PESADILLAS DEL INTERNET

Tecnologías digitales para el aprendizaje y la enseñanza

Mayte Carolina González Ramos
Escuela Normal de Cuautitlán Izcalli
Licenciatura en Educación Preescolar

Primer Semestre
1°4

Índice

Introducción

El internet es una red[1] de computadoras que se encuentran interconectadas a nivel mundial para compartir información. Se trata de una red de equipos de cálculo que se relacionan entre sí a través de la utilización de un lenguaje universal (Etecé, 2021). Esta red global que conecta a personas de todo el mundo ha evolucionado la forma en que compartimos información, nos comunicamos y accedemos a recursos, se convirtió en una parte fundamental de la vida cotidiana para millones de personas en todo el mundo. Aunque esta red mundial ofrece una gama infinita de oportunidades no está exenta de riesgos significativos que deben ser reconocidos y comprendidos.

La prevención de estas invasiones digitales requiere no solo la comprensión de los mecanismos de protección de la privacidad, sino también una toma de conciencia activa sobre el valor intrínseco de nuestros datos personales. La prevención no solo recae en las manos de los expertos en tecnología, sino también en la responsabilidad individual de adoptar prácticas seguras y mantenerse al tanto de las últimas tácticas utilizadas por los ciberdelincuentes.

El siguiente ensayo pretende hacer conciencia sobre los peligros que acechan en el vasto mundo del Internet, explorando desde amenazas comunes hasta cuestiones más complejas. A través de una investigación detallada, se buscará arrojar luz sobre las diversas formas en que los usuarios[2] pueden enfrentar estos desafíos y adoptar medidas preventivas efectivas. En un mundo cada vez más interconectado, comprender y reducir los riesgos de Internet se convierte en una tarea imperativa para salvar nuestra seguridad y preservar los principios fundamentales de la era digital.

[1] Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información.
[2] Persona que navega en internet.

Seguridad y privacidad en el internet

La privacidad y seguridad en Internet son de suma importancia en la sociedad digital actual. Estos aspectos no solo son fundamentales para la protección de los usuarios a nivel personal, sino que también son cruciales para la integridad de la sociedad en su conjunto. A continuación, se explicará sobre la importancia que tienen estos campos en el uso del internet:

¿Qué es la seguridad en internet?

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red, como infraestructura[3] e información, que suele ser la más afectada por delincuentes cibernéticos[4]. La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en la información y equipos físicos, como los computadores (GCFGlobal, 2018).

La seguridad en Internet es un esfuerzo continuo que requiere la participación activa de los usuarios, empresas y organizaciones. Al adoptar prácticas sólidas de seguridad y mantenerse al tanto de las amenazas emergentes, se puede reducir significativamente el riesgo de ataques cibernéticos y proteger la privacidad en línea.

¿Qué es la privacidad en internet?

La privacidad es un derecho importante y un facilitador fundamental de la autonomía personal, la dignidad y la libertad de expresión. Aunque no existe una definición de privacidad universalmente aceptada, en el contexto de Internet en general se conviene que privacidad es el derecho de determinar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros (Internetsociety, 2017).

[3] Conjunto de componentes necesarios para el funcionamiento de la tecnología.
[4] Persona que utiliza el internet y la tecnología para cometer actos ilícitos.

En la era digital actual, la información se puede recopilar de forma más rápida y fácil que nunca. Los avances en diferentes frentes tecnológicos han contribuido a este nuevo escenario.

Los datos se pueden intercambiar de forma rápida y distribuida, lo que permite su fácil proliferación; las herramientas de búsqueda en Internet pueden reconocer imágenes, rostros, sonidos, voces y movimientos, por lo que resulta fácil rastrear dispositivos y personas en línea a lo largo del tiempo y en diferentes lugares; se están desarrollando sofisticadas herramientas para vincular, correlacionar y agregar a gran escala datos que aparentemente no tienen ninguna relación entre sí; es cada vez más fácil identificar individuos a partir de datos supuestamente anonimizados[5] o desprovistos de identificación (Internetsociety, 2017).

La privacidad y seguridad en Internet son pilares esenciales para salvaguardar la integridad de los individuos, proteger sus derechos fundamentales y mantener la confianza en la sociedad digital en constante evolución. Su importancia solo aumentará a medida que la tecnología continúe desempeñando un papel central en nuestras vidas cotidianas.

[5] Que no se conoce al dueño o autor.

