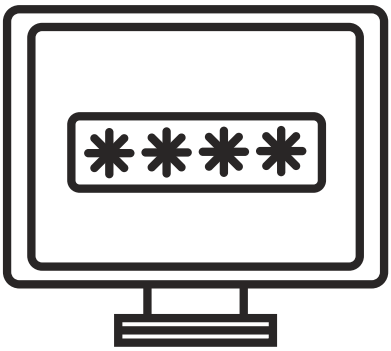
En cuanto a los motivos externos, estos pueden ser la posible ausencia de consecuencias graves contra la o el perpetrador, o el hecho de que el perpetrador puede ser reacio o temeroso de proceder en un encuentro cara a cara con la posible víctima (Slonje, Smith y Frisén, 2013).

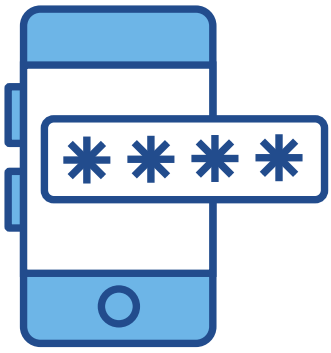
Consecuencias

1. La víctima y el agresor a veces experimentan emociones negativas como ira, tristeza, ansiedad, vergüenza, miedo, culpa a sí misma/o y falta de autoestima.
2. En cuanto al contexto escolar, se ha notado concentración afectada negativamente, bajo rendimiento académico, pero también ausencias de la escuela (Šléglová y Cerna, 2011).
3. Las víctimas pueden sentirse tan indefensas, solas, avergonzadas y desesperadas que pueden decidir suicidarse.
4. Tanto las víctimas como los agresores pueden estar socialmente marginados y, por tanto, las emociones antes mencionadas se intensifican.
5. Las víctimas pueden no intentar defenderse porque piensan que este comportamiento abusivo es “normal” o esperado o que lo merecen, al sentirse inferiores (Šléglová y Cerna, 2011).

Maneras de contrarrestarlo

1. Es realmente importante que tanto los adolescentes como los adultos estén informados y sean conscientes de la seguridad en Internet y las diferencias funcionales entre varios medios de tecnología (Olweus, 2012).
2. Otras soluciones prácticas son bloquear a personas desconocidas en las redes sociales y cambiar a menudo contraseñas y nombres de usuario.
3. Pide ayuda a una persona conocida o un experto (Slonje, Smith y Frisén, 2013). Habla sobre una mala experiencia por la que estés pasando o por la que pasaste en el pasado y comparte tus sentimientos. Esto te ayudará a sentirte más aliviada/o y te ayudará a encontrar una solución más fácilmente.
4. Los padres deben tener la mente abierta y ser esencialmente cercanos a sus hijos e hijas, para que estos se sientan libres de discutir temas como el ciberacoso y la cibervictimización.
5. Es de vital importancia, al navegar por Internet, conocer los derechos de las personas y cómo respetarlos.
6. Organizar cursos o seminarios de formación sobre ciberacoso y formas de contrarrestarlo.





Estudios de caso

Brandy Vela (1998-2016), de 18 años, estaba en el último año de la escuela secundaria y se suicidó en noviembre de 2016 después de años de acoso en persona y en línea por parte de sus compañeros en relación a su peso. Según su hermana, los acosadores crearon sitios web de citas, donde mintieron sobre su edad, publicaron su foto y usaron su número de teléfono para decirle a la gente que se está entregando por sexo gratis para llamarla. Brandy se disparó en el pecho con una pistola y murió en el hospital al día siguiente. Después de su muerte, un par de adolescentes fueron arrestados por intimidarla (colaboradores de Wikipedia, 2020).

Megan Meier (1992–2006), de 13 años, era una adolescente estadounidense de Missouri que se suicidó ahorcándose unas semanas antes de cumplir catorce años. Un año después, sus padres, tras haber realizado una investigación sobre el asunto de su suicidio, descubrieron que se le atribuía un ciberacoso a través de la red social Myspace. Las personas tenían la intención de usar los mensajes de Meier para aprender más sobre ella y luego humillarla (colaboradores de Wikipedia, 2020).

4.5. TÉCNICAS DE PHISHING

El robo de datos se llama el término inglés phishing que proviene de la pesca de contraseñas. Es una forma de fraude contra organizaciones o particulares al utilizar mensajes de correo electrónico no solicitados o páginas web falsificadas, con el objetivo de obtener claves para acceder a sistemas de información y otra información confidencial. datos.

La mayoría de las veces, los ataques de este tipo se dirigen contra clientes bancarios con el fin de averiguar sus contraseñas para conectarse a sistemas de banca electrónica o datos de tarjetas de crédito. Posteriormente, la información así obtenida puede ser utilizada en la comisión de hechos delictivos: conexiones ilegales a sistemas de información, sustracción de dinero de cuentas, o al pagar bienes con tarjetas extranjeras en el espacio electrónico.

El robo de datos se realiza de dos formas principales:

1. 1. Ponerse en contacto directamente con las personas y engañarlas para que revelen dicha información voluntariamente.
2. 2. Usar tecnologías dedicadas que copian datos de varios sitios web o dispositivos que se utilizan para navegar por Internet y / o utilizar servicios remotos.

El tipo más común de phishing es el llamado phishing engañoso. En este caso, un defraudador se hace pasar por una institución o empresa legítima (por ejemplo, agencia de gobierno, agencia de aplicación de la ley, proveedor de servicios financieros, empresa de marca reconocida, etc.) y se dirige directamente a las personas con una solicitud para completar los datos personales. El mismo correo electrónico u otro tipo de mensaje se envía a miles de personas con la esperanza de que algunas de ellas respondan.

Por lo general, dichos mensajes solicitan una reacción muy rápida, señalando que podría haber consecuencias negativas indeseables si una persona no responde a tiempo (por ejemplo, la institución tomará acciones legales, los fondos del banco de la persona podrían ser robados, el premio se otorgará a otra persona y etc.).

Muy a menudo, estos mensajes pueden contener enlaces maliciosos y / u otras referencias a sitios especiales que piden a las personas que ingresen la información solicitada allí. Tan pronto como una persona proporcione esta información en dichos sitios, estará indefensa ante el defraudador.

Las y los estafadores más avanzados pueden explotar el mecanismo de control de sesiones y secuestrar la sesión de un sitio legítimo. Cuando una persona inicia sesión en una aplicación web, el servidor establece una cookie de sesión temporal en su navegador. Los estafadores pueden robar dichas cookies de sesión o proporcionar a una persona un enlace que contenga una identificación de sesión preparada antes de que ingrese en dicha sesión de autenticación. Estas acciones permiten a los estafadores secuestrar posteriormente la sesión utilizando el mismo ID de sesión para su propia sesión de navegador.

Los métodos de suplantación de identidad también se pueden utilizar mediante la creación de tiendas electrónicas u otros sitios falsos. Para hacer que estos sitios sean más notorios, los estafadores atraen a las personas con precios bajos, entrega rápida de bienes u otros beneficios. Se utilizan varios motores de búsqueda para llegar a públicos específicos y dirigirlos a dichos sitios.

Los datos se roban mientras un individuo objetivo intenta registrarse o comprar los productos en dichos sitios. Los estafadores pueden aprovechar los sitios legítimos existentes alterando una dirección IP para que redirija a un sitio falso en lugar del sitio al que un individuo pretendía ir. El envío de enlaces u otras referencias a archivos infectados por ciertos virus también es una técnica muy popular. Dichos archivos infectan computadoras u otros dispositivos y pueden estar programados para solicitar que se vuelvan a escribir contraseñas u otras credenciales mientras se conecta a la banca en línea u otros servicios remotos solo con el fin de transferir dicha información a los estafadores.

En primer lugar, es importante comprender y ser consciente de que el phishing y el robo de datos pueden tener lugar en cualquier lugar, en cualquier forma y en cualquier momento, por lo que debe estar constantemente atento y alerta.

En segundo lugar, toma precauciones para mantener seguros los dispositivos que usas:

Utiliza herramientas y software que te ayuden a mantener tu ordenador u otro dispositivo seguro (programas antivirus, etc.). Descarga dichas herramientas o software solo de fuentes oficiales y confiables. Actualiza estas herramientas y software a tiempo.

Evita visitar sitios oscuros y poco confiables, regístrate o descarga archivos de dichos sitios. Dichos sitios pueden contener enlaces o archivos que pueden infectar tu ordenador u otro dispositivo con virus que recopilan tus datos personales.

Después de usar su cuenta personal, cierra la sesión y cierra la ventana del navegador.

Elige contraseñas seguras y seguras que constan de números, letras y otros símbolos. No utilices contraseñas fáciles de adivinar (por ejemplo, 12345, solo tu nombre o apellido o fecha de nacimiento). En caso de que tengas varias cuentas diferentes, utiliza siempre contraseñas diferentes.

Al crear cuentas o correos electrónicos, elige proveedores de servicios que utilicen sistemas de autenticación de dos factores (por ejemplo, una contraseña y un número de teléfono).

Tenga cuidado con las falsificaciones comunes en línea que imitan:
a) sitios web de correo electrónico que brindan servicio de correo (gmail.com, yahoo.com, hotmail.com, etc.);
b) sitios web sociales (facebook.com, vk.com);
c) correo electrónico, que es extremadamente popular en el extranjero. sistema de pago Paypal (paypal.com);
d) otros sitios web populares.

No haga clic en enlaces sospechosos o poco claros recibidos en correos electrónicos o que se encuentren en páginas web con contenido sospechoso.

Antes de ingresar sus datos personales en sitios web en línea, asegúrese siempre de que el sitio web no sea falso. Es necesario prestar atención al nombre de dominio y las direcciones de los enlaces en la página. Los sistemas de banca electrónica siempre utilizan un protocolo de conexión seguro SSL, la dirección debe tener HTTPS al principio y el certificado del sitio se puede verificar. La dirección de los sitios web falsos casi siempre comienza con HTTP (sin s).

En tercer lugar, ten en cuenta que las instituciones y empresas de servicios legítimas (por ejemplo, bancos u otros proveedores de servicios financieros) no solicitan a sus clientes que revelen sus contraseñas de inicio de sesión u otras credenciales. Dicha información es personal y solo tú puedes conocerla. Si dicha información llega a ser conocida por terceros, debes informar inmediatamente a estos proveedores de servicios sobre estas circunstancias y cambiar tus contraseñas u otras credenciales.

En cuarto lugar, si recibes una solicitud de información confidencial, presta atención a estas circunstancias

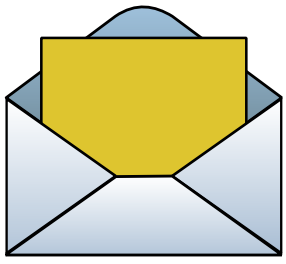
1. La dirección del remitente. Comprueba si los datos de la institución / empresa en el correo electrónico u otros mensajes coinciden con los datos publicados en sus sitios web oficiales u otras fuentes públicas. Las instituciones / empresas suelen utilizar sus buzones de correo dedicados en lugar de los buzones de correo generales disponibles públicamente (por ejemplo, @ gmail.com, @ yahoo.com, etc.).

