

Políticas de Internet:

Glosario de 75 términos clave para entender las políticas de Internet—2025

Los temas y debates sobre políticas que originan decisiones y leyes pueden parecer excesivamente complejos, técnicos, demasiado específicos o alejados de la vida cotidiana. Sin embargo, sus resultados determinan cómo experimentamos Internet y nuestra capacidad de conectarnos, crear y prosperar en línea.

Por eso, la alfabetización en políticas de Internet es para todos, no solo para los especialistas. Con el enfoque adecuado, cualquiera puede comprender los conceptos y marcar una diferencia.

Este glosario ofrece explicaciones rápidas y sencillas de vocabulario clave relacionado con las políticas de Internet en español.

Además de promover coherencia y participación

informada en todos los idiomas, este glosario es una herramienta que empodera a los usuarios de Internet para tomar medidas proactivas, reactivas o receptivas según sea necesario para decidir sobre políticas de Internet en momentos clave. Cuando resultan útiles, se incluyen hipervínculos a materiales de fuentes confiables que le ayudarán a comprender mejor el contexto y a tener una visión más profunda.

Internet es para todas las personas y sus políticas nos conciernen a todos. Cuanto más nos interese y comprendamos lo que está en juego, mejor preparados estaremos para contribuir a moldear, proteger, nutrir e influir en el futuro de Internet y del mundo digital que nos rodea, permitiendo que sea una fuerza positiva que beneficie a todas las personas, en todas partes.

A

TÉRMINO	DEFINICIÓN
Acceso	Capacidad de las personas de conectarse, permanecer conectadas y utilizar Internet como un recurso público para un mayor desarrollo económico, social y cultural. Incluye el acceso, por ejemplo, a conectividad y a contenido relevante, así como a idiomas y alfabetos locales. Hoy en día, más de dos mil millones de personas aún no tienen acceso a Internet confiable y asequible. Esta es la razón por la cual la comunidad global de Internet Society trabaja para conectar a los desconectados y así ayudar a cerrar la brecha digital.
Acceso por puerta trasera	Cualquier método que le permite a un tercero acceder a datos cifrados, creando así una vulnerabilidad que debilita la seguridad de la información personal de los usuarios y de Internet en general. Aunque pueda parecer una herramienta de seguridad, el acceso por puerta trasera puede abrir la posibilidad de un uso indebido, vigilancia o hackeo. Por lo tanto, saber sobre este tema le ayudará a tomar decisiones informadas sobre las herramientas y plataformas en las que confía.
Acceso universal	Parte del derecho universal a la libertad de expresión que permite que las personas tengan una Internet inclusiva, equitativa y asequible, sin importar dónde vivan o su origen. Conozca la inspiradora historia de Ulukhaktok, una comunidad remota que, en medio de la peor temporada de incendios forestales de Canadá, lanzó la primera red comunitaria del Ártico. Esta red fortalece la resiliencia local de Internet y ayuda a evitar que las personas pierdan conectividad cuando más la necesitan.
Accesibilidad	Diseño y regulación de los espacios digitales (y sus productos y servicios) para que todas las personas puedan acceder a ellos y utilizarlos eficazmente, incluidas las personas con discapacidad, las personas mayores y quienes tienen alfabetización o habilidades digitales limitadas. Comprender la accesibilidad ayuda a identificar cuándo los espacios digitales pueden ser usados por todos. También puede empoderarnos para apoyar el diseño inclusivo y promover mejores herramientas y servicios que garanticen que todos puedan participar plenamente en el mundo digital.



TÉRMINO	DEFINICIÓN
Aceptación universal	Principio de la internacionalización y la accesibilidad relacionado con el logro de una Internet multilingüe. El uso de alfabetos latinos no debería ser un requisito previo para usar Internet.
Alfabetización digital	Proceso de adquirir las habilidades digitales y técnicas necesarias para utilizar de forma segura y eficaz la tecnología digital, las herramientas de comunicación y las redes para desenvolverse en el mundo digital. Estas habilidades permiten a las personas utilizar la tecnología con confianza y responsabilidad para alcanzar diversos objetivos, desde aprender y trabajar hasta acceder a servicios e interactuar con las comunidades.
Algoritmo	Conjunto de construcciones matemáticas que sigue una computadora para resolver un problema o realizar una tarea. Es la lista inequívoca y precisa de operaciones simples que se aplican de forma mecánica y sistemática a un conjunto de tokens u objetos (definición de la OCDE). En el caso de las redes sociales, estas son las reglas propietarias que utilizan las plataformas para filtrar, definir y determinar lo que vemos en línea, es decir, noticias, anuncios, videos y resultados de búsqueda. Comprender el papel que desempeñan los algoritmos es importante, dado que moldean de manera silenciosa lo que vemos a diario en línea, incluso cuando no solemos percatarnos de ellos. Conocerlos nos permite cuestionar y dar forma a nuestra experiencia digital.
Apagón de Internet	Interrupción intencional de las comunicaciones basadas en Internet dentro de un área geográfica específica. Un apagón hace que los servicios en línea sean inaccesibles o que no estén disponibles para una población determinada. Ejemplos de ello incluyen los intentos de los gobiernos de controlar el flujo de información durante un proceso electoral o un examen a nivel nacional.



