Guía de seguridad digital para todos

Una publicación de

cameco+

Sobre esta pubicación

Nuestras vidas profesionales y personales están cada vez más digitalizadas, lo que nos obliga a cada uno de nosotros a enfrentarnos a una realidad llena de riesgos y nuevas oportunidades.

El reto consiste en aumentar nuestra comprensión de este fenómeno para que podamos permanecer alerta sin que cunda el pánico. La necesidad del momento es identificar los recursos que ya poseemos para hacer frente a los riesgos y a cualquier crisis potencial. La pregunta, por tanto, es: ¿Cómo podemos obtener un nivel de alfabetización digital adecuado sin que cada uno de nosotros tenga que convertirse en un experto en la materia?

Esta guía está destinada a cualquier persona, ya sea empleado o no, que esté dispuesta a comprender algunos de los conceptos clave en torno a la seguridad digital. El objetivo es dar a conocer a los lectores lo que dicen los expertos y ayudarles a aplicar las mejores prácticas para proteger sus datos, información y activos.

La guía comienza con una introducción a un concepto o categoría principal (por ejemplo, las redes privadas virtuales y la seguridad de las contraseñas), seguida de recomendaciones de uso pertinentes (cómo tener contraseñas más seguras, si se debe optar por una VPN personal, etc.).

La última parte de la guía consta de recomendaciones finales, un glosario, referencias y recursos adicionales para profundizar en los temas aquí tratados.

Recomendamos dedicar al menos dos horas a este documento. Si busca un tema concreto, consulte el índice.

Por último, expresamos nuestro agradecimiento a los expertos (y a las organizaciones) que trabajan en el ámbito de la seguridad digital y comparten nuestro interés y compromiso con la promoción de la seguridad en este ámbito. Su incansable labor sigue repercutiendo y mejorando vidas en el mundo digital.

La guía ha sido diseñada y redactada por Emy Osorio Matorel, Asesora de Análisis y Estrategia Digital de CAMECO.

¡Te deseamos la mejor de las suertes en tus esfuerzos por estar digitalmente seguro!

Sobre CAMECO

El Consejo Católico de Medios de Comunicación (CAMECO) es una consultoría sin ánimo de lucro especializada en medios de comunicación en África, Asia, América Latina, Europa Central y Oriental, Oriente Medio y el Pacífico. CAMECO ofrece sus servicios a socios locales, organizaciones activas en la prestación de ayuda a los medios de comunicación y donantes, entre ellos muchas agencias confesionales.

Con nuestro trabajo, pretendemos:

- Apoyar a los donantes en la valoración y evaluación de proyectos y propuestas de medios de comunicación y comunicación, identificar los riesgos y retos relevantes, así como las oportunidades y el potencial que ofrecen.
- Asesorar a las organizaciones asociadas sobre métodos y enfoques para desarrollar, planificar, ejecutar y supervisar proyectos de medios y comunicación, y sobre las formas y medios de establecer una base financiera y organizativa sostenible.
- Concientizar sobre los métodos de investigación, participación e interacción de la audiencia para construir y fortalecer una relación entre los medios y las iniciativas de comunicación y sus grupos objetivo.

Sobre la autora

Emy Osorio Matorel es una profesional de la Comunicación Social de la Universidad de Cartagena, Colombia. Especializada en periodismo y cultura, actualmente trabaja como Asesora de Análisis y Estrategia Digital en CAMECO, y es miembro de la Asociación para la Investigación en Medios y Comunicación (IAMCR).

Durante sus estudios, Emy pasó un año en el extranjero gracias a una beca Erasmus Mundus PUEDES Acción 2 en la Universidad Aristóteles de Tesalónica, Grecia.

Ha trabajado con entidades como el Foro Mundial para el Desarrollo de los Medios (GFMD), Internews, La Silla Vacia, la Fundación Kettering, la Fundación Gabo y Women's Link Worldwide. Esto le ha permitido desarrollar su gran habilidad en periodismo, comunicación estratégica y desarrollo, proporcionándole un amplio entendimiento en varios campos asociados con los medios de comunicación.

Gracias a ello, Emy ha desarrollado experticia en el desarrollo de medios de comunicación, la defensa de la pluralidad de medios, la gestión de relaciones entre grupos de interés y la investigación social de impacto. Asimismo, está profundamente comprometida con la promoción de la inclusión digital, el fomento de la ética de la digitalización, y contribuir al crecimiento de los medios en el Sur Global, especialmente en América Latina y el Caribe.

Tabla de contenidos

Tabla de contenidos

Seguridad digital

Sobre la seguridad digital

1. ¿Qué es la seguridad digital?

La seguridad digital se refiere a una serie de herramientas y métodos destinados a salvaguardar su identidad, datos y activos en línea, incluyendo recursos como servicios web, software antivirus, tarjetas SIM de teléfonos inteligentes, biometría y dispositivos personales seguros.

En pocas palabras, se trata de las medidas y precauciones que se deben tomar para mantener a salvo la identidad en línea.

2. ¿Son la seguridad digital y la ciberseguridad lo mismo?

Según explica la OCDE, la seguridad digital se refiere a los aspectos económicos y sociales de la ciberseguridad, frente a los puramente técnicos relacionados con la aplicación de la ley penal o la seguridad nacional e internacional. En otras palabras, la seguridad digital se centra en los medios a través de los cuales usted, como individuo, puede proteger su identidad en línea, sus datos y sus activos, mientras que la ciberseguridad pretende garantizar la protección frente a las ciberamenazas que plantean los sistemas conectados a Internet, los cuales implican hardware, software y datos.

3. ¿Por qué debería preocuparte por la seguridad digital?

Nuestras vidas están cada vez más digitalizadas. Aunque esto nos está ayudando a ser más eficientes en muchos aspectos, también está aumentando los riesgos inherentes a la realidad digital, y puede que ni siquiera seamos conscientes de ellos.

Si no vigilamos de cerca nuestra identidad digital, nuestros datos y nuestros activos, podemos vernos comprometidos tanto en el mundo digital como en el real.

4. ¿Cuáles son los ejemplos de riesgos para la seguridad digital?

No toda su información personal es valiosa para los ciberdelincuentes, pero puede interesar a algunas personas corrientes con malas intenciones. Por lo tanto, los datos que más debes tratar de asegurar son:

- Información de identificación personal (incluidos nombres, números de teléfono, direcciones, correos electrónicos, direcciones IP y números de la Seguridad Social, que suelen utilizarse en robos de identidad).
- Información personal de pago (por ejemplo, números de tarjetas de crédito o débito, información de banca online y PIN, que son objetivos frecuentes de estafas de phishing).
- Información personal sobre salud (historial médico, recetas y seguro médico, que son objeto de fraudes de seguros y de estafas con medicamentos).

¿Cómo puedes mantenerte seguro digitalmente?

- **Mantente actualizado sobre el tema.** Dado que este es un campo que cambia rápidamente, es de vital importancia mantenerse informado y al día con respecto a las últimas tendencias.