2. Calidad y contenido del texto. Los correos electrónicos o mensajes engañosos a menudo contienen errores administrativos o de estilo. El texto puede traducirse literalmente sin seguir las reglas de ese idioma (mediante el uso de programas de traducción disponibles públicamente). El texto también puede utilizar el idioma del hogar, nombres inexactos o formas legales de instituciones o empresas (por ejemplo: una autoridad pública puede denominarse empresa). Las razones u otras circunstancias para contactarlo pueden describirse de manera que puedan adaptarse a cualquier situación (por ejemplo, supuestamente el departamento de policía te informa que tus datos de inicio de sesión en los servicios bancarios han sido robados y debes cambiar dichos datos de inicio de sesión de inmediato, pero ni siquiera nombra el banco).

3. Enlaces que se proporcionan. Los enlaces fraudulentos suelen contener una serie de números o direcciones web desconocidas. Si no estás segura/o de que un enlace sea legítimo, no hagas clic en él.

4. Probabilidad de recibir la solicitud u oferta. Debes evaluar si podrías haber esperado tal carta y si se alinea con los hechos reales o la práctica normal (por ejemplo, recibes un correo electrónico que dice que ganaste la lotería, aunque no haya participado en ninguna lotería; recibes un mensaje supuestamente de su banco, aunque nunca envíe mensajes de este tipo).

Si tienes alguna duda sobre un correo electrónico o un mensaje que recibiste, comunícate con la institución / empresa (que supuestamente te contactó) por sus datos de contacto disponibles públicamente en su sitio web oficial u otra fuente confiable.



4.6. DELITOS FINANCIEROS Y FRAUDES DE INVERSIONES

Los delitos financieros son delitos en los que las organizaciones criminales se benefician económicamente. En los delitos financieros, por lo general, una de las partes proporciona un beneficio financiero y la otra parte sufre una pérdida financiera. Estos delitos se cometen con frecuencia para el beneficio personal del delincuente e implican la conversión ilegal de la propiedad en cuestión.

Cuando hablamos de "fraude al consumidor" cuando alguien sufre una pérdida financiera que implica el uso de prácticas comerciales engañosas, injustas o falsas. En los dos últimos años, por ejemplo, el 60% de los consumidores europeos que han comprado online en un plazo de 12 meses han sufrido fraudes. A pesar de las fuertes medidas de ciberseguridad adoptadas por las instituciones financieras (bancos, empresas de pago, etc.), los estafadores se siguen saliendo con la suya explotando el eslabón más débil de la cadena: los humanos y su predilección por confiar en sus pares.

Tipos de fraude más comunes

Phishing correos electrónicos y llamadas telefónicas, en las que las y los estafadores fingen ser una institución legítima para obtener datos personales de sus víctimas.

Pharming es una redirección automática del usuario a páginas falsas operadas por estafadores con el objetivo de robar información personal confidencial como contraseñas o números de cuentas bancarias. A diferencia de otros tipos de fraude, el pharming no requiere acciones especiales por parte del usuario (víctima). En el ataque, los estafadores simplemente cambian el DNS u otras consultas automáticamente, insertando sus propios sitios web en lugar de los que el usuario (víctima) quiere.

Manipulación de dispositivos piratería de sistemas “POS” (punto de venta), cajeros automáticos. Smartphones o PC para acceder a datos y / o dinero.

Fraude de identidad uso de los datos personales de los consumidores para cancelar tarjetas de crédito, cambiar contraseñas, abrir cuentas, etc.

Ingeniería social manipulación de víctimas para obtener información confidencial.

Mulas de dinero: engañar a personas inocentes para que blanqueen dinero robado o ilegal a través de su cuenta bancaria.

Cómo evitar convertirse en víctima de un fraude financiero:

1. Revisa tu cuenta bancaria con regularidad e informa de cualquier actividad sospechosa a tu banco.

2. Ten en cuenta que tu banco nunca te pedirá información confidencial (por ejemplo, credenciales de cuenta en línea) por teléfono o correo electrónico.

3. Si crees que has proporcionado los datos de tu cuenta a un estafador, ponte en contacto con tu banco de inmediato.

4. Realiza pagos en línea solo en sitios web seguros: consulta la barra de URL para el candado y https y use solo conexiones seguras (red móvil en lugar de Wi-Fi público).

5. Si una oferta parece demasiado buena para ser verdad, casi siempre es una estafa.

6. Mantén tu información personal segura y protegida.

7. Ten mucho cuidado con la cantidad de información personal que compartes en los sitios de redes sociales. Los estafadores pueden usar tu información e imágenes para crear una identidad falsa o para atacarlo con una estafa.

8. Siempre informa a la policía de cualquier intento de fraude sospechado, incluso si no fue víctima de la estafa. El fraude de inversiones implica la venta ilegal o supuesta venta de instrumentos financieros. Los esquemas típicos de fraude de inversiones se caracterizan por ofertas de inversiones de bajo o ningún riesgo, retornos garantizados, retornos excesivamente consistentes, estrategias complejas o valores no registrados.

.

El fraude de inversión implica la venta ilegal o supuesta venta de instrumentos financieros. Los esquemas típicos de fraude de inversiones se caracterizan por ofertas de inversiones de bajo o ningún riesgo, rendimientos garantizados, rendimientos excesivamente consistentes, estrategias complejas o valores no registrados.

Tipos de fraudes de inversión:

La estafa piramidal es cuando los estafadores afirman que pueden convertir una pequeña inversión en grandes ganancias en un corto período de tiempo. Pero en realidad, los participantes ganan dinero al incorporar nuevos participantes al programa. Los estafadores detrás de estos esquemas suelen hacer todo lo posible para que sus programas parezcan esquemas legítimos de marketing multinivel.

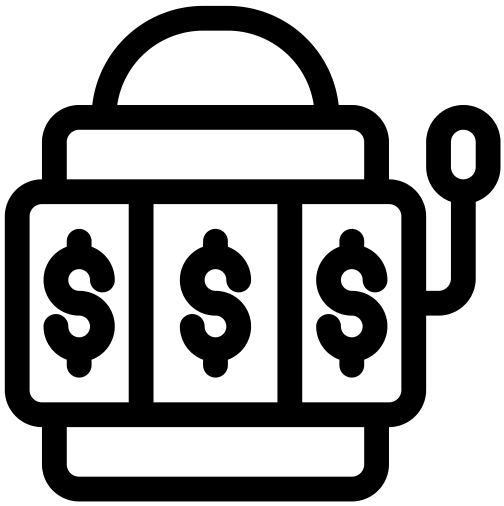
Estrafa de Ponzi es cuando un estafador o "centro" recolecta dinero de nuevos inversores y lo usa para pagar supuestos retornos a inversores en fases anteriores, en lugar de invertir o administrar el dinero como se prometió. Los esquemas piramidales Like, los esquemas Ponzi, requieren un flujo constante de efectivo entrante para mantenerse a flote. Pero a diferencia de los esquemas piramidales, los inversionistas en un esquema Ponzi generalmente no tienen que reclutar nuevos inversionistas para obtener una parte de las "ganancias".

„Pump-and-Dump“ es una estafa en la que un defraudador compra deliberadamente acciones de una acción a muy bajo precio de una empresa pequeña que cotiza en bolsa y luego difunde información falsa para generar interés en las acciones y aumentar el precio de las mismas. Se cree que se está obteniendo un buen trato con una acción prometedora; sin embargo, los inversores crean demanda de compra a precios cada vez más altos. El defraudador luego tira sus acciones al alto precio y desaparece, dejando a muchas personas atrapadas con acciones sin valor.

Advance Free Fraud es un tipo de fraude que juega con la esperanza de un inversor de poder revertir un error de inversión anterior que involucró la compra de acciones a bajo precio. La estafa generalmente comienza con una oferta para pagarle un precio tentadoramente alto por acciones sin valor. Para aceptar el trato, debe enviar una tarifa por adelantado para pagar el servicio. Pero si lo hace, nunca volverá a ver ese dinero, ni nada del dinero del trato.

Cómo evitar convertirse en víctima de un fraude de inversiones:

1. Verificar la licencia de la persona que vende la inversión.
2. Verifica que la inversión esté registrada.
3. Ten cuidado con las promesas de altas tasas de rendimiento y / o ganancias rápidas.
4. Sospecha de las ventas de alta presión.
5. Ten cuidado con las ofertas no solicitadas.
6. Solicita un prospecto o una circular de oferta.
7. Habla con un tercero.
8. Ten cuidado con las estafas en línea.



El texto del párrafo

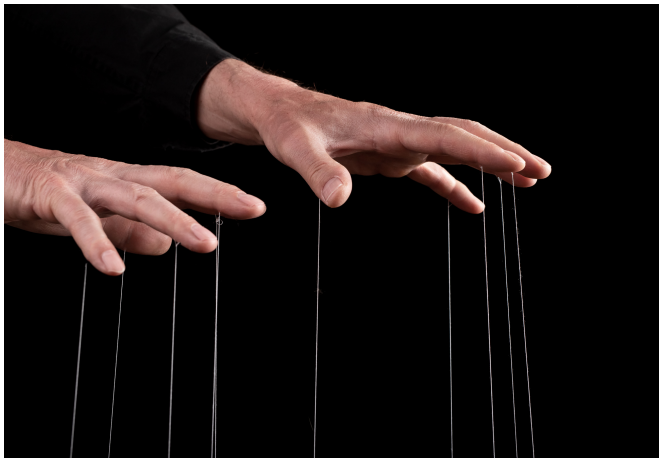
4.7. NOTICIAS FALSAS Y PROPAGANDA

La propaganda se define como la difusión deliberada y consistente de teorías e ideas en filosofía, ciencia, religión, etc., con el fin de educar a las personas que las utilizan y supone influir en las opiniones y estados de ánimo de las personas, manipular, promover ciertas acciones que contribuirían a los objetivos perseguidos por el propagandista. Es decir, la propaganda tiene como objetivo afectar las emociones y opiniones del grupo objetivo.

La eficacia de la propaganda se ve reforzada por decir parcialmente la verdad, pero no proporcionar toda la información y ocultar los hechos. Por lo tanto, reconocer la propaganda a veces puede ser difícil ya que esta presenta ciertos hechos correctos, pero cambia o distorsiona todo el contexto. Se puede comprobar la veracidad de los hechos presentados, por lo que el mensaje enviado por la propaganda parece ser cierto. Sin embargo, esto aspecto tiene la intención de ser engañoso.

La propaganda a menudo se define en un contexto negativo como un medio inaceptable basado en la desinformación para moldear la opinión pública. Los sinónimos utilizados para describir la propaganda incluyen, entre otros, mentira, engaño, distorsión, manipulación, lavado de cerebro, control del pensamiento y guerra psicológica.

