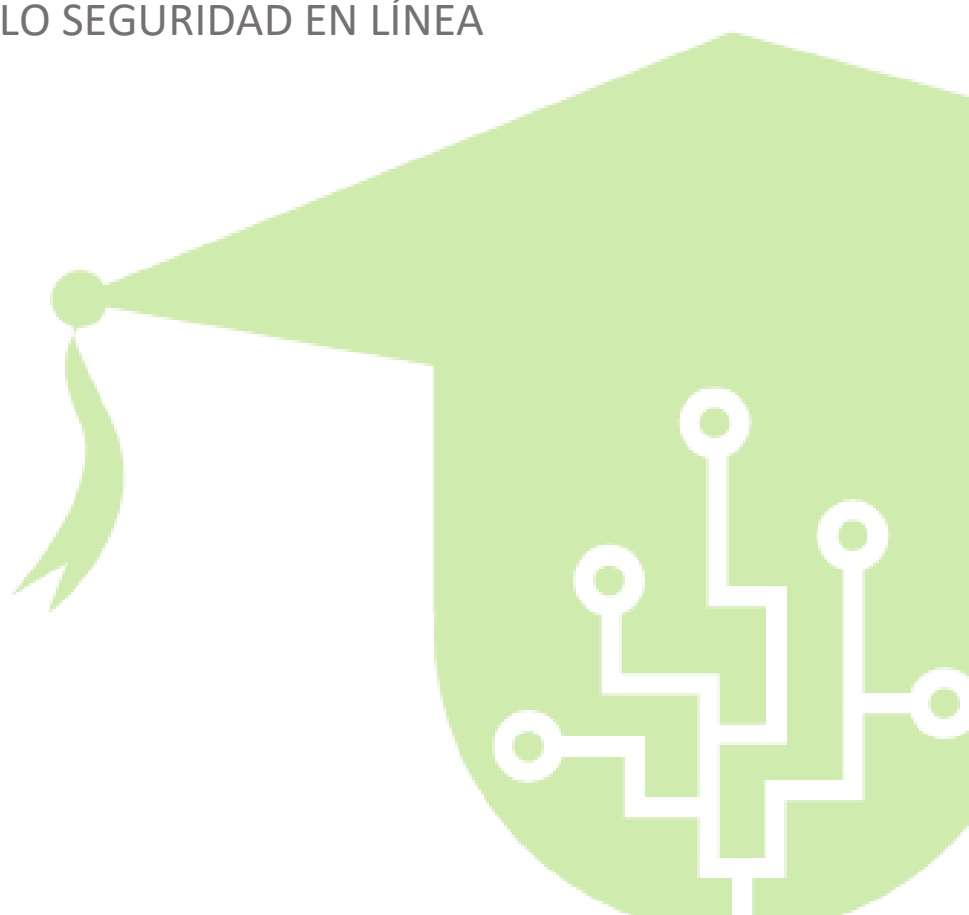
L2D

MEDIA LITERACY COMPETENCES
FOR YOUTH WORKERS

DIRECTRICES PARA EL USO SEGURO EN LÍNEA

MÓDULO SEGURIDAD EN LÍNEA



Título :	DIRECTRICES PARA EL USO SEGURO EN LÍNEA
Palabras clave:	Seguridad en línea, seguridad de Internet, privacidad digital, ciberseguridad, prácticas seguras en línea, protección de información personal, seguridad de datos, administración de contraseñas, amenazas en línea, informes de abuso, configuración de privacidad
Preparado por .	
Idioma :	Español
Objetivos:	● Definir la seguridad en línea: explique el concepto de seguridad en línea y su importancia en el mundo digital actual. ● Identificar amenazas en línea: ayude a los alumnos a reconocer diversas amenazas en línea, como phishing, malware, robo de identidad, ciberacoso y estafas. ● Comprender las preocupaciones sobre la privacidad: eduque a los participantes sobre la importancia de proteger la información personal en línea y las posibles consecuencias de las violaciones de la privacidad. ● Desarrollar contraseñas seguras: enseñe técnicas para crear contraseñas seguras y únicas para mejorar la seguridad de la cuenta. ● Protejer contra intentos de phishing: proporcione estrategias para detectar y evitar ser víctima de correos electrónicos, mensajes y sitios web de phishing. ● Perfiles de redes sociales seguros: ofrezcer pautas para ajustar la configuración de privacidad, controlar el intercambio de información personal y manejar solicitudes de amistad. ● Promover la comunicación segura en línea: enseñar formas eficaces de comunicarse de forma segura en las redes sociales, foros y plataformas de mensajería, haciendo hincapié en evitar compartir detalles confidenciales. ● Desarrollar habilidades de pensamiento crítico: fomentar la capacidad de evaluar la información y las fuentes de manera crítica, particularmente en el contexto de noticias falsas y desinformación en línea. ● Lidiar con el acoso y el acecho en línea: ofrecer orientación sobre cómo responder y denunciar casos de acoso o acoso en línea.
Los resultados del aprendizaje :	

Índice de contenido:

Co-funded by the European Union

Desarrollo de contenido :	1. SEGURIDAD DE INTERNET 1.1. DEFINICIÓN DE SEGURIDAD EN INTERNET La seguridad en Internet, también conocida como seguridad en línea, es la práctica de adherirse a pautas prácticas, obtener una comprensión integral de la tecnología moderna y salvaguardar proactivamente sus dispositivos digitales para defenderse de los diversos aspectos maliciosos del mundo en línea. A medida que el número de usuarios de Internet continúa aumentando a nivel mundial, varias partes interesadas, incluidos gobiernos, organizaciones y proveedores de servicios de Internet, se han preocupado cada vez más por la seguridad de las poblaciones vulnerables, como niños, adolescentes y ancianos, mientras interactúan con la comunidad. vasto reino virtual. Estadísticas alarmantes revelan que más del 45% de los usuarios de Internet han informado haber experimentado algún tipo de acoso cibernético, lo que subraya la necesidad urgente de promover prácticas en línea más seguras y cultivar una cultura de responsabilidad digital. Para abordar estas preocupaciones apremiantes y abogar por un panorama digital más seguro, cada febrero se celebra a escala mundial el Día de una Internet Segura. Este evento anual sirve como una plataforma dedicada a crear conciencia sobre la seguridad en Internet, alentando a las personas y comunidades a estar alerta, informadas y proactivas en sus interacciones en línea. Gobiernos, organizaciones sin fines de lucro y empresas de tecnología de todo el mundo participan activamente en las iniciativas del Día de una Internet más segura, organizando campañas de concientización, talleres educativos y eventos interactivos para dotar a los usuarios de Internet de los conocimientos y habilidades necesarios para navegar de forma segura en el mundo en línea. En el Reino Unido, la campaña Get Safe Online se ha convertido en una fuerza destacada en la promoción de la seguridad en Internet. Con el patrocinio vital de la agencia gubernamental Serious

	Organised Crime Agency (SOCA) y la colaboración con importantes empresas de Internet como Microsoft y eBay, la campaña tiene como objetivo brindar a los usuarios de Internet orientación práctica y recursos para protegerse contra las amenazas cibernéticas. A través de información, consejos y herramientas de fácil acceso, Get Safe Online se esfuerza por mejorar la resiliencia digital de las personas, haciendo que la comunidad de Internet del Reino Unido sea más sólida y menos susceptible a los peligros en línea. A medida que Internet continúa evolucionando y desempeñando un papel cada vez más integral en nuestra vida diaria, garantizar la seguridad en Internet se vuelve primordial. Al fomentar una cultura de comportamiento responsable en línea, generar conciencia a través de iniciativas como el Día de una Internet Segura y brindar recursos accesibles como la campaña Get Safe Online, podemos trabajar colectivamente para crear un entorno digital más seguro para todos. En nuestro mundo cada vez más conectado, no se puede subestimar la importancia de la seguridad en Internet. Internet ofrece oportunidades incomparables de aprendizaje, comunicación y entretenimiento, pero también expone a los usuarios a riesgos y peligros potenciales. A medida que la tecnología avanza y las amenazas en línea se vuelven más sofisticadas, mantenerse informado y proactivo sobre la seguridad en Internet es crucial para personas de todas las edades. Para los niños y adolescentes, que a menudo son nativos digitales, comprender la seguridad en Internet es esencial para tener interacciones en línea responsables y seguras. Los padres, educadores y tutores desempeñan un papel vital a la hora de guiar a los jóvenes usuarios de Internet, enseñándoles sobre los riesgos potenciales de compartir información personal, interactuar con extraños y participar en actividades en línea inseguras. Para mejorar la seguridad en Internet, es fundamental mantenerse actualizado sobre las últimas tendencias y mejores prácticas de

ciberseguridad. La actualización periódica del software y las aplicaciones, el uso de software antivirus confiable y la habilitación de actualizaciones automáticas pueden fortalecer la defensa de los dispositivos digitales contra amenazas emergentes. Además, incorporar autenticación multifactor siempre que sea posible agrega una capa adicional de protección a las cuentas en línea.

