



Civil Society Alliances for
Digital Empowerment



Co-funded by
the European Union

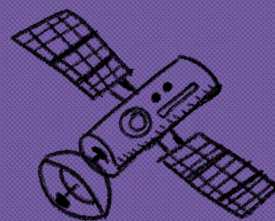
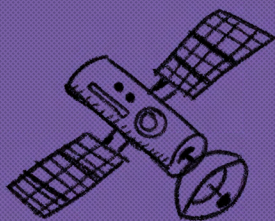
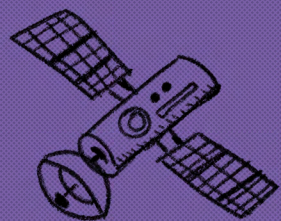
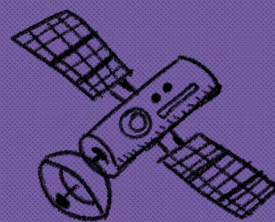
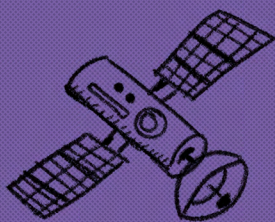
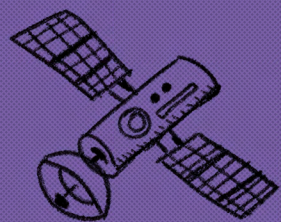
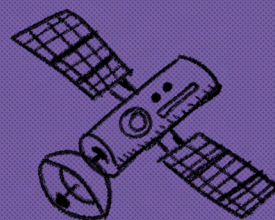
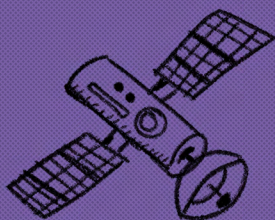
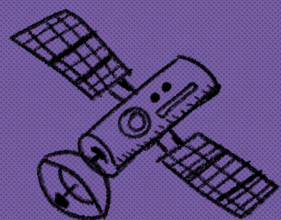
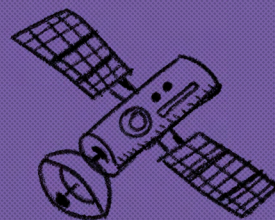
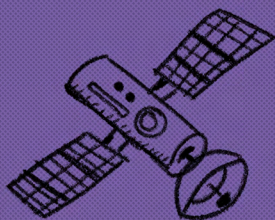
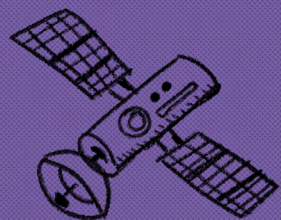
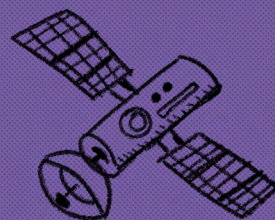
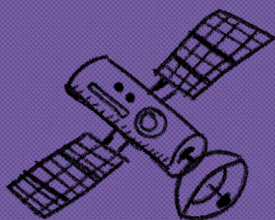
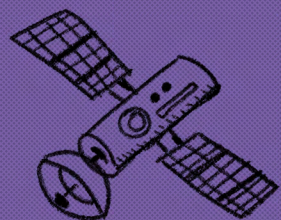
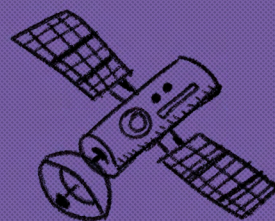
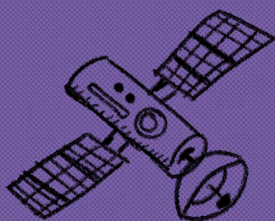
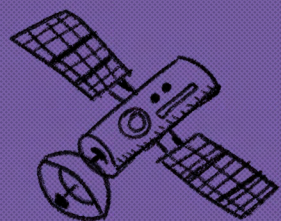
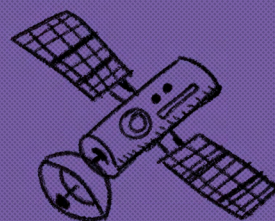
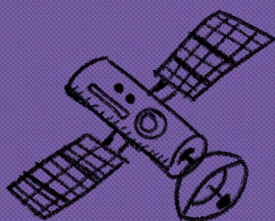
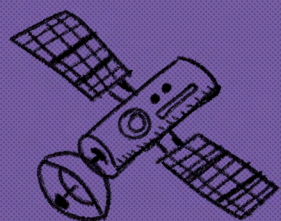
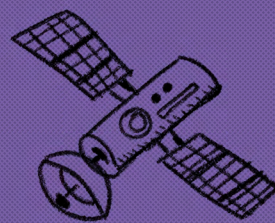
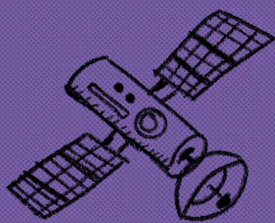
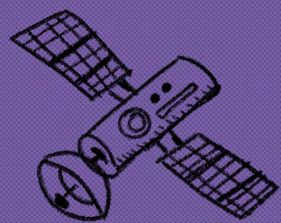
NAVEGANTES DE INTERNET:

Ciclo de formación para la gobernanza
de internet y la ciudadanía en lo digital



Ciclo formativo sobre
gobernanza de internet

Fundación
Karisma



NAVEGANTES DE INTERNET:

Ciclo de formación para la gobernanza de internet y la ciudadanía en lo digital

Fundación **Karisma**

Somos una organización de la sociedad civil que busca proteger y promover los derechos humanos y la justicia social en el diseño y uso de las tecnologías digitales. Trabajamos en la promoción de los derechos humanos en el mundo digital.

Autoría e investigación:

Módulo 1:

Michael Ruiz
Lorena Enciso
Camila Pardo.

Módulo 2:

Daniela Schnidrig
Edda Forero

Módulo 3:

Edda Forero

Coordinación

Paula Rodríguez Badillo
Maria Camila Galvis

Revisión

Paula Rodríguez Badillo
Michael Ruiz
Pilar Saenz

Dirección de Karisma

Catalina Moreno Arocha
Juan Diego Castañeda

Corrección de estilo

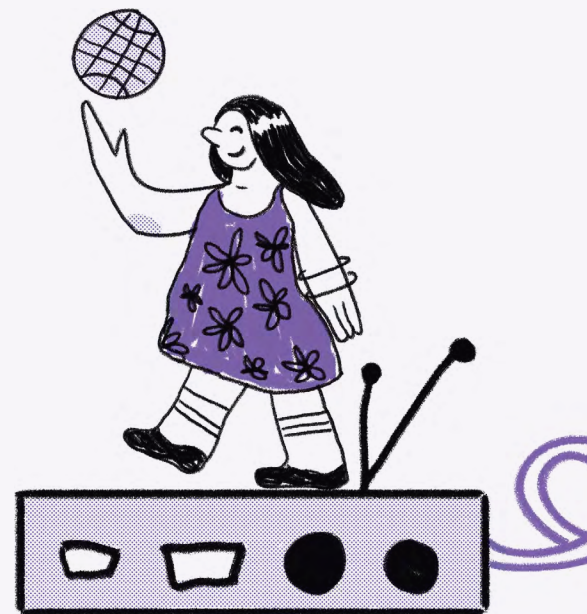
Laura Grisales Silva

Diseño editorial

Daniela Moreno Ramírez

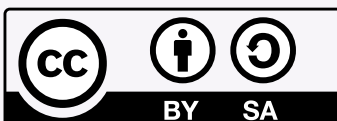
Coordinación editorial

Natalia Andrade Fajardo



Esta investigación se realizó en el marco del consorcio CADE. Ver más en
<https://cadeproject.org/>

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.



Este informe está disponible bajo Licencia Creative Commons Atribución 4.0. Esta licencia permite a otros distribuir, mezclar, ajustar y construir a partir de su obra, incluso con fines comerciales, siempre que le sea reconocida la autoría de la creación original.
<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

INTRODUCCIÓN

Este ciclo formativo busca acercar a jóvenes, docentes rurales, comunidades históricamente excluidas e interesados a los debates sobre la gobernanza de internet, entendida no sólo como un tema técnico, sino como un campo político en el que se definen derechos, oportunidades y formas de participación ciudadana. La idea central es que los espacios de gobernanza no se queden en conversaciones abstractas o dominadas por actores con más recursos, sino que integren las perspectivas y experiencias de nuestras comunidades en América Latina y el Caribe.

Este ciclo formativo se realiza en el marco del proyecto Civil Society Alliances for Digital Empowerment (CADE), una alianza que impulsa proyectos sobre gobernanza de internet y acceso a espacios de incidencia desde los países del Sur Global y cuenta con el apoyo financiero de la Unión Europea.



La propuesta se estructura en tres módulos que se articulan como sigue:

- **¿Cómo funciona internet?**

Presenta las bases técnicas y sociales de internet para comprender qué hay detrás de la pantalla, cómo viajan los mensajes, qué es la infraestructura digital y por qué estas cuestiones son claves para hablar de derechos y participación.

- **Gobernanza de internet: decisiones que nos afectan**

Explora quién toma las decisiones sobre internet, qué intereses están en juego y cuáles son los principales espacios y principios de gobernanza. El énfasis está en reconocer el papel de la sociedad civil y abrir oportunidades concretas de incidencia.

- **Digitalización de servicios y derechos ciudadanos**

Invita a reflexionar críticamente sobre cómo los Estados promueven la digitalización de servicios, cuáles son sus impactos en la vida cotidiana y cómo vincular estas discusiones con la gobernanza de internet, desde un enfoque de derechos, inclusión y soberanía digital.

En conjunto, estos tres módulos ofrecen un recorrido que va de lo técnico a lo político y de lo global a lo cotidiano: desde los cables, servidores y protocolos que sostienen la red, hasta las políticas públicas de digitalización que afectan la manera en que accedemos a salud, educación o justicia.

Objetivo general del ciclo formativo

Fortalecer las capacidades de jóvenes, docentes y comunidades vulnerables en América Latina y el Caribe para comprender y adquirir herramientas de participación e incidencia en los debates y decisiones de la gobernanza de internet, con el fin de que ampliar sus capacidad y propender porque sus experiencias locales sean reconocidas en la construcción de un entorno digital más justo, inclusivo y democrático.

Objetivos específicos

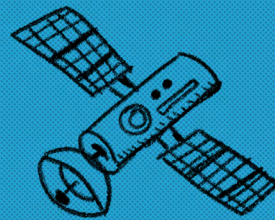
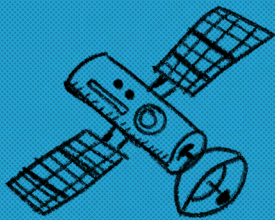
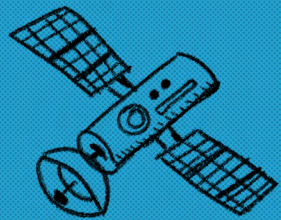
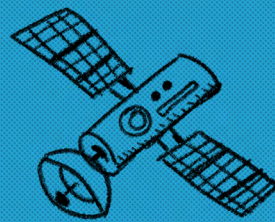
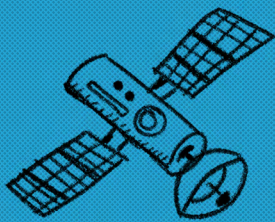
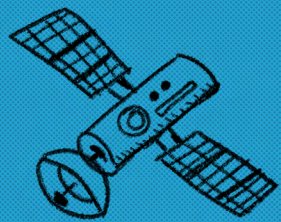
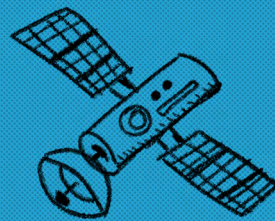
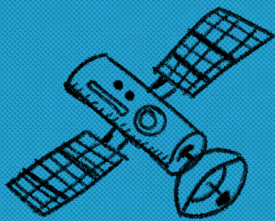
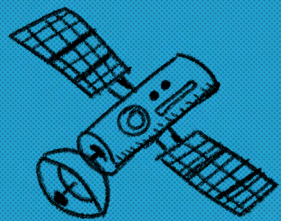
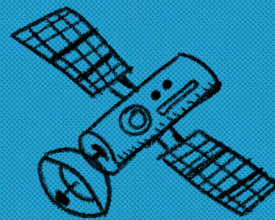
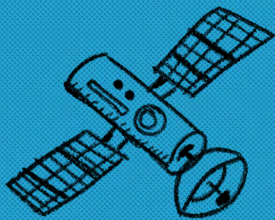
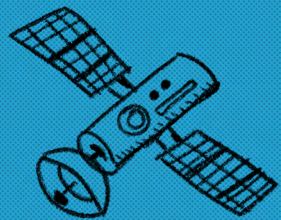
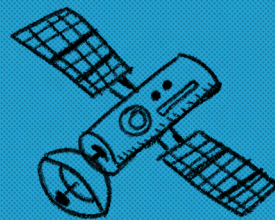
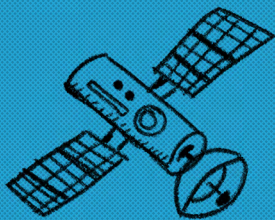
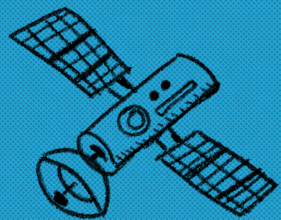
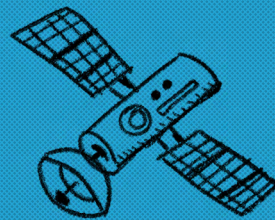
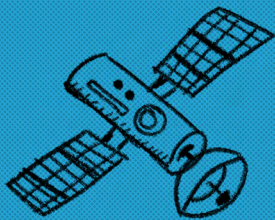
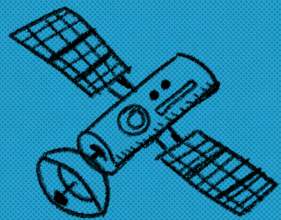
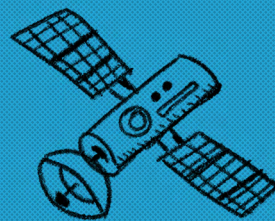
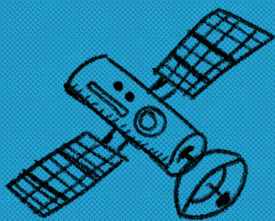
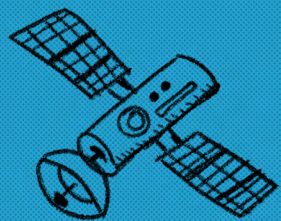
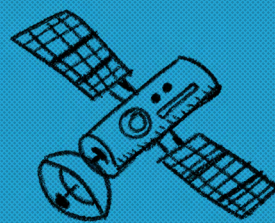
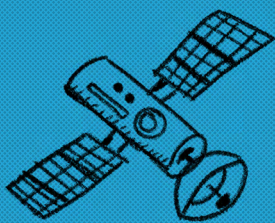
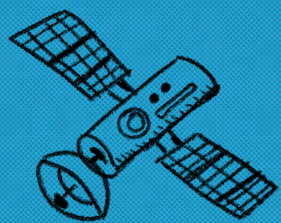
1. **Comprender** los fundamentos técnicos, sociales y políticos de internet, desde su infraestructura hasta su gobernanza multiactor.
2. **Analizar** los principales debates, actores y espacios de gobernanza de internet, visibilizando las tensiones de poder y las oportunidades de participación para la sociedad civil.
3. **Reflexionar** críticamente sobre los procesos de digitalización impulsados por los Estados y su relación con los derechos humanos y las desigualdades territoriales.
4. **Promover** la participación significativa de comunidades rurales, juventudes y sectores vulnerables en espacios de gobernanza de internet, vinculando experiencias locales con debates regionales y globales.
5. **Fomentar** la incidencia mediante propuestas concretas que integren perspectivas comunitarias en la agenda de gobernanza y digitalización, contribuyendo a que las tecnologías estén al servicio de las personas y los territorios.