Sin embargo, la propaganda también se utiliza con fines de marketing, sociales y educativos y puede funcionar en un contexto positivo, y lo más importante es para qué se utiliza. Por ejemplo, las representaciones de los prejuicios provocados por fumar en las cajetillas de cigarrillos. Se puede considerar propaganda porque tiene un intento de influir en las personas con emociones y así cambiar su comportamiento: obligarlos a dejar de fumar. Sin embargo, la propaganda se utiliza con mayor frecuencia con fines negativos para incitar al odio y la hostilidad.



La propaganda se ve constantemente afectada por cambios sociales, tecnológicos, culturales y económicos. Por lo tanto, debe adaptarse y actuar de manera acorde con la personalidad del hombre moderno. La propaganda a menudo se asocia con carteles de la Segunda Guerra Mundial, pero ahora ha adquirido una variedad de formas más sutiles. La forma en que funciona puede ser tan obvia como una esvástica o tan sutil como un comentario en un portal de noticias.

Según su objetividad, la propaganda se puede dividir en blanca, gris y negra.

Propaganda blanca

La propaganda blanca es la representación más transparente y abierta de los hechos. Se utiliza para diversos programas e iniciativas sociales y busca presentar los hallazgos de expertos independientes que reflejan puntos de vista clave.

Sin embargo, con la competencia vertiginosa entre diferentes organizaciones públicas y empresariales, cada vez es más difícil determinar la equidad del enfoque, y las opiniones de los expertos sobre los mismos temas se están volviendo muy diferentes. Por lo tanto, llamamos propaganda blanca a la intención de proporcionar explicaciones razonadas sin ningún esfuerzo por distorsionar los hechos.

La mayoría de las veces, la propaganda blanca habla de los logros del país, la empresa o la organización y se hace manera positiva. Por ejemplo, la República de Lituania se promueve de esta manera y se presenta como un puente entre Occidente y Oriente, donde existe un clima favorable a la inversión y donde se garantiza la seguridad financiera. Esto es propaganda, aunque se basa en una información proporcionada por fuentes oficiales.

Propaganda gris

Propaganda gris. Sus representantes asocian deliberadamente los hechos confirmados con los no confirmados, presentando sólo una interpretación a su favor, y deliberadamente distorsionan el contexto del hecho. La propaganda gris se utiliza intensamente en conflictos informativos, políticos o económicos guiados.

La propaganda gris se basa en un enfoque unilateral del tema, evitando la crítica. Tal propaganda, por ejemplo, afirma que el propio ejército siempre tiene la razón. Los representantes de esta propaganda evitan el diálogo abierto que puede terminar en una revelación, pero aun así no se apegan a una mentira unilateral, dejando su actitud en la oportunidad de cambiar.

La propaganda gris está muy extendida en los canales de televisión rusos ORT y RTV durante la presidencia de Vladimir Putin, cuando cualquier información sobre Putin y Rusia se presenta de manera positiva, a pesar de que el foro internacional critica fuertemente a Rusia por ciertas decisiones.

Propaganda negra

La propaganda negra se basa en la falsificación deliberada de eventos y hechos, es decir, en mentiras. Fue particularmente frecuente en la Alemania nazi, donde se utilizaron métodos de puesta en escena de eventos. Los nazis, por ejemplo, disfrazados con uniformes de soldados soviéticos, asolaron aldeas polacas, intimidando a los ciudadanos con el inminente régimen comunista y sus consecuencias.

La propaganda negra también se basa en tecnología negra. Por ejemplo, durante una eleacción, se difunde información a favor de uno de los oponentes, o se organizan eventos que luego complican mucho las posibilidades de que uno de los oponentes sea elegido. La propaganda negra y la tecnología negra están siendo perseguidas en muchas democracias.

Así, la comunicación propagandística no suele ser del todo objetiva y presenta los hechos de forma selectiva para influir en las actitudes. El lenguaje sobrecargado a menudo se usa para provocar una respuesta emocional a la información presentada en lugar de una respuesta objetiva.

En la era digital en la que vivimos ahora, este intento consciente de difundir información sesgada también tiene lugar en las plataformas digitales. Su propósito es engañar. En este sentido podemos hablar de "propaganda digital" (Bjola, 2018, p. 307).

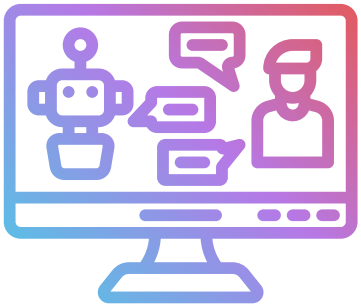
A medida que el proceso de propaganda se trasladó al espacio en línea surgieron nuevas formas de propaganda conocidas como trolls y bots. Su finalidad es influir en los resultados electorales, desmoralizar, desacreditar o aislar a los opositores políticos, participar en encuestas de opinión pública y difundir propaganda y noticias falsas.

Los trolls son decenas de miles de personas contratadas por propagandistas para trabajar todo el día (o la noche) en los portales de noticias del grupo objetivo, en las redes sociales para comentar las últimas noticias y publicaciones y así criar un referente entre los usuarios de Internet, difundir información errónea, despreciar los valores predominantes y ciertas actitudes (Grigaliūnas, 2016).

¿Cómo reconocer a un troll?

- Registros o mensajes de contenido propais;
- Errores de ortografía;
- A menudo, es una cuenta de usuario femenina;
- Pequeño número de seguidores;
- Compartir mensajes con el nombre de una persona específica, como @putin_leader;
- Afirma referirse a fuentes alternativas, pero no las indica;
- Comenta o comparte publicaciones solo sobre un tema específico.

Un bot es un programa informático que realiza automáticamente ciertas acciones que puede realizar una persona que trabaja en un ordenador. En propaganda, los bots se utilizan para escribir comentarios de propaganda en portales de noticias y publicaciones en redes sociales. Estos programas generan diferentes comentarios: se crea una plantilla y se genera un nuevo comentario a partir de esa plantilla. Los servidores proxy proporcionan diferentes direcciones IP, por lo que parece que muchas personas diferentes escriben comentarios. Por ejemplo, alrededor del 15 por ciento de los usuarios de la red social Twitter son bots.



¿Cómo reconocer un bot?

- Presta atención a la foto de perfil. Suelen ser dibujos, imágenes de la naturaleza, fotos de políticos o celebridades, o ninguna foto de perfil. Puede encontrar el origen de una foto de perfil utilizando la Búsqueda de imágenes de Google.
- Nombre de usuario largo. El nombre de usuario de muchos bots es inusual, con números o sin ningún significado.
- Contenido genérico o publicaciones o mensajes duplicados. Los bots están diseñados para dominar un tema o una etiqueta en particular en las redes sociales. Para lograr esto, un mensaje o publicación se comparte muchas veces.
- La cuenta de usuario está vacía. Las cuentas de usuario creadas por el hombre contienen una gran cantidad de información personal, la creada por bots no tiene ninguna o solo información básica.
- Los bots siguen a muchas más personas en las redes sociales que seguidores tienen.
- Los bots comparten muchas publicaciones y mensajes. Si un usuario comparte constantemente muchos registros, incluso de noche, es muy probable que se trate de un bot.
- Los bots comparten publicaciones o mensajes de contenido político radical. Suelen ser clichés ideológicos, textos patrióticos, militaristas, contra los valores y actitudes dominantes.
- Tienen muchas grabaciones estereotipadas, como sentimientos, videos con animales, etc., en la fuente de noticias del usuario. Los bots utilizan dicho contenido durante los recesos entre elecciones u otros eventos relevantes.

Puede verificar si no está siguiendo a los bots en la red social de Twitter aquí: : https://botcheck.me

Por cierto, no solo hay trolls sino también elfos. Suelen ser personas activas y cívicas que revelan diversas desinformaciones y manipulaciones, luchando contra los difusores de noticias falsas y propaganda en el espacio en línea.

Medios de influencia que pueden ser utilizados como propaganda

Generalización

La generalización es un intento de influir en las emociones mediante el uso de abstracciones y es una de las formas más simples de propaganda. Este método se utiliza a menudo durante las campañas electorales de los políticos. Este método es particularmente efectivo en tiempos difíciles, como una crisis económica. A menudo se utilizan declaraciones sumativas emocionales, como Merecemos vivir mejor; Para el futuro, el orden; Cada hombre es de suma importancia, etc.

Símbolos

Los símbolos ayudan a mejorar la imagen de uno. Por ejemplo, una persona en una fotografía está rodeada de ciertos objetos simbólicos que forman una imagen de que esa persona está promoviendo los valores simbolizados.

Etiquetado

El etiquetado es cuando una idea, acción o término negativo se asocia con una persona, organización, etc. A menudo se usa el sarcasmo o el ridículo. Esta es una forma efectiva de propaganda, porque las etiquetas adhesivas (mentirosos, terroristas, corruptos) son difíciles de eliminar.

Sentimiento de manada

El sentimiento de manada crea una imagen de que la idea tiene una aceptación generalizada, por lo que al rechazarla se corre el riesgo de quedar aislado y fuera de lugar.

Excitación emocional

La excitación emocional busca evocar emociones tan fuertes como el miedo, la ira, la tristeza y el resentimiento. El intento más común es mostrar que uno u otro fenómeno tendrá consecuencias negativas, utilizando una variedad de miedos humanos.

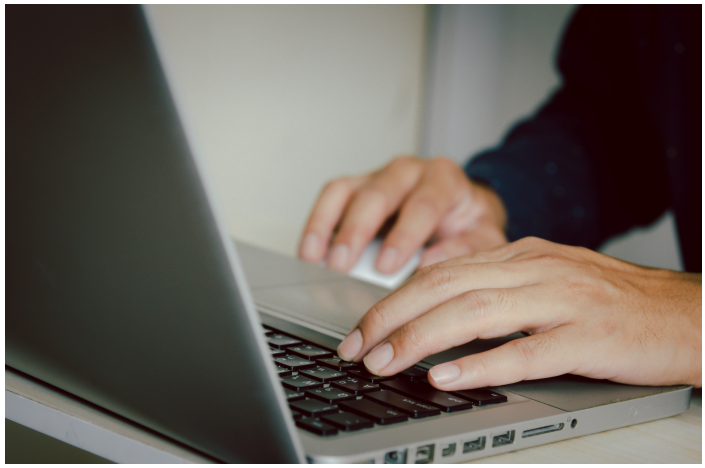
Apilamiento de cartas

El apilamiento de cartas es cuando solo se cuentan hechos positivos y se silencian los hechos negativos. Aunque los argumentos que se usan para usar esta técnica suelen ser válidos, a menudo se presentan estadísticas que pueden distorsionar la situación porque la información se saca de contexto o se omiten hechos importantes. En las campañas políticas, un candidato presenta solo el lado positivo, omitiendo el negativo.