Promover una comunidad en línea positiva y segura también requiere fomentar la empatía y el respeto digitales. Fomentar la amabilidad y la empatía en las interacciones en línea puede contrarrestar el ciberacoso y el comportamiento tóxico, haciendo de Internet un espacio más acogedor para todos.

1.2. ENTENDIENDO EL ALCANCE Y LA IMPORTANCIA

1.2. 1. Alcance de la seguridad en Internet

- Protección contra amenazas cibernéticas como virus, malware, phishing, ransomware y robo de identidad.
- Salvaguardar la información personal y la identidad digital del acceso no autorizado y el uso indebido.
- Navegar en las redes sociales de manera responsable y lidiar con el ciberbullying o el acoso en línea.
- Garantizar transacciones en línea seguras y proteger la información financiera al comprar o realizar operaciones bancarias en línea.
- Usar y administrar de forma segura dispositivos móviles para evitar filtraciones de datos y violaciones de privacidad.
- Reconocer y evitar estafas en línea, sitios web fraudulentos e intentos de phishing.
- Enseñar a niños y adolescentes sobre seguridad en línea y ayudarlos a desarrollar hábitos digitales responsables.

1.2.2. Importancia de la seguridad en Internet

- Protección de información personal y financiera: las medidas de seguridad en Internet salvaguardan los datos confidenciales, previniendo el robo de identidad y el fraude financiero.
- Mantener la privacidad y la reputación digital: ser consciente de las actividades en línea ayuda a las personas a preservar su privacidad y proteger su reputación digital.
- Protección contra amenazas cibernéticas: el conocimiento de los riesgos en línea y el seguimiento de prácticas de seguridad defienden contra las amenazas cibernéticas que pueden alterar la vida diaria, las operaciones comerciales o comprometer información confidencial.
- Potenciar experiencias digitales positivas: la seguridad en Internet permite a las personas tener experiencias positivas y enriquecedoras en línea sin temor a ser acosadas o victimizadas.
- Fomento de la ciudadanía digital: al practicar la seguridad en Internet, las personas contribuyen a construir una comunidad digital responsable y respetuosa.
- Impacto económico: los incidentes de ciberseguridad pueden tener graves consecuencias económicas para personas, empresas y gobiernos, lo que hace que la seguridad en Internet sea un aspecto esencial de la seguridad general.
- Proteger a los vulnerables: la seguridad en Internet es especialmente crucial para los niños, adolescentes y poblaciones vulnerables que pueden ser más susceptibles a los peligros en línea.

1.3. EVOLUCIÓN DE LOS CONCEPTOS DE SEGURIDAD EN INTERNET

La "Evolución de los conceptos de seguridad en Internet" se refiere a cómo la comprensión de la seguridad en Internet y las medidas tomadas para proteger a los usuarios de las amenazas en línea han evolucionado con el tiempo. A medida que Internet ha crecido y transformado, también lo han hecho los desafíos que plantean las amenazas cibernéticas, lo que ha llevado al desarrollo de nuevos conceptos y estrategias para garantizar la seguridad en línea. Esta sección profundiza en el contexto histórico y los hitos

	clave que han dado forma a las prácticas de seguridad en Internet. • Internet inicial: en los primeros días de Internet, el concepto de seguridad en línea era relativamente simplista. La mayoría de los usuarios eran personas o profesionales expertos en tecnología que entendían los riesgos asociados con compartir información personal en línea. Sin embargo, había una conciencia limitada entre el público en general sobre las posibles amenazas cibernéticas. • Aumento de la comunicación en línea: a medida que surgieron las plataformas de comunicación en línea y las redes sociales, la seguridad en Internet adquirió nuevas dimensiones. Los usuarios comenzaron a compartir más información personal, lo que generó mayores preocupaciones sobre la privacidad y el robo de identidad. Conceptos como phishing y correos electrónicos no deseados comenzaron a ganar importancia a medida que los ciberdelincuentes buscaban explotar la confianza de los usuarios. • Medidas pioneras en ciberseguridad: con el creciente panorama de amenazas, las medidas de ciberseguridad comenzaron a evolucionar. El software antivirus, los cortafuegos y las tecnologías de cifrado se convirtieron en herramientas esenciales para proteger contra el malware y el acceso no autorizado. Estas primeras soluciones de ciberseguridad sentaron las bases para mecanismos de protección más avanzados en el futuro. • Campañas e iniciativas de concientización: a medida que las amenazas cibernéticas se generalizaron, varias organizaciones, gobiernos y empresas de tecnología comenzaron a lanzar campañas e iniciativas de concientización para educar al público sobre la seguridad en Internet. Estos esfuerzos tenían como objetivo crear conciencia sobre los riesgos comunes en línea y alentar a los usuarios a adoptar prácticas en línea más seguras.

	• Preocupación creciente por el ciberacoso: El auge de las redes sociales y la comunicación en línea también atrajo la atención sobre el problema del ciberacoso. A medida que aumentaron los incidentes de acoso y ciberacoso en línea, los esfuerzos de seguridad en Internet se ampliaron para abordar esta forma de agresión digital y apoyar a las personas afectadas. • Internet móvil y nuevos desafíos: La llegada de los teléfonos inteligentes y el acceso a Internet móvil introdujo un nuevo conjunto de desafíos para la seguridad en Internet. Los riesgos únicos asociados con los dispositivos móviles, como los permisos de aplicaciones y el malware móvil, requirieron medidas de seguridad personalizadas. • Avances en autenticación: como las contraseñas por sí solas resultaron insuficientes para proteger las cuentas en línea, la autenticación de dos factores (2FA) y la autenticación de múltiples factores (MFA) ganaron popularidad. Estos métodos proporcionaron una capa adicional de seguridad, reduciendo el riesgo de acceso no autorizado. • Énfasis en la alfabetización digital: los conceptos de seguridad en Internet comenzaron a abarcar no sólo medidas de seguridad técnicas sino también alfabetización digital y habilidades de pensamiento crítico. Educar a los usuarios sobre cómo identificar información errónea, noticias falsas y estafas en línea se volvió vital para combatir las amenazas en línea. • El auge de la industria de la ciberseguridad: la creciente sofisticación de las ciberamenazas dio lugar a una sólida industria de la ciberseguridad. Las empresas y profesionales especializados en servicios de ciberseguridad, análisis de amenazas y respuesta a incidentes desempeñaron un papel crucial en la defensa contra la evolución de los riesgos en línea. • Integración de la seguridad en Internet en la educación: Al reconocer la importancia de la educación sobre seguridad en Internet, las

escuelas e instituciones educativas comenzaron a incorporarla en su plan de estudios. Enseñar a niños y jóvenes sobre comportamiento responsable en línea y ciudadanía digital se convirtió en un aspecto esencial de la educación moderna.
La alfabetización mediática es una asignatura docente que nace con el objetivo de dotar a las personas de todas las herramientas necesarias para comprender mejor las dinámicas y mensajes que ofrecen los medios de comunicación, y reelaborarlos de forma independiente y crítica.
Hoy en día es necesario enseñar a las personas a gestionar mejor su relación con las redes sociales, educarlas y formarlas sobre "qué y cómo publicar" o cómo reconocer las "noticias falsas".
El uso de Internet gracias a los teléfonos inteligentes ofrece infinitas posibilidades de aprendizaje, pero también riesgos relacionados con el "uso superficial de estas herramientas".
Los "inmigrantes digitales" corren mayor riesgo porque no están acostumbrados a lidiar con las reglas no escritas de un mundo virtual al que no pertenecen. Muchas veces desconocen los principales sistemas de comunicación y no tienen la capacidad de procesar nuevos mensajes para ofrecer su propio aporte a la comunidad, permaneciendo como elementos pasivos.