¿CÓMO FUNCIONA INTERNET?

¿Qué hay detrás de la pantalla?

Descifremos eso que llamamos "Internet".





CONTENIDO

☀ Introducción	8
☀ Unidad 1: ¿Cómo funciona Internet? Veamos el ejemplo de WhatsApp	10
● ¿Qué es Internet?	11
● ¿Cómo nace el Internet? Pequeño recorrido	15
● Cómo viajan los mensajes: del dispositivo al servidor y del servidor al destinatario - espectro radioeléctrico	17
● Las capas de Internet	17
• Capa 1: Infraestructura física	18
• Capa 2: Estándares y servicios técnicos (o capa lógica)	20
• Capa 3: Contenidos y aplicaciones	28
☀ Unidad 2: Manipulaciones de Internet y DNS	36
● Control, fallas y caídas de internet	37
● ¿Cómo funcionan los cortes de internet y qué implican?	37
● El caso de WhatsApp en China: Censura y control	40
● Servicios alternativos DNS	42
● ¿Quieres aprender a documentar y analizar casos de interrupciones de Internet? Te presentamos el Observatorio de Bloqueos de Internet OBI	45
☀ Conclusiones	46
☀ Referencias	47
☀ Material adicional de consulta	48

INTRODUCCIÓN

En la actualidad, Internet es una infraestructura esencial que conecta a miles de millones de personas, dispositivos y servicios en todo el mundo. Sin embargo, más allá de su uso cotidiano, entender qué es Internet en términos técnicos, sociales, económicos y políticos es fundamental para abordar su gobernanza de manera informada y efectiva.

Este módulo tiene como objetivo ofrecer una visión clara y accesible sobre qué es Internet: cómo funciona, cómo se desarrolló, cuáles son sus principales componentes técnicos y quiénes intervienen en su operación. También presentamos la naturaleza descentralizada de Internet, sus principios fundamentales como la interoperabilidad, la apertura y el acceso universal, y cómo estos influyen directamente en los debates y decisiones sobre su gobernanza.

Al final de este módulo contarás con más herramientas para comprender los desafíos y oportunidades que surgen al gestionar una red global, estas te permitirán participar de manera informada en las discusiones sobre políticas públicas, regulación y derechos digitales que configuran el presente y futuro de Internet.



OBJETIVOS DEL MÓDULO

Objetivo general:

Comprender de manera autónoma y crítica el funcionamiento técnico, social y político de Internet, mediante el análisis de sus capas, el trayecto de la información, usando como ejemplo la mensajería instantánea, y las dinámicas de control y bloqueos de Internet.

Objetivos específicos:

- Describir y explicar las tres capas de Internet (infraestructura física, estándares/servicios lógicos y contenidos/aplicaciones) y el recorrido de un mensaje desde el dispositivo al destinatario usando WhatsApp como ejemplo.
- Analizar los mecanismos y causas de cortes, fallas y controles de Internet —incluyendo la manipulación del DNS y la censura estatal— mediante el estudio de casos (p. ej., restricciones a WhatsApp en China).
- Presentar algunas metodologías básicas de documentación y análisis de interrupciones de Internet, utilizando herramientas y recursos como el Observatorio de Bloqueos de Internet (OBI) para registrar, interpretar y comunicar incidentes.

UNIDAD I: ¿CÓMO FUNCIONA INTERNET? VEAMOS EL EJEMPLO DE WHATSAPP

Con esta unidad buscamos dar un contexto sobre qué es y cómo funciona Internet a través del ejemplo de mensajería instantánea con WhatsApp, una herramienta de uso masivo y cotidiano.

Aquí mostramos la infraestructura de internet, la transmisión de datos y el funcionamiento de algunos aspectos de seguridad digital, elementos claves para entender Internet. Además, compartimos algunos los retos, riesgos y limitaciones del funcionamiento actual de esta gran red que nos conecta a todos a nivel global.

Objetivo general

Explicar el funcionamiento básico de Internet para ofrecer una comprensión estratégica desde la práctica, más allá de la teoría, abordando su definición, cómo opera, las herramientas que lo sostienen y los actores que participan en su funcionamiento.

Objetivos específicos

1. Comprender cómo se transmiten los mensajes a través de las redes que conforman Internet.
2. Introducir el rol de los protocolos de comunicación, especialmente TCP/IP, en el funcionamiento de internet.
3. Analizar cómo el control, las fallas técnicas y las caídas del servicio de internet pueden afectar el acceso a derechos y el trabajo de incidencia de las organizaciones sociales.

Temas

1. ¿Qué es internet?
2. Breve historia de la internet ¿Cómo comenzó? ¿Cuál fue la motivación para su inicio? ¿Cómo ha sido el avance y las etapas de internet?
3. Cómo viajan los mensajes: del dispositivo al servidor y del servidor al destinatario - espectro radioeléctrico.
4. El papel de los proveedores de servicios de internet.
5. Cifrado y privacidad.
6. Caso: restricciones a WhatsApp en distintos países.

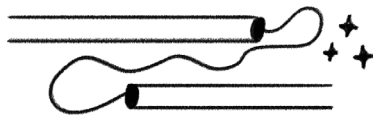
¿QUÉ ES INTERNET?

Internet es una red mundial de redes. Es decir, una gran estructura que conecta entre sí millones de computadoras, servidores, cables y otros dispositivos en todo el mundo. Esta conexión permite que puedan comunicarse y compartir información.

Aunque a veces se representa como una nube, en realidad Internet se basa en una infraestructura física: cables de fibra óptica, antenas, satélites y centros de datos que permiten que los datos viajen de un lugar a otro. Cada vez que enviamos un mensaje, abrimos una página web o vemos un video, estamos usando esa red de redes para intercambiar información.

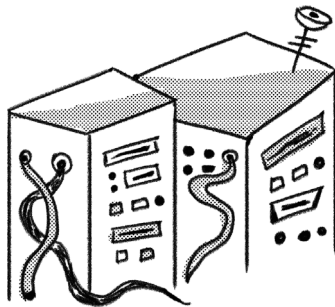
Internet: la Ciudad Digital

Imaginemos que Internet no es algo invisible y técnico, sino una ciudad enorme y compleja llamada **Ciudad Digital**. En esta ciudad, todo sucede a través del flujo constante de información:



Las calles son las **conexiones**

Hay diferentes tipos de calles, algunas son como autopistas rápidas (fibra óptica) que permiten que los datos viajen muy rápido y con alta capacidad. Otras son como caminos rurales o carreteras secundarias (satélite, cable coaxial) que son más lentas y tienen menor ancho de banda. Incluso hay calles llenas de semáforos y obstáculos (redes Wi-Fi congestionadas) que pueden ralentizar el tráfico.



Los edificios son los **servidores**

Estos edificios albergan la información o servicios de diferentes tipos: desde páginas web y videos, hasta correos electrónicos y archivos. Algunos almacenan grandes volúmenes de datos (grandes centros de datos), otros son pequeñas tiendas con información específica (servidores individuales). Son semejantes a locales, tiendas, centros comerciales, parques, hospitales, etc.



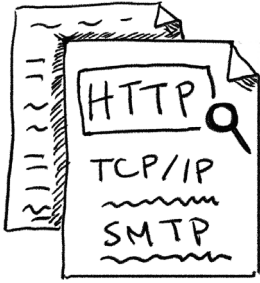
Las personas son los **dispositivos y usuarios**

Tenemos ordenadores, teléfonos inteligentes, tablets... Todos estos son ciudadanos o ciudadanas que viven en la Ciudad Digital y se comunican entre sí. Algunos son solo receptores de información (dispositivos pasivos), otros también son productores (usuarios que publican contenido en redes sociales o envían correos electrónicos).



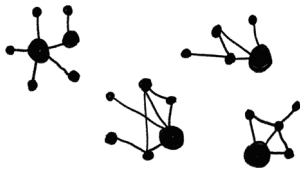
El tráfico es los **datos**

Cada mensaje, cada foto, cada video es un vehículo que viaja por las calles de la ciudad.



Las reglas y el orden son los **protocolos**

Como en cualquier ciudad, necesitamos reglas para que todo funcione bien. En Ciudad Digital, estas reglas son los protocolos, como HTTP (para navegar por páginas web), TCP/IP (la base del sistema de direcciones que identifica cada dispositivo) o SMTP (para enviar correos electrónicos). Estos protocolos aseguran que los datos lleguen a su destino correctamente y que las diferentes partes de la ciudad puedan comunicarse entre sí.



Los barrios son las **redes**

Las calles se agrupan en barrios, cada barrio tiene su propio administrador y sus propias reglas específicas. Por ejemplo, la red local de tu casa o la red social que utilizas.

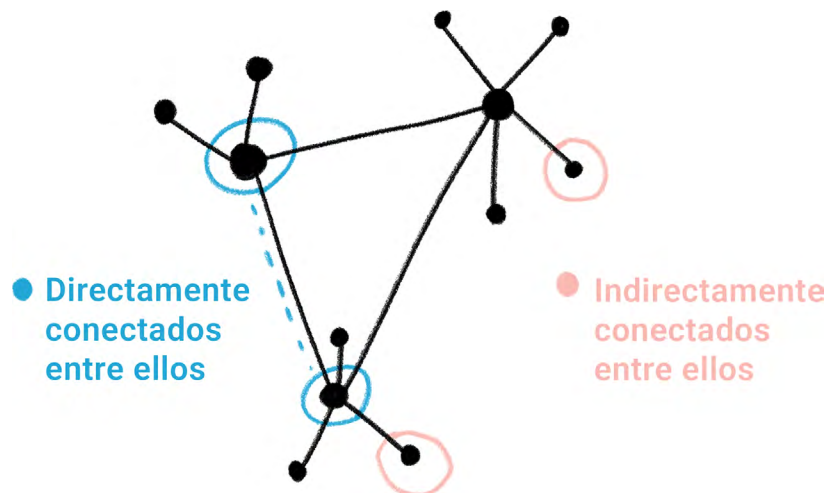


La policía y los bomberos son la **seguridad**

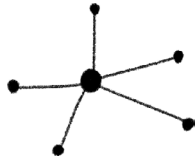
Imagina que suena una alarma, la policía (antivirus) intenta bloquear a los intrusos y rastrearlos; si el intruso entra y causa un incendio, llegan los bomberos (equipos de respuesta, copias de respaldo y recuperación), apagan el fuego, salvan lo que pueden y luego investigan cómo entró el intruso para que la policía pueda fortalecer la vigilancia.

Redes y nodos

Internet se define como una “red de redes” compuesta por redes más pequeñas llamadas nodos. Estos nodos actúan como centros de conexión, desde los cuales se extienden otros nodos. Imagina que cada nodo es un punto en una red, donde algunos están conectados directamente entre sí, mientras que otros lo están de manera indirecta a través de nodos intermedios. En el contexto de Internet, los nodos son dispositivos que pueden enviar y recibir información. Cada dispositivo tiene una dirección única, conocida como dirección IP, que permite localizarlo en la red. La información viaja de un nodo a otro, pasando por nodos intermedios que retransmiten los datos hasta que llegan al nodo destinatario.



Ahora bien, entre los tipos de redes encontramos:



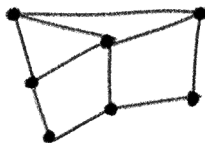
Redes centralizadas:

Cuando los diferentes nodos están conectados a través de un único nodo.



Redes descentralizadas:

Cuando muchos nodos se conectan a través de múltiples nodos, sin que uno solo aglomere todas las conexiones. Esto quiere decir que existen múltiples centros.



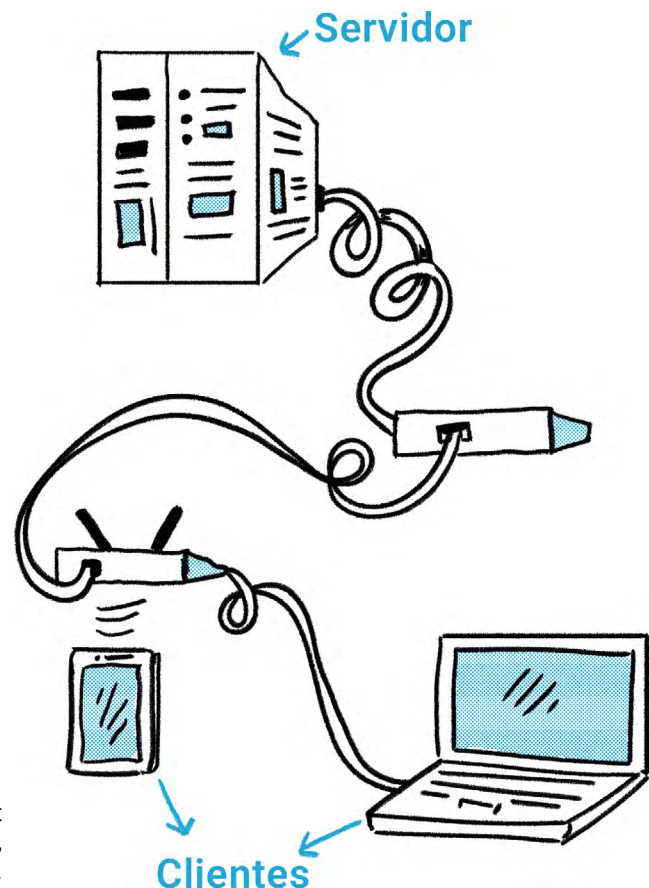
Redes distribuidas:

Cuando cada nodo está conectado de forma no jerárquica con los demás, ya que no existen centros ni pequeños ni grandes.