B

TÉRMINO	DEFINICIÓN
Bloqueo de contenido	Tendencia mundial y creciente en que los gobiernos o proveedores de servicios impiden el acceso a determinado material en línea, a menudo por razones como la protección infantil o la seguridad nacional. Aunque en algunos casos el bloqueo se aplica contra materiales ilegales (por ejemplo, contenido de abuso infantil), no existe consenso internacional sobre qué debería o no bloquearse. Si bien el bloqueo de contenido puede parecer una solución rápida, en realidad no elimina el contenido de Internet. Además, podría bloquear involuntariamente sitios web y servicios legítimos, perjudicando tanto a usuarios como a empresas. Quienes intentan eludir los bloqueos con herramientas como las VPN podrían acabar con menor privacidad o seguridad, lo que afectaría su seguridad al usar Internet.
Botnets	Grupo de computadoras de usuarios (bots) conectadas a Internet e infectadas con software malicioso (malware) que permite a un operador (pastor de bots) controlar remotamente las computadoras a través de un servidor de comando y control (C&C) para realizar tareas automatizadas, como robar información o lanzar ataques contra otras computadoras. Descubra más acerca de los desafíos, las consideraciones y los principios rectores en nuestro Informe de políticas sobre botnets.
Brecha digital	Brecha entre quienes tienen acceso a Internet y quienes no. La brecha digital es multifacética e incluye numerosos factores que contribuyen a la falta de acceso, entre ellos la conectividad física, la asequibilidad, la calidad de servicio y la relevancia.



TÉRMINO	DEFINICIÓN
Ciberacoso	Fenómeno en aumento que afecta a niños, niñas y jóvenes. Estudios indican que casi el 43 % de los menores son víctimas de ciberacoso (acoso en línea) y que las niñas tienen el doble de probabilidades de ser víctimas. Los estudiantes que sufren acoso en línea experimentan descensos en sus calificaciones y tienen una mayor incidencia de pensamientos suicidas que quienes nunca han lidiado con este tipo de agresiones por parte de sus pares. Existe una relación entre el ciberacoso, la victimización y la deserción escolar, lo que a su vez aumenta el riesgo de una educación deficiente y el abuso de sustancias en la adultez. La prevención del ciberacoso en las escuelas es fundamental para proteger a los estudiantes de esta nueva forma de violencia.
Ciberdelito	Delitos que se cometen en línea, como la piratería informática o las estafas en Internet. Las investigaciones indican que la ciberdelincuencia continúa creciendo con el aumento de la cantidad de dispositivos conectados y el valor de las actividades en línea. Para combatirlo se requieren medidas como la implementación uniforme de medidas básicas de seguridad (por ejemplo, actualizaciones periódicas y parches de software), una mayor cooperación internacional entre las fuerzas del orden y leyes de ciberseguridad más estrictas en varios países.
Ciberseguridad	Práctica de proteger la seguridad y la privacidad de las redes y los programas contra los ataques digitales mediante el uso de soluciones técnicas y tecnológicas. El objetivo de los ciberataques suele ser acceder, cambiar o destruir información sensible, extorsionar a los usuarios por medio de ransomware o interrumpir los procesos comerciales normales. El término ciberseguridad no abarca todos los delitos que ocurren en Internet.

TÉRMINO	DEFINICIÓN
Cifrado	Proceso que protege los datos contra visualizaciones no autorizadas al hacerlos ininteligibles para cualquiera que no tenga la clave para descifrarlos. Aunque una persona no autorizada acceda a los datos cifrados, no podrá distinguirlos de otros datos aleatorios. Todos debemos utilizar y defender el cifrado para proteger tanto los datos que almacenamos como los que transmitimos. Desempeña un papel fundamental en la protección de nuestras actividades digitales cotidianas, como la banca electrónica y las compras en línea, ya que asegura que nuestros mensajes privados permanezcan privados. Recurso adicional: Guía sobre el cifrado para padres y madres.
Cifrado de extremo a extremo (E2EE)	Proceso de cifrar los datos en el punto de transmisión y solo descifrarlos en el punto de recepción. El objetivo del cifrado de extremo a extremo es garantizar que ningún intermediario (por ejemplo, los servidores de correo electrónico o de mensajería) pueda acceder al contenido de la comunicación, incluso si desempeña un papel legítimo en la transmisión de datos del remitente al destinatario.
Código abierto	Modelo descentralizado de desarrollo de software que promueve la colaboración abierta, permitiendo que el código fuente esté disponible de forma gratuita para cualquier modificación o mejora.
Conectividad significativa	Significa más que tener acceso a Internet. También implica tener un acceso rápido, regular, confiable y seguro que permita a las personas participar plenamente en el mundo digital para trabajar, estudiar, comunicarse o acceder a servicios.
Confianza en línea	Percepción que tienen los usuarios de que Internet—y los sistemas, plataformas y servicios que se basan en ella—funcionarán de forma segura, confiable y respetando sus derechos, su privacidad y sus datos. Fortalecer esta confianza mediante la transparencia, la rendición de cuentas, tecnologías seguras y normas justas es clave para garantizar que personas y empresas sigan beneficiándose de Internet. Descubra más sobre por qué necesitamos esta confianza y cómo podemos lograrla.