1.4. Componentes clave de una experiencia en línea segura

Los "Componentes clave de una experiencia en línea segura" son elementos esenciales que contribuyen a crear un entorno seguro y protegido al utilizar Internet. Estos componentes abarcan diversas prácticas, comportamientos y herramientas que las personas pueden emplear para garantizar su seguridad y privacidad en línea. Comprender e implementar estos componentes clave es vital para una experiencia de Internet positiva y segura.

- Conciencia sobre la ciberseguridad: Desarrollar una sólida conciencia sobre la ciberseguridad es fundamental para una experiencia en línea segura. Esto implica mantenerse informado sobre las últimas amenazas cibernéticas, comprender los métodos de ataque comunes, como el

	phishing y el malware, y reconocer señales de advertencia de actividades sospechosas. La conciencia permite a las personas tomar decisiones informadas y tomar las precauciones necesarias mientras navegan por el mundo digital. • Protección de la privacidad: Proteger la privacidad es un aspecto crucial de la seguridad en Internet. Implica ser consciente de la información que se comparte en línea y evitar compartir demasiado datos personales. Proteger los datos confidenciales, como la información financiera y los documentos de identificación, es esencial para prevenir el robo de identidad y el fraude. • Autenticación sólida: es vital utilizar métodos de autenticación sólidos para cuentas en línea. Esto incluye emplear contraseñas únicas y seguras para cada cuenta y aprovechar capas de seguridad adicionales como la autenticación de dos factores (2FA) o la autenticación biométrica cuando esté disponible. Las sólidas medidas de autenticación ayudan a prevenir el acceso no autorizado a las cuentas y proteger la información confidencial. • Prácticas de navegación segura: es necesario practicar hábitos de navegación seguros para evitar sitios web maliciosos y amenazas potenciales. Esto incluye verificar las URL de los sitios web antes de ingresar información confidencial, evitar hacer clic en enlaces o ventanas emergentes sospechosos y utilizar navegadores seguros con protecciones integradas. • Actualizaciones periódicas de software: mantener el software, los sistemas operativos y las aplicaciones actualizados es esencial para mantener una experiencia en línea segura. Las actualizaciones periódicas suelen incluir parches de seguridad que abordan vulnerabilidades conocidas, lo que dificulta que los ciberdelincuentes las exploten. • Redes seguras: conectarse a redes seguras y confiables es fundamental para proteger los datos

en tránsito. Evitar las redes Wi-Fi públicas sin las medidas de seguridad adecuadas es fundamental para evitar posibles interceptaciones de datos y accesos no autorizados.

- Prácticas seguras en las redes sociales: ser cauteloso al utilizar las plataformas de redes sociales es crucial para proteger la información personal y evitar ser víctima de ataques de ingeniería social. Ajustar la configuración de privacidad, ser selectivo con las solicitudes de amistad y abstenerse de compartir datos confidenciales públicamente son prácticas de seguridad esenciales en las redes sociales.

- Vigilancia contra el phishing: Es vital estar atento a los intentos de phishing. Esto implica verificar las identidades de los remitentes de los correos electrónicos, no hacer clic en enlaces sospechosos ni descargar archivos adjuntos de fuentes desconocidas y denunciar intentos de phishing.

- Controles y supervisión parentales: para los padres y tutores, implementar controles parentales y monitorear las actividades en línea de los niños son componentes críticos de una experiencia segura en Internet para los usuarios jóvenes. Esto garantiza el acceso a contenidos apropiados para su edad y protege a los niños de contenidos en línea potencialmente dañinos.

- Alfabetización digital y pensamiento crítico: desarrollar habilidades de alfabetización digital y pensamiento crítico es fundamental para identificar información errónea, noticias falsas y estafas en línea. Comprender cómo evaluar las fuentes de información y verificar la credibilidad del contenido contribuye a una experiencia en línea más segura.

2. AMENAZAS EN LÍNEA

2.1. TIPOS DE AMENAZAS EN LÍNEA

	Los tipos de amenazas en línea se refieren a diversas actividades y ataques maliciosos que pueden poner en peligro la seguridad, la privacidad y la integridad de los usuarios de Internet y sus datos. Comprender estas amenazas es crucial para que las personas tomen las precauciones adecuadas y se protejan mientras navegan por el panorama digital. A continuación, se muestran algunos tipos comunes de amenazas en línea: **Phishing:** el phishing es una técnica engañosa utilizada por los ciberdelincuentes para engañar a los usuarios para que revelen información confidencial, como credenciales de inicio de sesión, detalles financieros o datos personales. Los intentos de phishing a menudo implican correos electrónicos, sitios web o mensajes falsos que imitan a entidades legítimas para atraer a las víctimas a proporcionar su información. **Malware:** El malware es software malicioso diseñado para infectar y dañar dispositivos o redes. Esto incluye virus, gusanos, troyanos, ransomware y software espía. El malware puede comprometer datos, robar información, interrumpir operaciones o incluso inutilizar los dispositivos. **Ransomware:** el ransomware es un tipo específico de malware que cifra los datos de un usuario, bloqueándolo de manera efectiva fuera de sus propios archivos o sistemas. Los ciberdelincuentes exigen el pago de un rescate para proporcionar la clave de descifrado, pero no hay garantía de que el pago del rescate resulte en la devolución de los datos. **Ingeniería social:** la ingeniería social implica la manipulación de personas para obtener acceso no autorizado a información o sistemas confidenciales. Esto se puede hacer mediante la suplantación de identidad, la manipulación o la explotación de la psicología humana para engañar a los usuarios y lograr que revelen información confidencial. **Violaciones de datos:** una violación de datos ocurre cuando los ciberatacantes obtienen acceso no autorizado a los datos de una organización o individuo. Esto puede incluir información personal, registros financieros o propiedad intelectual. Las violaciones de datos pueden tener graves consecuencias para la privacidad de las

	personas y provocar robo de identidad o pérdidas financieras. **Robo de identidad: el** robo de identidad implica robar información personal, como números de seguro social, detalles de tarjetas de crédito o credenciales de inicio de sesión, para hacerse pasar por otra persona con fines fraudulentos. Los ciberdelincuentes pueden utilizar esta información robada para obtener beneficios económicos o para cometer otros delitos. **Acoso cibernético:** el acoso cibernético es una forma de acoso o intimidación en línea, que suele ocurrir en plataformas de redes sociales o a través de aplicaciones de mensajería. Implica enviar mensajes hirientes, difundir rumores o compartir contenido vergonzoso con la intención de dañar, intimidar o humillar a la víctima. **Ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS):** los ataques DoS y DDoS tienen como objetivo abrumar un sitio web o servicio en línea con una avalancha de tráfico, haciéndolo inaccesible para los usuarios legítimos. Estos ataques pueden interrumpir los servicios en línea y causar pérdidas financieras a las empresas. **Ataques Man-in-the-Middle (MitM): los** ataques MitM implican interceptar y escuchar a escondidas la comunicación entre dos partes, como un usuario y un sitio web. El atacante puede entonces ver o manipular los datos intercambiados sin el conocimiento de las partes que se comunican. **Exploits de día cero:** los exploits de día cero se dirigen a vulnerabilidades de software que el proveedor o los desarrolladores aún no conocen. Los ciberdelincuentes utilizan estas vulnerabilidades para lanzar ataques antes de que esté disponible un parche o solución, lo que hace que sea difícil defenderse de ellas. **Vulnerabilidades de Internet de las cosas (IoT):** a medida que más dispositivos se conectan a Internet, las vulnerabilidades de IoT se han convertido en una preocupación. Las débiles medidas de seguridad de los dispositivos IoT pueden aprovecharse para obtener acceso a las redes domésticas o comprometer la privacidad.

2.2. RECONOCER LAS SEÑALES DE ADVERTENCIA

Reconocer las señales de advertencia es una habilidad crucial cuando se trata de seguridad en Internet. Implica estar alerta a los indicadores de que algo puede estar mal o ser potencialmente dañino al utilizar Internet. Al reconocer las señales de advertencia, las personas pueden tomar medidas inmediatas para protegerse de las amenazas en línea y evitar ser víctimas de estafas, ataques cibernéticos u otras actividades maliciosas. Aquí hay algunas señales de advertencia clave a las que debe prestar atención:

Comunicación no solicitada: tenga cuidado con los correos electrónicos, mensajes o solicitudes de amistad no solicitados de fuentes desconocidas o sospechosas. Los ciberdelincuentes suelen utilizar estos medios para iniciar intentos de phishing o distribuir malware.