  La mayoría de las revistas y periódicos cuentan con una buena sección de tecnología. Recomendamos revisar wired.com, technologyreview.com, computerworld.com, technowize.com, analyticsinsight.net y sciencefocus.com/future-technology, por mencionar algunos.

- **Considera asistir a capacitaciones en línea y presenciales**. Estas pueden ayudarte a adquirir el conocimiento y las habilidades relevantes necesarias para reconocer y mitigar las amenazas digitales de manera efectiva.

  Muchas organizaciones ofrecen capacitaciones pagadas y certificadas. Una opción en línea gratuita es el curso de Seguridad Digital para periodistas y defensores de derechos humanos, desarrollado por Meta y ICFJ.

- **Ten en cuenta tu presencia en línea.** Abordaremos temas específicos en las siguientes páginas, pero ten en cuenta que debes verificar qué aplicaciones tienes en tu teléfono, qué aplicaciones utilizas y qué información sobre ti está disponible en línea. La conciencia es un componente clave de tu capacidad para evaluar los riesgos a los que podrías enfrentarte.

- **Asegúrate de que tu software esté siempre actualizado.** Las actualizaciones de software a menudo contienen parches para vulnerabilidades conocidas.

  Los ciberdelincuentes aprovechan estas debilidades, por lo que mantener tu software actualizado ayuda a proteger contra posibles brechas de seguridad.

Ten en cuenta que proteger tus datos requiere vigilancia constante para garantizar su seguridad.

Huellas digitales

Sobre las huellas digitales

1. ¿Qué es una huella digital?

Una huella digital es un registro de todo lo que hacemos en Internet. Es lo que dejamos atrás cada vez que utilizamos Internet y constituye una especie de reflejo de quiénes somos, incluso cuando no estamos en línea.

Todo lo que hacemos en Internet (publicar, buscar o compartir) crea un rastro de datos. La gente puede utilizar este rastro para hacerse una idea de quién eres. Por eso, es importante ser consciente de lo que se hace en Internet y tomar medidas para mantener segura la información.

2. ¿Cómo funcionan las huellas digitales y por qué deberías tener cuidado con sus riesgos?

Cuando utilizamos Internet, dejamos involuntariamente un rastro de datos, similar a cómo caminamos. Los motores de búsqueda, las plataformas de redes sociales, la publicidad y otras empresas recopilan y almacenan esta información. Si bien cierta información se vuelve pública, otros aspectos permanecen privados.

Los datos de nuestras huellas digitales pueden ser utilizados para rastrear nuestro comportamiento en línea. En algunos casos extremos, esta información puede ser utilizada para crear perfiles fraudulentos.

3. ¿Cuáles son los beneficios y desventajas de tener una huella digital en línea?

Estos son algunos aspectos negativos de los que debes estar al tanto:

- Preocupación sobre la privacidad debido a la información accedida y utilizada sin tu consentimiento.
- Daño a la reputación.
- Desafios laborales derivadas de una huella digital negativa.

Dicho esto, también existen aspectos positivos, como:

- Mayor confianza, por parte de terceros, derivada de tener una presencia en línea.
- Mayor cantidad de oportunidades profesionales gracias a tener una huella digital positiva.

Sobre las huellas digitales

3. ¿Cuántos tipos de huellas digitales existen?

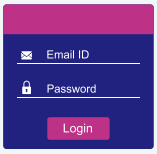
Los expertos han identificado seis (6) tipos de huellas digitales:

- **Huellas digitalmente identificables** son tu nombre, dirección postal, dirección de correo electrónico y número de teléfono, los cuales pueden ser utilizados para identificarte exactamente. Dado que comprenden los tipos de datos más sensibles, deben ser protegidos a toda costa.

- **Huellas digitales activas:** Estas son huellas que creamos a propósito. Incluyen cosas como los comentarios que dejamos en las redes sociales, las publicaciones que compartimos y las búsquedas que realizamos. Es fácil hacer un seguimiento de ellas, ya que generalmente somos conscientes de dónde están.

- **Huellas digitales pasivas:** Típicamente creadas sin nuestro conocimiento o consentimiento, estas huellas incluyen los sitios web que visitamos, los videos que vemos y los anuncios que vemos mientras estamos en línea. Debido a que generalmente no somos conscientes de tales huellas digitales creadas de forma pasiva, es más difícil mantener una huella digital positiva de este tipo.

- **Huellas de entrada de usuario:** Estas se crean cuando insertamos información como nuestro nombre de usuario, contraseña y número de tarjeta de crédito en un sitio web o aplicación. Tales huellas siempre deben protegerse porque pueden ser utilizadas para robar nuestros recursos e identidades.



- **Huellas de datos de sensores:** Los dispositivos que usamos crean tales huellas, que incluyen información sobre nuestra ubicación, edad y género. Las huellas de datos de sensores pueden ser utilizadas para rastrear nuestro comportamiento y preferencias personales.

¿Cómo proteger o borrar tu huella digital?

Si deseas proteger tu huella digital:

- Considera utilizar una VPN para ocultar y proteger tus huellas digitalmente identificables.
- Usa contraseñas fuertes y complejas, ya que dificultan que los hackers accedan a tu información.
- Ten cuidado con las redes sociales que utilizas y con la información personal que compartes y guardas en línea.
- Adhiérete a buenas prácticas de ciberseguridad (por ejemplo, utilizando software antivirus, actualizando tu software regularmente y teniendo cuidado con los sitios web que visitas).

Si deseas borrar tu huella digital:

- Desactiva y elimina tus cuentas de redes sociales para eliminar de Internet una gran parte de la información asociada contigo.
- Désuscribirse de listas de correo para evitar que guarden tu información.
- Elimina las cookies porque rastrean tus actividades en línea y recopilan información sobre ti.
- Envía una solicitud de eliminación de listado de Google si deseas eliminar tu nombre e información de contacto de los resultados de búsqueda.

Si deseas borrar tu información personal, puedes hacerlo contactando al sitio web u organización que tenga tu información y solicitándoles que la eliminen.

Servicios como Ghostery pueden ser una buena opción porque escanean Internet en busca de información sobre ti y la eliminan.

Redes privadas virtuales (VPN)

Sobre las VPN

1. ¿Qué es una VPN?

Una VPN, abreviatura de red privada virtual, protege tu conexión a internet y tu privacidad en línea. Establece un túnel de datos cifrados, protege tu dirección IP y garantiza un uso seguro de Wi-Fi público y redes abiertas.

2. ¿Cuántos tipos de VPN hay?