TÉRMINO	DEFINICIÓN
Contenido local	Contenido generado localmente, relevante y adaptado a las realidades propias de un país determinado. Este contenido impulsa el crecimiento de Internet a nivel local, regional o nacional, ya que es relevante para las comunidades y las economías de ese país específico.
Correo no deseado	Cualquier tipo de correo electrónico, mensaje de texto, llamada telefónica o mensaje no deseado y molesto que se recibe de forma masiva de personas o empresas que desean anunciar sus productos o difundir sus opiniones políticas o sociales.

D

TÉRMINO	DEFINICIÓN
Datos	Cualquier información recopilada, almacenada, procesada o transmitida en línea, como nuestra ubicación, clics, imágenes o mensajes. En muchas jurisdicciones se exige que los datos se almacenen de determinadas maneras o dentro de ubicaciones geográficas específicas, lo que suele llamarse localización de los datos. La intención de estos requisitos es proteger la privacidad, la seguridad o cumplir con las leyes locales. Es importante tratar y compartir los datos sensibles de forma intencionada, por lo que resulta fundamental defender las mejores prácticas de manejo responsable de los datos.
Datos personales	Cualquier información que, una vez reunida, se pueda utilizar para identificar a una persona en particular.
Derecho al olvido	Derecho legal de una persona de solicitar que cierta información específica se disocie de su nombre, creando así un obstáculo para su búsqueda en línea. (Por ejemplo, al buscar “fraude de John Smith”, esta información no se recuperaría.)
Desinformación	Información creada deliberadamente para engañar a las personas. Difiere de la información engañosa, también conocida como “información errónea”.



TÉRMINO

DEFINICIÓN

Dirección del Protocolo de Internet (dirección IP)

Identificador único asignado a cada computadora y dispositivo conectado a Internet (por ejemplo, impresoras, enrutadores, dispositivos móviles, etc.). Se usa para localizar e identificar cada nodo en comunicación con otros nodos de la red, permitiendo que los dispositivos se comuniquen a través de Internet.

Doxing

Publicar en línea información privada o de identificación personal de una persona (como su nombre completo, domicilio o datos familiares) sin su consentimiento, con la intención de acosarla o causarle daño.

El doxing es preocupante, ya que cualquiera puede convertirse en víctima y sus consecuencias son reales para quienes lo sufren. Conocer sus consecuencias para la privacidad puede ayudarnos a reducir significativamente los datos personales que compartimos, exigir mejores directrices digitales y tomar medidas activas para proteger nuestros datos personales en línea.

E

TÉRMINO

DEFINICIÓN

Enfoque de múltiples partes interesadas

Modelo de gobernanza que implica la participación y colaboración de diversas partes interesadas de diferentes sectores de la sociedad en los procesos de toma de decisiones relacionados con la gobernanza y la gestión de Internet.

Estas partes interesadas incluyen, por ejemplo, los gobiernos, la comunidad técnica, la sociedad civil, el mundo académico y los usuarios finales. A diferencia de los modelos de gobernanza tradicionales que se caracterizan por tener estructuras jerárquicas de arriba hacia abajo y un control centralizado, el enfoque de múltiples partes interesadas pone énfasis en la inclusión, la transparencia y la colaboración entre los diversos grupos de partes interesadas.

Descubra [por qué funciona el enfoque de múltiples partes interesadas](#).