Riesgos en el internet

Si bien el internet ha venido a revolucionar la era digital con muchos beneficios y se ha convertido en una herramienta para el ser humano en su vida cotidiana, sin embargo, los usuarios se encuentran inmersos en un entorno virtual que, si bien ofrece innumerables oportunidades, también está plagado de peligros y amenazas. Algunos de los riesgos más destacados que enfrentan los usuarios en Internet son:

Riesgos de privacidad y manejo de la información confidencial

Son aquellos que tienen que ver con la preservación de los datos personales del usuario. Estos riesgos vinculados con la privacidad y la seguridad de la información son probablemente los más comunes para todo tipo de usuarios de internet, y consisten en la pérdida del control sobre información personal importante, sensible de ser utilizada por terceros para su beneficio (Editorial Etecé, 2023). Como pueden ser los siguientes:

El phishing o fingimiento de identidad

Ocurre cuando terceros se hacen pasar por una institución u organización de confianza en correos electrónicos y páginas web fraudulentas, para tener acceso a la información confidencial del usuario, como claves bancarias o números de tarjeta de crédito (Editorial Etecé, 2023).

Robo de información

El robo de datos es el acto de robar información digital almacenada en equipos, servidores o dispositivos electrónicos para obtener información confidencial o afectar la privacidad. El robo de datos suele ocurrir debido a que los criminales desean vender la información o usarla para el robo de identidad. El robo de datos solía ser un problema principalmente para las empresas y organizaciones, pero, desafortunadamente, es un problema cada vez más usual para los usuarios (Kaspersky, 2023).

Aunque el término hace referencia a un “robo”, el robo de datos no significa necesariamente que se le quita la información a la víctima. En cambio, en un robo de datos, el atacante simplemente copia o duplica la información para su propio uso.

El malware y virus

Se trata de programas informáticos diseñados para descargarse e infiltrarse en la computadora del usuario y adueñarse de sus datos sin su consentimiento, o abrir puertas para que un tercero pueda espiar su información (Editorial Etecé, 2023).

Estafas, robos y engaños en línea

Así como ocurre en la vida offline[6], en internet existen personas que ofrecen servicios falsos, venden productos engañosos o solicitan donaciones para causas ficticias, con el fin de enriquecerse ilegalmente (Editorial Etecé, 2023).

Hackeo o pirateo cibernético

Se trata de usuarios con un alto nivel de conocimiento técnico y especializado que utilizan distintos programas para tener acceso a computadoras ajenas y robar información. Esto puede ocurrirle a un usuario cualquiera, instituciones o incluso grandes corporaciones, razón por la cual estas invierten mucho dinero en seguridad informática (Editorial Etecé, 2023).

Riesgos propios de la interacción con terceros

Internet es una herramienta de comunicación masiva, de modo que, en la mayoría de los casos, nuestras interacciones en línea se dan con otros usuarios que están conectados a través de su teléfono o computadora, a menudo usando cuentas anónimas o ficticias. Esto se da especialmente en el mundo de las redes sociales, los foros y aplicaciones sociales o de citas. Editorial Etecé (2023) menciona los sigueintes ejemplos como riesgos de la intercción con terceros en el internet:

[6] Estado del usuario cuando se desconecta del internet.

Ciberacoso o ciberbullying

Se trata de la versión en línea del bullying[7] o acoso, que si bien no suele incluir violencia física (dado que las interacciones son a distancia) sí suele abarcar diferentes formas de violencia psicológica y social, como la humillación pública, el acoso masivo a través de cuentas de redes sociales y la publicación en línea de contenidos personales sensibles (direcciones, números telefónicos, fotografías íntimas).

Manipulación sexual o grooming

Se trata de la manipulación y el engaño sin fines económicos claros, sino en busca de placer personal, sexual o de otros tipos. Ya sea que se le haga a un adulto o a un menor de edad (en este caso se suele hablar de grooming), este tipo de interacciones suele ser muy riesgosa ya que normalmente conduce a encuentros en la vida real, en los que la persona contactada puede resultar muy distinta de lo que decía ser en línea.

Cibersecuestros, extorsión y otras formas de delito informático

Ocurre cuando un usuario pierde el control de su correo electrónico o cuenta de redes sociales, y normalmente se utiliza su información para fingir un secuestro real y extraerles dinero a sus familiares, o bien para extorsionar al usuario bajo amenaza de divulgar datos sensibles de sus cuentas personales.

Riesgos de acceso a información falsa o sensible

Son aquellos que tienen que ver con el acceso a la pornografía, el material cruento y mórbido, o también las fake news[8]. Debido a que el internet ofrece una gran cantidad de información, sin embargo, no todo el contenido al que se puede acceder mediante sus páginas es confiable, legítimo o adecuado para el usuario en cuestión, especialmente cuando se trata de un niño o adolescente. Algunos ejemplos que Editorial Etecé (2023) considera de este tipo son los siguientes:

[7] Agresión constante que se ejerce para hacer sentir inferior a una persona.
[8] Noticias e información falsa que se encuentra en el internet.