Una vez identificados, sabemos que aunque todos estos tipos de redes coexisten en Internet, el tipo de estructura que predomina es la descentralizada. Sin embargo, cuando abordemos las problemáticas de la gobernanza de Internet veremos que crecientemente algunos servicios marcan una pauta centralizadora del Internet.

Tipos de nodos: servidores, clientes y routers

Ahora que sabemos que Internet se compone de nodos, es importante distinguir los tipos principales: **servidores, clientes y dispositivos de red.**



Fuente: Adaptado y traducido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021.

Servidores

Los servidores son nodos que funcionan como computadoras conectadas a una red en la que proporcionan servicios y aceptan conexiones desde otros dispositivos o aplicaciones (a los que llamamos clientes). Su tarea principal es recibir, procesar y enviar información según lo soliciten esos dispositivos. Por ejemplo:

- Un servidor de correo electrónico recibe mensajes, los almacena y los entrega a los destinatarios.
- Un servidor de videojuegos coordina partidas, mantiene el estado del juego y sincroniza a los jugadores.
- Un servidor de mensajería (como WhatsApp) enruta y entrega mensajes entre usuarios y guarda históricos cuando es necesario.

A diferencia de una computadora personal, un servidor está optimizado para soportar muchas conexiones simultáneas, funcionar continuamente y manejar grandes volúmenes de datos. En pocas palabras: es una computadora potente diseñada para gestionar y distribuir información que otros dispositivos le piden.

Los servidores son nodos conectados físicamente a una red que ofrecen servicios y pueden aceptar conexiones de otros nodos. Su función principal suele ser enviar, recibir o procesar información. Algunos ejemplos son los servidores de videojuegos, de correo electrónico o de mensajería instantánea (como WhatsApp). Podemos pensarlos como una potente computadora diseñada para gestionar la información enviada mediante otros dispositivos.

Clientes

Son aquellos nodos que establecen conexiones con los servidores, es decir, aquellos que hacen uso de los servicios ofrecidos por uno o varios servidores. Por ejemplo, cuando queremos leer el correo electrónico necesitamos una aplicación cliente (como Outlook, Thunderbird o Gmail) que se conecte al servidor para autenticar la cuenta, sincronizar carpetas y descargar o mostrar los mensajes. Este cliente usa un protocolo como IMAP/POP3, además, ofrece la interfaz para redactar, buscar, organizar mensajes y guardar una copia local temporal si es necesario.

Lo mismo ocurre con la mensajería instantánea: WhatsApp requiere la aplicación cliente en el teléfono o el escritorio para enviar o recibir mensajes a su servidor y mostrar notificaciones. El cliente maneja la interfaz y la gestión de conversaciones, pero la entrega y el enrutamiento de los mensajes pasan por los servidores del servicio.

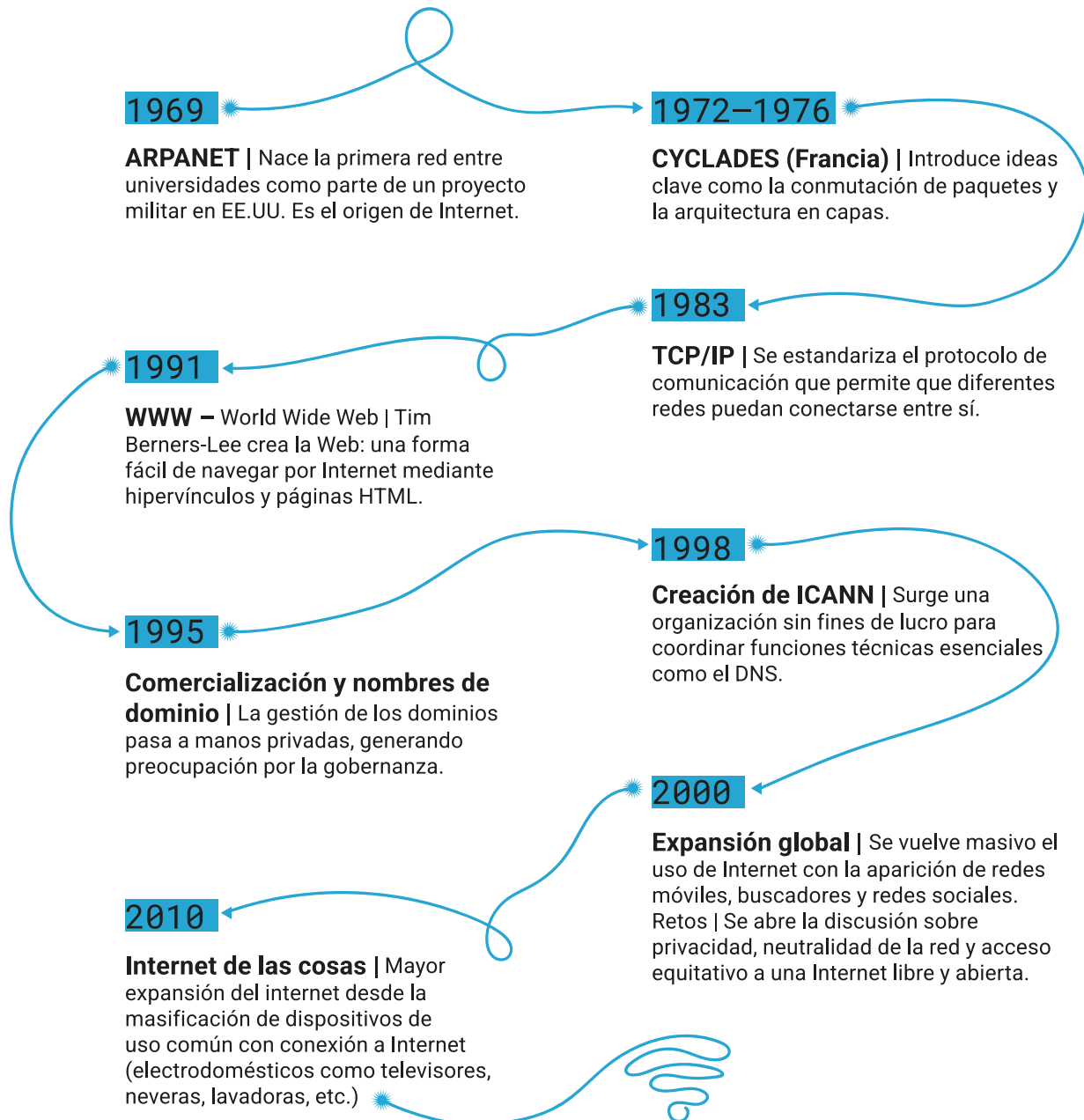
Dispositivos de red

Los dispositivos de red son de distintos tipos, capacidades, funciones y alcances. Facilitan la interconexión entre clientes y servidores para permitir el intercambio de información y el establecimiento de conexiones. Algunos ejemplos cotidianos de dispositivos de red son los routers, los puntos de acceso WiFi o los switches de red¹.

¹ Un switch de red puede entenderse como un repartidor inteligente dentro de una oficina o casa conectada: recibe paquetes (datos) que llegan por sus puertos y los entrega exactamente al destinatario correcto, en vez de enviarlos a todos. ¿Cuándo necesitas uno? Si tienes varios dispositivos cableados y quieres conexiones fiables y rápidas entre ellos (o hacia un router), un switch es la pieza que los conecta y organiza el tráfico entre los distintos dispositivos.

¿CÓMO NACE EL INTERNET? PEQUEÑO RECORRIDO.

Línea de tiempo de la historia de Internet



Internet no nació como un producto comercial, sino como un experimento colaborativo entre universidades, gobiernos y empresas. Su evolución muestra cómo una infraestructura pensada para compartir recursos entre investigadores se convirtió en una red global crítica para la información, los derechos y la participación ciudadana.

Por lo anterior, nos gustaría resaltar cuatro momentos clave:

1. **Internet: inicios en el sector defensa y la academia:** Todo comenzó con un grupo de personas que soñaban con conectar computadoras para compartir información, incluso a distancia. El primer experimento grande fue ARPANET, una red creada por el Departamento de Defensa de Estados Unidos (a través de la agencia DARPA) para que las computadoras de distintas universidades y centros de investigación pudieran “hablarse”. Su objetivo no solo era compartir recursos y datos académicos, sino también probar ideas de comunicaciones resilientes y distribuidas que permitieran mantener el intercambio de información, aún si partes de la red quedaban fuera de servicio —una preocupación estratégica del sector defensa durante la Guerra Fría. DARPA financió y coordinó la construcción de nodos y protocolos (como NCP y luego TCP/IP), promoviendo la colaboración entre investigadores militares y académicos y sentando las bases técnicas y organizativas que luego permitieron la expansión de la red hacia usos civiles y comerciales.
2. **Reglas comunes:** A medida que se sumaban más redes, era necesario que todas hablaran el mismo “idioma”. Así nacieron los protocolos TCP/IP, un conjunto de reglas que permiten que redes muy distintas se conecten entre sí.
3. **Triple W:** En los años 90 llegaron los navegadores web (por ejemplo Netscape Navigator e Internet Explorer), y con ellos Internet se volvió mucho más accesible y fácil de usar. Antes de los navegadores gráficos la mayoría de los recursos en la red se consultaban mediante interfaces de texto, comandos o programas especializados. Los navegadores introdujeron varias transformaciones claves: interfaz gráfica e hipervínculos, estándar HTML y URL, integración multimedia y scripts, búsqueda y directorios, comercialización, diseño web y adopción masiva.
4. **Gobernanza colaborativa:** Desde el comienzo, las decisiones sobre cómo debía funcionar Internet se tomaron de forma abierta y participativa a través de grupos de trabajo y documentos públicos como la [Solicitud de Comentarios](#) (RFC, por sus siglas en inglés de Request for Comments).

Hoy, el funcionamiento del Internet sigue dependiendo de una **infraestructura física robusta**, de normas técnicas compartidas (como **TCP/IP**) y de una **gobernanza colaborativa** donde participan tanto actores técnicos como sociales, asegurando que siga siendo una herramienta pública, abierta y universal.

CÓMO VIAJAN LOS MENSAJES: DEL DISPOSITIVO AL SERVIDOR Y DEL SERVIDOR AL DESTINATARIO - ESPECTRO RADIOELÉCTRICO

LAS CAPAS DE INTERNET

Hay diferentes modelos que explican cómo funciona internet: un modelo de tres capas que facilita el entendimiento práctico y general de Internet, el modelo TCP/IP de cuatro capas y el modelo OSI de 7 capas. Aunque en este documento nos enfocamos en el modelo de las tres capas, acá te presentamos un cuadro comparativo entre los diferentes modelos.

Modelo de tres capas	Modelo OSI	Modelo TCP/IP
Capa 1: Infraestructura física	Capa 1: Física	Capa 1: Acceso al medio
Capa 2: Estándares y servicios técnicos	Capa 2: Enlace de datos	
	Capa 3: Red	Capa 2: Internet
	Capa 4: Transporte	Capa 3: Transporte
Capa 3: Estándares de contenidos y aplicaciones	Capa 5: Sesión	Capa 4: Aplicación
	Capa 6: Presentación	
	Capa 7: Aplicación	

Modelo de 3 capas

El modelo de 3 capas es una forma simplificada de entender cómo está organizada Internet y cómo interactúan sus diferentes elementos para permitirnos conectarnos, comunicarnos y compartir información. Este modelo nos ayuda a visualizar que Internet no es una sola cosa, sino una red compleja compuesta por distintos niveles, cada uno con funciones específicas.