TÉRMINO	DEFINICIÓN
Enfoques de concesión de licencias (redes comunitarias)	Una licencia es el permiso legal necesario para operar partes de una red comunitaria. Cada país tiene diferentes normas y algunos permiten mayor flexibilidad a las redes comunitarias o proponen licencias asequibles de modo que las comunidades puedan construir su propia red cuando los proveedores de servicios no lo hacen. Un enfoque de concesión de licencias que apoye a estas redes permite que las personas intervengan, establezcan una conectividad asequible y conecten sus comunidades a Internet. Explore los enfoques de concesión de licencias que ayudan a cerrar la brecha digital.
Enfoques de espectro	En el contexto de las redes comunitarias, se refiere a una estrategia flexible que permite diferentes formas de acceder y gestionar las señales de manera que los proyectos locales impulsados por la comunidad también puedan construir y mantener sus propias redes. Ayudar a abogar por un enfoque de espectro más justo significa que las personas en zonas remotas o desatendidas puedan crear una Internet local asequible, sin tener que esperar por las grandes empresas.
Equidad digital	Concepto de que todas las personas deben tener las mismas oportunidades de acceder a las tecnologías digitales, incluida Internet.
Escaneo del lado del cliente (CSS)	Método mediante el cual dispositivos como una computadora o teléfono escanean el contenido antes de cifrarlo y enviarlo, para detectar material ilegal. Esto debilita el cifrado en nombre de la seguridad y puede convertir su dispositivo personal en una herramienta de vigilancia sin que usted lo sepa.
Estándares de código abierto	Reglas o directrices disponibles públicamente que cualquiera puede usar, compartir o desarrollar libremente. En los ámbitos de gobernanza de Internet, Internet se basa fundamentalmente en la existencia de estándares abiertos y no propietarios. Estos son claves para permitir que diferentes dispositivos, servicios y aplicaciones puedan interoperar en una red de redes amplia y dispersa. Lea sobre las organizaciones que respaldan los estándares abiertos de Internet, asegurando que sus especificaciones sean de libre acceso, sin restricciones, de desarrollo abierto y en constante evolución.



F

TÉRMINO	DEFINICIÓN
Filtrado de contenido	Práctica mediante la cual se niega a los usuarios de Internet el acceso a determinado contenido en línea, generalmente ilegal, en cumplimiento de requisitos gubernamentales. Las autoridades nacionales pueden establecer políticas públicas para restringir o impedir el acceso a contenido como material de abuso infantil, contenido que infringe las leyes de propiedad intelectual, amenaza la seguridad nacional o está prohibido por una variedad de razones culturales o políticas.
Fragmentación	División de la Internet unificada, abierta y global en redes más pequeñas y aisladas, cada una sujeta a diferentes reglas, regulaciones y estándares técnicos, que tal vez no puedan interconectarse o interoperar entre sí. Este es un gran problema, ya que el resultado son sitios bloqueados que afectan nuestra experiencia en línea. Descubra por qué debemos prestarle atención a este tema.

G

TÉRMINO	DEFINICIÓN
Gobernanza de Internet	Políticas, normas y procesos de toma de decisiones que definen cómo se gestiona y se usa Internet. Involucra a actores clave como gobiernos, empresas privadas, la comunidad técnica y organizaciones de la sociedad civil. La forma en que se gobierna Internet impacta directamente en su funcionamiento, en quién accede a ella y en qué tan abierta, segura e inclusiva se mantiene. Consulte el informe Huellas de 20 años del Foro de Gobernanza de Internet para averiguar cómo Internet se gobierna con éxito gracias a un modelo consultivo y de múltiples partes interesadas.



TÉRMINO

DEFINICIÓN

Gobernanza de los datos

Normas que regulan cómo se recopilan, utilizan y protegen los datos.

Internet Society aboga por marcos de gobernanza de datos transparentes y responsables que protejan la privacidad y los datos personales. Para garantizar que las políticas de datos se diseñen de manera que protejan los derechos de los usuarios y, a la vez, fomenten la innovación y la confianza en el ecosistema digital, apoyamos el uso de estándares abiertos para la gestión de los datos y abogamos por el uso del cifrado y otras tecnologías que mejoren la seguridad de los datos. Además, promovemos la colaboración global para desarrollar leyes de protección de datos que aseguren el respeto de la integridad de los datos y que, a la vez, equilibren la necesidad de mantener la interoperabilidad digital a nivel mundial.

H

TÉRMINO

DEFINICIÓN

Huella digital

Rastro de datos que deja la actividad en línea de una persona. Incluye todas las interacciones digitales y la información asociada con una persona en las diversas plataformas y los diferentes servicios en línea, entre ellos, las redes sociales, las compras en línea, el historial de navegación, el uso de aplicaciones y los datos de ubicación. Cada vez más, nuestras huellas digitales incluyen datos recolectados de forma pasiva por sistemas como el reconocimiento automático de matrículas, los sistemas de CCTV urbanos, los monitores de actividad física, las redes de telefonía móvil, etc. Nuestra huella digital también abarca datos que no son el resultado de nuestras actividades deliberadas en línea.