Mala gramática y ortografía: muchos correos electrónicos de phishing y mensajes fraudulentos contienen errores gramaticales, faltas de ortografía o lenguaje incómodo. Estos errores pueden ser una señal de que la comunicación no proviene de una fuente legítima.

Solicitudes de información personal: tenga cuidado con las solicitudes de información confidencial, como credenciales de inicio de sesión, detalles financieros o números de seguro social, especialmente si la solicitud llega inesperadamente o parece innecesaria.

Lenguaje urgente o amenazante: los mensajes que utilizan un lenguaje urgente o amenazante para presionarlo a tomar medidas inmediatas podrían ser indicadores de una estafa o un intento de phishing.

Enlaces o URL inusuales: pase el mouse sobre los enlaces en correos electrónicos o mensajes para ver el destino URL real. Tenga cuidado con las URL acortadas o los enlaces que redirigen a sitios web sospechosos.

URL falsas o que no coinciden: tenga en cuenta las URL que parecen legítimas pero que tienen variaciones o errores ortográficos sutiles. Los estafadores pueden utilizar nombres de dominio que se parecen mucho a sitios web conocidos para engañar a los usuarios.

Remitentes de correo electrónico desconocidos: verifique la identidad de los remitentes de correo electrónico, especialmente si el mensaje contiene archivos adjuntos inesperados o solicitudes de información confidencial.

Descargas inesperadas: tenga cuidado con las descargas o archivos adjuntos que no inició o que no esperaba, ya que pueden contener malware.

Actividad inusual de la cuenta: revise periódicamente la actividad de su cuenta en línea y esté alerta ante cualquier inicio de sesión o transacción no autorizados.

Comportamiento inexplicable del sistema: si su computadora o dispositivo se comporta de manera inusual, como fallas frecuentes, desaceleraciones o ventanas emergentes inesperadas, podría indicar malware u otros problemas de seguridad.

Advertencias del software de seguridad: preste atención a las advertencias o alertas de su antivirus o software de seguridad, ya que pueden indicar amenazas potenciales o actividades sospechosas.

Ofertas y promociones no solicitadas: tenga cuidado con las ofertas o promociones no solicitadas que parecen demasiado buenas para ser verdad, ya que pueden ser estafas que intentan atraerlo para que proporcione información personal.

2.3. CONSECUENCIAS DE IGNORAR LAS AMENAZAS EN LÍNEA

Ignorar las amenazas en línea puede tener consecuencias graves y de gran alcance que pueden afectar negativamente a las personas, las empresas e incluso a la sociedad en su conjunto. No abordar o tomar medidas adecuadas contra las amenazas en línea puede dejar a uno vulnerable a diversos riesgos cibernéticos, lo que genera pérdidas financieras, violaciones de la privacidad, daños a la reputación e incluso repercusiones legales. Estas son algunas de las consecuencias clave de ignorar las amenazas en línea:

Pérdida financiera: Ser víctima de estafas, ataques de phishing o esquemas fraudulentos en línea puede resultar en pérdidas financieras significativas. Los ciberdelincuentes pueden robar credenciales bancarias, información de tarjetas

	de crédito o realizar transacciones no autorizadas, lo que genera cuentas bancarias vacías y dificultades financieras. **Robo de identidad:** ignorar las señales de advertencia de robo de identidad puede permitir a los ciberdelincuentes robar información personal, como números de seguro social, fechas de nacimiento y direcciones. Pueden utilizar esta información robada para cometer fraude financiero, abrir cuentas a nombre de la víctima o participar en otras actividades delictivas, causando graves consecuencias a largo plazo para la víctima. **Violaciones de datos:** no implementar medidas de seguridad sólidas o abordar las vulnerabilidades puede provocar violaciones de datos para individuos y organizaciones. Una violación de datos puede exponer información confidencial, incluidos datos de clientes, secretos comerciales o propiedad intelectual, lo que resulta en sanciones financieras, responsabilidades legales y daños a la reputación de la organización. **Ataques de ransomware:** ignorar las prácticas de ciberseguridad puede hacer que las personas y las empresas sean susceptibles a ataques de ransomware. Cuando los sistemas se ven comprometidos por ransomware, se pueden cifrar datos valiosos y los atacantes exigen el pago por la clave de descifrado. Pagar el rescate no garantiza la recuperación de datos y las víctimas pueden sufrir pérdida de datos o interrupciones operativas. **Daño a la reputación:** ser víctima de ciberacoso o ataques en las redes sociales puede causar un daño significativo a la reputación de individuos y organizaciones. La información falsa, las críticas negativas o el contenido dañino difundido en línea pueden dañar la reputación personal o de marca, afectando la posición social, las oportunidades profesionales y la confianza de los clientes. **Pérdida de privacidad:** ignorar las preocupaciones sobre la privacidad puede llevar a la exposición de información privada, incluidas conversaciones, imágenes o videos personales. Esta pérdida de privacidad puede tener consecuencias emocionales y psicológicas, así como posibles amenazas de chantaje. **Consecuencias legales:** ignorar las amenazas cibernéticas y no implementar las medidas de seguridad necesarias puede tener consecuencias legales. Las personas u organizaciones

	pueden enfrentar acciones legales, multas o sanciones regulatorias por violaciones de datos, violaciones de privacidad o incumplimiento de los estándares de ciberseguridad. **Interrupción de los servicios:** las empresas que ignoran las amenazas en línea pueden experimentar interrupciones en sus operaciones. Los ciberataques, como los ataques distribuidos de denegación de servicio (DDoS), pueden sobrecargar los sitios web o las redes, haciendo que los servicios sean inaccesibles para los clientes y provocando una pérdida de ingresos y credibilidad. **Impacto social y emocional:** ignorar el acoso cibernético, el acoso en línea o el comportamiento depredador puede tener graves consecuencias sociales y emocionales para las víctimas. Puede provocar ansiedad, depresión, autoaislamiento e incluso pensamientos de autolesión. **Preocupaciones de seguridad nacional:** ignorar las amenazas en línea puede extenderse más allá de los niveles individuales u organizacionales y convertirse en una cuestión de seguridad nacional. Los ataques cibernéticos a infraestructuras críticas o sistemas gubernamentales pueden interrumpir servicios esenciales, comprometer información confidencial y socavar la estabilidad nacional. 3. PROTECCIÓN DE LA INFORMACIÓN PERSONAL 3.1. IMPORTANCIA DE LA PROTECCIÓN DE LA PRIVACIDAD La protección de la privacidad es de suma importancia en la era digital actual debido al uso generalizado de la tecnología e Internet. Se refiere a proteger la información personal, los datos y las actividades en línea de un individuo contra el acceso no autorizado, el mal uso y la explotación. La importancia de la protección de la privacidad puede entenderse desde varias perspectivas: **Seguridad y protección personal:** La protección de la privacidad garantiza que la información personal confidencial, como números de seguro social, datos financieros o direcciones particulares, permanezca confidencial y segura. Evitar el acceso no autorizado a esta información ayuda a prevenir el robo de identidad, el fraude financiero y otras formas de delitos cibernéticos que pueden tener graves consecuencias para las personas.