Existen tres tipos de redes privadas virtuales o VPN:

- **VPN de acceso remoto:** permiten a los usuarios conectarse a una red remota, frecuentemente a través de software especializado. Si alguna vez necesitaste acceder a la red de tu oficina de forma remota, probablemente utilizaste una VPN de acceso remoto. Mejora la seguridad y la conveniencia de trabajar fuera de la oficina, permitiendo a los empleados acceder a datos y recursos desde cualquier ubicación.
- **VPN de sitio a sitio:** son utilizadas principalmente por empresas, especialmente grandes corporaciones, para facilitar el acceso seguro a la red entre ubicaciones seleccionadas. Sirven como un excelente medio para interconectar todas las oficinas de la empresa, permitiendo que diferentes sucursales compartan recursos e información de manera segura.
- **VPN personales:** operan de manera similar a las VPN de acceso remoto, pero en lugar de conectarse a una red privada y restringida (como tu lugar de trabajo), te conectas a los servidores de tu proveedor de VPN para obtener seguridad y privacidad en Internet.

3. ¿Necesitas una VPN personal?

Debes tener cuidado al acceder, descargar o cargar contenido en Internet. Para garantizar la seguridad mientras navegas por la web, el uso de una VPN personal es particularmente importante cuando:

- te conectas a redes inalámbricas públicas y abiertas;
- accedes a contenido que normalmente está restringido en áreas específicas, ya sea que estés en casa o en el extranjero;
- quieres mantener tus datos personales privados (nombres de usuario, contraseñas, direcciones de correo electrónico, información de tarjetas de crédito, etc.);
- y deseas ocultar tu dirección IP.

¿Cómo puedes elegir la VPN personal adecuada?

- **Opta por una VPN paga en lugar de una VPN gratuita.** Ten en cuenta que todas las empresas necesitan ganar dinero para cubrir sus costos, por lo que las VPN gratuitas tienden a obtener ganancias mediante la publicidad y la venta de datos de sus usuarios. Además, las VPN gratuitas suelen proporcionar velocidades de conexión más lentas y menos funciones.

- **El lugar donde se encuentra tu proveedor de VPN es muy importante.** Dependiendo de las leyes de su país de origen, pueden verse obligados a recopilar y compartir datos con las autoridades, lo que puede afectar tu privacidad. Por otro lado, las VPN en lugares con menos regulaciones de datos también pueden ser arriesgadas. Por lo tanto, conocer el origen de tu VPN es importante.

- **Revisa la política de privacidad de tu VPN.** Muchas proveedores afirman que no registran ningún dato, pero la mayoría de ellas necesitan mantener algunos registros, como datos de conexión, para funcionar correctamente. Sin embargo, cierta información, como tus actividades en Internet, debería permanecer privada. Asegúrate entonces de verificar las declaraciones de tu proveedor de VPN y lee cuidadosamente su política de privacidad.

- **Investiga los proveedores que ya están en el mercado y compara las reseñas publicadas sobre ellos.** Algunos de los proveedores de VPN personal más reputados son ExpressVPN, NordVPN, Surfshark, ProtonVPN, CyberGhost, TunnelBear, Norton Secure VPN y Private Internet Access VPN.

Antes de adquirir y utilizar una VPN personal, conoce tus necesidades: ¿privacidad, contenido geo-restringido o Wi-Fi público seguro? Elige un proveedor basado en tus necesidades.

Contraseñas

Sobre las contraseñas

1. ¿Qué es una contraseña?

Es un conjunto único de caracteres utilizado como medida de seguridad para autenticar tu identidad de usuario y proteger los datos personales y el acceso al sistema contra accesos no autorizados.

2. ¿Por qué son necesarias las contraseñas fuertes?

Una contraseña fuerte y compleja será más difícil de vulnerar. Para crear una contraseña segura, el sitio web, plataforma o aplicación requerirá que utilices palabras, frases y fechas inusuales, o combinaciones de letras, números y símbolos.

Por ejemplo, las peores contraseñas que podrías crear serían aquellas que contienen tu nombre, el nombre de un objeto común o un lugar que aprecias, o tu fecha de nacimiento.

3. ¿Cómo descifran las contraseñas los hackers?

Utilizan una variedad de métodos, como:

- Método de diccionario: los hackers utilizan software que prueba palabras de un diccionario como contraseñas, lo que hace que las palabras comunes sean riesgosas.
- Fuerza bruta: software de hacking sofisticado que intenta varias combinaciones de palabras y caracteres, alimentado por aprendizaje automático e inteligencia artificial.
- Ataques de tabla arcoíris y análisis de red: los ciberdelincuentes utilizan estos métodos para hacer coincidir contraseñas con claves de descifrado o interceptar datos de red para la extracción de información.
- Phishing e ingeniería social: el phishing descarga malware a través de enlaces, mientras que la ingeniería social engaña a los usuarios para que revelen credenciales de inicio de sesión.
- Spidering: los criminales se hacen pasar por contratistas o clientes, entablando conversaciones para obtener información sobre las redes de la empresa o sistemas vitales.

Sobre las contraseñas

4. ¿Existen muchos tipos de contraseñas?

En términos generales, existen solo dos tipos de contraseñas: débiles y fuertes. Sin embargo, algunos expertos las subcategorizan de la siguiente manera:

Contraseñas débiles:

- **Simples.** Podría ser una palabra común del diccionario. Es importante entender aquí que agregar un dígito a una palabra común no mejoraría la seguridad de la contraseña. Por lo tanto, «commun1cation» será tan débil como «communication».
- **Fáciles de adivinar.** Estas contraseñas típicamente incluirían un nombre o término que podría estar vinculado a ti con un poco de investigación. Si tu contraseña actual es, por ejemplo, tu dirección de calle, el nombre de tu hijo o mascota, o tu cantante favorito, podrías ser hackeado bastante fácilmente.
- **Fechas.** Tu cumpleaños, tu número favorito o tu aniversario de bodas, por mencionar algunos, no son materiales para contraseñas seguras. Podrían ser adivinados por los hackers en cuestión de minutos.
- **Contraseñas universales.** Sería una única contraseña que utilizas en múltiples sitios web. La contraseña en sí misma puede ser muy fuerte y segura, pero no puedes estar seguro de la seguridad de los sitios o plataformas donde la utilizas. Si un sitio es hackeado, los atacantes tendrán acceso a esta contraseña universal tuya y la usarán para acceder a tus otras cuentas.