Si bien es imposible no tener una huella digital, sí podemos tomar algunas [medidas sencillas para reducirla](#).

I

TÉRMINO

DEFINICIÓN

Incidencia

Apoyar o promover activamente una causa, o amplificar la voz de la comunidad en temas como los derechos digitales, la seguridad en línea o el acceso asequible mediante la concientización pública, la educación y la colaboración con los formuladores de políticas con el fin de frenar las amenazas legislativas a Internet.

[Comprender la incidencia](#) y el poder de nuestra voz puede ayudarnos a crear una Internet más abierta e inclusiva.



TÉRMINO	DEFINICIÓN
Inclusión digital	Enfoque integral para brindar a todas las personas un acceso equitativo a los servicios y las tecnologías digitales (por ejemplo, a los jóvenes, a las mujeres, a los ancianos, a las minorías y a las personas con discapacidad).
Información errónea	Información falsa o engañosa producto de una interpretación equivocada de los hechos. Se diferencia de la desinformación, que es información falsa creada y difundida de manera deliberada con el fin de engañar o manipular, a menudo con motivaciones políticas, económicas o ideológicas.
Informe de impacto sobre Internet	Informes breves producidos por Internet Society, miembros de nuestra comunidad y otros colaboradores. Analizan cómo diferentes políticas o nuevas tecnologías pueden afectar lo que Internet necesita para existir y prosperar. ¿Le gustaría producir su propio Informe de impacto sobre Internet? Consulte nuestro Kit de herramientas para la evaluación del impacto sobre Internet y descubra cómo hacerlo.
Internet	Una “red de redes” formada por casi 70.000 redes independientes que utilizan los mismos protocolos técnicos y eligen colaborar e interconectarse. Explore en mayor profundidad cómo funciona Internet, quién la gestiona y qué comportamientos son deseables, así como cuáles están limitados por sus realidades técnicas. Hacer de Internet un espacio seguro y una fuerza positiva es una responsabilidad colaborativa y colectiva.
Internet abierta	Una Internet libre, accesible y que no es controlada por ningún grupo en particular. Una de las características operativas clave de Internet es que está diseñada como una plataforma abierta para la innovación y el intercambio de ideas.
Internet de las cosas (IoT)	Objetos cotidianos conectados a Internet que tienen poderosas capacidades de análisis de datos y que prometen transformar nuestra forma de trabajar, vivir y divertirnos. La IoT es objeto de amplio debate, ya que plantea preocupaciones con respecto a la vigilancia y la privacidad (por ejemplo, los dispositivos electrónicos y los electrodomésticos inteligentes).



TÉRMINO

DEFINICIÓN

Internet Society (ISOC)

Organización benéfica global cuya misión es promover y desarrollar [una Internet abierta, segura y confiable para todas las personas](#).

[Internet Society](#) apoya y promueve el desarrollo de Internet como una infraestructura técnica global de gran impacto, un recurso para enriquecer la vida de las personas y una fuerza positiva en la sociedad.

Internet Society Foundation

Es la rama filantrópica de Internet Society que financia iniciativas en todo el mundo para ayudar a que Internet sea abierta, segura y accesible para todos.

A través de una docena de [programas de subvenciones](#), apoya a la comunidad global de Internet—investigadores, desarrolladores, organizaciones sin fines de lucro, educadores y más—que promueve el uso de Internet como una infraestructura técnica esencial para brindar a las comunidades mejor educación, atención médica y oportunidades económicas, entre otras áreas de enfoque.

Internet Society Pulse

[Pulse](#) es un sitio web que recopila datos confiables y precisos sobre Internet de múltiples fuentes y ofrece información sobre temas como el impacto de los apagones de Internet y la resiliencia de Internet en cada país. Esto les ofrece antecedentes y contexto a los periodistas que cubren temas de Internet alrededor del mundo.

L

TÉRMINO

DEFINICIÓN

Líneas de acción (CMSI)

Entre 2003 y 2005, la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de las Naciones Unidas definió una lista de “Líneas de Acción”. Se trata de un conjunto de áreas de enfoque como el acceso, las habilidades, la seguridad en línea y la diversidad cultural, que sirven de guía para que los países y las organizaciones puedan construir un mundo digital más inclusivo.

Conocer estas líneas de acción es importante porque convierten grandes objetivos globales en pasos concretos, facilitando que gobiernos, organizaciones y comunidades trabajen juntos sobre cómo las personas usan y se benefician de Internet.

En 2025, la Asamblea General de las Naciones Unidas revisará los avances logrados en la implementación de las Líneas de Acción de la CMSI, lo que lo convierte en un año fundamental para Internet. Descubra más sobre la [mejor manera de enfrentar los desafíos actuales con una visión de futuro, tomando como base el marco de la CMSI](#).