	Privacidad y control de datos: las personas tienen derecho a controlar cómo las organizaciones recopilan, almacenan y utilizan sus datos. La protección de la privacidad garantiza que las personas puedan tomar decisiones informadas sobre cómo compartir sus datos y dar su consentimiento para su uso para fines específicos. **Mantener la confianza:** la protección de la privacidad es esencial para generar y mantener la confianza entre personas y organizaciones. Cuando los usuarios confían en que su información personal se manejará de manera responsable y segura, es más probable que interactúen con servicios en línea, realicen transacciones y compartan información con confianza. **Preservar la libertad personal:** Respetar la privacidad significa permitir que las personas se expresen libremente, sin temor a ser vigiladas o discriminadas por sus actividades o preferencias en línea. La protección de la privacidad es esencial para defender el derecho a la libertad de expresión. **Prevención del acoso y el acecho en línea:** la protección de la privacidad protege a las personas del acoso y el acecho en línea. Al restringir el acceso a la información personal, las medidas de privacidad reducen el riesgo de ataques dirigidos o ciberacoso. **Protección de las relaciones personales:** la protección de la privacidad permite a las personas comunicarse y compartir información dentro de los límites de las relaciones de confianza, lo que garantiza que las conversaciones e interacciones privadas sigan siendo confidenciales. **Evitar el uso indebido de datos:** la protección de la privacidad mitiga el riesgo de que los datos personales sean explotados para fines distintos a los previstos por el individuo. Esto incluye evitar campañas de marketing no deseadas, correos electrónicos no deseados o contenido personalizado que pueda infringir el espacio personal. **Prevención de la discriminación y la elaboración de perfiles:** proteger la privacidad puede ayudar a prevenir la elaboración de perfiles y la discriminación de personas en función de su información personal o su comportamiento en línea. La recopilación de datos sin protecciones adecuadas de la privacidad puede dar lugar a una toma de decisiones injusta y sesgada.

Ciberseguridad y confianza digital: la protección de la privacidad y la ciberseguridad están interconectadas. Una violación de la privacidad puede provocar incidentes de ciberseguridad y viceversa. Al priorizar la privacidad, las personas y las organizaciones pueden fomentar una cultura de confianza y seguridad digitales.

3.2. GESTIÓN SEGURA DE CUENTAS EN LÍNEA

La gestión segura de cuentas en línea es un conjunto de prácticas y estrategias destinadas a proteger y gestionar las cuentas en línea de una manera que minimice el riesgo de acceso no autorizado y violaciones de datos. La gestión adecuada de cuentas en línea es crucial para mantener la privacidad de la información personal, prevenir el robo de identidad y salvaguardar los activos digitales. A continuación se detallan algunos aspectos clave y mejores prácticas para la gestión segura de cuentas en línea:

Contraseñas seguras y únicas: utilice contraseñas seguras y únicas para cada cuenta en línea. Evite el uso de contraseñas fáciles de adivinar, como "123456" o "contraseña". En su lugar, cree contraseñas complejas con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

Administradores de contraseñas: considere utilizar un administrador de contraseñas confiable para generar, almacenar y administrar contraseñas de forma segura. Los administradores de contraseñas lo ayudan a mantener contraseñas seguras y únicas para cada cuenta sin la necesidad de recordarlas todas.

Habilite la autenticación de dos factores (2FA): siempre que sea posible, habilite la autenticación de dos factores para sus cuentas en línea. 2FA agrega una capa adicional de seguridad al requerir una segunda forma de verificación, como un código de un solo uso enviado a su dispositivo móvil, además de su contraseña.

Supervise la actividad de la cuenta: revise periódicamente la actividad de su cuenta y esté atento a inicios de sesión no autorizados o acciones sospechosas. Si nota alguna actividad inusual, tome medidas inmediatas para proteger su cuenta, como cambiar su contraseña y comunicarse con el proveedor de la cuenta.

Evite computadoras públicas y Wi-Fi: absténgase de acceder a cuentas confidenciales, como correo electrónico o banca, desde computadoras públicas o redes Wi-Fi no seguras. Las computadoras públicas pueden almacenar credenciales de inicio de sesión y una conexión Wi-Fi no segura puede exponer sus datos a posibles escuchas ilegales.

Tenga cuidado con los intentos de phishing: tenga cuidado con los correos electrónicos, mensajes o enlaces no solicitados que soliciten información confidencial o le soliciten que inicie sesión en sus cuentas. Verifique la legitimidad del remitente y del sitio web antes de proporcionar cualquier información.

Actualice periódicamente la información de recuperación de la cuenta: mantenga actualizada la información de recuperación de su cuenta, como direcciones de correo electrónico o números de teléfono alternativos. Esto garantiza que pueda recuperar el acceso a su cuenta si olvida su contraseña o tiene otros problemas de inicio de sesión.

Revisar la configuración de privacidad y seguridad: revise periódicamente la configuración de privacidad y seguridad de sus cuentas en línea. Ajuste la configuración según sus preferencias y necesidades para garantizar el equilibrio adecuado entre privacidad y funcionalidad.

Cerrar sesión y proteger dispositivos: cierre siempre la sesión de sus cuentas cuando termine de usarlas, especialmente en dispositivos públicos o compartidos. Además, proteja sus dispositivos personales con contraseñas seguras o autenticación biométrica.

Cambie las contraseñas periódicamente : considere cambiar sus contraseñas periódicamente, especialmente para cuentas críticas como correo electrónico y banca. La actualización periódica de las contraseñas añade una capa adicional de seguridad.

Habilite las opciones de recuperación de cuenta: configure opciones de recuperación de cuenta, como preguntas de seguridad o códigos de respaldo, para recuperar el acceso a su cuenta en caso de que esté bloqueado.

3.3. COMPARTIR RESPONSABLEMENTE EN REDES SOCIALES

	El intercambio responsable en las redes sociales se refiere al enfoque consciente y consciente de compartir contenido en plataformas de redes sociales de una manera que respete la privacidad, promueva interacciones positivas y evite contribuir a la desinformación o al daño. Practicar el intercambio responsable en las redes sociales es crucial para mantener la etiqueta digital, fomentar una comunidad en línea positiva y proteger el bienestar personal y colectivo. Estos son algunos aspectos clave del intercambio responsable en las redes sociales: **Protección de la información personal:** tenga cuidado al compartir información personal confidencial, como direcciones particulares, números de teléfono o detalles financieros, en las redes sociales. Proteger la información personal ayuda a protegerse contra el robo de identidad y otros riesgos relacionados con la privacidad. **Ajuste de la configuración de privacidad:** revise y ajuste periódicamente su configuración de privacidad en las plataformas de redes sociales. Personalice la audiencia para cada publicación, asegurándose de que solo la audiencia prevista pueda ver e interactuar con su contenido. **Respetar el consentimiento:** obtener el consentimiento de las personas antes de compartir sus fotografías o información personal en las redes sociales. Sea considerado con las preferencias de las personas con respecto a ser etiquetado en publicaciones o mencionado en el contenido. **Verificación de hechos y evitar información errónea:** antes de compartir artículos de noticias, información o imágenes, verifique su exactitud a partir de fuentes confiables. Evite difundir información errónea o contenido no verificado que pueda contribuir a la difusión de rumores o narrativas falsas. **Sea consciente del momento y la frecuencia:** evite compartir de forma excesiva o inapropiada, ya que puede generar una sobrecarga de información para sus seguidores. Tenga en cuenta el momento de sus publicaciones para respetar las diferentes zonas horarias y las preferencias de su audiencia. **Promoción de contenido positivo:** comparta contenido que sea edificante, informativo o inspirador. El intercambio positivo contribuye a un entorno en línea más saludable y fomenta un sentido de comunidad entre sus seguidores.

Manejar los desacuerdos con respeto: participar en debates respetuosos y constructivos en las redes sociales, incluso cuando no esté de acuerdo con los demás. Evite participar en discusiones en línea o recurrir a ataques personales.

Evitar contenido dañino u ofensivo: abstenerse de compartir contenido que pueda resultar ofensivo, discriminatorio o perjudicial para otros. Sea consciente del impacto potencial de sus publicaciones en diferentes personas y comunidades.

Protección de los derechos de autor: Respete las leyes de derechos de autor y evite compartir material protegido por derechos de autor sin la autorización o atribución adecuada. Da crédito a los creadores originales cuando compartas su trabajo.

Revisión de contenido compartido: revise periódicamente su contenido compartido para asegurarse de que se alinee con sus valores y la imagen que desea mostrar en línea. Elimine o actualice publicaciones que quizás ya no reflejen sus perspectivas actuales.

Promoción de la bondad digital: sea amable y empático en sus interacciones en las redes sociales. Evite participar o difundir ciberacoso, incitación al odio o cualquier forma de comportamiento dañino.

Fomentar una cultura positiva en línea: anime a otros a practicar el intercambio responsable en las redes sociales dando un ejemplo positivo. Participar en debates sobre ciudadanía digital y la importancia de ser ciudadanos digitales responsables.