En este modelo, las capas que conforman Internet son:

- (1) capa de infraestructura física
- (2) capa de estándares y servicios técnicos
- (3) estándares de contenidos y aplicaciones

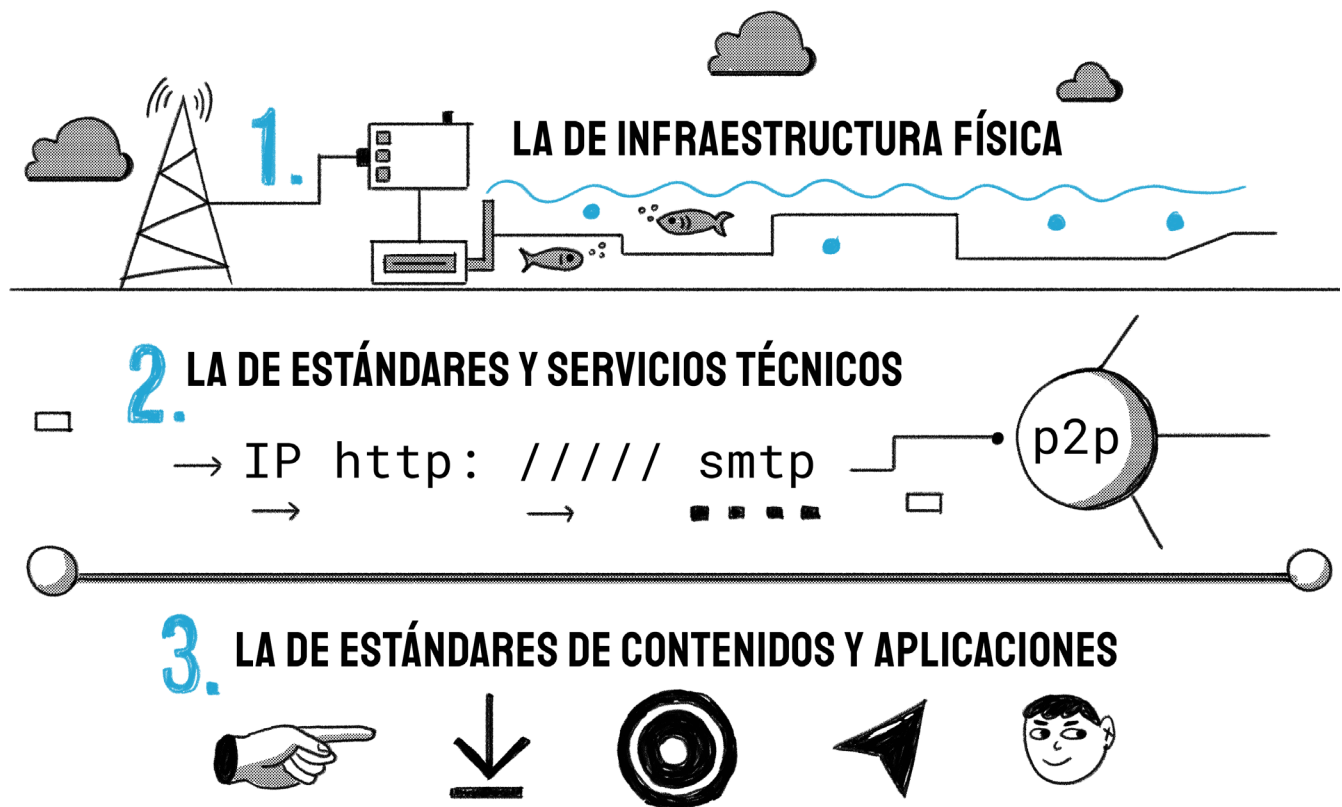


Imagen 1: tomado de *Cómo funciona internet*, Karisma

CAPA I: INFRAESTRUCTURA FÍSICA

La capa física es la infraestructura tangible por la que viaja Internet. Incluye antenas, satélites, cables convencionales y de fibra óptica. Aunque no la vemos en la pantalla, sin esta red de equipos y tendidos no podríamos enviar mensajes ni subir o recibir fotos. En resumen: **es el conjunto de elementos físicos que transportan todos los datos que enviamos y recibimos.**

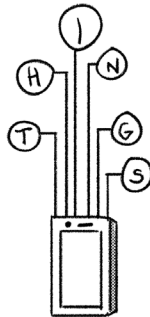
La capa física del Internet está compuesta por cables y equipos como routers que conectan entre sí a múltiples Sistemas Autónomos (AS) en puntos clave llamados Internet Exchange Points (IXP). Estos últimos permiten intercambiar datos entre sí, y suelen estar ubicados en grandes centros de datos que están encendidas todo el tiempo.

La componen los siguientes elementos:

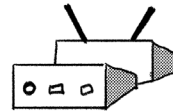
- Cables submarinos y terrestres
- Antenas y torres
- Centros de datos
- Routers, switches
- Puntos de Intercambio de Internet (IXP)



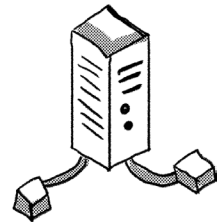
Computadores
(servidores, computadoras personales, dispositivos móviles)



Internet de las cosas
(IoT, en inglés Internet of Things.)



Dispositivos de red
(routers, puertas de enlace, conmutadores, repetidores, etc.)



Centros de datos
(en inglés, data centers)

Fuente: Adaptado y traducido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021.

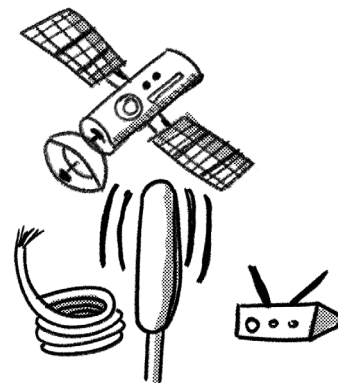
¿Para qué sirve esta capa?

- Conecta a todo el mundo en una sola red.
- Transporta los datos de forma rápida y eficiente.
- Interconecta redes distintas, haciendo que las comunicaciones no tengan fronteras.
- Soporta todos los demás niveles de Internet. Sin esta capa, nada funciona.

Un **Sistema Autónomo (AS)** es una gran red independiente (por ejemplo, un proveedor de Internet, una universidad o empresa grande) que controla su propio tráfico interno.

Los IXP son lugares físicos donde muchos AS se interconectan y comparten datos de forma directa, haciendo que Internet sea más rápido, estable y barato.

Los cables físicos (especialmente de fibra óptica) transportan datos a gran velocidad entre continentes, países y ciudades. Los routers y switches se encargan de dirigir esa información por la mejor ruta posible, asegurando que los datos lleguen a su destino correcto. Son grandes redes independientes, de proveedores de Internet, universidades o empresas que gestionan sus propias rutas internas de datos.



Cables de telecomunicación, redes inalámbricas, redes satelitales

Elemento	¿Que hace?	Ejemplo
Cables de fibra óptica	Transportan datos a gran velocidad usando luz.	Cable submarino entre continentes
Antenas y torres	Envían datos por el aire.	Torre de celular
Satélites	Permiten conexión en lugares remotos.	Internet en zonas rurales
Routers y switches	Redirigen datos hacia su destino.	Router de tu casa o empresa
Centros de datos	Lugares donde muchas redes se conectan.	Punto de intercambio de tráfico (IXP)

CAPA 2: ESTÁNDARES Y SERVICIOS TÉCNICOS (O CAPA LÓGICA)

Esta capa se encarga del correcto funcionamiento de Internet a nivel técnico. Si la capa anterior se asemejaba a las autopistas, calles y puentes de nuestra Ciudad Digital, esta podría traducirse en las reglas de circulación de las vías. Por ejemplo, cómo operan las señales de tránsito, por dónde transitan los datos y cómo deben hacerlo, las velocidades máximas y mínimas, entre otros aspectos. Esta capa requiere una gran participación de instituciones privadas y agrupaciones profesionales que determinan las condiciones técnicas y estándares que facilitan el intercambio de información en

Internet.

¿Cómo se comunican los nodos en una red?

El Internet necesita que distintos nodos (clientes, servidores y dispositivos de red) se comuniquen entre ellos, para que esto ocurra se requiere un lenguaje común que permita a los diferentes nodos entenderse. Por eso se creó un sistema de reglas con una sintaxis particular que permite dicho entendimiento. Dicho sistema de reglas responde a las siguientes preguntas:

- ¿Puedo poner un paquete de datos dentro de otro?
- ¿Qué pasa si un paquete no tiene información de dirección o destinatario?
- ¿Cómo se envían los datos a través de Internet? ¿Se envía un solo paquete grande o se divide en partes más pequeñas?
- ¿Se puede modificar una información mientras viaja por Internet?
- ¿Qué pasa cuando una información se pierde? ¿Se puede perder información mientras viaja por la ciudad digital?
- ¿Qué detalles necesita un paquete de datos para viajar por Internet?

¿Qué son los paquetes?

Los paquetes son las unidades en que se divide la información para viajar por una red. Es decir, todo dato que pretende enviarse a través de una red se divide en paquetes. Cada paquete contiene dos partes principales:

- **Cabecera (header):** lleva metadatos necesarios para que la red entregue el paquete correctamente —por ejemplo, direcciones IP de origen y destino, números de puerto, información de fragmentación, control de errores y de enrutamiento.
- **Carga útil (payload):** es el contenido real que se está enviando (fragmento del archivo, parte de un correo, una petición HTTP, etc.).

Características importantes

- **Fragmentación y reensamblado:** un mensaje grande se divide en varios paquetes; el receptor los vuelve a juntar adecuadamente.
- **Enrutamiento:** los routers leen la cabecera del paquete para decidir por qué camino enviar cada paquete a su destinatario.
- **Fiabilidad vs. velocidad:** protocolos como TCP añaden control de errores y confirmaciones para asegurar entrega; UDP prioriza rapidez sin garantías.
- **Tamaño limitado:** cada medio/red impone un tamaño máximo por paquete (MTU); paquetes demasiado grandes se fragmentan.

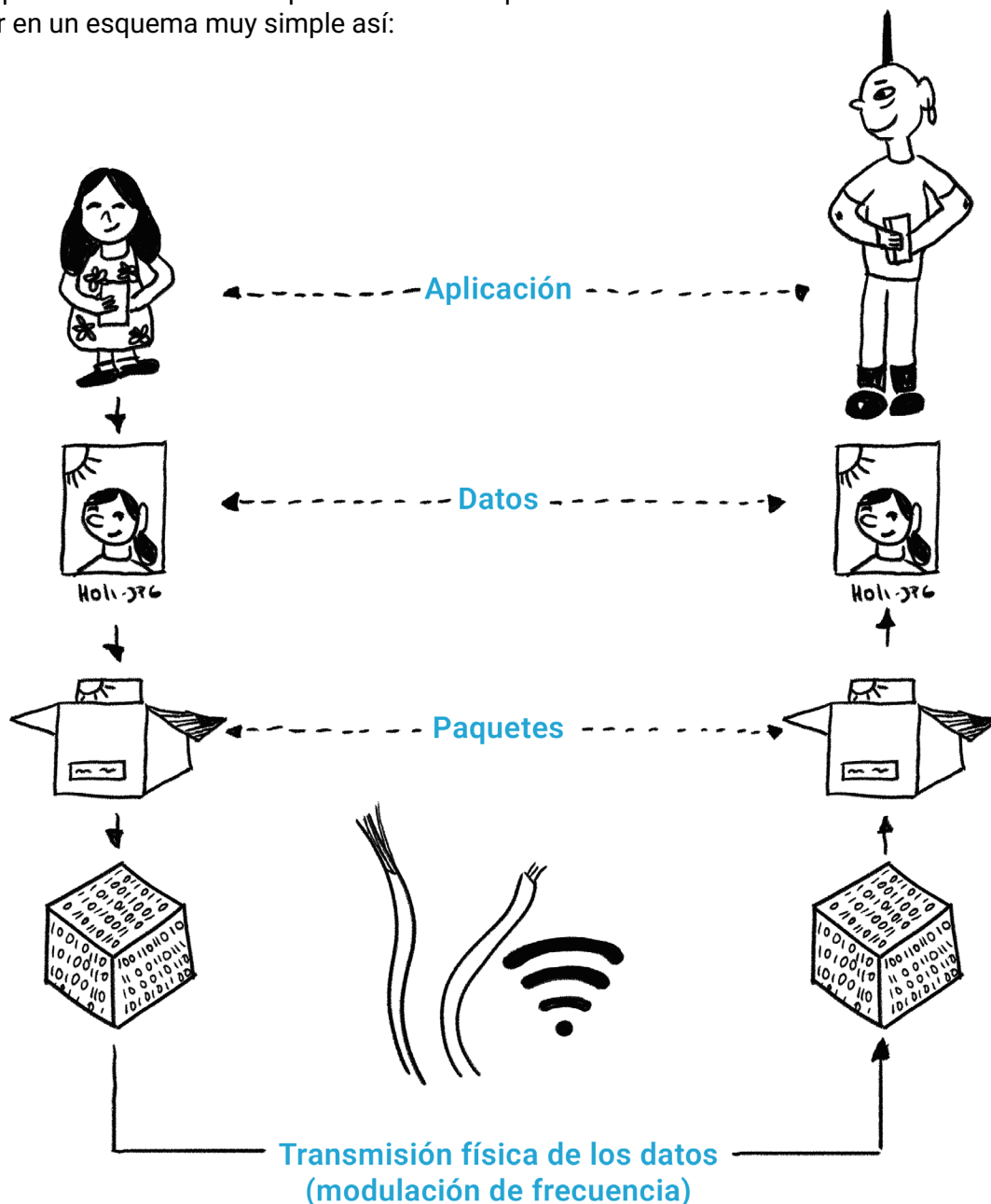
Piensa en un envío por mensajería. La cabecera equivale a la etiqueta externa con la dirección, el remitente, instrucciones de manejo y datos de seguimiento; la carga útil equivale al objeto dentro de la caja.

Te ponemos el ejemplo del envío de un video o una fotografía por WhatsApp o cualquier otro medio de mensajería: dicho elemento sería descompuesto en varios paquetes que se envían de forma independiente. Esto es muy útil pues supón que tu foto se pierde completa, tendría que enviarse por completo de nuevo, mientras que si se pierde una pieza de esa foto es mucho más fácil reenviar solo esa parte.

¿De qué están compuestos los paquetes?

En el mundo digital, los datos siempre son presentados en su nivel más básico desde un sistema binario, esto es ceros (0) y unos (1). Este es el sistema de datos que pueden procesar las computadoras. Dicha codificación cambia dependiendo del medio, es decir, puede cambiar si pasa por ondas, cable de cobre o fibra óptica.

Desde el punto de vista de las capas de Internet el proceso de comunicación entre nodos se puede visualizar en un esquema muy simple así:



Fuente: Adaptado y traducido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021.

El protocolo TCP/IP

Toda esta comunicación requiere reglas, las cuáles llamaremos protocolos. Si bien hay diferentes tipos, el principal a nivel de Internet es el Internet Protocol (IP). Este se encarga de definir el formato del encabezado de los paquetes que viajan por Internet, esto es, entre los dispositivos de red desde su emisor hasta su destinatario. Incluye, por supuesto, la información que lleva el encabezado de los paquetes y su formato.

La principal virtud de este y otros protocolos es que permiten enlazar distintos tipos de dispositivos (por ejemplo, un computador, un celular o un servidor) que ejecutan sistemas operativos distintos (Windows, Linux, Android o MacOS) sobre distintos tipos de redes.

¿Cómo funciona?

Primero, a todo dispositivo conectado a una red se le asigna una dirección IP. Este aspecto es clave para comunicarse a través de Internet, siempre que la dirección respete el estándar. Existen dos tipos de direcciones IP:

- **Públicas:** Aquellas que tienen acceso directo a Internet.
- **Privadas:** Aquellas que no tienen acceso directo a Internet, pero se conectan a este a través de un intermediario. Por ejemplo, el router de una oficina o casa.

El router como dispositivo de red tiene asignada una dirección IP pública, determinada por el Proveedor de Servicio de Internet (hablaremos de esto más adelante) y, a su vez, provee a cada dispositivo conectado a su red local (LAN) una IP privada.