TÉRMINO

DEFINICIÓN

Localización de los datos

Requisito de almacenar los datos dentro de las fronteras de un país.

Lejos de mejorar la seguridad, los requisitos de localización de los datos tienen el efecto contrario: fragmentan Internet y dificultan la protección de los datos frente a las amenazas de ciberseguridad.

Los países y el público deben abogar por políticas que promuevan la seguridad y la privacidad de los datos mediante la cooperación internacional y la adopción de estándares de ciberseguridad sólidos, y deben oponerse a las medidas proteccionistas que aíslan a los países, perjudican a las empresas y limitan el libre flujo de información.

Localización obligatoria de los datos

Requerimientos gubernamentales que controlan el almacenamiento y el flujo de los datos para mantenerlos dentro de una jurisdicción específica. El objetivo de las leyes de localización de datos—a veces también llamada “residencia de datos” o “soberanía de datos”—suele ser mantener los datos de transacciones personales o financieras dentro del país, donde están sujetos a acceso y regulaciones locales.

Las medidas de localización obligatoria de los datos abarcan desde el requisito de localizar físicamente los datos dentro del país donde se originan hasta restringir o incluso prohibir su transferencia a otros países. Aquí presentamos un caso práctico que ilustra lo que esto [significa para el modo Internet de interconectarse](#):

M

TÉRMINO

DEFINICIÓN

Manejo responsable de los datos

Principios éticos de transparencia, equidad y respeto que se utilizan para tratar los datos sensibles. El manejo responsable de los datos puede proteger nuestra privacidad y autonomía, y generar la confianza necesaria para que la innovación digital prospere de maneras que benefician a todos.

[Descubra más sobre las razones, los desafíos y las mejores prácticas del manejo responsable de los datos.](#)

Moderación de contenido

Proceso mediante el cual empresas privadas como Facebook, TikTok o YouTube monitorean, revisan, eliminan o marcan contenido en sus plataformas de acuerdo con sus propias normas (normas comunitarias o términos de servicio).

Esto afecta lo que podemos decir y ver en línea; sin embargo, a menudo carece de transparencia y rendición de cuentas.



TÉRMINO	DEFINICIÓN
Modo Internet de interconectarse	La base de una Internet sólida y exitosa que funciona como lo hace gracias a cinco propiedades esenciales que, al combinarse, impulsan su funcionamiento y evolución.

N

TÉRMINO	DEFINICIÓN
Neutralidad de la red	Principio según el cual todos los datos en línea deben ser tratados de la misma manera. Si bien los operadores de red pueden utilizar técnicas de gestión de tráfico para mantener su desempeño, existe la preocupación de que estas prácticas puedan utilizarse para favorecer a ciertos datos, bloquear contenido de la competencia u otorgar ventajas desleales, especialmente cuando son motivados por intereses económicos. Estas acciones corren el riesgo de socavar la naturaleza abierta y transparente de Internet y perjudicar a los usuarios finales.

P

TÉRMINO	DEFINICIÓN
Pacto Digital Global	Marco integral propuesto con el propósito de establecer principios compartidos para un futuro digital seguro, inclusivo, abierto y centrado en el ser humano, desarrollado por las Naciones Unidas. Su objetivo es guiar la gestión global de las tecnologías digitales, especialmente de Internet. Esto es importante porque podría influir en el futuro de Internet y cómo accedemos a ella, con impacto en la conectividad digital, la fragmentación de Internet, la protección de los datos, los derechos humanos en línea y la promoción de una Internet confiable.
Phishing	Ataque que busca robar nuestro dinero o nuestra identidad al lograr que revelemos información personal como números de tarjetas de crédito, información bancaria o contraseñas, en sitios web que simulan ser legítimos.



Privacidad

Nuestro derecho a controlar quién ve nuestra información personal en línea. Privacidad también significa respetar a las personas mediante un tratamiento justo y transparente de sus datos personales, limitando la información que se recopila y utiliza, y asegurando la gestión responsable y la seguridad de los datos.

[Consulte aquí las mejores prácticas en materia de privacidad y otros recursos relacionados.](#)

Privacidad de los datos

Protección de la información personal (datos en línea) contra el acceso, el uso o la divulgación no autorizados. Implica asegurar que las personas controlen cómo las organizaciones o entidades recopilan, almacenan, procesan y comparten sus datos.

Existen numerosas herramientas de privacidad en línea muy útiles. Úselas para proteger su privacidad en línea y para realizar un seguimiento de la información que comparte al navegar. A continuación, compartimos dos enlaces a recursos que esperamos le resulten relevantes y útiles.

Tutoriales de Internet Society sobre identidad, privacidad y gestión de su huella digital:

- [Identidad digital y privacidad](#)
- [Huellas digitales](#)

Saber que sus datos pueden ser recopilados y comprender sus derechos le ayudará a evitar riesgos y recuperar el control cada vez que utilice una aplicación o un sitio web.