4. NAVEGAR EN LAS REDES SOCIALES DE FORMA SEGURA

4.1. AJUSTAR LA CONFIGURACIÓN DE PRIVACIDAD

Ajustar la configuración de privacidad se refiere al proceso de personalizar el nivel de acceso y visibilidad de la información personal en diversas plataformas, sitios web y aplicaciones. Implica tomar decisiones informadas sobre qué datos se comparten, con quién se comparten y cómo los utilizan terceros. Al ajustar la configuración de privacidad,

	las personas pueden mantener un mayor control sobre su huella digital y proteger su información personal de una exposición innecesaria. A continuación se ofrece una explicación detallada de la importancia y los pasos necesarios para ajustar la configuración de privacidad: **Importancia de ajustar la configuración de privacidad:** **Protección de la información personal:** ajustar la configuración de privacidad permite a las personas limitar la cantidad de información personal visible para otros, lo que reduce el riesgo de robo de identidad, acoso o ataques de ingeniería social. **Controlar el intercambio de datos:** al personalizar la configuración de privacidad, las personas pueden controlar qué datos comparten con plataformas de redes sociales, sitios web y aplicaciones, limitando la recopilación y el uso de su información. **Prevención de publicidad dirigida:** la configuración de privacidad puede ayudar a las personas a optar por no recibir publicidad dirigida y contenido personalizado, brindando una experiencia en línea más privada y menos intrusiva. **Evitar el uso indebido de datos:** ajustar la configuración de privacidad reduce las posibilidades de uso indebido de datos por parte de terceros no autorizados, lo que protege contra posibles infracciones y acceso no autorizado a información confidencial. **Mejora de la seguridad en línea:** restringir el acceso a la información personal a través de configuraciones de privacidad puede mejorar la seguridad en línea y minimizar el riesgo de ingeniería social o ataques de phishing. **Pasos para ajustar la configuración de privacidad:** **Revisar la configuración de la cuenta:** en las plataformas de redes sociales, revise la configuración de la cuenta o la sección de configuración de privacidad para acceder a las opciones para personalizar las preferencias de privacidad. **Elija audiencia para publicaciones:** determine quién puede ver sus publicaciones, como amigos, amigos de amigos o el público. Opte por una audiencia más reducida para limitar la visibilidad de su contenido.

	Controlar la información del perfil: decida qué información del perfil es visible para otros, como su dirección de correo electrónico, número de teléfono o fecha de nacimiento. Minimice la visibilidad de datos confidenciales si es posible. **Administrar permisos de aplicaciones:** en aplicaciones móviles, revise y administre los permisos de aplicaciones en la configuración del dispositivo. Permita solo los permisos necesarios para cada aplicación y revoque los permisos para las aplicaciones que no los requieran. **Exclusión voluntaria de la recopilación de datos:** algunas plataformas y sitios web ofrecen la opción de excluirse de la recopilación y el intercambio de datos con fines publicitarios. Aproveche estas opciones para reducir el seguimiento de datos. **Personaliza la ubicación compartida:** elige cuándo y con quién compartes tu ubicación. Desactive el uso compartido de ubicación cuando no sea necesario o limítelo a aplicaciones confiables específicas. **Considere la navegación anónima:** utilice modos de navegación privados o de incógnito para evitar el almacenamiento del historial de navegación y las cookies en su dispositivo. **Verifique el acceso a aplicaciones de terceros:** revise y administre aplicaciones de terceros que tienen acceso a la información de su cuenta. Revocar el acceso a aplicaciones que ya no estén en uso o que no necesiten acceso. **Tenga cuidado con la configuración predeterminada:** muchas plataformas tienen configuraciones de privacidad predeterminadas que pueden ser más permisivas de lo deseado. Tómese el tiempo para ajustar estas configuraciones según sus preferencias. **Revisar y actualizar periódicamente:** revise y actualice periódicamente su configuración de privacidad, ya que las plataformas y aplicaciones pueden introducir nuevas funciones o cambios que afecten su privacidad. 4.2. MANEJO DE SOLICITUDES DE AMIGOS Y MENSAJES

	Manejar solicitudes de amistad y mensajes en plataformas de redes sociales y aplicaciones de mensajería implica ser cauteloso, perspicaz y respetuoso en sus interacciones con los demás. Es esencial mantener los límites personales, proteger su privacidad y fomentar una experiencia en línea positiva. Aquí hay algunas pautas para manejar solicitudes de amistad y mensajes: **Manejo de solicitudes de amistad:** **Verificar identidad:** antes de aceptar una solicitud de amistad, asegúrese de conocer a la persona o de tener amigos en común. Tenga cuidado al aceptar solicitudes de perfiles desconocidos o sospechosos. **Verifique la configuración de privacidad:** ajuste su configuración de privacidad para controlar quién puede enviarle solicitudes de amistad. Limite las solicitudes de amistad a amigos de amigos o grupos específicos para reducir las posibilidades de recibir solicitudes de extraños. **Evite aceptar extraños:** sea selectivo al agregar nuevas conexiones. Evite aceptar solicitudes de amistad de personas que no conoce personalmente, especialmente si no tienen conexiones mutuas. **Bloquear o informar cuentas sospechosas:** si recibe solicitudes de amistad de cuentas sospechosas o falsas, considere bloquearlas o informarlas a los administradores de la plataforma. **Revisar la información del perfil:** antes de aceptar una solicitud de amistad, revise el perfil del solicitante para asegurarse de que parezca genuino y se ajuste a sus valores e intereses. **Respete los límites:** está bien rechazar solicitudes de amistad si no se siente cómodo conectándose con alguien. Respete sus propios límites y no se sienta obligado a aceptar todas las solicitudes. **Manejo de mensajes:** **Sea respetuoso:** responda los mensajes de manera educada y respetuosa. Trate a los demás como le gustaría que lo trataran a usted en una conversación en línea.

Verificar remitentes: si recibe un mensaje de un remitente desconocido, tenga cuidado. Evite hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocidas.

Evite compartir información confidencial: absténgase de compartir información personal confidencial, detalles financieros o contraseñas a través de aplicaciones de mensajería. Tenga cuidado al compartir información privada con personas que no conoce bien.

Informar acoso o abuso: si recibe mensajes ofensivos, amenazantes o acosadores, informe al remitente a los administradores de la plataforma o al equipo de soporte de la aplicación de mensajería.

Establecer privacidad de mensajes: ajuste la configuración de privacidad de sus mensajes para controlar quién puede enviarle mensajes. Limite el acceso a la mensajería a sus amigos o contactos.

Utilice la función de bloqueo: si alguien le molesta o le envía mensajes inapropiados, utilice la función de bloqueo para evitar que esa persona se comunique más.

Sea consciente del tono y la intención: los mensajes pueden malinterpretarse fácilmente debido a la falta de tono y expresiones faciales. Sea consciente de su propia comunicación y trate de evitar malentendidos.

Tome descansos de la mensajería: está bien tomar descansos de la mensajería y las redes sociales para concentrarse en otras actividades y reducir la sobrecarga digital.

4.3. DENUNCIAR Y BLOQUEAR CUENTAS ABUSIVAS

Denunciar y bloquear cuentas abusivas es un paso crucial para mantener un entorno en línea seguro y positivo. Las cuentas abusivas pueden incurrir en comportamientos dañinos, como ciberacoso, acoso, incitación al odio y otras formas de abuso en línea. Informar y bloquear estas cuentas ayuda a protegerse a sí mismo y a los demás de sus acciones dañinas. A continuación se ofrece una explicación de cómo funcionan los informes y el bloqueo y por qué son importantes:

	Denunciar cuentas abusivas: **Identifique un comportamiento dañino:** si encuentra una cuenta que presenta un comportamiento abusivo o dañino, como acoso, amenazas o discursos de odio, es importante reconocerlo. **Informar la cuenta:** la mayoría de las plataformas de redes sociales y servicios en línea tienen un mecanismo de denuncia. Utilice la función de informes de la plataforma para informar a los administradores o moderadores sobre el comportamiento abusivo. **Proporcionar pruebas:** al denunciar una cuenta abusiva, puede resultar útil proporcionar pruebas, como capturas de pantalla o enlaces al contenido ofensivo, para respaldar su denuncia. **Elija la categoría adecuada:** las plataformas de redes sociales suelen ofrecer diferentes categorías de informes. Seleccione la categoría que mejor se ajuste al tipo de abuso que está denunciando. **Respete las pautas de presentación de informes:** familiarícese con las pautas de presentación de informes de la plataforma para asegurarse de que está informando cuentas por motivos válidos. Evite informes falsos, ya que pueden obstaculizar la eficacia del sistema de informes. **Bloqueo de cuentas abusivas:** **Protéjase:** bloquear una cuenta abusiva evita que esa cuenta interactúe con usted. Puede ayudar a proteger su bienestar mental y crear un espacio en línea seguro para usted. **Evite contactos no deseados:** cuando bloquea una cuenta, el usuario detrás de esa cuenta no podrá seguirlo, enviarle mensajes ni comentar sus publicaciones. **Anonimato:** El bloqueo suele ser una acción privada. El usuario que bloquees no recibirá ninguna notificación de que ha sido bloqueado. **No más interacción:** después de bloquear una cuenta, ya no verás su contenido o actividad, y ellos no podrán ver la tuya. **Por qué son importantes informar y bloquear:**

Prevención de daños: denunciar cuentas abusivas puede llevar a que se tomen medidas contra la cuenta, lo que puede evitar mayores daños a usted o a otros.