Prueba C.R.A.P

Se puede realizar una verificación rápida de la precisión de la información en el sitio web utilizando la prueba C.R.A.P. (Currency, Reliability, Authority, and Purpose / Point of View - Actualidad, Confiabilidad, Autoridad y Propósito/Punto de Vista). Esta prueba permite conocer cuándo y en qué circunstancias se escribió el texto publicado, qué tan confiable es su autor y, finalmente, el propósito y la actitud de esta información.
(CyberWise, 2019).

Actualidad • ¿Qué tan reciente es la información? • ¿Qué tan recientemente se actualizó el sitio web? • ¿Es lo suficientemente actual para su tema?	**Fiabilidad** • ¿Qué tipo de información se incluye en el recurso? • ¿El contenido del recurso es principalmente una opinión? ¿Está equilibrado? • ¿Proporciona el creador referencias o fuentes de datos o citas?
Autoridad • ¿Quién es el creador o autor? • ¿Cuáles son las credenciales? ¿Puedes encontrar alguna información sobre los antecedentes del autor? • ¿Quién es el patrocinador? • ¿Tienen buena reputación? • ¿Cuál es el interés del editor (si lo hay) en esta información? • ¿Hay anuncios en el sitio web? Si es así, ¿están marcados claramente?	**Propósito/Punto de vista** • ¿Es esto un hecho o una opinión? ¿El autor enumera las fuentes o cita referencias? • ¿Es parcial? ¿El autor parece estar tratando de impulsar una agenda o un punto de vista en particular? • ¿El creador/autor está tratando de venderte algo? Si es así, ¿está claramente identificado?



Maneras de contrarrestar

Con tanta información disponible en todas las plataformas digitales, es fácil dejarse engañar. Los estudios muestran que aproximadamente el 75% de las personas que ven noticias falsas no pueden reconocer que en realidad son falsas.

Por tanto, una forma rápida de comprobar si un dato es real o no, es utilizando el C.R.A.P. Prueba. Averigüe si el artículo es actual, confiable, si el autor es creíble y, finalmente, el propósito y el punto de vista del artículo (CyberWise, 2019).

Definitivamente el sentido común siempre es necesario. Algunas formas de detectar noticias falsas se muestran brevemente a continuación (Cómo detectar noticias falsas, sin fecha).

- Considere la fuente: intente obtener más información sobre la fuente y considere si es creíble.
- Leer más allá: los titulares pueden ser escandalosos para obtener más clics. Busca más información sobre la historia narrada e intenta descubrir la verdad.
- Verifique el autor: ¿El autor ha realizado otras publicaciones, además de la actual? ¿Ha recibido algún comentario o juicio sobre su credibilidad?
- Fuentes de apoyo: por lo general, un sitio web enumera otros enlaces relacionados con el tema del artículo proporcionado. Compruebe si esos enlaces están realmente relacionados con el artículo inicial o simplemente son engañosos.

- Verifique la fecha: ¿La información está actualizada o se volvió a publicar?
- ¿Es una broma? En caso de que la información sea realmente extraña, podría ser una sátira. Tienes que comprobar de nuevo el autor y la fuente, para estar seguro.

- Revisa tus sesgos: Piensa si las noticias que estás leyendo, cómo influyen en tus propios sesgos. Probablemente podría rechazarlos, porque no está de acuerdo. Pero esto no hace que la noticia sea falsa.
- Pregúntele a los expertos: hay algunos sitios de verificación de hechos que puede visitar para estar seguro de la información proporcionada.

Estudios de caso

Un ejemplo de campaña de propaganda es la que tuvo lugar entre Rusia y los Estados Unidos de América, en relación con las elecciones presidenciales de 2016. La principal razón detrás de la configuración de los resultados de las elecciones fue la aparición de una variedad de noticias falsas con el fin de dirigir a los ciudadanos estadounidenses a votar para Trump.

Cambridge Analytica, una empresa que se especializa en analizar datos y construir perfiles psicológicos con fines políticos utilizando datos recopilados de usuarios estadounidenses de Facebook, compiló los perfiles electorales de miles de personas en el período previo a las elecciones presidenciales para apoyar la campaña electoral de Donald Trump.

Los usuarios de Facebook que fueron analizados se dividieron en dos categorías. El primero incluyó a los votantes que tenían la intención de votar por el oponente de Trump, mientras que el segundo incluyó a los que tenían la intención de abstenerse. Esto fue seguido por una campaña de noticias falsas dirigida sobre Hillary Clinton.

La "noticia" presentada a los votantes de primera clase tenía la intención de persuadirlos de que no votaran, mientras que las vistas en el teléfono celular de segunda clase tenían la intención de instarlos a votar por Trump. Según una encuesta de la Universidad de Stanford, el 41% de las noticias falsas en el último mes antes de las elecciones se volvieron virales. Facebook ha admitido oficialmente que 126 millones de estadounidenses, alrededor del 40% de la población total de Estados Unidos, vieron noticias y publicaciones en las redes sociales, que fueron "plantadas" por la ahora infame Agencia de Investigación de Internet, con sede en San Petersburgo (Tsompanidis, 2018).

Un ejemplo de la facilidad con la que se difunden las noticias falsas en la actualidad es el descubrimiento de nuevas recetas caseras, que se supone que matan al Covid-19, el nuevo coronavirus. Escuchamos cosas como "beber alcohol mata el virus", "beber dióxido de cloro estimula el sistema inmunológico". Estas opiniones son, al menos, peligrosas. Pero una receta que circuló rápidamente en las redes sociales fue la que apoyaba que el ajo hervido mata al Covid-19: “Buenas noticias, el coronavirus de Wuhan se puede curar con un tazón de agua de ajo recién hervida. El viejo médico chino ha demostrado su eficacia. Muchos pacientes también han demostrado que esto es efectivo. Ocho (8) dientes de ajo picado agregue siete (7) tazas de agua y deje hervir. Comer y beber el agua de ajo hervida, mejora y cura durante la noche. Me alegra compartir esto " (Spencer, 2020).

Este rumor fue tan difundido que la Organización Mundial de la Salud (OMS) lo derribó informando: “El ajo es un alimento saludable que puede tener algunas propiedades antimicrobianas. Sin embargo, no hay evidencia del brote actual de que comer ajo haya protegido a las personas del nuevo coronavirus” (Spencer, 2020).

Las mejores formas de repeler la propaganda:

- Medios de comunicación responsables e independientes;
- Deconstrucción de mitos y comunicación estratégica;
- Sociedad libre y educada;
- Desarrollar continuamente la capacidad de evaluar críticamente la información;
- Formación y fortalecimiento de la narrativa y la memoria histórica nacional.

EJEMPLO: historia lituana de Bayraktar

Cientos de lituanos recaudaron 4,7 millones en tres días y medio. para comprar el Bayraktar no tripulado en Ucrania. Este fue derribado 3,5 minutos después de su primer ascenso'.

La noticia se presenta en un ‚canal de Twitter anónimo que publica noticias ficticias'. Los comentaristas no parecieron prestar atención a este detalle y tomaron el mensaje en serio.
En mayo de 2022, cientos de lituanos se unieron para comprar un dron militar avanzado para Ucrania en su guerra contra Rusia en una muestra de solidaridad con un país compañero de la ex Unión Soviética.


Lithuania Posts English › الارشيف › Breaking News

Russian propaganda lie: Bayraktar, for whom Lithuanians raised money, has already been shot down

BREAKING NEWS Glenn Breaking News 3 months ago 190

El objetivo de 5 millones de euros se recaudó en solo tres días y medio, en su mayoría en pequeñas cantidades de entre 5 y 100 euros, para financiar la compra de un dron militar Byraktar TB2, según Laisves TV, la cadena lituana de Internet que lanzó el conducir.

El dron ha demostrado su eficacia en los últimos años contra las fuerzas rusas y sus aliados en los conflictos de Siria y Libia, y su compra está siendo orquestada por el Ministerio de Defensa de Lituania.

Historia completa en https://lithuania.postsen.com/news/7172/Russian-propaganda-lie-Bayraktar-for-whom-Lithuanians-raised-money-has-already-been-shot-down.html

Para obtener más información sobre la propaganda en la era digital y las noticias falsas, puede visitarit:
https://www.youtube.com/watch?v=5__dZBZuzZc&ab_channel=OsloFreedomForum
https://www.youtube.com/watch?v=V4o0B6lDo50&ab_channel=CyberWise
https://www.cyberwise.org/fake-news
https://www.cybercivics.com/

TAREA PRÁCTICA. Mueve al perro

Anime a los participantes de la capacitación a ver Wag the Dog / La cortina de humo, una película de comedia negra de sátira política estadounidense de 1997 producida y dirigida por Barry Levinson y protagonizada por Dustin Hoffman y Robert De Niro.

El objetivo de la actividad:
practicar y analizar las habilidades de observación personal / pensamiento crítico.

Habilidades que desarrolla la actividad:
observación crítica.

Para cuántas personas es adecuada la actividad:
trabajo individual con una discusión en grupo final

Requisito de tiempo de la actividad:
97 minutos para ver una película y hasta 15 minutos para una discusión moderada.

¿Cuántos instructores se necesitan?
Uno para moderar la discusión.

Otros requisitos de la actividad (espacio, equipamiento...):
en casa/auditorio/sesión online.

Descripción de la actividad:

-Mientras ven la película, pida a los participantes que observen cómo se desarrollan las cosas.
-Invite a los miembros del grupo a reflexionar sobre varios aspectos de la frase política 'menear al perro'.

oEn primer lugar, se puede utilizar para indicar que la atención se desvía deliberadamente de algo de mayor importancia a algo de menor importancia.

oEn segundo lugar, cuando la cola intenta mover al perro, quieres decir que una parte pequeña o sin importancia de algo se está volviendo demasiado importante y lo está controlando todo.

4.8. PUBLICIDAD FRAUDULENTA (PRODUCTOS FALSIFICADOS, SUPLEMENTOS)

Siempre que haya dinero de por medio existe la posibilidad de un fraude. Desde una perspectiva técnica, el fraude publicitario en línea ha sido un negocio relativamente fácil (y sí, lucrativo) para los estafadores y un desastre financiero para los anunciantes, editores y las propias plataformas de anuncios en línea.

El negocio de la publicidad en línea se construyó sobre una serie de tecnologías de estándar abierto de Internet que nunca pretendieron ser a prueba de fraude / estafa / robo. Como consecuencia, los estafadores publicitarios obtuvieron una gran ventaja. Según Juniper, en 2019, la industria de la publicidad en línea se enfrentaba a una impresionante pérdida de 42.000 millones de dólares debido al fraude publicitario y, lamentablemente, no hay ninguna razón para creer que la cifra será menor este año.

Para aclarar, el fraude publicitario digital es una actividad intencional que evita que los anuncios se entreguen a la audiencia o ubicación correctas. Los riesgos maliciosos que enfrentan los especialistas en marketing en la actualidad son cada vez más sofisticados y, por lo tanto, mayores de lo que se anticipaba anteriormente.