Proyecto de ley

Propuesta formal para crear una ley nueva o modificar una existente. En el ámbito de las políticas de Internet, un proyecto de ley podría afectar el derecho de los usuarios a la privacidad, el acceso, la libertad de expresión o la seguridad en línea. Para profundizar en los temas clave, consulte estos [informes de políticas](#).

Seguir de cerca el ámbito de las políticas para saber qué proyectos de ley se están debatiendo brinda la oportunidad de opinar e influir en las decisiones antes de que se conviertan en ley. Expresar, compartir o hacerse eco de las preocupaciones, o incluso firmar peticiones, puede ayudar a exigir responsabilidad a los formuladores de políticas.

R

TÉRMINO	DEFINICIÓN
Ransomware	Tipo de ataque de malware mediante el cual los hackers pueden infiltrar nuestros datos. Aquí encontrará seis consejos para protegerse contra el ransomware .
Regulaciones	Leyes o normas establecidas por las autoridades para controlar el uso de Internet o el comportamiento en línea. Si bien las regulaciones buscan atender los riesgos en línea para la sociedad, muchas veces están mal definidas o son poco prácticas, lo que a menudo provoca daños involuntarios a la infraestructura de Internet.
Regulación de contenido	Cómo los gobiernos utilizan las leyes, políticas o mandatos oficiales para definir qué tipos de contenido están permitidos o prohibidos en línea. La regulación de contenido puede limitar el acceso de los usuarios a la información. Últimamente, este tema ha generado preocupación y debate público, resaltando la necesidad de sensibilizar sobre la existencia de leyes y medidas nacionales que plantean riesgos para los derechos humanos. En este contexto, la censura es la principal preocupación.
Responsabilidad de las plataformas	Regulación que responsabiliza a las plataformas digitales (como Facebook, YouTube y otras) por la manera en que gestionan el contenido, los datos de los usuarios, los algoritmos y otros aspectos de sus servicios que impactan a la sociedad. Esto tendría un efecto negativo en tres pilares de Internet: su arquitectura abierta de componentes básicos interoperables y reutilizables; la gestión descentralizada y el enrutamiento distribuido; y su carácter de red tecnológicamente neutral y de propósito general. También podría haber un aumento de los costos y riesgos para los operadores o proveedores de servicios, lo que llevaría a una menor inversión, el desvío de recursos críticos a actividades no esenciales, una limitación de la innovación y una red menos efectiva en general. Esto podría influir en lo que vemos, compartimos y creemos en línea, y afectar cómo se gestionan nuestros datos personales.



TÉRMINO

DEFINICIÓN

Responsabilidad de los intermediarios

Se refiere a si las plataformas en línea o los proveedores de servicios como Amazon, Facebook, WhatsApp o YouTube pueden ser considerados legalmente responsables por lo que publican sus usuarios. Estas plataformas no crean el contenido, sino que solo lo alojan o transmiten.

Si las plataformas temen ser sancionadas por el contenido generado por sus usuarios, podrían bloquearlo excesivamente para protegerse, limitando así lo que los usuarios pueden decir, compartir o ver en Internet.

Entenderlo permite a los usuarios apoyar políticas y regulaciones equilibradas que protejan la expresión libre y responsable y que a la vez aborden los daños reales.

[Aquí encontrará más recursos sobre este tema, en inglés, francés, español, portugués y árabe.](#)

Robo de identidad

Vulneración de la privacidad que ocurre cuando delincuentes roban credenciales de usuario, contraseñas e información asociada con el objetivo de suplantar la identidad de otros usuarios de Internet. La motivación principal del robo de identidad suele ser económica: al robar nuestros datos y hacerse pasar por nosotros, los delincuentes pueden solicitar bienes y servicios, desviar envíos existentes o transferir fondos.

Aunque la tecnología ha cambiado, las motivaciones y comportamientos básicos de este tipo de ladrones son los mismos de siempre. Existen numerosas protecciones legales, como las leyes de defensa del consumidor, que también pueden aplicarse a los usuarios de Internet. La mejor práctica en el ámbito de las políticas es equilibrar la protección de la privacidad con el desarrollo económico y una Internet abierta.

S

TÉRMINO

DEFINICIÓN

Seguridad de los datos

Medidas que se utilizan para proteger todo tipo de información personal y no personal en línea (datos) para que permanezca confidencial y disponible.