Hacer cumplir las pautas de la plataforma: denunciar comportamientos abusivos ayuda a hacer cumplir los términos de servicio de la plataforma y las pautas de la comunidad, creando un entorno más seguro para todos los usuarios.

Apoyando la salud de la comunidad: al denunciar y bloquear cuentas abusivas, contribuyes a fomentar una comunidad en línea saludable y respetuosa.

Empoderar a los usuarios: denunciar y bloquear permite a las personas tomar el control de sus experiencias en línea y protegerse de interacciones abusivas o dañinas.

5. CIBERSEGURIDAD Y DISPOSITIVOS MÓVILES

5.1. PROTECCIÓN DE SMARTPHONES Y TABLETAS

Proteger los teléfonos inteligentes y las tabletas es esencial en el mundo actual impulsado por los dispositivos móviles, donde estos dispositivos almacenan una gran cantidad de información personal y datos confidenciales. Proteger estos dispositivos ayuda a proteger contra el acceso no autorizado, las filtraciones de datos y los ataques de malware. A continuación se presentan algunas medidas clave para garantizar la seguridad de los teléfonos inteligentes y tabletas:

Habilitar seguridad de pantalla de bloqueo: configure un método seguro de pantalla de bloqueo, como PIN, patrón, contraseña o biométrico (huella digital o reconocimiento facial). Esto evita el acceso no autorizado a su dispositivo en caso de pérdida o robo.

Mantenga el software actualizado: actualice periódicamente el sistema operativo y las aplicaciones de su dispositivo. Los fabricantes publican actualizaciones para corregir vulnerabilidades de seguridad, por lo que mantener su dispositivo actualizado es crucial para mantenerse protegido contra posibles vulnerabilidades.

	Instale solo aplicaciones confiables: descargue aplicaciones de tiendas de aplicaciones oficiales (por ejemplo, Google Play Store, Apple App Store) y evite instalar aplicaciones de fuentes desconocidas. Las aplicaciones maliciosas de fuentes no oficiales pueden comprometer la seguridad y privacidad de su dispositivo. **Revisar los permisos de las aplicaciones:** tenga cuidado al otorgar permisos a las aplicaciones. Revise los permisos solicitados por cada aplicación y considere si son necesarios para la funcionalidad de la aplicación. Evite otorgar permisos innecesarios que puedan comprometer su privacidad. **Utilice una VPN en Wi-Fi público:** cuando utilice redes Wi-Fi públicas, considere utilizar una red privada virtual (VPN) para cifrar su tráfico de Internet y proteger sus datos de posibles escuchas o espionaje. **Navegación móvil segura:** utilice navegadores seguros que ofrezcan conexiones cifradas (HTTPS) para sitios web. Evite el acceso a información confidencial, como la banca en línea, en redes públicas o no seguras. **Haga una copia de seguridad de los datos con regularidad:** haga una copia de seguridad de los datos de su dispositivo con regularidad en un servicio de nube seguro o en un dispositivo externo. Esto garantiza que su información importante esté segura incluso si su dispositivo se pierde, se daña o se reinicia. **Evite hacer clic en enlaces sospechosos:** tenga cuidado al hacer clic en enlaces en correos electrónicos, mensajes o ventanas emergentes de fuentes desconocidas. Hacer clic en enlaces maliciosos puede provocar intentos de phishing o la instalación de malware. **Utilice bloqueos de aplicaciones para aplicaciones confidenciales:** considere usar bloqueos de aplicaciones o una función de modo de invitado para restringir el acceso a aplicaciones o contenidos confidenciales en su dispositivo. Esto proporciona una capa adicional de seguridad, especialmente cuando comparte su dispositivo con otras personas. **Cifre los datos del dispositivo:** si su dispositivo lo admite, habilite el cifrado para proteger sus datos del acceso no

autorizado, incluso si otra persona accede físicamente al dispositivo.

5.2. PERMISOS DE APLICACIONES Y ACCESO A DATOS

Los permisos de aplicaciones y el acceso a datos se refieren a los permisos solicitados por las aplicaciones móviles (aplicaciones) para acceder a diversas funciones y datos en el dispositivo de un usuario. Cuando los usuarios instalan y usan aplicaciones en sus teléfonos inteligentes o tabletas, es posible que las aplicaciones requieran acceso a ciertos recursos del dispositivo e información personal para funcionar correctamente. Estos permisos permiten que las aplicaciones ofrezcan funcionalidades específicas y mejoren la experiencia del usuario. Sin embargo, es esencial que los usuarios comprendan y administren estos permisos para proteger su privacidad y seguridad. Aquí hay un vistazo más de cerca a los permisos de las aplicaciones y el acceso a los datos:

Tipos de permisos de aplicaciones: los permisos de las aplicaciones pueden variar según la funcionalidad de la aplicación y la plataforma (Android o iOS). Los tipos comunes de permisos de aplicaciones incluyen acceso a la cámara, micrófono, ubicación, contactos, calendario, almacenamiento, SMS, registros de llamadas y más del dispositivo. Algunas aplicaciones también pueden solicitar permiso para utilizar otros dispositivos conectados, como periféricos Bluetooth.

Solicitudes de permiso: cuando los usuarios instalan una aplicación, la aplicación puede solicitar permisos específicos que necesita para funcionar. Las solicitudes de permiso generalmente se presentan durante el proceso de instalación de la aplicación o cuando la aplicación intenta acceder por primera vez a una función en particular. Los usuarios pueden otorgar o denegar estos permisos.

Propósito de los permisos de la aplicación: los permisos de la aplicación son necesarios para habilitar ciertas funciones de la aplicación. Por ejemplo, una aplicación de edición de fotografías necesita acceso a la cámara y al almacenamiento del dispositivo para capturar y guardar fotografías. Una aplicación de navegación requiere acceso a la ubicación para proporcionar indicaciones precisas.

Protección de la privacidad: si bien los permisos de las aplicaciones suelen ser esenciales para su funcionalidad, los usuarios deben tener cuidado al otorgar permisos sin considerar el propósito de la aplicación y si los permisos solicitados son razonables. Otorgar permisos excesivos podría comprometer la privacidad o permitir que las aplicaciones accedan a datos confidenciales sin una necesidad legítima.

Administrar los permisos de las aplicaciones: la mayoría de los sistemas operativos modernos permiten a los usuarios administrar los permisos de las aplicaciones. Los usuarios pueden revisar y modificar los permisos de las aplicaciones en la configuración del dispositivo, lo que les permite otorgar o revocar permisos específicos para aplicaciones individuales en cualquier momento.

Leer los permisos con atención: antes de otorgar permisos, los usuarios deben leer atentamente los permisos solicitados por una aplicación. Si una aplicación solicita permisos que parecen no estar relacionados con su funcionalidad, puede ser una señal de alerta y los usuarios deben tener cuidado o considerar el uso de aplicaciones alternativas.

Permisos y actualizaciones de aplicaciones: al actualizar aplicaciones, es esencial revisar los permisos nuevos o modificados. A veces, las actualizaciones de la aplicación pueden introducir permisos adicionales y los usuarios deben asegurarse de que se ajusten a sus preferencias y necesidades.