El entorno de la publicidad digital ahora involucra a miles de intermediarios, presentando una plétora de rincones oscuros en los que las y los estafadores pueden ocultar actividades delictivas. Los estafadores saben cuándo están siendo observados y se han vuelto aún más peligrosos, lo que dificulta aún más la prevención del fraude publicitario

Como resultado, el 96 por ciento de los consumidores dicen que tienen poca confianza en la publicidad digital, lo que dificulta que los especialistas en marketing demuestren que sus anuncios son legítimos. Entonces, ¿qué medidas deben tomar las organizaciones para evitar perder gran parte de su presupuesto por fraude y, con ello, la confianza de la consumidora / del consumidor?

Incluso si un pequeño porcentaje de consumidores todavía hace clic en los anuncios fraudulentos y compra productos o servicios falsos, sigue siendo una gran meta comercial y monetaria desarrollar las técnicas y los esfuerzos de marketing.

El consumidor inteligente debe asumir parcialmente la responsabilidad de mitigar el fraude en la publicidad al denunciar la falsificación y desalentar a las personas menos hábiles que lo rodean a interactuar con dichos anuncios.

¿Cómo reconocer anuncios falsos?

Es relativamente fácil una vez que se comprende y conoce el patrón:

1. La calidad de los anuncios en línea suele ser deficiente y el contenido repetitivo.
2. Reclamaciones y promesas enormes y poco realistas de ofrecer resultados bastante imposibles, ya sea para hacerse rico rápidamente o para que vuelva a crecer el cabello perdido.
3. Las páginas de destino se alojarán bajo nombres de dominio extraños, se utilizarán marcas desconocidas, fotos de celebridades o profesionales inexistentes.
4. La tipografía utilizada en las “landing pages”[1] destaca por ser colorida, muy incentivante para actuar y se ofrecen grandes descuentos.
5. La página de destino y la página de descripción del producto pueden contener una gran cantidad de críticas falsas y en su mayoría muy positivas.

[1] Nota del T. “Landing pages” = “páginas de destino” en inglés.

4.9. ADICCIÓN AL PC/ AL JUEGO Y AL CASINO EN LÍNEA

El juego es un impulso humano innato, que aparece en la primera infancia (Kuss & Griffiths, 2012, p. 5). Después del milenio, los juegos en Internet han aumentado significativamente debido al enorme desarrollo tecnológico. Los juegos de PC y, en general, los juegos en línea brindan a las y los jugadores la oportunidad de experimentar diferentes entornos de juego simultáneamente, de diseñar y desarrollar personajes virtuales con los que puedan identificarse y también de jugar con otros jugadores de todo el mundo en cualquier momento (Kuss & Griffiths, 2012, pág.5).

Además, los juegos en línea permiten a los jugadores comunicarse con otros a través del chat y, por lo tanto, formar nuevas relaciones (Kuss, 2013, p. 125). Una razón más por la que los juegos en Internet parecen tan atractivos para algunas personas es que les brinda la oportunidad de escapar de los problemas de la vida real y, de esta manera, los juegos en línea se convierten en una estrategia de afrontamiento. (Kuss, 2013, pág. 125).

Una de las categorías más famosas de juegos en línea son los juegos de rol multijugador masivo en línea (MMORPG), como “World of Warcraft”. Este tipo de juegos permite a los jugadores establecer metas y alcanzarlas, como avanzar de nivel, obteniendo así un mayor estatus virtual y poder en el entorno de juego. Las y los jugadores también pueden ser motivados debido a la admiración que pueden recibir de la comunidad de jugadores (Kuss, 2013, p. 125).

Por otro lado, los aspectos de socializar y escapar pueden predecir una adicción a los juegos en línea (Kuss, 2013, p. 125). Otras consecuencias negativas son el desconocimiento de las relaciones de la vida real, el rechazo al sueño, el trabajo y los estudios, la obsesión por el juego, la falta de atención que genera agresión y el aumento del estrés como consecuencia, dificultades con la memoria verbal y altos niveles de soledad (Kuss, 2013 , pág.125).

En algunos países, como los países del sudeste asiático, las consecuencias negativas de los juegos en línea han sido tan graves que los gobiernos tomaron medidas y tomaron medidas para reducir estos impactos negativos. Por ejemplo: en Japón, el gobierno ha reconocido la severidad de las consecuencias que conducen al desarrollo de “campamentos de ayuno”, donde las personas adictas a los juegos en línea son ayudadas al ser desconectadas totalmente de la tecnología Kuss, 2013, p. 125).

Adicción al casino en línea

El juego de casino es una actividad muy popular en todo el mundo. El entorno de los juegos de azar de los últimos quince años ha cambiado significativamente debido a la mayor disponibilidad de los juegos de azar en línea (Gainsbury, 2015, p. 190). Hoy en día, un dispositivo con acceso a Internet y un clic en un botón es todo lo que necesita para tener acceso a un entorno de juego. Además de eso, el acceso también está habilitado debido a la facilidad con la que se puede gastar el dinero a través de tarjetas de crédito, transferencias bancarias electrónicas y billeteras electrónicas.

Los casinos en línea y los juegos de azar han suscitado controversias con respecto a la posible adicción consecuente (Gainsbury, 2015, p. 190). La quinta edición del Manual diagnóstico y estadístico de los trastornos mentales (DSM-5) agregó una nueva categoría de adicción al comportamiento sin sustancias dentro del contexto de la categoría de adicción a sustancias. Para diagnosticar una adicción al juego, el individuo debe mencionar cuatro o más de los siguientes (DSM-5):

Necesita apostar con cantidades crecientes de dinero para lograr la emoción deseada.

Está inquieto o irritable cuando intenta reducir o dejar de jugar.

Ha realizado repetidos esfuerzos infructuosos para controlar, reducir o dejar de jugar.

A menudo está preocupado por los juegos de azar (por ejemplo, tiene pensamientos persistentes de revivir experiencias pasadas de juegos de azar, incapacitar o planificar la próxima aventura, pensar en formas de obtener dinero para jugar).

A menudo juega cuando se siente angustiado (por ejemplo, indefenso, culpable, ansioso, deprimido).

Miente para ocultar el grado de participación en el juego.

Ha puesto en peligro o perdido una relación, un trabajo o una oportunidad educativa o profesional importante debido al juego.

Depende de otros para obtener dinero para aliviar situaciones financieras desesperadas causadas por el juego.

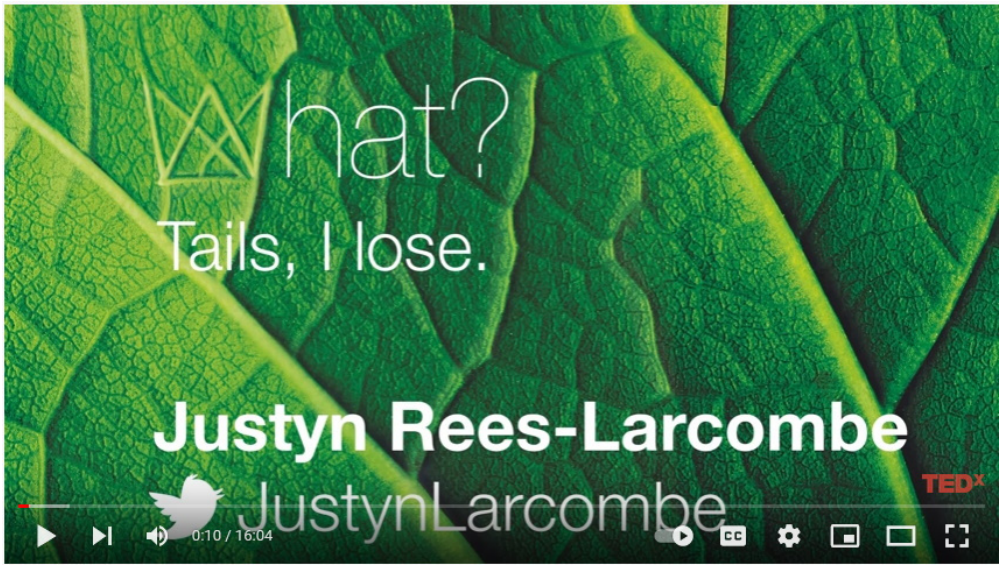
Factores de riesgo de los juegos de azar en Internet (Gainsbury, 2015, p. 190)

- Adultos más jóvenes y adolescentes mayores.
- Hombre.
- Abuso de alcohol o drogas.
- Cogniciones irracionales.
- Fuerza de voluntad para ganar dinero rápida y fácilmente.

Sin embargo, los estudios realizados hasta ahora no definen un patrón personal y de comportamiento específico para distinguir entre los jugadores con problemas de Internet y los que no los tienen.

En el siguiente enlace puedes encontrar la historia de un hombre, llamado Justyn Rees Larcombe, que se jugó 750.000 libras esterlinas y también perdió a su familia.

https://www.youtube.com/watch?v=7AN3VLLIkdI&ab_channel=TEDxTalks



Co-funded by the
Erasmus+ Programme
of the European Union

PAPEL DEL GOBIERNO E INSTITUCIONES DONDE POSTULARSE

5.1. REGULACIÓN DE PRIVACIDAD ELECTRÓNICA EN LA UE

El “ePrivacy Regulation” (ePR) es una propuesta para la regulación de varios temas relacionados con la privacidad, principalmente en relación con las comunicaciones electrónicas dentro de la Unión Europea. Su nombre completo es "Reglamento del Parlamento Europeo y del Consejo relativo al respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas” y por el que se deroga la Directiva 2002/58 / CE (Reglamento sobre Privacidad y Comunicaciones Electrónicas). Derogaría la Directiva de privacidad y comunicaciones electrónicas de 2002 (Directiva de privacidad electrónica) y sería lex specialis del Reglamento general de protección de datos. Particularizaría y complementaría este último en lo que respecta a temas relacionados con la privacidad. Los campos clave del reglamento propuesto son la confidencialidad de las comunicaciones, los controles de privacidad a través del consentimiento electrónico y los navegadores y las cookies.

El alcance del Reglamento de privacidad electrónica aún se está debatiendo. Según algunas propuestas, se aplicaría a cualquier empresa que procese datos en relación con cualquier forma de servicio de comunicación en línea y que utilice tecnologías de seguimiento en línea o participe en marketing directo electrónico.

Algunas de las disposiciones electrónicas más importantes de la regulación de privacidad que aún están en discusión:

Nuevos participantes en el mercado

El 92% de los europeos dice que es importante para ellos que el correo electrónico y los mensajes en línea se mantengan confidenciales. Sin embargo, la Directiva de privacidad electrónica actual solo se aplica a los operadores de telecomunicaciones tradicionales. Las reglas de privacidad ahora también se aplicarán a los nuevos proveedores de servicios de comunicación electrónica como WhatsApp, Facebook Messenger, Skype, Gmail, iMessage o Viber.