Contraseñas fuertes

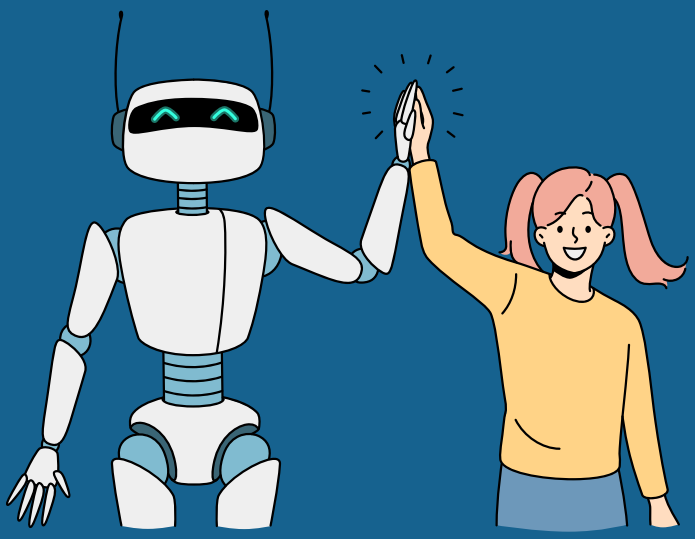
- **Alfanuméricas.** Una contraseña fuerte contendría letras y números. También podría incluir caracteres especiales, lo que aumentaría su efectividad. El uso de palabras aleatorias aumenta aún más la fuerza de la contraseña. (Por ejemplo, r3M3mB3R tH!$?)
- **Aleatorias.** Podría ser aún mejor crear contraseñas utilizando caracteres aleatorios, que no formen ninguna palabra, frase o oración. Esto haría extremadamente difícil, si no imposible, descifrar tales contraseñas.
- **Basadas en patrones.** Puedes idear una contraseña única utilizando patrones de teclado. Este tipo de contraseña no requerirá que recuerdes una combinación de símbolos. En su lugar, utilizarás caminos de teclado memorables para crear una contraseña aleatoria que realmente puedas recordar.

¿Cómo reforzar tus contraseñas?

- **Evita contraseñas comunes y ordinarias.** El uso de contraseñas fácilmente adivinables como «123456» o «contraseña» pone en riesgo tus cuentas. En su lugar, crea contraseñas únicas y complejas.
- **Nunca uses la misma contraseña para múltiples sitios.** Reutilizar contraseñas significa que si una cuenta se ve comprometida, todas las cuentas vinculadas se vuelven vulnerables. Mantén tus contraseñas privadas y no las compartas con nadie. Compartir contraseñas, incluso con personas de confianza, puede provocar violaciones de seguridad. Mantén tus contraseñas confidenciales.
- **Considera el uso de generadores de contraseñas.** Pueden crear contraseñas fuertes y aleatorias que son difíciles de adivinar para los hackers.
- **Considera el uso de un administrador de contraseñas confiable.** Ayudan a almacenar y organizar contraseñas de manera segura. Solo necesitas recordar una contraseña maestra para acceder a todas las demás.
- **Acostúmbrate a cambiar contraseñas.** Cambiar regularmente las contraseñas añade una capa adicional de seguridad. Evita el acceso no autorizado, incluso si alguien ha descubierto una contraseña antigua.
- **Considera el uso de administradores de contraseñas.** Almacenar contraseñas en lugares inseguros como notas adhesivas o documentos de Word es riesgoso. Los administradores de contraseñas ofrecen una alternativa más segura y organizada.
- **Emplea métodos de seguridad adicionales.** La autenticación de dos factores (2FA), la autenticación multifactor (MFA) y las contraseñas de un solo uso (OTP) agregan capas adicionales de protección a tus cuentas al requerir más que solo una contraseña para acceder.

Practica una mejor higiene de contraseñas utilizando una contraseña única y compleja para cada cuenta que tengas. Un gestor de contraseñas puede ayudar a generarlas y almacenarlas. Finalmente, habilita un método de identificación adicional siempre que esté disponible.

Inteligencia artificial generativa (IA generativa)



Inteligencia artificial generativa

1. ¿Qué es la Inteligencia artificial generativa ?

La inteligencia artificial generativa se refiere a modelos de aprendizaje profundo con la capacidad de crear texto, imágenes y contenido diverso de alta calidad utilizando el conocimiento adquirido de su entrenamiento. Ejemplos conocidos incluyen ChatGPT, Bard, DALL-E, Midjourney y DeepMind.

2. En términos simples, ¿cómo funciona la IA generativa?

La inteligencia artificial generativa, al igual que todos los modelos de aprendizaje profundo, puede procesar datos en bruto y conjuntos extensos como Wikipedia. A través de dicho procesamiento, puede aprender cómo producir salidas estadísticamente probables en respuesta a solicitudes específicas.

Estos modelos generativos básicamente codifican una versión simplificada de los datos en los que fueron entrenados y los utilizan para crear nuevo contenido que se asemeje, aunque no sea idéntico, al conjunto de datos original.

3. ¿Los modelos de IA generativa son nuevos?

Para nada. Estos han sido utilizados durante años en estadísticas para analizar datos numéricos. El surgimiento del aprendizaje profundo, sin embargo, ha hecho posible extender el uso de tales modelos a imágenes, voz y otros tipos de datos complejos.

4. ¿Cuáles son los nuevos riesgos que la inteligencia artificial generativa podría traer a la seguridad digital?

- **Engañar a las víctimas.** La inteligencia artificial generativa crea imitaciones convincentes de texto, videos, grabaciones de voz e imágenes, lo que permite que estafas y deepfakes difundan información falsa y engañen a las víctimas.
- **Crear malware mejorado y más sofisticado.** Las herramientas impulsadas por inteligencia artificial automatizan tareas, imitan el comportamiento humano y aprenden de ataques pasados, lo que dificulta la detección y defensa contra el malware.
- **Explotar vulnerabilidades de aplicaciones.** Los posibles backdoors de códigos generados por IA son inciertos. Si la IA puede rastrear exploits conocidos, puede crear ataques adaptativos que son difíciles de contener.
- **Seguridad de datos.** La mayoría de las inteligencias artificiales generativas carecen de garantías de privacidad de datos, lo que ha llevado a críticas y escrutinio regulatorio, como se vio en la prohibición temporal de ChatGPT debido a problemas de privacidad.

¿Cómo puedes reforzar tu seguridad digital en medio del auge de la IA generativa?

- Mantente informado sobre los avances en la inteligencia artificial generativa y sus posibles riesgos. Comprender la tecnología es el primer paso para proteger tu organización y a ti mismo.

- Ten cuidado con los deepfakes porque la inteligencia artificial generativa puede crear videos y audio deepfake convincentes.

- Verifica la información cruzando datos de múltiples fuentes confiables, especialmente en casos donde existe la posibilidad de desinformación generada por inteligencia artificial.

- Protege tus datos personales utilizando contraseñas fuertes y únicas, habilitando la autenticación de dos factores y monitoreando tus cuentas en línea en busca de cualquier actividad inusual.

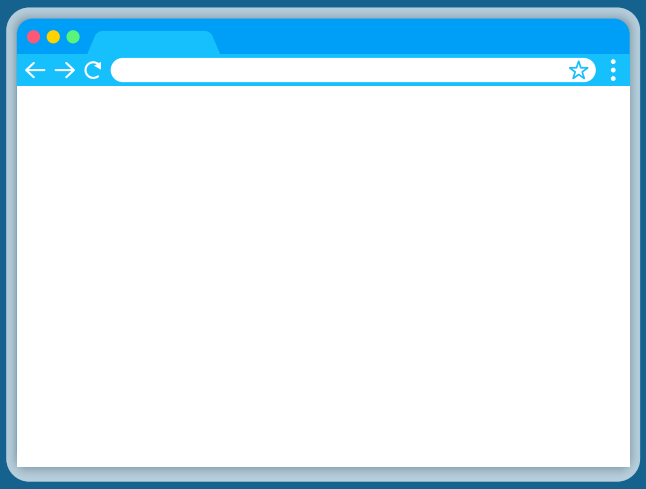
- Utiliza plataformas de redes sociales y comunicación confiables que inviertan en herramientas de detección de inteligencia artificial para combatir el contenido falso.