Una condición importante para las IP públicas y privadas es que toda dirección debe ser única dentro de la red. Esto quiere decir que nadie en la extensión de Internet puede tener la misma dirección IP que otro nodo/dispositivo. Siempre hay un destinatario y un emisor con una dirección IP única que evita que haya confusiones durante la comunicación. Imagínate que ordenas algo a domicilio y en tu mismo barrio o ciudad hay dos personas con la misma dirección. ¡Qué confusión!

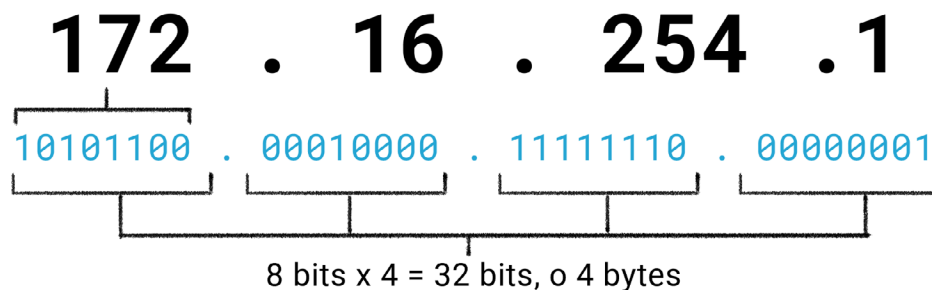
¿Cómo se ven las direcciones IP?

Actualmente, existen dos versiones de direcciones IP, cada una luce diferente:

- **IPv4:** La versión más usada en Internet, aunque que no tiene tantas direcciones disponibles (solo dispone 4.300 millones) para todos los dispositivos y personas que ahora se conectan a Internet.
Se componen de cuatro series numéricas entre 0 y 256, separadas por puntos
- **IPv6:** La versión más reciente y eficiente, es capaz de cubrir la inmensidad de los dispositivos conectados a Internet por muchos muchísimos años. No ahondaremos en la composición de esta versión, pero por si te da curiosidad, se ven así:
2001 : 0DB8 : 0000 : 0001 : 0000 : 0000 : 0010 : 01FF

¿Te acuerdas que dijimos que todo viaja en Internet con el sistema binario? A modo de ilustración, así se representa la siguiente IPv4 en número binario:

Estructura de una dirección IP (Versión 4 o "IPv4")



Tomado de Paz Peña (2013, p. 17)

¿Cómo se usan las direcciones para enviar los paquetes por Internet?

Cada paquete lleva en su encabezado la **dirección IP de origen** y la **dirección IP de destino**. Esas direcciones permiten que la red sepa de dónde viene el paquete y a dónde debe llegar. El envío funciona así:

1. El dispositivo emisor crea el paquete con la dirección IP destino en la cabecera y lo envía al router local (por ejemplo, el router de casa).
2. El router local examina la dirección destino y consulta su tabla de enrutamiento para decidir cuál es el siguiente salto —normalmente envía el paquete al router del proveedor de Internet (ISP)—.
3. Cada router intermedio repite el proceso: lee la IP destino, consulta su tabla de rutas y reenvía el paquete al siguiente router que lo acerque al destino. Los routers no necesitan conocer la ruta completa, solo el mejor siguiente salto.
4. El paquete avanza por una cadena de routers y redes (backbones del ISP, routers regionales, etc.) hasta que llega a un router que está en la misma red que el dispositivo destino.
5. Este último router entrega el paquete al dispositivo receptor para la entrega final.
6. En el destino, el paquete se reensambla con otros paquetes (si el mensaje fue fragmentado) y la capa de transporte (p. ej. TCP) verifica integridad y orden; si falta algún paquete, el receptor solicita reenvío.

DNS: Sistemas de Nombres de Dominio

¿Qué es un servidor ?

Los contenidos y servicios de internet se encuentran almacenados en computadores de la red. Los sitios web, por ejemplo, están alojados en estos tipos de computadores que llamamos servidores. Un servidor es una computadora especializada que almacena datos y servicios disponibles en internet. A diferencia de un computador personal, un servidor está diseñado para responder de forma continua y eficiente a múltiples solicitudes de otras computadoras (como la tuya) que buscan acceder a sitios web, correos electrónicos, archivos o plataformas.

Usualmente, en lugar de usar una dirección IP para acceder a los contenidos, los encontramos a través de su **nombre de dominio**. Este nombre permite acceder a los sitios y servicios en Internet sin tener que recordar la dirección IP y para ello nos servimos del servicio **DNS** (Domain Name System, por sus siglas en inglés) que funciona de forma parecida a un directorio telefónico, permitiendo encontrar una dirección IP a partir del nombre de dominio. Por ejemplo, el dominio karisma.org.co resuelve la dirección IP 5.9.111.213 .

Los servidores web pueden estar en cualquier parte del mundo y una sola IP puede alojar muchas páginas distintas. Por ejemplo, una empresa puede tener varias páginas alojadas en un mismo servidor. El lugar físico donde se encuentra un servidor (es decir, en qué país o región está alojado) determina qué leyes le aplican. Por ejemplo, en Europa, los servidores deben cumplir con el Reglamento General de Protección.

Los nombres de dominio funcionan como un traductor de direcciones IP a nombres que podemos recordar más fácilmente. Aquí es importante saber cómo funcionan las páginas web y el caché, pero antes de profundizar en el tema, volvamos a nuestra Ciudad Digital.

Cada casa o edificio necesita una dirección clara para que otras personas puedan llegar a ella sin dificultades. Sin embargo, cuando se trata de sitios web, tendríamos que consultarlos sabiendo la dirección IP del sitio. Imagina que siempre que quieras entrar a tu red social favorita o al sitio web de tu universidad o colegio tuvieras que escribir una dirección IPv4 como **172.16.254.1** o, peor aun, en IPv6 algo como **2001:0DB8:0000:0001:0000:0000:0010:01FF** ¿Difícil verdad?, pues imagina que los DNS se asemejan a un directorio telefónico que nos evita tener que recordar las direcciones IP de todos los sitios. Esto significa que, en adelante, solo tendrás que recordar el nombre del sitio web que quieres visitar y el navegador o aplicación que utilices resolverá la dirección del sitio web que estás queriendo consultar —mucho más fácil, ¿no te parece?—. Esto implica que no pueden haber dos nombres exactamente iguales.

Los nombres de dominio son una base de datos pública y descentralizada que asocia un nombre único a una dirección IP junto a otros datos. Al igual que otros protocolos en Internet, los nombres de dominio tienen algunas reglas, aquí te presentamos las principales:

- **Subdominio:** El dueño de un dominio registrado puede crear los subdominios que desee, incluso sub-subdominios, sub-sub-subdominios y así consecutivamente. Nadie puede registrar o comprar un subdominio de otro dominio de forma separada.
- **Dominio:** Cualquier personas u organización puede comprar un nombre de dominio a una organización o empresa avalada por el ICANN.
- **TLD (top level domain):** Existen más de 300 TLD comunes.
- **Raíz:** Son los servidores DNS que resguardan en el nivel más alto los registros de todos los TLD y es mantenido por ICANN.

Esto en conjunto se ve, por ejemplo, así:



Cuando haces la búsqueda en el motor de búsqueda de tu preferencia, se hace una solicitud en los servidores DNS para dar con la dirección IP que estás solicitando.

Si deseas aprender más y de forma interactiva sobre los DNS, te recomendamos este recurso:

[Cómo funciona DNS](#)

Aspectos comerciales de la infraestructura de Internet: los ISP

Para tener acceso a Internet desde cualquier dispositivo es necesario contar con las condiciones técnicas —que ya hemos visto a lo largo del curso— pero también con las condiciones comerciales de obtener acceso a Internet. Acá debemos añadir a las organizaciones intermediarias que invierten en condiciones técnicas y físicas para dar cobertura de Internet y obtener una retribución económica a cambio. Los llamaremos **proveedores de servicio de internet** (ISP, por su siglas en inglés: Internet Service Provider). Empresas como Claro, Movistar y Tigo en Colombia, o internacionales como AT&T y Verizon.

Los ISP son los intermediarios entre las personas usuarias y la infraestructura de Internet. Es importante tener presentes características como cobertura, tecnología (cable, fibra óptica, banda ancha, etc.) y velocidad. Los ISP cumplen un rol fundamental en el funcionamiento de internet porque permiten que las personas y organizaciones se conecten con el resto de la red.

Entre sus funciones y capacidades están:

- Asignar direcciones IP a los dispositivos.
- Enrutar el tráfico, es decir, decidir por dónde viajan los datos para llegar a su destino.
- Administrar la infraestructura técnica que hace posible la conexión.
- Filtrar, bloquear o priorizar ciertos contenidos o servicios, lo que les da un gran poder sobre el tipo de acceso que tienen las personas.
- Ofrecer planes diferenciados que afectan la velocidad o disponibilidad de aplicaciones específicas.

El acceso a internet puede darse de distintas formas dependiendo de la tecnología disponible, la ubicación geográfica y las decisiones de los proveedores. Cada tipo de acceso tiene implicaciones en la velocidad, calidad, precio y estabilidad de la conexión y puede influir directamente en quién accede, cómo lo hace y para qué.

Esto son los tipos más comunes de acceso a internet:

- **Banda ancha:** Provee internet a través de cables o líneas telefónicas. Es común en servicios de televisión por cable. Tiene buena velocidad, pero es menos estable que la fibra. Muchos hogares en ciudades todavía acceden a Internet de esta manera.
- **Fibra óptica:** Es una de las conexiones más rápidas y estables. Usa cables especiales que transmiten datos a través de la luz. Suele estar disponible en zonas urbanas, es costosa de instalar en zonas rurales. Los ISPs que ofrecen este servicio suelen ser grandes operadores.
- **DSL:** funciona a través de líneas telefónicas. Es más lenta y está siendo reemplazada por tecnologías más modernas. Aún se usa en zonas con infraestructura limitada.
- **Inalámbrica:** Redes satelitales o móviles (comunes en zonas rurales).
- **Internet móvil (3G, 4G, 5G):** Utiliza redes celulares. Es muy común en zonas donde no hay conexiones fijas o cuando se accede desde teléfonos móviles. Depende de la cobertura de las antenas instaladas por las empresas de telecomunicaciones.
-

¿Qué instituciones regulan y se involucran directamente en estos estándares?

ICANN: Coordina nombres de dominio y direcciones IP con participación global y abierta. Las decisiones se toman por consenso. Un ejemplo de gestión de este espacio son las [Políticas sobre datos de registro](#) y [transferencia de dominios](#).

IETF (Internet Engineering Task Force): Organismo que establece estándares técnicos TCP/IP a través de consensos abiertos. Estos estándares son adoptados por personas usuarias, redes y fabricantes para construir el Internet que usamos. Si bien es un espacio técnico, las organizaciones de la sociedad podrían aliarse para generar una participación a través de equipos técnicos y no técnicos que puedan incidir en consideraciones de seguridad y privacidad en este espacio. No obstante, la influencia práctica suele requerir contribuciones técnicas (propuestas, implementación, pruebas). La IETF no es un foro político amplio; su lenguaje y procesos son técnicos, por lo que la entrada efectiva para actores no técnicos suele necesitar apoyo.

IANA (Autoridad de Números Asignados de Internet): Es una organización parte de ICANN, responsable de coordinar con registros regionales de Internet (RIRs, por ejemplo, LACNIC para América Latina y el Caribe), proveedores de servicios, operadores de redes y la comunidad técnica para garantizar que los identificadores de Internet sean únicos y estén bien coordinados. Sus funciones cubren: asignación y gestión de espacio de direcciones IP y la gestión de nombres de dominio de alto nivel.

LACNIC: Registro regional de Direcciones IP de América Latina: Es la organización regional (RIR) responsable de la asignación y administración de recursos numéricos de Internet (IP) en América Latina y el Caribe.

CAPA 3: CONTENIDOS Y APLICACIONES

La capa de contenidos y aplicaciones es la que usamos directamente cuando navegamos por Internet. Es lo que vemos, tocamos y con lo que interactuamos: páginas web, correos electrónicos, aplicaciones de mensajería, redes sociales, videos, entre otros.

Normalmente la asociamos con “Internet”, porque es la más visible y cotidiana. Pero, como ya vimos, debajo existen otras capas que hacen posible que todo esto funcione.

Una metáfora para entenderlo

Si seguimos con la comparación vial, esta capa serían los vehículos que circulan por las calles:

- Gracias a ella podemos movernos, comunicarnos y transportar información.
- Aquí están los espacios donde nos expresamos, compartimos saberes, construimos comunidad y ejercemos ciudadanía.



Todas nuestras acciones en Internet ocurren aquí: buscar en Google, mandar un correo, chatear en WhatsApp, hacer una videollamada o subir un video. En ella los datos circulan y permiten la conexión con otras personas en cuestión de segundos.

Y cuando decimos que “aquí están los espacios donde nos expresamos, compartimos saberes, construimos comunidad y ejercemos ciudadanía”, señalamos que Internet no es solo tecnología: también es un espacio social y político. En Internet nos organizamos, denunciemos, compartimos aprendizajes, hacemos campañas o celebramos. En otras palabras, esta capa puede entenderse como una plaza pública digital donde ocurre nuestra vida en línea y donde se juegan derechos como la libertad de expresión y el acceso a la información.

¿Por qué es importante esta capa?

La capa de contenidos y aplicaciones es donde realmente vivimos Internet: es el espacio visible y tangible que usamos para comunicarnos, aprender, entretenernos y organizarnos. Aquí convergen páginas web, mensajería, redes sociales, plataformas de video, correos y aplicaciones diversas; son los espacios de encuentro en donde ocurren nuestras conversaciones, conocimientos y experiencias sociales. Al interactuar con una app o abrir una página no vemos los cables ni los protocolos, pero sí sentimos de inmediato la experiencia —la rapidez, la interfaz, la posibilidad de compartir— que define cómo nos relacionamos en línea.

Además, esta capa es también un espacio social y político: en ella ejercemos derechos digitales como la libertad de expresión, el acceso a la información y la asociación. Es la plaza pública digital donde construimos comunidad, denunciemos injusticias, difundimos aprendizajes y organizamos iniciativas colectivas. ¿Una plaza pública digital? Sí, pero a diferencia de una plaza física que pertenece a todas las personas, esta plaza digital está en gran parte gestionada por plataformas privadas como Meta, Google, X, TikTok, etc., que deciden qué se puede mostrar, qué se oculta y qué se elimina. Por eso su diseño, gobernanza y accesibilidad importan tanto como la infraestructura técnica que la sostiene: limitar, censurar o dificultar el acceso a estos contenidos equivale a restringir la vida pública y democrática que hoy circula en Internet.