Reglas más estrictas

El hecho de que se proponga actualizar la directiva actual con una regulación directamente aplicable significa que todos los ciudadanos y empresas de la UE tendrán garantizada la misma protección para sus comunicaciones electrónicas, y se aplicará un conjunto común de reglas en toda la UE.

Contenido y Metadatos de las Comunicaciones

Se propone garantizar la privacidad del contenido y los metadatos (como la hora y el lugar de la llamada) de las comunicaciones electrónicas. Tanto el contenido como los metadatos de las comunicaciones electrónicas son altamente privados, y las normas propuestas exigirían que se anonimizaran o destruyeran (a menos que dichos datos se necesiten con fines de facturación) si los usuarios no dan su consentimiento para su procesamiento.

Nuevas oportunidades de negocio

Al obtener permiso para procesar datos de comunicaciones (contenido y/o metadatos), los operadores de telecomunicaciones tradicionales tendrán más oportunidades de utilizar los datos y brindar servicios adicionales. Por ejemplo, podrán producir mapas en color que muestren dónde están las personas; dichos mapas podrían ser útiles para las autoridades públicas y las empresas de transporte a la hora de preparar nuevos proyectos de infraestructura.

Reglas de cookies más simples

Se simplificaría la denominada política de cookies, que obliga a los usuarios de Internet a responder constantemente a las solicitudes para permitir el uso de cookies. Las nuevas reglas darían a los usuarios más control sobre su configuración de navegación al proporcionar una forma sencilla de aceptar o rechazar las cookies persistentes y otros identificadores si la privacidad está en riesgo. La propuesta aclara que ya no será necesario el consentimiento para las cookies no invasivas (como las cookies para recordar lo que se ha añadido al carrito de la compra) utilizadas para garantizar la comodidad de la navegación en línea. El consentimiento ya no sería necesario para las cookies utilizadas para contar los visitantes del sitio web.

Proteccion ante Correo no deseado

Entre las propuestas propuestas se encuentra un esfuerzo por establecer la prohibición de enviar mensajes no solicitados por todos los medios de comunicación electrónica, como correo electrónico o mensaje SMS, y en principio también por teléfono, si no se ha obtenido el permiso del usuario. Los Estados miembros pueden optar por utilizar la opción para dar a los consumidores el derecho a optar por no recibir llamadas de telemarketing, por ejemplo, poniendo su número en una lista de no llamar. Las personas que llaman de marketing deberán mostrar su número de teléfono o usar un código especial para identificarlo como una llamada de marketing.

Cumplimiento más efectivo

Las autoridades nacionales de protección de datos se encargarían de garantizar el cumplimiento de las normas de confidencialidad establecidas en el Reglamento.

Las sanciones propuestas por incumplimiento serían de hasta 20 millones de euros o, en el caso de una empresa, de hasta el 4% del volumen de negocios anual total mundial. Originalmente, se pretendía que el Reglamento de privacidad electrónica entrara en vigor el 25 de mayo de 2018, junto con el RGPD, pero aún no se ha adoptado.

Video:El impacto del reglamento europeo de ePrivacy
https://www.youtube.com/watch?v=Q8YFLkvEcLE

Diferencia entre regulación y directiva

1. El (nuevo) Reglamento de privacidad electrónica derogará la Directiva de privacidad electrónica (actual).

2. Contrariamente a una Directiva de la UE, un Reglamento de la UE es un acto legal de la Unión Europea que entra en vigor inmediatamente como ley en todos los estados miembros simultáneamente.

3. La actual Directiva de ePrivacy es un acto legal de la Unión Europea que requiere que los estados miembros logren un resultado particular sin dictar los medios para lograr ese resultado. Por lo tanto, se ha incorporado a las leyes y reglamentos nacionales.

4. Si el Reglamento de privacidad electrónica propuesto entrara en vigencia, estas leyes serían reemplazadas y (por razones de claridad) probablemente serán derogadas. El Reglamento de privacidad electrónica sería autoejecutable y no requeriría muchas medidas de implementación.

5.2. GDPR Y CCPA

El Reglamento general de protección de datos (GDPR) es una ley de privacidad y seguridad relativa a la protección de datos personales. Se considera datos personales cualquier información que pueda, directa o indirectamente, conducir a la identificación de un individuo (Goddard, 2017, p. 703). Los datos personales incluyen información sobre la ubicación, etnia, género, datos biométricos, creencias religiosas o cookies web. Los datos seudónimos también se pueden incluir en el contexto de los datos personales; sí, es fácil revelar la identidad de una persona. GDPR fue implementado y aprobado por la Unión Europea (UE), sin embargo, impone obligaciones a las organizaciones de todo el mundo siempre que interactúen y recopilen datos relacionados con los ciudadanos de la UE (Wolford, 2019). De esta manera, todos los residentes de la UE están protegidos de la ubicación del procesamiento de datos.

Breve mirada histórica

1950 El Convenio Europeo de Derechos Humanos declaró que "toda persona tiene derecho a proteger su vida privada y familiar"	**1995** La Directiva europea de protección de datos implementó los estándares mínimos de privacidad y seguridad de los datos	**2000** Muchas organizaciones financieras ofrecieron transacciones en línea
2006 Facebook hizo su primera aparición	**2011** Un usuario de Google procesó a la empresa por revisar sus correos electrónicos	**2016** El Parlamento Europeo pone en vigor el RGPD

Sanciones

En caso de que se infrinja el RGPD, las multas son realmente elevadas. Hay dos tipos de sanciones. La primera es una multa de unos 20 millones de euros o el 4% de los ingresos globales, y la segunda es que las personas, cuyos datos no estaban protegidos, tienen derecho a solicitar una indemnización (Wolford, 2019).

Principios de protección de datos (Wolford, 2019).

El procesamiento de datos personales debe llevarse a cabo de acuerdo con siete principios básicos:

1. Transparencia - Licitud - Equidad.
2. Limitación de la finalidad: Los datos solo deben utilizarse para las finalidades sobre las que se ha informado al/a la interesado/a.
3. Minimización de datos: debe recopilar solo los datos que sean totalmente necesarios para su propósito.
4. Exactitud: los datos deben mantenerse precisos y actualizados.
5. Limitación de almacenamiento: puede guardar los datos durante el tiempo que su propósito lo requiera.
6. Integridad y confidencialidad: El tratamiento de los datos debe realizarse de tal forma que se garantice la protección y la confidencialidad.
7. Responsabilidad: La persona que procesa los datos es la encargada de demostrar el cumplimiento del RGPD con todos los principios antes mencionados.

Consentimiento

Es obligatorio que los interesados presten su consentimiento, con el fin de permitir el tratamiento de sus datos. Pero, ¿qué constituye el consentimiento?

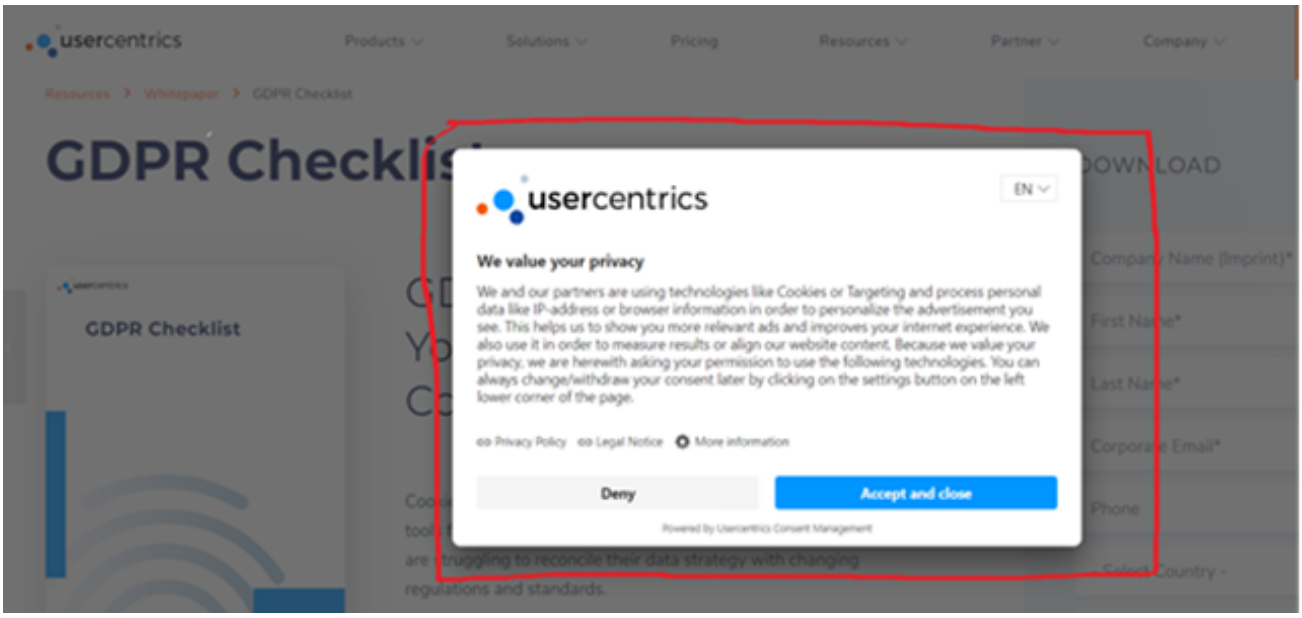
- El consentimiento debe darse libremente, ser específico e inequívoco.
- Las solicitudes de consentimiento deben ser claras, distinguibles y presentarse en palabras sencillas.
- Los interesados tienen derecho a retirar su consentimiento en cualquier momento que lo deseen.
- Cuando se trata de niños menores de 13 años, es obligatorio el permiso de los padres.
- Es necesario guardar evidencia documental del consentimiento.

Derechos de privacidad.

La persona que acepta revelar datos personales también tiene derechos de privacidad. Se enumeran a continuación (Wolford, 2019):

- El derecho a ser informado.
- El derecho de acceso.
- El derecho a la corrección.
- El derecho a la supresión.
- El derecho a limitar el procesamiento.
- El derecho a la portabilidad de datos.
- El derecho a expresar objeciones.
- Derechos en relación con la toma de decisiones automatizada y la elaboración de perfiles.

Figura 18. Un ejemplo de cómo se solicita el acceso a los datos personales a través de internet.



La Ley de Privacidad del Consumidor de California (CCPA) refuerza los derechos de privacidad y las protecciones del consumidor para los residentes de California. Es una ley del estado de California que en realidad se votó en junio de 2018, pero no entró en vigencia hasta el 1 de enero de 2020 (Cooman, 2020).

Según la CCPA, se considera que los datos personales son cualquier información que pueda conducir a la identificación de una persona (como nombre, dirección, correo electrónico, número de pasaporte, número de seguro social, etc.), información comercial (como productos comprados), actividades de redes electrónicas, audio o datos visuales y conclusiones extraídas de cualquiera de la información antes mencionada para crear un perfil sobre un consumidor que refleje sus preferencias.