- Reporta contenido sospechoso generado por inteligencia artificial utilizado para fines dañinos a las plataformas y autoridades relevantes.

- Actualiza tus configuraciones de privacidad revisando y ajustando regularmente las configuraciones de privacidad en tus cuentas en línea para controlar la información que compartes.

Manteniéndote vigilante y adaptando tus prácticas de seguridad digital al panorama en constante evolución de la inteligencia artificial generativa, puedes protegerte mejor de posibles amenazas.

Navegadores o «browsers»



Sobre los navegadores

1. ¿Qué son los navegadores?

Los navegadores son aplicaciones de software que permiten a los usuarios buscar y acceder a información en Internet. Estos presentan contenido de páginas web en varios dispositivos como computadoras, tabletas o dispositivos móviles conectándose a páginas web a través de hiperenlaces identificados con identificadores uniformes de recursos (URI).

La mayoría de los navegadores muestran texto, imágenes y gráficos de Internet. Sin embargo, ciertos navegadores pueden requerir «complementos» adicionales, que integran funcionalidades adicionales en una aplicación de computadora independiente, para manejar contenido multimedia como audio y video.

2. ¿Qué tan seguros son los navegadores web?

Los navegadores suelen configurarse para la comodidad del usuario, a veces comprometiendo la seguridad del usuario. Por lo tanto, es crucial utilizar un navegador web seguro,pues usar uno inseguro puede exponer a los usuarios a riesgos como piratería informática, robo de datos, seguimiento, *malware* y otras amenazas.

Dicho eso, es importante tener en cuenta que incluso un navegador seguro no proporciona seguridad absoluta. Un paso valioso es adoptar buenas prácticas de higiene web. Adicionalmente, es recomendable mejorar la protección a través de capas adicionales de seguridad.

3. ¿Cuáles son los principales desafíos a los que te puedes enfrentar a través del navegador que utilizas?

- **Ataques de intermediarios.** Los ciberdelincuentes pueden interceptar la comunicación entre el usuario y un sitio web, lo que lleva al robo de datos sensibles o la inyección de contenido malicioso.
- **Robo de credenciales.** Los actores maliciosos pueden intentar robar credenciales de inicio de sesión a través de diversos medios, como sitios de phishing o keyloggers, comprometiendo cuentas de usuario e información sensible.
- **Secuestro de navegador.** Los usuarios pueden instalar sin saberlo secuestradores de navegador que alteran la configuración del navegador, redirigen el tráfico o insertan anuncios no deseados, afectando la experiencia de navegación en general y comprometiendo potencialmente la seguridad.
- **Ataques de ingeniería social.** Consiste en emplear técnicas de ingeniería social para engañar a los usuarios y que realicen acciones que comprometan su seguridad digital, como descargar archivos maliciosos o revelar información sensible.
- **Rastreo de datos y creación de perfiles.** Algunos sitios web y rastreadores de terceros recopilan datos de usuario con fines publicitarios y de creación de perfiles, comprometiendo la privacidad.
- **Descargas automáticas.** Visitar sitios web comprometidos o maliciosos puede resultar en descargas no deseadas de malware, lo que representa un riesgo para el dispositivo y los datos del usuario.

¿Cómo proteger tu navegador?

No importa qué navegador elijas para tus dispositivos, asegúrate de seguir estas recomendaciones de seguridad:

- Mantén actualizado tu navegador web. La mayoría de los navegadores conocidos reciben actualizaciones regularmente para corregir errores, añadir nuevas funcionalidades y parchar vulnerabilidades de seguridad.
- Utiliza la menor cantidad posible de extensiones. Cuantas más extensiones uses, mayor será la probabilidad de que tu información se vea comprometida.
- Instala un bloqueador de anuncios fiable. Estos bloquean anuncios maliciosos, varias molestias, amenazas a la privacidad, rastreadores y más. Algunas de las opciones disponibles son: uBlock Origin, Adblock Plus y AdBlock.
- Bloquea las ventanas emergentes. Son molestas y peligrosas porque a menudo conducen a sitios web maliciosos. Afortunadamente, la mayoría de los navegadores populares pueden bloquear las ventanas emergentes sin necesidad de una extensión de terceros.
- Elimina las cookies no deseadas. Haz esto para evitar que las cookies te rastreen y comprometan tu privacidad.
- Desactiva la función de autocompletar. Facilita la entrada de información sensible en un formulario creado por un ciberdelincuente. Además, cualquiera con acceso a tu ordenador puede recuperar la información guardada.
- Utiliza una Red Privada Virtual (VPN). Como se mencionó en capítulos anteriores, una VPN permite transportar datos de forma segura a través de Internet público, impidiendo que terceros vean lo que haces en línea.

Aprovecha la navegación privada o el modo incógnito.

El propósito de este no es ocultar tu actividad en línea, como muchos creen, sino eliminar toda la información sobre tu sesión de navegación, incluyendo tu historial, descargas y cookies, al cerrar la ventana privada.

Sobre las redes sociales

Sobre las redes sociales

1. ¿Qué son las redes sociales?

Son formas de medios que permiten a las personas comunicarse con otros usuarios, empresas, comunidades y contenido. También les permiten a los usuarios compartir información utilizando Internet o dispositivos como computadoras, laptops y tabletas, entre otros.

2. ¿Cuáles son los ejemplos más destacados de plataformas de redes sociales?

Actualmente, algunas de las plataformas más populares son Facebook, YouTube, WhatsApp, Instagram, TikTok, Snapchat, Pinterest, Reddit, LinkedIn y Twitter (ahora conocido como X).

Estas plataformas sirven para diversos propósitos, desde comunicación personal y compartir contenido hasta redes profesionales y entretenimiento. Cada una tiene sus propias características únicas y comunidades de usuarios.

3. ¿Cuáles son los beneficios y desventajas de tener cuentas en redes sociales?

Algunos de los beneficios son:

- Conocer y participar en causas importantes;
- Poder promocionar y publicitar productos/contenidos;
- Conectar con personas y formar comunidades;
- Mantenerse actualizado a través de buenas fuentes de información;
- Tener mayores oportunidades para aprender y diversificar la educación;
- Poder dirigir el tráfico a un sitio web u otras plataformas;
- Llegar a audiencias más grandes y diversas;
- Poder tener comunicación directa con individuos e instituciones;
- Encontrar más opciones de entretenimiento.