Implica el uso de cifrado y control de acceso para asegurar y salvaguardar sus datos. Más información: [Mejores prácticas para la seguridad de los datos y de la información.](#)



TÉRMINO	DEFINICIÓN
Seguridad en línea	Conjunto de políticas, regulaciones y medidas destinadas a proteger a las personas de riesgos como el ciberacoso, las violaciones de la privacidad y la exposición a contenido dañino o ilegal mientras usan Internet. La seguridad en línea afecta la experiencia de todos, especialmente de niños, jóvenes y usuarios marginados. Se trata de un esfuerzo colaborativo, una responsabilidad compartida que ninguna entidad puede lograr por sí sola.
Seguridad infantil en línea	Esfuerzos legales y regulatorios dirigidos a proteger a los niños en Internet. Los países aplican una combinación de medidas como filtros de contenido, empoderamiento del usuario y cooperación con las partes interesadas. Si bien hay quienes sostienen que el cifrado dificulta la protección infantil en línea, su papel fundamental en la protección de la privacidad y seguridad de la infancia suele pasarse por alto en los debates sobre políticas.
Soberanía digital	Capacidad de una nación de determinar su autonomía digital y las políticas impulsadas por el gobierno que la promueven explícitamente. Si bien las necesidades y los objetivos de Internet varían según el país, las políticas de soberanía digital incluyen esfuerzos para fragmentar Internet, aislando regiones de la red global.
Soluciones de acceso lícitas	Mecanismo que permite a las autoridades gubernamentales acceder a comunicaciones o datos privados, a menudo a través de una orden judicial, debilitando así la seguridad de todos. Si no se regula cuidadosamente para garantizar una estricta supervisión, transparencia y límites claros, este tipo de acceso puede amenazar la privacidad y la libertad. Abre la puerta a la vigilancia masiva o a mandatos de puerta trasera en nombre de medidas “lícitas” contra el cifrado.

T

TÉRMINO	DEFINICIÓN
Tasa cero	Práctica mediante la cual los proveedores de telefonía móvil permiten que los usuarios accedan a ciertas aplicaciones o servicios sin consumir sus datos. Aunque muchas veces se promociona como un beneficio para los usuarios, suele implicar acuerdos entre grandes empresas tecnológicas y de telecomunicaciones. Si bien puede reducir los costos para los usuarios, también plantea preocupaciones con respecto a la competencia y la neutralidad de la red, es decir, la idea de que todo el contenido en línea debe recibir el mismo trato. Descubra cómo funciona.

V

TÉRMINO	DEFINICIÓN
Verificación de edad	Proceso de determinar la edad de un usuario antes de permitirle acceder a determinados contenidos, plataformas o servicios en línea. El término <i>aseguramiento</i> de edad abarca todos los métodos de comprobación de edad. <i>Verificación de edad</i> es el término más habitual, aunque se aplica específicamente a los métodos que utilizan fuentes autenticadas, como una identificación oficial o una cuenta bancaria. Los gobiernos exigen cada vez más la verificación de edad para intentar restringir el acceso a determinados tipos de contenidos y servicios en línea. Aunque estas leyes pueden tener buenas intenciones y su objetivo puede ser evitar la exposición de la infancia a contenidos para adultos, también pueden plantear riesgos de accesibilidad, privacidad y seguridad para usuarios de todas las edades.
Vigilancia	Observar o rastrear las acciones de las personas para recopilar información sobre ellas, a menudo mediante cámaras, datos o herramientas en línea. Esto suele ser realizado por los gobiernos, aunque no son los únicos en hacerlo. No se trata simplemente de “no tener nada que ocultar”, sino del derecho a la privacidad, el consentimiento y el control sobre nuestra vida digital, que debe protegerse, ya que también previene graves riesgos de seguridad en caso de que los datos se utilicen indebidamente.



TÉRMINO

DEFINICIÓN

Vigilancia masiva

Vigilancia generalizada del comportamiento o las comunicaciones de las personas. En el contexto de Internet, la vigilancia masiva es el objetivo de ciertas políticas gubernamentales, especialmente en sociedades represivas o autoritarias.

Independientemente de la justificación que se alegue (por ejemplo, razones de seguridad nacional o de lucha contra el terrorismo o el abuso infantil), la vigilancia masiva es, por definición, desproporcionada en una sociedad democrática. Esta práctica amenaza la libertad de expresión en línea y la seguridad, la privacidad y la autonomía de la ciudadanía.

Internet es para todas las personas

Fundada en 1992, Internet Society es una organización benéfica global que cree que Internet es para todas las personas. A través de nuestra comunidad de miembros, grupos de interés especial y más de 120 capítulos en todo el mundo, defendemos y promovemos políticas, estándares y protocolos de Internet que mantienen a Internet como una red abierta, globalmente conectada y segura.

Más información: InternetSociety.org



Internet Society es una organización benéfica 501(c)(3) registrada en Estados Unidos (EIN 54-1650477) reconocida varias veces por Charity Navigator con su máxima distinción, una clasificación de 4 estrellas.