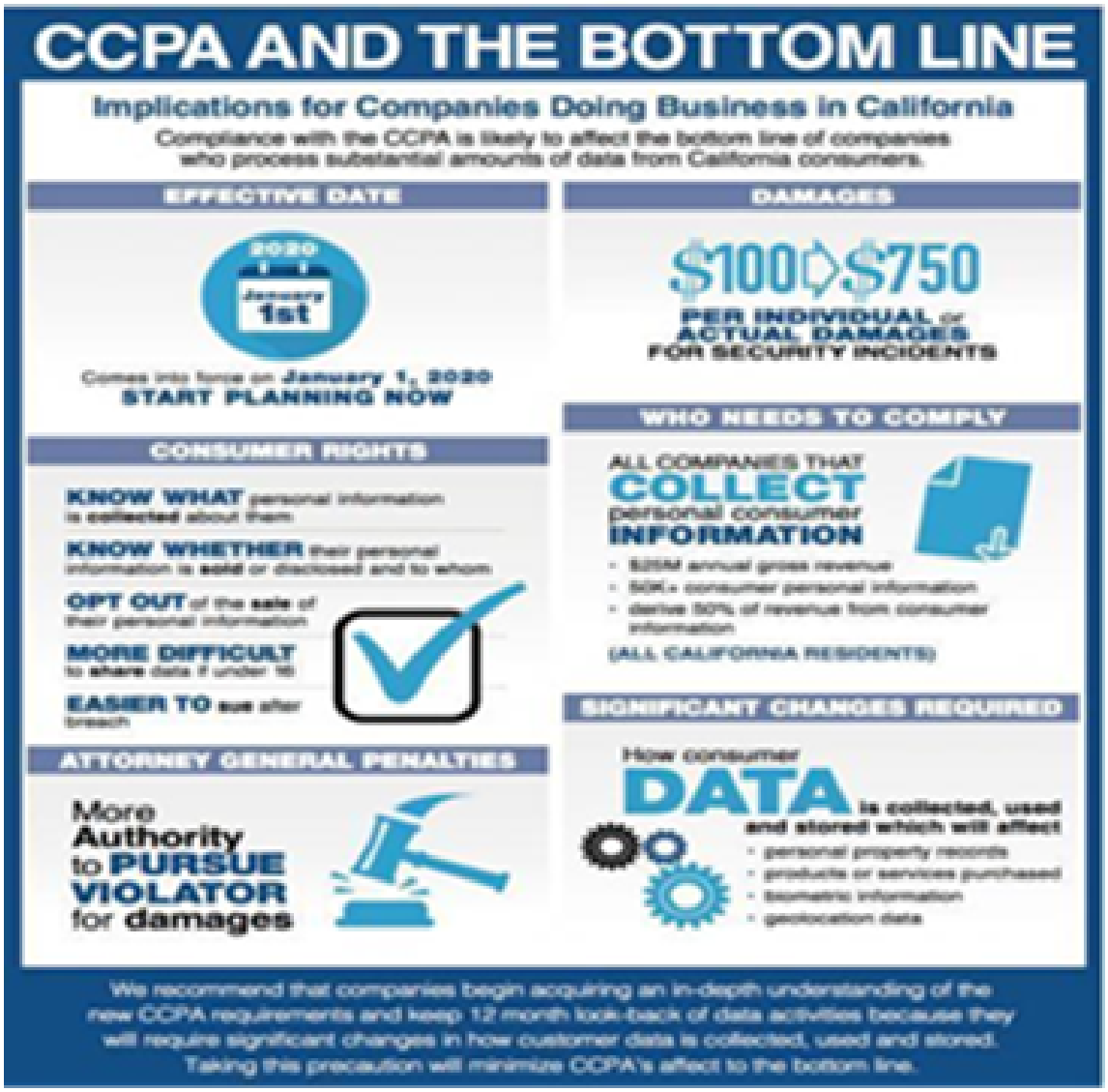
Al igual que el RGPD, la nueva ley CCPA de California consagra los derechos de las personas a obtener información de las empresas de tecnología sobre los datos que han recopilado sobre un usuario en particular y exigir que las empresas eliminen todos los datos personales del usuario.

Uno de los aspectos clave de la CCPA se ocupa de la venta de datos personales de los consumidores: la CCPA establece que los consumidores no solo tienen derecho a exigir que las empresas revelen qué datos sobre un consumidor en particular se recopilan con fines comerciales y de ventas, sino también que los consumidores pueden exigir que sus datos personales no sean vendidos.

.Objetivos de CCPA:

1. Se propietario/a de tus datos personales.
2. Controlar tus datos personales.
3. Proteger tus datos personales.
4. Responsabiliza a las grandes empresas.

Figura 19. Elementos básicos de CCPA



Principales diferencias entre GDPR y CCPA

Aunque GDPR y CCPA comparten puntos en común, no son intercambiables. Sus diferencias clave se relacionan con el alcance territorial y la aplicación de la ley, con las sanciones, en caso de violación, con la naturaleza y las limitaciones de recopilación y con el hecho de que GDPR requiere una base legal para todo el procesamiento de datos personales (A., 2021). Lo anterior se indica en la siguiente imagen (A., 2021).

5.3. AUTORIDADES ESTATALES DE PROTECCIÓN DE DATOS

Las Autoridades Estatales de Protección de Datos (DPA)[1] son autoridades públicas independientes a cargo de supervisar la implementación de las leyes de protección de datos, a través de poderes de investigación y corrección (¿Qué son las Autoridades de Protección de Datos (DPA)? 2018).

Las DPA ofrecen asesoramiento experto en materia de protección de datos y son responsables de atender las denuncias realizadas por infracciones del Reglamento General de Protección de Datos (RGPD) y las respectivas leyes nacionales. En el contexto del RGPD, todos los Estados miembros de la UE deberían tener una autoridad de protección de datos, que actúe como mediadora entre las partes interesadas dentro de ese Estado miembro (Clerck, 2019).

[1] Nota del t. DPA = "Data Protection Authorities" ("Autoridades de protección de datos" en inglés).

Autoridades estatales de protección de datos en los países socios del proyecto:

- Lituania: Inspección Estatal de Protección de Datos (https://vdai.lrv.lt/lt/)
- Austria: Autoridad de Protección de Datos de Austria (https://www.dsb.gv.at/)
- España: Agencia Española de Protección de Datos (https://www.aepd.es/es)
- Grecia: Autoridad Helénica de Protección de Datos (https://www.dpa.gr/en)
- Chipre: Oficina del Comisionado para la Protección de Datos Personales http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
- Italia: Autoridad Italiana de Protección de Datos (https://www.garanteprivacy.it)





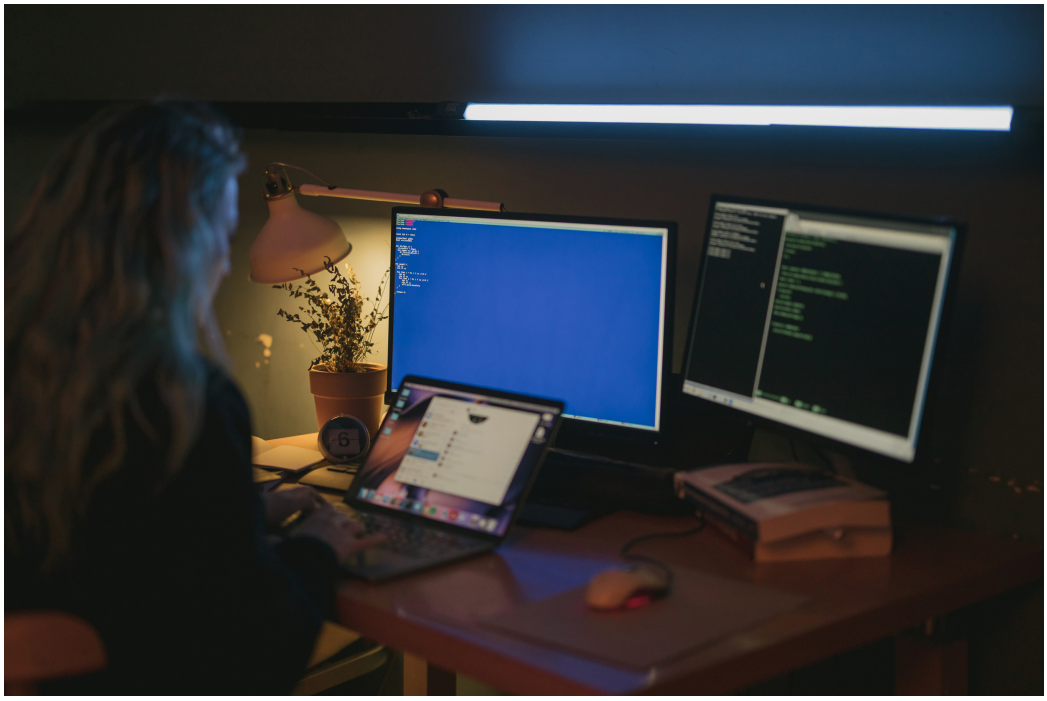

6 MODULO

Co-funded by the Erasmus+ Programme of the European Union

CREW
Creativity, Resilience and Empowerment for Work

PALABRAS FINALES

6.1. EVADA LA "CRISIS" DE MITAD DE CARRERA: MANTÉNGASE ACTUALIZADO CON LA TECNOLOGÍA



La tecnología se integra cada día más en todos los aspectos de nuestra vida. Muchas personas comparten su preocupación respecto al hecho de que el mundo está cambiando tan rápidamente y que podrían encontrarse fuera del circuito. Este es un pensamiento muy legítimo en la actualidad, más común de lo que uno supondría.

No importa en qué campo te encuentres, es particularmente importante estar al día con la tecnología para influir en tu vida personal y profesional. La tecnología ha aumentado rápidamente en las últimas décadas y las cosas que antes se pensaba que eran imposibles se están haciendo posibles a un ritmo muy rápido. Conocer los avances en tecnología es en sí mismo un placer fascinante para la mente.

También es importante familiarizarse con la nueva tecnología, porque la tecnología antigua con la que estás acostumbrada/o a trabajar se volverá obsoleta rápidamente. Obtendrás ventajas en todos los campos si tus conocimientos en tecnología están actualizados. En la siguiente sección, se presentará la importancia de mantenerse al día con las nuevas tendencias en el desarrollo de tecnología, necesarias para la vida cotidiana.

.

La tecnología nos mantiene conectados (especialmente con nuestra familia y amigos)

A medida que las familias continúan creciendo, los miembros a menudo se mudan de casa para ir a la escuela, al trabajo o para seguir a sus propias familias. Afortunadamente, con la ayuda de la tecnología, la comunicación nunca ha sido tan fácil. Ya sea a través de mensajes de texto, FaceTime o Skype, o cualquiera de los diversos sitios de redes sociales, es fácil mantenerse conectado con familiares y amigos desde lejos. Casi todas las tabletas, computadoras y teléfonos móviles modernos tienen la capacidad de usar cualquiera de las formas de comunicación anteriores para mantener a familiares y amigos conectados sin importar en qué parte del mundo se encuentren.