Algunos de los riesgos son:

- Ser vulnerable al ciberacoso;
- Mayor riesgo de ser hackeado;
- Reducción de espacios y habilidades cara a cara;
- Recibir y difundir información errónea y desinformación;
- El riesgo de adicción;
- Daño físico y mental para la salud;
- Desperdicio de tiempo;
- La disminución de la capacidad de atención.

¿Cómo utilizar las redes sociales de forma segura?

- **Administra tus ajustes de privacidad.** Estos te ayudan a controlar quién ve lo que publicas y gestionar tu experiencia en línea de manera positiva.

- **Protege tu reputación en las redes sociales.** Todo lo que publicas en línea permanece en línea. Incluso si eliminas una publicación, aún puede existir en copias de seguridad o ser archivada por otros.

- **Ten en cuenta el contexto.** Si te encuentras en un entorno de riesgo, ten cuidado de no compartir demasiada información sobre ti mismo o sobre las personas con las que trabajas.

- **Mantén la información personal privada.** Cuanta más información publiques, más fácil podría ser para alguien usar esa información para robar tu identidad, acceder a tus datos o cometer otros delitos como el acoso.

- **Conoce qué acciones tomar en situaciones específicas.** Por ejemplo, si alguien te está acosando o amenazando, elimínalo de tu lista de amigos, bloquéalo y repórtalo al administrador del sitio. Además, considera involucrar a las autoridades en casos que te hagan sentir que estás en riesgo.

- **Sé cauteloso en las redes sociales.** Incluso los mensajes o enlaces que parecen provenir de amigos a veces pueden contener software dañino o formar parte de un ataque de phishing. Si tienes alguna sospecha, no hagas clic en el botón o enlace. Contacta a tus amigos y conocidos para verificar su validez.

- **No compartas información sensible (texto, video o imágenes) a través de sistemas de mensajería.** Son susceptibles a hackeos, violaciones de datos e interceptación, poniendo en peligro la confidencialidad y privacidad de tus datos.

Recuerda: lo que compartes, por más inocente que parezca, puede ser una pieza del rompecabezas que los criminales y personas malintencionadas utilicen para fines negativos.

Aspectos socioculturales de la seguridad digital

Sobre los aspectos socioculturales de la seguridad digital

1. ¿Por qué el contexto es importante cuando se trata de seguridad digital?

Un contexto dado puede influir en la percepción y práctica de la seguridad digital, ya sea a nivel individual, comunitario u organizacional. Cómo percibes la privacidad o qué compartes en línea puede haber sido determinado por, entre otros factores, las normas sociales del lugar donde naciste, tu edad y tus opiniones políticas e ideológicas.

2. ¿Cuáles son las amenazas a las que te puedes enfrentar basadas en aspectos socioculturales?

Aunque todos están expuestos a riesgos y amenazas en línea, algunas personas son más vulnerables debido a su raza, etnia, género, nacionalidad, credo u otros factores relacionados con su identidad. Por ejemplo, las mujeres pueden ser acosadas en línea simplemente por su género. Y los acosos pueden manifestarse en formas como difamación, suplantación de identidad, extorsión, acoso, vigilancia sexual, daño emocional e incluso amenazas de violación y muerte.

Las amenazas que enfrentan algunas comunidades en el mundo real pueden migrar al ámbito digital, que en sí mismo puede ser un terreno fértil para nuevas formas de amenaza.

3. ¿Existen otros riesgos a los que todos son vulnerables?

Los desafíos para el bienestar, la cultura de cancelación y la autocensura pueden crear un entorno en línea menos seguro e inclusivo. Los trastornos mentales derivados de experiencias negativas en internet pueden afectar la habilidad de una persona para explorar el mundo digital de manera segura y plena. La cultura de cancelación y la autocensura pueden limitar la libre expresión de ideas, lo que impide la creación de un discurso virtual diverso.

- **Retos para la salud:** La salud mental y emocional de las personas puede verse afectada de manera considerable por el entorno digital. Por ejemplo, las redes sociales pueden causar ciberacoso, comparación social y presión para mantener una imagen en línea cuidadosamente construida.
- **Cultura de cancelación:** Consiste en dejar de respaldar a personas o entidades cuyas acciones o palabras se consideran ofensivas o inaceptables, resultando usualmente en la vergüenza pública y la exclusión social. Los individuos pueden tener miedo de expresar opiniones diferentes o participar en un diálogo abierto debido al temor a posibles represalias públicas, lo cual impacta la libertad de expresión y el intercambio de ideas.
- **Autocensura:** puede suprimir la creatividad, las diferentes perspectivas y el diálogo constructivo, ya que se basa en el temor a críticas, acoso o ser cancelado. Puede establecer un entorno en el cual las personas se vean forzadas a aceptar opiniones mayoritarias en lugar de compartir sus propias perspectivas genuinas.

¿Cómo mantenerte seguro en Internet teniendo en cuenta tu entorno sociocultural?

La respuesta a esta pregunta dependerá de tu situación. Sin embargo, aquí tienes algunas recomendaciones generales y útiles:

Cultiva la alfabetización digital y la conciencia cultural:

- Desarrolla una sólida comprensión de la alfabetización digital para navegar efectivamente en los espacios en línea.
- Sé consciente y respeta las diferencias culturales en el comportamiento y la comunicación en línea.
- Mantente informado sobre los matices socioculturales para evitar malentendidos no intencionados.

Promueve un comportamiento en línea positivo:

- Fomenta un ambiente en línea positivo participando en una comunicación respetuosa y constructiva.
- Anima al diálogo abierto y a perspectivas diversas en las comunidades en línea.
- Evita participar o promover la cultura de la cancelación; en su lugar, participa en debates respetuosos.

Utiliza los ajustes de privacidad de manera efectiva:

- Ajusta la configuración de privacidad en las plataformas de redes sociales para controlar quién puede acceder a tu información.
- Revisa y actualiza regularmente estos ajustes de acuerdo con tu nivel de comodidad y las normas culturales.

Ten en cuenta tu bienestar:

- Establece límites para tus actividades en línea para evitar el agotamiento y el estrés.
- Prioriza la salud mental y toma descansos de las redes sociales si es necesario.
- Sé consciente del impacto potencial de las interacciones en línea en tu bienestar emocional y psicológico.

Utiliza las redes sociales de manera responsable:

- Ten cuidado con el contenido que compartes en las redes sociales, considerando las posibles implicaciones socioculturales.
- Piensa antes de publicar para evitar causar ofensas involuntarias o contribuir a dinámicas negativas en línea.

Fomenta la empatía digital:

- Fomenta la empatía en las interacciones en línea, considerando los sentimientos y perspectivas de los demás.
- Reporta y aborda el acoso en línea para crear un espacio en línea más seguro y empático.

Busca apoyo y reporta incidentes:

- Busca apoyo si experimentas acoso en línea o te sientes inseguro.
- Reporta los incidentes a las plataformas o autoridades pertinentes, enfatizando la importancia de una comunidad digital solidaria.