¿Para qué sirve esta capa?

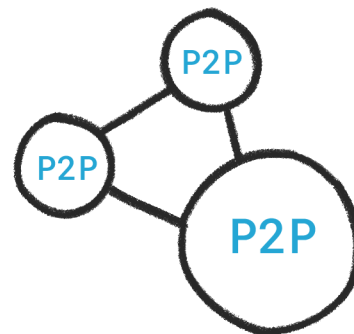
Sirve para mucho más que “chatear” o “ver videos”. Aquí se organiza y da forma a nuestras interacciones digitales. En ella se definen muchas reglas invisibles:

- Qué aparece primero en una búsqueda.
- Qué contenido se recomienda en nuestro muro.
- Qué publicaciones se eliminan por incumplir normas de la comunidad.
- Qué mensajes o videos se vuelven virales y cuáles quedan escondidos.
-

En otras palabras, esta capa no solo conecta personas, también influye en qué información circula y cómo se distribuye.

Algunos protocolos detrás de escena

Dentro de esta capa se contienen reglas técnicas que hacen que todo funcione:



Tomado de Fundación Karisma (2024)

HTTP y HTTPS

Cuando entras a una página web y escribes algo como `www.fundacionkarisma.org` tu navegador necesita un protocolo para pedirle al servidor que te muestre esa página. Ese protocolo se llama **HTTP (Hypertext Transfer Protocol)**.

- **HTTP (Hypertext Transfer Protocol)**

Es el protocolo más antiguo y tradicional para navegar por Internet.

- Funciona como si mandarás una postal sin sobre: la información viaja “a la vista”.
- Cualquier persona que intercepte la comunicación podría leer lo que haces, por ejemplo si usas una red Wi-Fi pública o si alguien está espiando el tráfico.
- Eso significa que tus datos (como lo que escribes en un formulario) pueden ser vistos o modificados.

- **HTTPS (Hypertext Transfer Protocol Secure)**

Es la versión segura de HTTP.

- Aquí la postal viaja dentro de un sobre cerrado con candado. Ese candado es el cifrado que protege la comunicación usando un sistema llamado TLS (Transport Layer Security).
- Con HTTPS, aunque alguien intercepte la conexión, no podrá leer lo que envías ni lo que recibes (como contraseñas, mensajes o números de tarjeta).
- Los navegadores suelen mostrar un candadito al lado de la dirección web para indicar que la conexión es segura.

En pocas palabras: si ves HTTP, desconfía para cosas sensibles; si ves HTTPS, tienes una capa extra de seguridad.

Si deseas aprender más y de forma interactiva sobre los DNS, te recomendamos este recurso:

[Cómo funciona HTTPS](#)

SMTP: el cartero de los correos electrónicos

El correo electrónico también necesita un protocolo para funcionar. Cuando escribes un mensaje y haces clic en “**enviar**”, tu aplicación de correo (Gmail, Outlook, Thunderbird, etc.) usa **SMTP (Simple Mail Transfer Protocol)**.

- Piensa en SMTP como el **cartero digital**: recoge tu correo y lo entrega al servidor de destino.
- Importante: SMTP **sólo envía correos**, no los recibe.
- Para recibirlos, se usan otros protocolos llamados **POP3** o **IMAP**.
 - **POP3** descarga los correos a tu dispositivo.
 - **IMAP** permite verlos desde varios dispositivos porque los mantiene sincronizados en el servidor.

Aunque muchas veces solo vemos la interfaz de Gmail o Outlook, en el fondo son estos protocolos los que hacen posible que tus mensajes viajen de un lugar a otro.

Conocer estos protocolos no es solo “tecnicismo”, nos da herramientas para tomar decisiones más seguras. Por ejemplo, saber que HTTPS protege nuestros datos o que IMAP permite mantener sincronizada la bandeja de correo en el celular y el computador.

Veamos cómo funciona la capa de trasportes en dos escenarios cotidianos:

PARTE I - ¿CÓMO ACCEDEMOS A LOS CONTENIDOS EN INTERNET ?

Cuando entramos a nuestro navegador de Internet para buscar algo —por ejemplo, “seguridad digital”, una noticia o un video de música— normalmente no sabemos en qué lugar del mundo está esa información ni en qué computadora está guardada. Puede estar en Colombia, en Estados Unidos o en un servidor en otro continente.

Lo sorprendente es que, aunque físicamente puede estar muy lejos, llegamos a ella en segundos. Eso es posible gracias a una serie de pasos que ocurren en segundo plano que permiten que la información viaje desde donde está almacenada hasta tu pantalla.

Paso 1: usamos un buscador

Casi siempre, lo primero que hacemos para ingresar a Internet es abrir un buscador como Google, DuckDuckGo o Bing. Escribimos una palabra o una pregunta (“qué es phishing”, “recetas de arroz con coco”, “cómo proteger mi contraseña”), y en milésimas de segundo nos aparece una lista de páginas relacionadas.

Pero ojo: los buscadores no son neutrales. Ellos deciden qué mostrar primero y qué esconder más abajo.

- Factores como cuánta gente visita una página, qué tan confiable parece, si tiene enlaces de otros sitios o incluso si está pagando publicidad influyen en el orden de los resultados.
- En otras palabras, el buscador no solo nos ayuda: también filtra, organiza y prioriza lo que podemos ver.

Pensemos en un ejemplo cotidiano, preguntas en tu barrio dónde venden buen pan. Cada persona te recomendará algo distinto: la panadería más famosa, la que queda más cerca o la de su primo. El buscador hace algo parecido, pero a gran escala.

Actividad rápida: Ingresa la misma palabra en Google y en DuckDuckGo. ¿Qué diferencias encuentras en los primeros resultados que aparecen?

Paso 2: Abrimos una página web utilizando una URL

Cuando hacemos clic en un resultado, estamos entrando a una página web que tiene una dirección como www.karisma.org.co o www.wikipedia.org.

Paso 3: el dominio se convierte en una dirección IP (DNS)

Aquí entra en acción el DNS (Sistema de Nombres de Dominio), el cual traduce el nombre de la página en la dirección IP que indica exactamente en dónde está alojado y disponible el sitio web o servicio que estamos solicitando (siempre que, en efecto, exista).

Pensemos en otro ejemplo sencillo: cuando marcas “Mamá” en tu celular, no estás escribiendo el número completo, pero tu teléfono lo busca en su agenda y marca el número correcto. El DNS hace lo mismo, pero a escala global.

Paso 4: el servidor responde

Cuando visitas una página, tu computadora envía una solicitud al servidor donde está guardada esa página, utilizando la dirección IP. Este servidor es esa gran computadora que almacena todos los archivos: textos, imágenes, videos, etc. Si el servidor está disponible, te responde enviándote el contenido que pediste.

Ejemplo: Pides una pizza a domicilio. Tú llamas (haces la solicitud), la pizzería prepara y envía tu pedido (el servidor responde), y al final disfrutas tu pizza en casa (tu navegador muestra la página).

PARTE 2 ¿CÓMO VIAJA UN MENSAJE DE WHATSAPP O POR MENSAJERÍA INSTANTÁNEA ?

Ahora pensemos en algo más cotidiano: enviar un mensaje por WhatsApp.

Paso 1:

Tú escribes un mensaje (“voy en camino”) y presionas enviar

Paso 2:

Tu celular lo convierte en un lenguaje que entiende la red: ceros y unos (bits).

Paso 3: Según tu conexión:

- Si estás en Wi-Fi, esos bits viajan como ondas de radio hasta tu router.
- Si estás en red móvil (4G/5G), viajan como ondas hasta la antena celular más cercana

Paso 4:

Luego, tu router o antena los manda por cables de fibra óptica hacia la red de tu proveedor de Internet.

Paso 5:

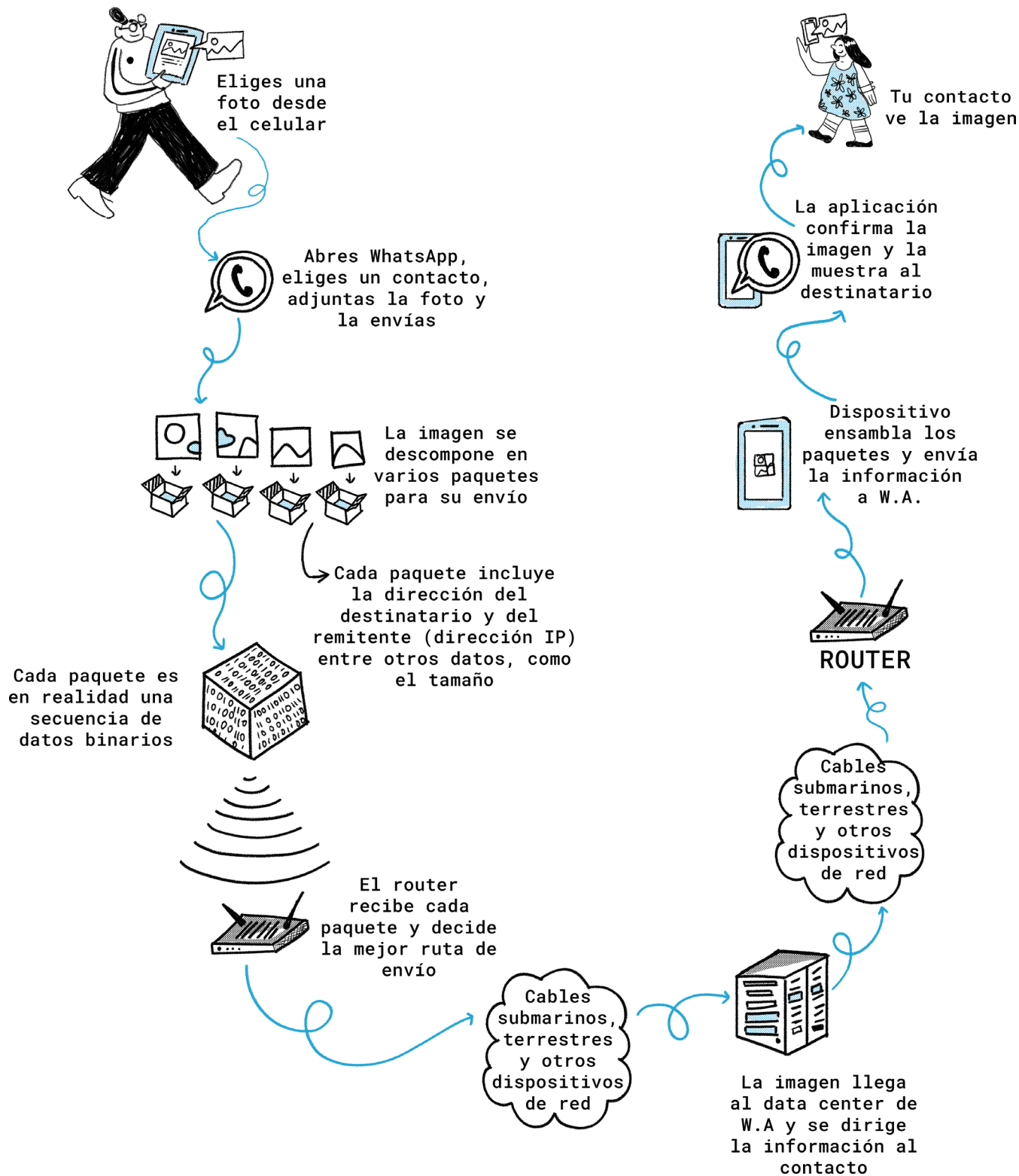
Esa señal llega a los servidores de WhatsApp (en la nube). Allí pasa algo clave:

- El mensaje se cifra para protegerlo.
- El sistema identifica quién es el destinatario y prepara el camino de vuelta.

Paso 6:

Finalmente, el mensaje hace el recorrido inverso hasta llegar al celular de tu amiga o amigo.

Imagínatelo como enviar una carta muy rápida. El sobre (cifrado) garantiza que nadie la lea en el camino, el cartero (servidor) decide a dónde debe ir, y la carta pasa por varias calles y oficinas de correo (routers, antenas, proveedores) hasta llegar a la casa correcta.



Cifrado y privacidad: También, si eres una persona usuaria de WhatsApp habrás notado que en la parte superior de los chats aparece el texto cifrado de extremo a extremo. Esto es muy importante, ya que significa que el mensaje se “cubre”/ “oculta” en tu celular y solo el otro celular puede leerlo. Ni siquiera WhatsApp puede hacerlo.

Si enviamos un mensaje en una caja cerrada, solo tú y la otra persona tendrían la llave para abrirla. Esto tiene sentido por varias razones, entre ellas porque en internet también tenemos derecho a la intimidad. La información que compartimos, enviamos y recibimos debe quedarse entre las personas que nosotras decidamos.

REFERENCIAS

- Cómo funciona internet: los cables submarinos que conectan al mundo
- How Does the Internet Work?
- Internet shutdowns: What happens when the internet shuts down? | World Economic Forum
- EL MISTERIO DETRÁS DE LOS CORTES DE INTERNET EN CALI DURANTE EL PARO DE 2021 : Fundación Karisma

UNIDAD 2: MANIPULACIONES DE INTERNET Y DNS

Como ya lo explicamos en la unidad anterior, Internet opera a través de un vasto sistema de protocolos interconectados y estructuras de gobernanza. En esta unidad abordaremos el fenómeno de las manipulaciones de Internet, entendidas como los bloqueos, caídas y cortes de Internet.

Además, aprovecharemos el conocimiento que ya obtuvimos sobre DNS y veremos cómo se puede usar para evadir cierto tipo de cortes de Internet, mientras sumamos privacidad y seguridad a nuestro uso de Internet.

Comprender cómo funciona el filtrado, el bloqueo y los DNS alternativos es esencial para quienes participan en la gobernanza de Internet, especialmente para las organizaciones sociales que trabajan por los derechos humanos, la libertad digital y el acceso equitativo a la información.