Solicitudes de permisos de aplicaciones para iOS y Android: si bien iOS y Android manejan los permisos de las aplicaciones de manera diferente, ambas plataformas ofrecen a los usuarios la posibilidad de administrar los permisos en sus respectivas configuraciones. En iOS, los usuarios pueden revisar y administrar los permisos en la configuración de la aplicación en "Privacidad". En Android, los usuarios pueden administrar los permisos yendo a "Aplicaciones y notificaciones" o "Administrador de aplicaciones" en la configuración del dispositivo.

5.3. PROTECCIÓN DE DISPOSITIVOS MÓVILES CONTRA ROBOS Y PÉRDIDAS

Proteger los dispositivos móviles contra robos y pérdidas es crucial para salvaguardar la información personal, prevenir

	el robo de identidad y preservar la privacidad de los datos confidenciales. Los dispositivos móviles, como los teléfonos inteligentes y las tabletas, suelen ser el objetivo de los ladrones debido a su portabilidad y la valiosa información que almacenan. La implementación de medidas de seguridad puede reducir significativamente los riesgos asociados con el robo o la pérdida. A continuación se detallan algunos pasos importantes para proteger los dispositivos móviles: **Configurar la seguridad de la pantalla de bloqueo:** habilite un método seguro de pantalla de bloqueo, como un PIN, patrón, contraseña o biométrico (huella digital o reconocimiento facial). Esto evita el acceso no autorizado a su dispositivo si cae en las manos equivocadas. **Usar los servicios de Buscar mi dispositivo:** habilite la función "Buscar mi dispositivo" o "Buscar mi iPhone" en su dispositivo. Estos servicios le permiten localizar, bloquear o borrar su dispositivo de forma remota en caso de pérdida o robo. **Mantenga el software y las aplicaciones actualizados:** actualice periódicamente el sistema operativo y las aplicaciones de su dispositivo para asegurarse de tener los últimos parches de seguridad y correcciones de errores. Los fabricantes lanzan actualizaciones para abordar vulnerabilidades y mejorar la seguridad del dispositivo. **Evite dejar dispositivos desatendidos:** tenga cuidado al dejar su dispositivo móvil desatendido en lugares públicos, como restaurantes, transporte público o gimnasios. Mantenga su dispositivo con usted o guárdelo de forma segura para reducir el riesgo de robo. **Manténgase alerta en áreas concurridas:** preste atención a su entorno en áreas concurridas, especialmente donde es más probable que ocurran carteristas y robos. Tenga cuidado al utilizar su dispositivo en espacios concurridos. **Guarde su dispositivo de forma segura en casa:** mantenga su dispositivo móvil en un lugar seguro cuando no esté en uso, especialmente en casa. Evite dejarlo en mostradores, cerca de ventanas abiertas o áreas de fácil acceso. **Utilice bloqueos de aplicaciones para aplicaciones confidenciales:** considere usar bloqueos de aplicaciones o funciones del modo invitado para restringir el acceso a aplicaciones o contenidos confidenciales en su dispositivo.

	Esto agrega una capa adicional de seguridad, especialmente cuando comparte su dispositivo con otras personas. **Cifre los datos del dispositivo:** si su dispositivo lo admite, habilite el cifrado para proteger sus datos del acceso no autorizado, incluso si otra persona accede físicamente al dispositivo. **Evite las estaciones de carga públicas:** absténgase de utilizar estaciones de carga públicas o puertos USB, ya que pueden verse comprometidos y representar un riesgo de robo de datos o instalación de malware. **Haga una copia de seguridad de los datos con regularidad:** haga una copia de seguridad de los datos de su dispositivo con regularidad en un servicio de nube seguro o en un dispositivo externo. Esto garantiza que su información importante esté segura incluso si su dispositivo se pierde, se daña o se reinicia. **Utilice protectores de pantalla de privacidad:** considere usar protectores de pantalla de privacidad para evitar que miradas indiscretas vean su pantalla en espacios públicos. **Registre dispositivos con las autoridades:** registre sus dispositivos móviles con las autoridades locales o bases de datos relevantes. Esto puede ayudar en el proceso de recuperación si le roban el dispositivo.
Glosario :	1. Seguridad en línea La práctica de seguir pautas prácticas, comprender la tecnología moderna y proteger los dispositivos digitales para defenderse de partes maliciosas del mundo en línea. 2. Seguridad en Internet Medidas y prácticas tomadas para proteger computadoras, redes y datos de amenazas cibernéticas, como malware, virus y acceso no autorizado. 3. Privacidad digital El derecho a controlar y proteger la información y los datos personales para que no sean accedidos, utilizados o compartidos sin consentimiento. 4. Ciberseguridad La protección de dispositivos digitales, redes y sistemas de información contra amenazas cibernéticas, incluidos

	piratería informática, violaciones de datos y ataques cibernéticos. 5. Prácticas seguras en línea El conjunto de pautas y comportamientos que las personas deben seguir para garantizar que sus actividades en línea sean seguras y protejan su privacidad. 6. Protección de información personal La salvaguardia de los datos sensibles y personales frente al acceso no autorizado o uso indebido, previniendo la suplantación de identidad y el fraude. 7. Etiqueta en las redes sociales El comportamiento adecuado y respetuoso que las personas deben seguir al utilizar las plataformas de redes sociales. 8. Seguridad de los datos Medidas y protocolos adoptados para proteger los datos digitales del acceso, modificación o destrucción no autorizados. 9. Prevención del robo de identidad Técnicas y prácticas para salvaguardar la información personal y evitar que los delincuentes la utilicen para hacerse pasar por personas. 10. Gestión de contraseñas La práctica responsable de crear contraseñas únicas y seguras y administrarlas de forma segura para proteger las cuentas en línea. 11. Amenazas en línea Diversos riesgos y peligros que se encuentran al utilizar Internet, como phishing, malware, estafas y ciberacoso. 12. Concientización sobre el phishing La capacidad de reconocer y evitar intentos de phishing, en los que los atacantes engañan a las personas para obtener información confidencial, a menudo a través de correos electrónicos o sitios web fraudulentos. 13. Configuración de privacidad Las opciones personalizables en las plataformas en línea que permiten a los usuarios controlar la visibilidad de su información personal y la audiencia de su contenido. 14. Denunciar abuso

	El proceso de informar a los administradores o moderadores de la plataforma sobre comportamientos abusivos o dañinos en la plataforma, como acoso o discurso de odio. 15. Bloqueo de cuentas La acción de evitar que una cuenta abusiva o no deseada interactúe con usted o vea su contenido en plataformas de redes sociales. 16. Transacciones seguras en línea Garantizar que las transacciones en línea, como compras o transacciones financieras, se realicen de forma segura para evitar el fraude. 17. Huella digital El rastro de datos e información que dejan las actividades en línea de un individuo, incluidas publicaciones en redes sociales, historial de búsqueda e interacciones en línea. 18. Prevención del ciberacoso Medidas tomadas para detener y prevenir el acoso, la intimidación o el acoso en línea. 19. Autenticación de dos factores (2FA) Una capa adicional de seguridad que requiere que los usuarios proporcionen dos formas de identificación (por ejemplo, contraseña y un código único enviado a su teléfono) para acceder a una cuenta. 20. Hábitos de navegación segura Prácticas y pautas para garantizar una navegación segura y protegida en Internet, evitando sitios web y contenidos de riesgo.
Bibliografía:	Consejos y reglas de seguridad en Internet (kaspersky.com) Seguridad en línea (para Adolecentes) - Nemours KidsHealth ¿Qué es la seguridad en línea? | SWGfL Conversación sobre seguridad en línea | LearnEnglish Teens (britishcouncil.org) Seguridad en Internet - Wikipedia Cuestiones de seguridad en línea - Consejos para apoyar a los niños | Asuntos de Internet

	Seguridad en Internet: Introducción a la seguridad en Internet (gcfglobal.org) indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001 "Seguridad en Internet" en: La Enciclopedia Internacional de Alfabetización Mediática en Línea (researchgate.net) İnternette Güvenlik İpuçları - Google Güvenlik Merkezi (safety.google) Estar seguro en línea | Comisionado de seguridad electrónica Cómo mantenerse seguro en línea: consejos y recursos de seguridad en Internet (reviews.org)
Recursos (vídeos, enlace de referencia)	https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D