Glosario: conceptos clave

Sobre las «cookies»

¿Qué es una «cookie»?

En el ámbito digital, una cookie (también conocida como cookie HTTP, cookie del navegador o cookie de Internet) se refiere a un sistema que rastrea tu actividad en los sitios web. El objetivo de las cookies es recordar información sobre ti, incluido un registro de tus visitas y actividad en los sitios web.

Las cookies no siempre son malas. Y mediante una gestión cuidadosa, puedes asegurarte de que los sitios web solo estén recopilando información que sea útil para tu experiencia de usuario. Con nuestros consejos sobre cookies, puedes navegar por la web con confianza.

¿Cuántos tipos de cookies existen?

Hay cuatro tipos:

- **Cookies persistentes.** Están diseñadas para almacenar datos durante un período prolongado de tiempo. Cada cookie persistente tiene una fecha de vencimiento, que va desde unos pocos días hasta varios años después de tu visita al sitio. Por ejemplo, cuando inicias sesión en un sitio y le pides que te recuerde, una cookie persistente almacena tu nombre de usuario y contraseña, lo que te permite iniciar sesión más rápido en el futuro.

- **Cookies de sesión.** Son temporales y se eliminarán cuando cierres tu navegador. Cuando estás comprando en línea en un sitio específico, una cookie de sesión mantiene los elementos que has seleccionado en tu carrito de compras, incluso si haces clic en diferentes páginas alrededor del sitio.

- **Cookies de terceros o cookies de seguimiento.** Recopilan datos sobre tu comportamiento en línea y los transmiten al sitio web que creó las cookies, generalmente para obtener información publicitaria. Por ejemplo, cuando ves un artículo pero no lo compras, las cookies de terceros almacenan la información sobre tu visualización en línea y la transmiten a los anunciantes. Al día siguiente, encuentras un anuncio en tu cuenta de redes sociales para el artículo exacto que viste en línea el día anterior.

- **Supercookies.** No se almacenan a nivel del navegador sino a nivel de la red. Pueden viajar entre navegadores y son permanentes. El mayor riesgo relacionado con estas cookies es que pueden acceder a información como tus hábitos de navegación, credenciales de inicio de sesión y cachés de imágenes incluso después de que hayas eliminado tus cookies.

Si quieres protegerte de las cookies maliciosas, acepta solo las cookies necesarias cuando estés navegando. Además, utiliza una conexión cifrada o una red privada virtual (VPN). private network (VPN).

Sobre el «software»

¿Qué es un «software»?

Un software es un conjunto de programas que permite a los usuarios realizar una función definida o una tarea específica. Es responsable de dirigir todos los dispositivos relacionados con la computadora y les indica cómo realizarla.

¿Cuántos tipos de software hay?

Hay dos tipos de software, cada uno subdividido en varios módulos:

Software del sistema

Este involucra programas de computadora que ayudan al usuario a ejecutar el hardware o el software de la computadora y administrar la interacción entre ellos.

a) Sistemas operativos: un grupo de software que maneja la ejecución de programas y ofrece servicios generales para la aplicación que se ejecuta en la computadora. Ejemplos: Microsoft Windows, MacOS de Apple, Android, Ubuntu, Linux.

b) Controladores de dispositivos: un tipo de software que opera o controla dispositivos de hardware específicos conectados a su sistema. Ejemplos: controladores de pantalla, controladores de impresora, etc.

c) Firmware: un tipo de software incrustado en un dispositivo de hardware y no en una computadora. Ejemplo: software de impresora.

d) Utilidad: su trabajo es ofrecer soporte a la infraestructura del sistema. Ejemplos: Norton y McAfee Antivirus, WinRAR, WinZip, Explorador de archivos de Windows.

Programas de aplicación o aplicaciones de software

Son programas de computadora desarrollados principalmente para proporcionar funcionalidades específicas, como asistir al usuario.

a) Procesador de textos: estas son aplicaciones utilizadas para la documentación, tomar notas y escribir datos. Ejemplos: MS Word (Microsoft), iWork-Pages (Apple) y Google Docs.

b) Software de base de datos: se utiliza para crear, administrar, modificar y organizar una gran cantidad de datos que se pueden recuperar rápidamente. Ejemplos: Oracle, MS Access, SQLite, FileMaker, dBase.

c) Software multimedia: permite a los usuarios reproducir, crear o grabar imágenes, música y archivos de video. Ejemplos: Windows Movie Maker, iMovie, etc.

d) Navegadores web: se utilizan para navegar por Internet. Ejemplos: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, Safari.

Sobre el «software»

¿Existen más tipos de software?

Según la disponibilidad y la capacidad de compartir, hay una clasificación adicional del software:

a) Software gratuito: es gratuito y disponible por tiempo ilimitado. Cualquier usuario puede descargar fácilmente dicho software de Internet y comenzar a usarlo instantáneamente sin pagar ningún cargo o tarifa. Ejemplos: Adobe Reader, Zoom, Skype, Audacity, Anydesk.

b) Shareware: está disponible en Internet para descargarlo en una base de prueba fija. Se distribuye gratuitamente con un límite de tiempo establecido, y al final del período de prueba, se le pide al usuario que pague la tarifa o desinstale el software. Ejemplos: Grammarly, Adobe Suite, WinZip.

c) Código abierto: a diferencia del software gratuito, este tipo de software está disponible en línea junto con su código fuente. Esto significa que el usuario puede cambiar, transformar e incluso agregar funciones adicionales a un software de código abierto. Según el servicio, puede ser de pago o gratuito. Ejemplos: Mozilla Firefox, OpenOffice, MySQL, Thunderbird.

¿Por qué es importante actualizar el software?

Las actualizaciones de software son importantes por razones como:

- Reparar vulnerabilidades de seguridad para corregir errores informáticos. Las actualizaciones también pueden agregar nuevas funciones a tus dispositivos y eliminar las obsoletas.
- Incluir parches de software, que cubren agujeros de seguridad para mantener a raya a los hackers.
- Proteger tu información de ataques de ransomware, que pueden apuntar a tus correos electrónicos, dirección de casa e incluso información relacionada con tu cuenta bancaria.
- Proteger tus dispositivos de ser infectados por virus y transferirlos a los de tu familia o colegas.
- Mejorar los sistemas y evitar que se bloqueen. Las actualizaciones regulares también garantizan más estabilidad, mejorando el rendimiento y la velocidad del programa, entre otras cosas.

Algunas actualizaciones requieren que tu dispositivo esté conectado a Wi-Fi o a la corriente eléctrica, tenga suficiente almacenamiento o se reinicie. En esos casos, sigue las instrucciones que te dé tu dispositivo.

Sobre el «hardware»

¿Qué es el «hardware»?

Mientras que el software abarca la parte intangible de un dispositivo, el hardware implica sus componentes físicos, responsables de almacenar y ejecutar las instrucciones proporcionadas por el software.

¿Cuál es la diferencia entre hardware interno y externo?