Objetivo general

Introducir los conocimientos clave en torno a las dinámicas de control, fallas y manipulación de Internet, mostrando cómo ocurren los bloqueos, las estrategias y técnicas empleadas, y las medidas básicas para evadir o sortear los bloqueos (como el uso de DNS alternativos).

Objetivos específicos

1. Identificar las diferencias entre fallas, cortes y bloqueos de Internet, y reconocer las estrategias y técnicas más comunes de restricción a un nivel conceptual.
2. Examinar, mediante el caso de China y WhatsApp, cómo se aplican estas técnicas en la práctica y qué efectos tienen sobre la comunicación y los derechos digitales.
3. Guiar en pasos sencillos para configurar DNS alternativos y entender sus beneficios y limitaciones como medida introductoria de evasión de censura.

CONTROL, FALLAS Y CAÍDAS DE INTERNET

Recuerda que las redes pueden entregar paquetes siempre que estos tengan cabeceras correctas, independientemente de su contenido, siempre que los paquetes sean enrutables; es decir, que tengan claro su remitente y su destino. A esto lo llamamos neutralidad de la red. Sin embargo, a veces los Estados, las instituciones u otras autoridades quieren impedir que las personas accedan a determinados contenidos en Internet. Estas medidas pueden tener graves consecuencias para los derechos humanos y las libertades civiles.

A nivel nacional, los ISP podrían ser obligados a implementar medidas que incluyan bloqueos y filtros en todo el tráfico que entre y salga del país. En lo que respecta al control regional de contenido, múltiples nodos de la red pueden colaborar en lugar de depender de sistemas centralizados. Además, entidades como bibliotecas, universidades, lugares de trabajo y cibercafés tienen la capacidad de establecer sus propios controles de bloqueo y filtrado de contenidos, adaptándose a sus necesidades específicas.

¿CÓMO FUNCIONAN LOS CORTES DE INTERNET Y QUÉ IMPLICAN?

Existen al menos tres estrategias:

Bloqueo

Hace que un sitio web o servicio sea inaccesible para un conjunto específico de usuarios, a menudo se pone en marcha con la cooperación de los ISP locales. El bloqueo es una forma más directa de impedir el acceso a contenidos, servicios o plataformas en línea. A diferencia del filtrado, que puede ser selectivo o parcial, el bloqueo suele ser total e impedir el acceso completo a un sitio web o servicio, con el objetivo de evitar que las personas usuarias lleguen a determinados sitios o aplicaciones. El bloqueo puede:

- Limitar el derecho a la información y la libertad de expresión.
- Ser aplicado de forma arbitraria, sin transparencia ni justificación clara.
- Dificultar el acceso a servicios digitales esenciales², como servicios públicos, servicios de salud, canales de comunicación y expresión en línea (por ejemplo, redes sociales y aplicaciones de mensajería instantánea segura) o servicios de almacenamiento en la nube.
- Generar efectos colaterales: al bloquear un servidor completo, pueden verse afectados otros sitios no relacionados.

² Entendemos como servicios digitales esenciales a aquellos servicios y recursos cuya disponibilidad es crítica para la vida cotidiana, la seguridad pública, el funcionamiento económico y el ejercicio de derechos fundamentales.

Filtrado

Es un enfoque más general que trata de impedir el acceso a contenido basándose en características definidas, como el uso de determinadas palabras o el contenido de imágenes. El filtrado puede tener consecuencias directas sobre los derechos digitales:

- Puede afectar la libertad de expresión y el acceso a la información.
- Puede ser arbitrario o desproporcionado si no se hace con criterios claros y mecanismos de rendición de cuentas.
- En contextos autoritarios, es una forma de censura que silencia voces críticas o invisibiliza temas sociales y políticos.

Estrangulamiento (o degradación)

Se utiliza para hacer que el acceso a algunos servicios o sitios web sea muy difícil, lento o prácticamente imposible para algunas personas.

Técnicas

Bloqueo de IP

Son bloqueos de la dirección IP de origen y destino. Se puede usar para bloquear rangos de direcciones IP.

Filtrado de contenido

Quién administra o tiene control de un router es capaz de ver el tráfico que pasa a través de este. Se pueden leer los encabezados con información de los sitios web que estamos visitando. Si una conexión no está cifrada, podrá ver el contenido mismo. Esto permite filtrar, por ejemplo, sitios web que contienen determinadas palabras.

Filtrado de URL

Esta forma de filtrado escanea las URL en búsqueda de palabras determinadas para bloquear el acceso.

Bloqueo DNS

El bloqueo DNS es un método que impide el funcionamiento normal del sistema DNS, lo cual dificulta la resolución de ciertos nombres de dominio. Los ISP aplican estos bloqueos en los resolvers DNS bajo su control, generalmente predeterminados al suscribirse a su servicio de Internet. Si se implementa un bloqueo DNS, al intentar acceder a un sitio web, el resolver DNS del ISP puede simular que no encuentra el servidor correspondiente o proporciona una dirección IP diferente, como mensajes de advertencia. Este tipo de bloqueo afecta a todos los protocolos que dependen del sistema DNS, incluyendo HTTP(S), FTP, POP y SSH.

Filtrados de paquetes

Los routers implementan en la lectura de los paquetes algunos filtros con el fin de buscar incumplimientos de protocolos, virus, spam o intrusiones, bloqueando dichos paquetes como consecuencia. Estos filtros también pueden proteger las redes de ataques cibernéticos.

Inspección profunda de paquetes (DPI: *Deep Packet Inspection*)

Similar al filtrado de paquetes, en lugar de limitarse a mirar las cabeceras de los paquetes, también lee los datos que contienen. La DPI es un software de procesamiento de datos que puede ser útil para ver el interior de los paquetes con el fin de identificar, supervisar y solucionar anomalías en la red, pero los enrutadores y servidores también pueden utilizarla para la extracción de datos, la escucha clandestina y la censura en Internet. Esta tecnología puede redirigir, etiquetar, bloquear, limitar la velocidad e informar, o puede descartar silenciosamente los paquetes que marque como sospechosos.

Apagones de Internet

Los Estados pueden cerrar fácilmente una red entera manipulando el protocolo que traza el mapa de Internet (BGP: Border Gateway Protocol). Además, pueden producirse cortes por la desconexión o daño físico a la Infraestructura de Internet.

Contenido y remoción de resultados de búsqueda

Las técnicas de censura pueden aplicarse en la fuente del contenido, no sólo a través de la red. Los editores, autores y proveedores de servicios tienen que cumplir las peticiones legítimas o las leyes aplicables para retirar, anular la publicación, suprimir de la lista u ocultar contenidos cuando así lo exijan la ley o las peticiones gubernamentales.

Bloqueo por puerto o protocolo

Interrumpe ciertos servicios (como WhatsApp o Tor) al impedir la comunicación en los canales que usan.

Caso: restricciones a WhatsApp en distintos países.

Los gobiernos o proveedores de internet (ISPs) no necesitan “hackear” WhatsApp. Lo que sí pueden hacer es bloquear el acceso a nivel de red. Esto impide que funcione WhatsApp en tu celular o computador. Esto puede pasar durante protestas sociales, elecciones o crisis políticas para evitar que las personas se comuniquen o compartan información.

Método	¿Qué hacen?	¿Qué notas tú?
Bloqueo de IPs	Bloquean los servidores de WhatsApp.	No se envían ni llegan mensajes.
Manipulación de DNS	Cambian o bloquean el nombre “whatsapp.com”.	Aparece “servidor no encontrado”.
Throttling (limitación del ancho de banda)	Baja la velocidad solo para WhatsApp.	El texto llega lento. Audios, videos o llamadas no funcionan.
Bloqueo de protocolos	Filtran y bloquean llamadas y mensajes cifrados.	No puedes hacer llamadas.
Bloqueo de versión web	Cortan el acceso a WhatsApp desde navegadores.	Funciona en el celular, pero no en el computador.

EL CASO DE WHATSAPP EN CHINA: CENSURA Y CONTROL

China mantiene uno de los sistemas de censura de internet más estrictos del mundo, conocido como el “Gran Cortafuegos”. Plataformas extranjeras como Facebook, Twitter, Google y WhatsApp están bloqueadas porque el gobierno no puede controlarlas fácilmente ni acceder a los datos que circulan por ellas.

¿Por qué está bloqueado WhatsApp?

Cifrado de extremo a extremo: WhatsApp cifra los mensajes de extremo a extremo, lo que impide que el gobierno chino pueda interceptar o monitorear las conversaciones, a diferencia de aplicaciones como WeChat.

Control de la información: El gobierno chino promueve el uso de plataformas nacionales que cooperan con las autoridades y permiten el monitoreo y la censura, como WeChat (propiedad de Tencent).

Sensibilidad política: Aplicaciones como WhatsApp han sido usadas para organizar protestas o difundir información crítica al régimen, lo cual es considerado una amenaza por las autoridades chinas.



Cronología:

- En 2017, el acceso a WhatsApp comenzó a ser restringido: primero las videollamadas y el envío de archivos.
- A finales de 2017, WhatsApp fue bloqueado completamente en China.
- Actualmente, solo se puede acceder a WhatsApp en China usando VPNs, que también están cada vez más restringidas por el gobierno.

Implicaciones:

- Este caso muestra la tensión entre la comunicación digital cifrada y el control autoritario de la información.
- También evidencia cómo las políticas nacionales pueden redefinir el acceso a tecnologías globales, afectando la libertad de expresión y la privacidad.

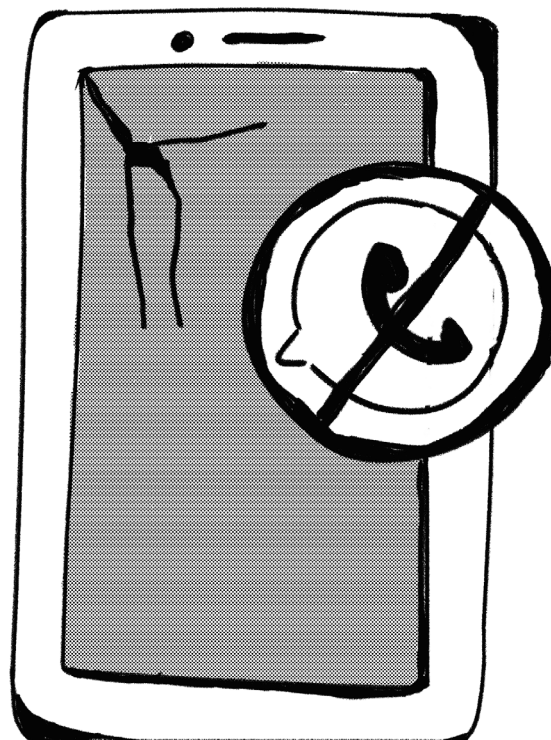
Además de prácticas técnicas de censura y control, el bloqueo de WhatsApp en China se inscribe en dinámicas geopolíticas y de soberanía tecnológica. Los Estados —no solo China— toman decisiones sobre qué plataformas permitir o restringir con base en consideraciones de seguridad nacional, autonomía tecnológica, protección de datos y control del flujo de información. En ese marco, promover plataformas locales (como WeChat) forma parte de una estrategia más amplia para reducir dependencia de proveedores extranjeros, fortalecer industrias nacionales y ejercer capacidad de regulación sobre datos y contenidos.

No obstante, desde la perspectiva de derechos humanos la clave es la responsabilidad del Estado en garantizar que las medidas que afecten el acceso a la información y la libre expresión sean necesarias, proporcionadas y sometidas a normas y vías de reparación. El bloqueo de WhatsApp ilustra cómo políticas orientadas a la soberanía tecnológica pueden traducirse en restricciones concretas a la comunicación privada y pública: el cifrado de extremo a extremo protege la privacidad y la libertad de expresión de las personas usuarias, pero también dificulta la vigilancia exigida por el Estado; la respuesta estatal —bloquear la aplicación o limitar funciones— restringe derechos sin procesos transparentes ni recursos efectivos para las personas afectadas.

El caso muestra tres tensiones centrales:

- **Soberanía tecnológica vs. derechos individuales y colectivos**
La búsqueda de autonomía y control puede entrar en conflicto con la protección de privacidad, la libertad de expresión y otros derechos humanos conexos.
- **Seguridad nacional y orden público vs. proporcionalidad y transparencia**
Las medidas de bloqueo suelen justificarse en seguridad, pero con frecuencia carecen de controles independientes y evaluación de impactos.
- **Dependencia tecnológica global vs. gobernanza local**
La infraestructura y servicios globales no operan en un vacío político; las decisiones regulatorias nacionales reconfiguran el acceso a tecnologías y mercados.

Enfocar la discusión desde los derechos humanos permite evaluar las medidas más allá del juicio geopolítico: se trata de preguntar si las restricciones son legales, necesarias, proporcionadas y sujetas a supervisión independiente; si existen canales para la reparación; y cómo afectan a grupos vulnerables. Mantener ese enfoque evita simplificaciones que asocien automáticamente modelos tecnológicos con valores culturales o civiles, y pone el centro en la protección de libertades fundamentales y la responsabilidad estatal en cualquier contexto político.



SERVICIOS ALTERNATIVOS DNS

Uno de los principios clave de la gobernanza de Internet es que la red debe ser abierta, interoperable y accesible para todas las personas. Los bloqueos suelen realizarse a través de DNS. Ante esta situación, han surgido servicios alternativos de DNS como una herramienta técnica que permite a las personas usuarias y organizaciones sortear bloqueos injustificados, mejorar su privacidad y garantizar una experiencia de navegación más libre.

Los servicios DNS alternativos permiten reemplazar el servidor DNS que te da por defecto tu proveedor de Internet por otro que sea más rápido, más privado o menos propenso a aplicar bloqueos. Cuando el DNS de tu proveedor filtra o bloquea contenido, puedes cambiar a un servicio DNS alternativo para tener acceso más libre y seguro.

Ejemplos de DNS alternativos

1.1.1.1 – Cloudflare (rápido y con enfoque en privacidad).

8.8.8.8 y 8.8.4.4 – Google Public DNS.

9.9.9.9 – Quad9 (con protección contra malware).

Nuestra recomendación:

- [Quad9](#) (excepcional para el filtrado de malware)
- [Mullvad DNS](#) (útil para maximizar la privacidad)
- [NextDNS](#) (para quienes quieren tener mucho más control de su información, filtros y seguridad)

Ten en cuenta que si bien es una herramienta útil, no protege contra bloqueos más sofisticados, como los que se hacen por IP o inspección profunda de paquetes.