La tecnología te ayuda a mantenerte informado/a

La forma más rápida y asequible de conocer lo que está sucediendo en todo el país o en todo el mundo es "haciendo clic" y "desplazándose" por los portales de noticias en Internet. También puedes suscribirte al proveedor de noticias de tu elección o descargar la aplicación de teléfono móvil (en la mayoría de los casos de forma gratuita) y te permitirá recibir notificaciones sobre los eventos actuales que te mantendrán informada/o.

La tecnología mejora tu productividad

Hay muchas aplicaciones de productividad que pueden ayudarte a mantenerte productiva y organizada. Por ejemplo, "Evernote" es una aplicación de productividad que funciona como un increíble archivador. Ayuda a mantener a raya el desorden mental, ya que organiza todo para ti.

Utilización de portales de empleo como la técnica más eficaz para la búsqueda de empleo.

Hemos recorrido un largo camino desde buscar la siguiente opción de carrera en las editoriales de carrera de todos los periódicos y correr la voz sobre nuestro desempleo en circuitos cerrados de familiares y amigos solo con la esperanza de obtener una referencia antes. Sin embargo, la última sensación digital es nuestra salvación y nuestro tiempo, aquí las carreras se hacen con solo unos clics. Los portales de empleo son la última opción para todos los solicitantes de empleo que buscan comenzar, están interesados en un cambio de carrera o simplemente quieren trabajar fuera de sus viejos muros o encontrar un trabajo en general.

Servicios electrónicos que te facilitan la vida (banca en línea, por ejemplo)

No hay duda de que la digitalización ha supuesto una revolución en materia financiera. La banca en línea se realiza a través de una computadora portátil, tableta o aplicación de teléfono que ahora es la norma. Las y los usuarios del banco ahora pueden verificar sus pagos entrantes y salientes de forma remota, así como organizar transferencias de dinero y pagos de facturas. Fuera de la banca, otros asuntos financieros, como la compra y venta de divisas y acciones, pueden tratarse en línea. La transferencia de dinero entre cuentas tanto a nivel nacional como internacional también ha experimentado una gran cantidad de innovación en los últimos años.

6.2. JUEGOS Y APLICACIONES INTERACTIVOS

DUOLINGO (https://www.duolingo.com/) hte ayuda a aprender un idioma extranjero.

STUDYBLUE (https://www.studyblue.com/) ies un compañero de estudio móvil diseñado para ayudarte a "conquistar tu curso" mediante tarjetas, notas, guías de estudio y más.

TYPINGCLUB (https://www.typingclub.com/) las actividades gamificadas basadas en datos ayudan a dominar las habilidades con el teclado.

TED (https://www.ted.com/) difusión de pensamientos intrigantes o inspiradores, generalmente en videos de 18 minutos o menos.

YOUTUBE (https://www.youtube.com/) escribe las palabras "cómo..." en la barra de búsqueda de la aplicación y encontrarás de todo.

QUIZLET

(https://quizlet.com/) – ayuda de estudio flexible apoya el aprendizaje en el hogar, en la escuela y mientras viajas.

LEARN CRYPTIC CROSSWORDS

(https://www.learncrypticcrosswords.com/) – Los crucigramas crípticos no son tan crípticos una vez que comienzas a aprender algunos de los métodos para resolverlos. Esta aplicación hace un muy buen trabajo al explicar cómo abordar acertijos, poniéndote a prueba con ejercicios.

ELEVATE: BRAIN TRAINING

(https://elevateapp.com/) – El autoaislamiento no tiene por qué significar estancamiento. Las aplicaciones de entrenamiento mental como ELEVATE están diseñadas para mantener tu ingenio agudo con breves ejercicios diarios que ponen a prueba tu memoria, tus matemáticas y otras habilidades.

SKILLSHARE

(https://www.skillshare.com/) dibujo, fotografía, diseño gráfico y otras disciplinas creativas.

COURSERA

(https://www.coursera.org/) ofrece programación, arte y diseño, ciencias y negocios y otras materias a través de 3500 cursos de aprendizaje en línea, completos con video conferencias e instructores, con becarios para charlar

GOOGLE ARTS AND CULTURE

(https://artsandculture.google.com/) – viitas culturas a más 2000 "instituciones culturales" de todo el mundo, utilizando fotos, videos y realidad virtual.

Obtén más información sobre juegos y aplicaciones en:

https://bit.ly/2KOFFiK
https://bit.ly/2NA3Br9
https://bit.ly/39b33

Bibliografia

1. Wheeler, S. (2009, Ed) Connected Minds, Emerging Cultures: Cybercultures in Online Learning. Charlotte, NC: Information Age.
2. Anderson, J. (2010) ICT Transforming Education: A Regional Guide. Bangkok: UNESCO Publication
3. Kress, G. (2009) Literacy in the New Media Age. Abingdon: Routledge.
4. Van Dijk, J. (2005). The Deepening Divide. Inequality in the Information Society. London: Sage Publications
5. Carr, N. (2008) Is Google Making us Stupid? The Atlantic, July/August Issue Retrieved May 21, 2012, from
6. http://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/6868/#
7. Keen, A. (2007) The Cult of the Amateur: How Today's Internet is Killing our Culture and Assaulting our Economy. London: Nicholas Brealey.
8. International Society for Technology in Education (2007). iste.nets.s: Advancing Digital Age Learning. Iste.org/nets.
9. http://www.newmedialiteracies.org/files/working/NMLWhitePaper.pdf
10. Qiu, Jack Linchuan. 2018. "China's Digital Working Class and Circuits of Labor." Communication and the Public 3 (1): 5–18. https://doi.org/10.1177/2057047318755529.
11. Refine web searches: https://support.google.com/websearch/answer/2466433?hl=en
12. https://ec.europa.eu/digital-single-market/en/trust-services
13. Nika, D., Gioldasi, P., & Vitta, F. (2017). Cyber bullying) vs cyber stalking.
14. Olweus, D. (2012). Cyberbullying: An overrated phenomenon?. European journal of developmental psychology, 9(5), 520-538.
15. Šléglová, V., & Cerna, A. (2011). Cyberbullying in adolescent victims: Perception and coping.
16. Cyberpsychology: journal of psychosocial research on cyberspace, 5(2).
17. Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for
18. prevention. Computers in human behavior, 29(1), 26-32.
19. Savižudybių, priskirtų patyčioms, sąrašas. Vikipedija.
20. https://en.wikipedia.org/wiki/List_of_suicides_that_have_been_attributed_to_bullying
21. Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election.
22. Journal of Economic Perspectives, 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211
23. Bjola, C. (2018). The Ethics of Countering Digital Propaganda. Ethics & International Affairs,
24. 32(3), 305–315. https://doi.org/10.1017/s0892679418000436
25. CyberWise. (2019, August 10). What Is Fake News? YouTube.
26. https://www.youtube.com080/21670811.2017.1360143

Erasmus+

Co-funded by the Erasmus+ Programme of the European Union

Bibliografia

27. How to spot fake news. n.d. [Illustration].
28. https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps
29. Spencer, S. H. (2020, February 11). Fake Coronavirus Cures, Part 2: Garlic Isn't a "Cure." FactCheck.Org.
30. https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/
31. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). Defining "Fake News." Digital Journalism, 6(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143
32. Tsompanidis, G. (2018) "Translated bibliography". Propaganda from the point of view of modern international law.
33. Gainsbury, S. M. (2015). Online Gambling Addiction: The Relationship Between Internet Gambling and Disordered Gambling. Current Addiction Reports, 2(2), 185–193.
34. https://doi.org/10.1007/s40429-015-0057-8
35. Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework.
36. Journal of Substance Use, 10(4), 191–197.
37. Kuss, D. J. (2013). Internet gaming addiction: current perspectives. Psychology research and
38. behavior management, 6, 125.
39. Kuss, D. J., & Griffiths, M. D. (2012). Online gaming addiction in children and adolescents: A
40. review of empirical research. Journal of behavioral addictions, 1(1), 3-22.
41. 2019 is the Year of . . . CCPA? [Infographic]. (2019). The National Law Review. https://www.natlawreview.com/article/2019-year-ccpa-infographic
42. A. (2021, January 7). CCPA vs. GDPR – differences and similarities. Data Privacy Manager.
43. https://dataprivacymanager.net/ccpa-vs-gdpr/
44. Cooman, G. (2020, January 28). What is CCPA and why should it matter to you? Proxyclick.
45. https://www.proxyclick.com/blog/what-is-ccpa-and-why-does-it-matter-to-you#DDP
46. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 59(6), 703–705. https://doi.org/10.2501/ijmr-2017-050
47. Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? GDPR.Eu.
48. https://gdpr.eu/what-is-gdpr/
49. What are Data Protection Authorities (DPAs)? (2018, August 1). European Commission - European Commission.
50. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

Erasmus+

Co-funded by the Erasmus+ Programme of the European Union

Bibliografia

51. Clerck, J. (2019, November 25). Supervisory authorities: consistency and Data Protection Authorities (DPAs) under GDPR. I-SCOOP.
52. https://www.i-scoop.eu/supervisory-authorities-consistency-and-data-protection-authorities-dpas/
53. Allcott, H., & Gentzkow, M. (2017). Socialinė žiniasklaida ir netikros naujienos 2016 m. rinkimuose. Journal of Economic Perspectives, 31 (2), 211–236.
54. https://doi.org/10.1257/jep.31.2.211
55. Bjola, C. (2018).
56. Kovos su skaitmenine propaganda etika. Etika ir tarptautiniai reikalai, 32 (3), 305–315. https://doi.org/10.1017/s0892679418000436
57. „CyberWise“. (2019 m., rugpjūčio 10 d.). Kas yra netikros naujienos? „YouTube“. https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise
58. Kaip aptikti netikras naujienas.
59. https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps
60. Spenceris, S. H. (2020 m., Vasario 11 d.). Netikri koronaviruso vaistai, 2 dalis: česnakai nėra „gydymas“. „FactCheck.Org“.
61. https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/
62. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). „Netikrų naujienų“ apibrėžimas. Skaitmeninė žurnalistika, 6 (2), 137–153. https://doi.org/10.1080/21670811.2017.1360143
63. http://esaugumas.lt/lt/duomenu-vagystes.html
64. Gintautas Mažeikis. Metodinis leidinys „Propaganda“. Šiauliai, 2006.
65. https://atviri.emokymai.vu.lt/mod/book/tool/print/index.php?id=12
66. https://www.stuff.co.nz/technology/digital-living/68293880/japans-first-internet-fasting-camp-for-teens-a-success
67. Julius Zaleskis. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė (GDPR). Registrų centras, 2019.
68. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en
69. https://www.europarl.europa.eu/factsheets/en/home
70. https://researchguides.ben.edu/source-evaluation

Co-funded by the Erasmus+ Programme of the European Union