Pornografía, crueldad y contenidos morbosos

El libre acceso de los niños y adolescentes a información que no sean capaces de comprender cabalmente, especialmente en ausencia de acompañamiento parental[9], constituye un importante riesgo de internet y las redes sociales. Existen todo tipo de contenidos en línea, por lo que resulta importante contar con algún tipo de control parental o de dinámica familiar de confianza para hacerles frente.

Radicalización y exposición a contenidos tóxicos

En la era de las redes sociales, el florecimiento de comunidades de usuarios organizados en torno a creencias radicales o conductas sociales tóxicas se ha convertido en un verdadero problema, ya que estos cultos fomentan las conductas fanáticas en torno a causas políticas y sociales a través de contenidos ficticios o manipuladores.

Compras inducidas y otras formas de publicidad engañosa

Dado que mucha de la información disponible en internet es gratuita, la publicidad es el principal mecanismo a través del cual se rentabiliza la atención de los usuarios. Esto, junto a la falta de una legislación[10] en línea, permite el florecimiento de publicidad engañosa y todo tipo de promesas para llevar al usuario a concretar, voluntaria o involuntariamente, compras reales en las que tiene poco o ningún control.

Riesgos derivados del mal uso de internet

Existen algunos riesgos que no resultan inherentes a internet, sino al uso que hagan de ella los usuarios. Es decir, al mal uso de esta herramienta, que al igual que cualquier otra, puede convertirse en un peligro si se usa de modo indebido. Son ejemplos de este tipo de riesgos (Editorial Etecé, 2023):

[9] Control que tiene un padre o adulto sobre la información de un menor de edad.
[10] Conjunto de leyes que regulan en este caso el buen uso del internet.

Adicción a internet

Se han descrito diferentes formas de adicción psicológica a internet, tanto en las redes sociales, los videojuegos en línea u otras plataformas que le brindan al usuario una gratificación instantánea y un sentido de pertenencia a los que puede resultar difícil renunciar para algunos usuarios. En estos casos, el usuario adicto sacrifica otros aspectos importantes de su vida (familia, amigos, trabajo) con tal de continuar jugando o conectándose a la red social.

Aislamiento social

La socialización en línea puede ser rica y compleja, tanto como la socialización real, pero esto puede resultar problemático cuando los usuarios renuncian a la vida real, invirtiendo el máximo de tiempo posible a estar en internet. Esto implica salir poco o nada de casa, renunciar a la familia y otras relaciones sociales reales significativas, y concentrar el total de la atención y la energía mental a la red, lo cual trae consigo, además, problemas físicos de salud asociados a la vida sedentaria[11].

La importancia de conocer los riesgos del Internet se presenta como un pilar fundamental en la sociedad digital actual. Más allá de ser una simple precaución, esta conciencia se erige como un escudo protector que resguarda nuestra privacidad, seguridad y capacidad para interactuar en línea de manera informada y responsable.

La red global, con su vastedad y accesibilidad, ofrece oportunidades inigualables, pero también alberga amenazas sutiles y complejas. Comprender los riesgos del Internet no solo es una medida defensiva contra ciberataques y fraudes, sino también un acto de empoderamiento para los individuos en un entorno virtual en constante evolución, además estar consciente de la realidad y la falsedad en línea son habilidades cruciales que derivan de conocer los riesgos del Internet. Este conocimiento no solo protege nuestras identidades digitales, sino que también contribuye a la construcción de comunidades en línea más seguras y confiables.

[11] Persona con un modo de vida de poco movimiento.

Prevención de riesgos en el mundo del internet

Aunque no existe una solución mágica para prevenir el uso peligroso o ilícito de internet, sí existen un conjunto de premisas que un usuario responsable puede emplear como guías o directrices, mediante las cuales hacer un empleo saludable de la llamada "red de redes". Algunas de estas medidas de preventivas son (Editorial Etecé, 2023):

Antivirus

Emplear un antivirus, firewall[12] y otros programas de seguridad informática. Con estos se podrá proteger la computadora de la mayoría del software malicioso, los hackeos y los virus.

Educación tecnológica

En todos los casos se puede hacer un curso de informática, un taller de uso de internet o solicitar la supervisión de un familiar más instruido si se siente que la interfaz supera las propias capacidades.

Instalar un programa de control parental

Con este tipo de software es posible bloquear páginas pornográficas, de contenido ilícito o inmoral, para impedir que los niños accedan a ellas. Otra opción sería tener sesiones con contraseñas diferentes, cada una con cierto tipo de permisos asignados.

No olvidemos utilizar una buena contraseña, de como mínimo 8 caracteres que contenga letras mayúsculas, minúsculas, números y algún carácter especial. Además, es conveniente que la cambiemos cada cierto tiempo (Computing, 2023).