El hardware de computadora puede clasificarse en componentes internos y externos.

Los componentes internos de hardware son aquellos necesarios para el correcto funcionamiento de la computadora, mientras que los componentes externos de hardware se conectan a la computadora para agregar o mejorar la funcionalidad.

a) Hardware interno
Los componentes internos procesan o almacenan colectivamente las instrucciones entregadas por el programa o sistema operativo (SO).

Estos incluyen la placa base, CPU, RAM, disco duro y disipador de calor, entre otros.

b) Hardware externo
Los componentes de hardware externo son elementos que se conectan externamente a la computadora para controlar funciones de entrada o salida.

Estos dispositivos de hardware están diseñados para proporcionar instrucciones al software (entrada) o mostrar resultados de su ejecución (salida).

Algunos ejemplos de componentes de hardware de entrada son el ratón, teclado, escáner, cámara y tarjeta de memoria. Por otro lado, los monitores, impresoras, altavoces y auriculares son componentes de hardware de salida.

El hardware y el software son complementarios. Un dispositivo puede funcionar eficientemente y producir resultados útiles solo cuando tanto el hardware como el software funcionan juntos adecuadamente.

Recomendaciones finales y otros recursos

Recomendaciones finales

1 Utiliza la autenticación de dos factores en tantos dispositivos y cuentas como sea posible

Este método de seguridad proporciona protección adicional durante el proceso de inicio de sesión y hace que sea mucho más difícil para los atacantes acceder a los dispositivos o cuentas en línea. Incluso si un hacker obtiene una contraseña, no será suficiente para pasar la verificación de seguridad.

2 Considera tener un teléfono o computadora portátil exclusivamente para el trabajo

Tener dispositivos exclusivamente dedicados al trabajo mejora la seguridad al reducir el riesgo de comprometer accidentalmente datos sensibles en aplicaciones o sitios web personales. Esto ayuda a proteger los datos, especialmente si manejas información sensible o enfrentas una filtración o violación de datos, lo cual garantiza el cumplimiento de las leyes de protección de datos y privacidad.

3 Ten en cuenta las regulaciones específicas de cada país; el contexto es importante

Es posible que el uso de una VPN personal esté permitido en tu país, pero sea ilegal en otros. Investiga siempre que viajes para asegurarte de cumplir con las leyes locales.

4 Puede que no seas famoso, pero aún así puedes ser un objetivo

Incluso si no eres una celebridad, la seguridad digital es importante porque protege tu información personal, activos financieros y privacidad de las amenazas digitales que pueden interrumpir tu vida y provocar pérdidas financieras o robo de identidad.

5 Pequeñas acciones pueden marcar la diferencia.

No necesitas comprar los dispositivos más caros ni ser experto en cada software. Simplemente haciendo actualizaciones regulares del software en cada dispositivo que uses, o cambiando tus contraseñas por otras más fuertes, puedes hacer una diferencia significativa en tu seguridad digital.

6 No existe una seguridad digital al 100%.

Dada la rápida evolución de las amenazas, los factores humanos y la naturaleza interconectada del mundo digital, la seguridad digital total es imposible.

Sin embargo, aún puedes aspirar a estar lo más seguro posible adoptando las mejores prácticas y manteniéndote actualizado sobre las últimas tendencias e informes.

Recursos adicionales

Para obtener más conocimientos en **seguridad digital**, considera los siguientes cursos de formación:

- Introducción a la seguridad digital personal, impartido por Codeacademy.
- Seguridad digital y derechos humanos, ofrecido por Amnistía Internacional.
- Seguridad y protección digital, impartido por la Universidad Estatal de Arizona.
- Mira la grabación del seminario web de formación «Seguridad Digital para Periodistas y Defensores de Derechos Humanos», ofrecido por el Centro Internacional para Periodistas (ICFJ), en colaboración con el Centro Fronterizo para Periodistas y Blogueros (BCJB) y Meta.

Para obtener más conocimientos y capacitación en **ciberseguridad**:

- Introducción a la ciberseguridad, impartido por The Open University.
- Fundamentos de ciberseguridad, ofrecido por The Linux Foundation.

Para obtener conocimientos y capacitación adicionales en el **bienestar digita**l:

- Introducción al bienestar digital, ofrecido por Google.
- Herramientas digitales y bienestar, impartido por la Universidad Estatal de Arizona.
- Bienestar digital, enseñado por la Universidad de York.

Para obtener conocimientos y capacitación adicionales en **diversos temas digitales y tecnológicos**:

- Mira los videos educativos y materiales publicados por IBM en su canal de YouTube.
- Escucha las Charlas de Google publicadas en su canal de YouTube.
- Aprende una nueva habilidad digital clave con Google Garage.

Referencias

Estas fuentes fueron útiles y valiosas en el desarrollo de esta guía. Recomendamos revisarlas si deseas obtener más información detallada sobre los temas mencionados:

Britannica: *www.britannica.com/technology/browser*

Capterra: *www.capterra.com/glossary/browser/*

Data Prot: *www.dataprot.net/articles*

Digital Scholar: *www.digitalscholar.in/pros-and-cons-of-social-media/*

Free Code Camp: *www.freecodecamp.org*

F-Secure: *www.f-secure.com/en*

Java Point: *www.javatpoint.com*

National Cyber Security Centre - UK: *www.ncsc.gov.uk*

NordVPN: *www.nordvpn.com*

Norton Blog: *www.us.norton.com/blog*

OECD Digital: *www.oecd.org/digital/digital-security*

OSIbeyond: *www.osibeyond.com/blog/tips-for-making-web-browsing-more-secure*

Security Boulevard: *www.securityboulevard.com*

Simplilearn: *www.simplilearn.com*

Software Lab: *www.softwarelab.org*

Standford: *https://share.stanford.edu/education-and-outreach/learn-topics/digital-safety*

Tech Target: *www.techtarget.com*

University of Pittsburgh - Information Technology: *www.technology.pitt.edu/security*

De la teoría a la práctica

Esta guía contiene conceptos y nociones, así como recomendaciones, para ayudarte a comprender y mejorar tu higiene digital. Después de leerla, te sugerimos utilizar la lista de verificación complementaria (o checklist) tan a menudo como sea posible (es decir, cada mes, trimestre, semestre o año).

Ten en cuenta que debes evaluar personalmente las recomendaciones para asegurarte de su relevancia en tu contexto y necesidades específicas.

Contacto

Cameco está abierto al aprendizaje y al intercambio entre pares. Si tienes comentarios, preguntas o sugerencias, contacta a Emy Osorio Matorel, Asesora en Análisis y Estrategia Digital, a través del correo electrónico emy.osorio@cameco.org.

Guía de seguridad digital para todos

Publicado por
CAMECO

Apartado postal 10 21 04
52021 Aquisgrán
Alemania

Para consultas, por favor contactar a:

Emy Osorio Matorel (emy.osorio@cameco.org)
Oficina General de Cameco (cameco@cameco.org)

cameco+