Poner límites al tiempo de navegación

Hay que saber cuándo parar, ya sea que estemos en redes sociales o jugando en línea, conviene tener algún tipo de alarma o señal que nos permita tener control

[12] Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

sobre el tiempo que invertimos en línea. En ningún momento internet debe suplantar la vida real, ni convertirse en una forma de escapar de las situaciones reales, por desagradables o retadoras que sean.

Para proteger y prevenir a los niños y los adolescentes a sufrir conductas adictivas frente a al consumo masivo al que son muy permeables se pueden aprovechar las defensas técnicas como los filtros de contenidos, los programas de control de acceso o las configuraciones del navegador para supervisar y controlar los riesgos relacionados con los contenidos (Computing, 2023).

Desconfiar de lo que se ve o se lee

No todo lo que está en internet, ni todo lo que comparten nuestros amigos en redes sociales, es fidedigno y confiable. Una actitud prudente hacia la información en línea pasa por una dosis de escepticismo, una mínima verificación y, en la medida de lo posible, por el sentido común: si una oferta es demasiado buena para ser verdad, seguramente no lo sea.

También no abrir mensajes o documentos adjuntos de dudosa procedencia, ni acceder a direcciones sospechosas. Y es que en el mejor caso suelen terminar cambiando la configuración de navegación o añadiendo funcionalidades no solicitadas, y en el peor de ellos infectando nuestro dispositivo con virus u otros bichos que pueden ralentizar el sistema, transmitir información personal y hasta eliminar o secuestrar el contenido del ordenador (Computing, 2023).

Conclusión

Podemos decir que la complejidad de estos riesgos, desde el robo de identidad hasta la desinformación, requiere que construyamos nuestras conexiones en línea con una mentalidad informada y preventiva.

La privacidad es el núcleo de la experiencia en línea y se ve amenazada por la recopilación continua de datos y la proliferación de ataques cibernéticos. Perder el control sobre nuestra información personal puede tener consecuencias de gran alcance, por lo que es esencial comprender la importancia de configurar correctamente nuestra configuración de privacidad y revisar periódicamente nuestras prácticas de gestión de datos.

En un sentido más amplio, la ciberseguridad abarca desde monitorear amenazas como malware y phishing hasta la protección contra ataques más sofisticados, no basta simplemente con reconocer la existencia de estas amenazas; se requiere una participación activa en la adopción de buenas prácticas de seguridad, como actualizar periódicamente el software, utilizar contraseñas seguras e implementar medidas de autenticación de dos factores.

La lucha contra la desinformación es un riesgo menos tangible pero igualmente peligroso que se centra en desarrollar la capacidad de distinguir la verdad de la falsedad en línea. La concientización de los medios y la verificación de datos son herramientas importantes para limitar la difusión de información errónea y garantizar que nuestras decisiones y opiniones se basen en hechos confiables.

La prevención de los ciberriesgos no es sólo una responsabilidad individual, sino también colectiva, as empresas y organizaciones deben asumir un papel activo para proteger sus plataformas y servicios y al mismo tiempo proteger la privacidad de los usuarios. Las instituciones educativas desempeñan un papel crucial a la hora de impartir conocimientos sobre ciberseguridad y desarrollar habilidades digitales desde una edad temprana.

En última instancia, gestionar el riesgo cibernético es un esfuerzo colaborativo que requiere un compromiso continuo con la educación, la adaptabilidad y la rendición de cuentas. La era digital es un campo de juego apasionante y lleno de posibilidades, pero nuestra tarea colectiva es garantizar que naveguemos por este vasto mundo de la web con astucia, conciencia y resiliencia. Sólo así podremos disfrutar plenamente de los beneficios de Internet sin comprometer nuestra seguridad y privacidad en el proceso.

Referencias

Computing, R. (10 de mayo de 2023). *Computing*. Obtenido de 9 consejos para reducir los peligros al navegar por internet.: https://www.computing.es/noticias/que-es-un-smart-home-usos-y-caracteristicas-de-los-hogares-inteligentes/

Editorial Etecé. (26 de febrero de 2023). *Concepto*. Obtenido de Riesgos de Internet: https://concepto.de/riesgos-de-internet/

Etecé, E. (5 de agosto de 2021). *concepto*. Obtenido de Internet: https://concepto.de/internet/

GCFGlobal. (Julio de 2018). Obtenido de Seguridad en Internet: ¿Qué es ciberacoso y cómo prevenirlo?: https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-la-seguridad-en-internet/1/

Internetsociety. (septiembre de 2017). Obtenido de Introducción a la privacidad en Internet: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-Privacy-20151030-es.pdf

Kaspersky. (17 de agosto de 2023). Obtenido de ¿Qué es el robo de datos y cómo evitarlo?: https://latam.kaspersky.com/resource-center/threats/data-theft