También, en algunos países, cambiar el DNS podría ser monitoreado o restringido, aunque en la mayoría de contextos es legal.

DNS over HTTPS

DNS over HTTPS (DoH) es una tecnología que cifra las solicitudes DNS que hace tu navegador o dispositivo, y las envía a través del protocolo HTTPS, el mismo que se usa para conexiones seguras a sitios web. Esto significa que nadie entre tú y el servidor DNS puede ver qué sitios estás buscando. Normalmente, cuando visitas un sitio web, tu dispositivo le pregunta a un servidor DNS “¿Dónde está [www.organizacion.org?](#)”. Esa solicitud, en la mayoría de los casos, no está cifrada. Cualquier persona que intercepte tu tráfico (proveedor de Internet, red pública, incluso gobiernos) puede ver qué sitios estás tratando de visitar - incluso si después el contenido de la página está protegido por HTTPS.

ACTIVIDAD PRÁCTICA:

en el celular cambia el DNS a Quad9

Objetivo: Aprender a cambiar los servidores DNS predeterminados para mejorar la privacidad, velocidad de navegación y sortear bloqueos.

- ¿Qué beneficios trae cambiar el DNS en tu dispositivo?
- Privacidad: cifra las consultas DNS entre tu dispositivo y el resolutor, evitando que terceros en la red (por ejemplo, el proveedor de Internet, redes públicas Wi-Fi o atacantes en la misma red) vean qué dominios consultas.
- Integridad y seguridad: al usar DoT (DNS over TLS) se reduce el riesgo de manipulación por actores intermedios de las respuestas DNS.
- Protección en redes abiertas: en Wi-Fi públicas o redes no confiables, evita que un atacante intercepte o reescriba las respuestas DNS.
- Compatibilidad con posturas de seguridad y privacidad: permite implementar un servicio de DNS que filtra sitios maliciosos así como rastreadores invasivos con la privacidad.
- Evita filtrado pasivo y la censura por DNS: dificulta que operadores realicen análisis pasivo del tráfico DNS para perfiles o segmentación de usuarios y bloqueo de servicios en Internet.

¿Qué efectos negativos podría llegar a tener cambiar el DNS?

Dependiendo de la calidad, estabilidad y distancia geográfica del servidor DNS que configures, podrías experimentar latencia, algo que en términos prácticos significa que algunos sitios web tarden en cargar un poco más, desde lo imperceptible hasta lo significativo. Sin embargo, también es posible que incluso experimentes lo contrario: sitios web que cargan mucho más rápido que con el DNS predeterminado. No te preocupes, siempre puedes experimentar con el servidor que mejor funcione en tu situación, te recomendamos que pruebes con Quad9, Mullvad DNS, NextDNS y Cloudflare DNS (este último es la opción usualmente más rápida disponible, pero con menos enfoque en la privacidad).

¿Qué necesitas?

Un celular con acceso a Internet Android o iOS.

Datos de configuración para Quad9

Cuando configures tu DNS tendrás que poner algunos de los siguientes datos. Según el dispositivo, podrías necesitar poner la dirección IPv4, la dirección HTTPS o la dirección TLS (esta es la necesaria en los casos de Android). Esta es la forma en que tu dispositivo sabrá a quién le está haciendo la consulta DNS y utilizando qué protocolo.

IPv4

9.9.9.9

149.112.112.112

HTTPS (DoH)

<https://dns.quad9.net/dns-query>

TLS (DoT)

dns.quad9.net

Sigue las instrucciones oficiales:

[Guía para configurar el DNS en Android](#)

[Guía para configurar el DNS en iOS](#)

Para verificar que quedó configurado exitosamente, visita

<https://on.quad9.net/>

¿QUIERES APRENDER A DOCUMENTAR Y ANALIZAR CASOS DE DISRUPCIONES DE INTERNET?

Te presentamos el Observatorio de Bloqueos de Internet OBI

Creemos en un Internet libre de censura y bloqueos arbitrarios. Por eso, OBI pone a disposición herramientas, guías y pasos simples para que te unas a esta causa. A continuación, te explicamos cómo usarlo paso a paso. El Observatorio de Bloqueos de Internet (OBI) es una iniciativa de Karisma para que cualquier persona pueda identificar, documentar y denunciar bloqueos en la red. Creemos en un Internet libre de censura y bloqueos arbitrarios. Por eso, OBI pone a disposición herramientas, guías y pasos simples para que te unas a esta causa. A continuación, te explicamos cómo usarlo de forma general.

1. Ingresa al sitio oficial

Ve a <https://obi.karisma.org.co/guia/>.

Allí encontrarás información clave, tutoriales y enlaces que pueden ser útiles.

2. Descarga la guía “¿Está bloqueado?”

Haz clic en el botón o enlace que dice “Descargar guía” o “¿Está bloqueado?” Esta guía gratuita está pensada para cualquier persona, sin necesidad de ser experta.

- **Te enseña cómo:**

Detectar un posible bloqueo

Confirmar si es un error o un bloqueo real

Documentar lo que encontraste

Reportarlo para que otras personas lo sepan

3. Usa herramientas recomendadas por OBI

Dentro de la guía y el sitio encontrarás herramientas como:

OONI Probe: app gratuita que puedes instalar en tu celular o PC. Y realiza pruebas automáticas para detectar si una página web está siendo bloqueada desde tu red.

VPN: para saltar restricciones geográficas o de red.

En las guías del sitio web OBI, encontrarás cómo usarlas paso a paso.

4. Documenta el bloqueo

Cuando detectes un bloqueo:

Anota qué sitio o servicio está afectado

Desde qué red (Wi-Fi, datos móviles)

Fecha y hora

Qué mensaje de error aparece (si lo hay)

También puedes hacer una captura de pantalla

5. Reporta el caso

Puedes enviar tu reporte a OBI de manera confidencial.

En el sitio web hay formularios o correos de contacto. Así, tu experiencia se suma a una base de datos colectiva que ayuda a:

Visibilizar patrones de censura

Promover la transparencia

Defender un Internet libre para todas las personas

CONCLUSIONES

A lo largo de este módulo, exploramos las capas fundamentales que permiten que Internet funcione: desde cómo los nombres de dominio se traducen en direcciones IP mediante el sistema DNS, hasta cómo este sistema puede ser manipulado para bloquear, filtrar o restringir el acceso a ciertos contenidos.

Aprendimos que tecnologías como HTTPS y DNS sobre HTTPS (DoH) no solo hacen más segura la navegación, sino que también se han convertido en herramientas de resistencia ante la censura, la vigilancia y los bloqueos injustificados. También vimos que cambiar el servidor DNS es una acción sencilla pero poderosa que puede mejorar la privacidad y el acceso a la información.

Ahora que ya entendemos cómo funciona Internet en sus capas técnicas y cómo circula la información, podemos preguntarnos: ¿quién decide las reglas de ese funcionamiento?, ¿quién controla lo que pasa en esta gran red? Esto lo veremos en nuestro siguiente módulo sobre Gobernanza de Internet.

REFERENCIAS

- Asociación para el Progreso de las Comunicaciones. (n.d.). The (Internet) shutdown game. Recuperado en Septiembre 3 de 2025 de <https://shutdowngame.apc.org/>
- Cute, B. (2019, December 23). Evolución del modelo de múltiples partes interesadas de la ICANN: plan de trabajo y próximos pasos. ICANN. <https://www.icann.org/es/blogs/details/evolving-icanns-multistakeholder-model-the-work-plan-and-way-forward-23-12-2019-es>
- Fundación Karisma. (2024). Cómo funciona Internet. Fundación Karisma. https://web.karisma.org.co/wp-content/uploads/2024/01/Como_funciona_internet.pdf
- Fundación Karisma & K+Lab. (n.d.-a). Guía para investigar bloqueos de Internet. Observatorio de Bloqueos de Internet. Recuperado en Septiembre 3 de 2025 de <https://obi.karisma.org.co/guia/>
- Fundación Karisma & K+Lab. (n.d.-b). Observatorio de Bloqueos de Internet. OBI. Recuperado en Septiembre 3 de 2025 de <https://obi.karisma.org.co/>
- Fundación Karisma & K+Lab. (2021, May 14). Bloqueo de archive.org y ghostbin.co en Colombia durante Paro Nacional. Observatorio de Bloqueos de Internet. <https://obi.karisma.org.co/2021-05-14-colombia-bloqueo-de-archive.org-ghostbin.co-paro-nacional/>
- ICANN. (2012). ¿Qué hace ICANN? <https://www.icann.org/resources/pages/what-2012-02-25-es>
- ICANN. (2024, September). The Multistakeholder Model of Internet Governance. <https://itp.cdn.icann.org/en/files/government-engagement/ge/multistakeholder-model-internet-governance-fact-sheet-05-09-2024-en.pdf>
- International Centre on Censorship - Article 19 (with Uhlig, U., Knodel, M., Ten Oever, N., & Cath, C.). (2021). How the Internet really works: An illustrated guide to protocols, privacy, censorship, and governance. No Starch Press.
- Paz Peña, O. (2013). ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/Como_funciona_internet-ebook.pdf
- RIPE NCC. (n.d.). What is IANA? RIPE Network Coordination Center. Recuperado en Septiembre 3 de 2025 de <https://www.ripe.net/community/internet-governance/internet-technical-community/iana/iana-stewardship-transition/3-what-is-iana/>

MATERIAL ADICIONAL DE CONSULTA

1. Infraestructura y Funcionamiento de Internet

- [A Brief History of the Internet](#) - Internet Society.
- [“How the Internet Works”](#) – Cloudflare Learning.
- [“Internet basics”](#) - CGF Global.
- [Who Makes the Internet Work](#): The Internet Ecosystem
- [¿Cómo funciona internet?](#) - Mozilla

2. Gobernanza de Internet y DNS

- ICANN Learn Platform: Cursos gratuitos sobre gobernanza y políticas de Internet [ICANN for Beginners](#)
- ¿Qué es el Internet de las cosas (IoT)? - [¿Qué es el Internet de las cosas \(IoT\)? | IBM](#)

3. Políticas de Acceso y Brechas Digitales

- ITU Report on Internet Accessibility in Developing Countries [Facts and Figures 2024](#)
- “Community Networks: The Internet by the People, for the People” – Internet Society [Dynamic Coalition on Community Connectivity](#)
- Regulación del Espectro en América Latina – LACNIC
- [Investigación clave sobre uso del Espectro IMT en Colombia](#)

¿EL INTERNET TIENE REGLAS?

Hablemos de Gobernanza de Internet

¿Qué está en juego para la sociedad civil?



CONTENIDO

☀ Introducción	54
☀ Objetivos del módulo	55
☀ Unidad 1	56
● Tema 1: Introducción a la gobernanza de Internet.....	56
● ¿Qué entendemos por sociedad civil?	56
● Definiciones clave: ¿qué es la gobernanza de Internet?	57
● Gobernanza multilateral vs “multistakeholder” (o de múltiples partes interesadas)	61
○ ¿Por qué un modelo de múltiples partes interesadas y no otro?.....	61
● Principios fundamentales de la gobernanza de Internet	61
● Tema 2: Actores y espacios de toma de decisión	65
● Mapeo de actores clave en la gobernanza de Internet.....	65
● Interacciones, tensiones y asimetría de poder.....	66
● Mapeo de espacios clave en la gobernanza de Internet	66
● Espacios nacionales y locales.....	69
○ El contexto en Latinoamérica	69
● Tema 3: Gobernanza de Internet y derechos humanos.....	71
● Gobernanza de Internet y derechos humanos - un vínculo clave	71
○ Ejemplo 1: Moderación de contenidos y censura.....	72
○ Ejemplo 2: Vigilancia estatal y privada.....	73
○ Ejemplo 3: Discriminación y exclusión en entornos digitales	73
● Tema 4: Participación de la sociedad civil.....	75
● ¿Puede la sociedad civil participar en la gobernanza de Internet?.....	75
● ¿Cuáles son las barreras de acceso?.....	75
● ¿Por qué es importante que las organizaciones de sociedad civil participen en el modelo de múltiples partes interesadas de gobernanza de Internet?	77
● Estrategias de participación desde sociedad civil	78
○ Ejemplos de incidencia exitosa.....	80

☀ Unidad 2	81
● Tema 5: Tendencias y debates actuales	81
• Fragmentación de Internet	81
• Regulación de inteligencia artificial y algoritmos	82
• Ciberseguridad	82
• Plataformas y economía digital	82
● Tema 6: Acceso y conectividad	86
• Digitalización, desarrollo sostenible e inclusión	86
• Brechas digitales: ¿quién accede y quién no?	86
• Conectividad básica vs. acceso significativo	87
• Redes comunitarias y modelos alternativos de conectividad	87
• Gobernanza en las redes comunitarias	87
○ Juventudes y acceso: entre la oportunidad y la exclusión	89
• Medios alternativos de participación	91
○ Mastodon	91
● Tema 7: Gobernanza de Internet y justicia medioambiental	93
• Cambio climático y tecnologías digitales	93
• Extractivismo digital y extracción de datos	94
• Pueblos originarios: participación e incidencia en la gobernanza	94
● Tema 8: Gobernanza de plataformas digitales e igualdad de género	96
• ¿Qué es la gobernanza de plataformas digitales?	96
• Violencia de género digital: una expresión estructural	96
○ Tipos de violencia digital	96
• Feminismo y tecnología: Hacia una Internet feminista	97
☀ Conclusiones	100

INTRODUCCIÓN

Internet es fundamental para la transformación de la vida de las personas y las sociedades a través de la digitalización, entendida no solo como la adopción de tecnologías, sino también como la creación de nuevas formas de interacción social, acceso al conocimiento, innovación en los modelos productivos y ampliación de oportunidades para la participación ciudadana. Sin embargo, para que esta transformación sea inclusiva y democrática es necesario comprender no sólo cómo funciona la web, sino también los diferentes mecanismos que determinan el acceso, el uso y el desarrollo de Internet en nuestra región.

Este módulo ofrece una **visión general de lo que está en juego para la sociedad civil**, en particular, para juventudes, personas que viven en contextos rurales y comunidades con poca representación, en relación con la gobernanza de Internet. **Analizaremos cómo las decisiones técnicas y de políticas sobre Internet impactan los derechos humanos, la participación democrática y el desarrollo sostenible.**



OBJETIVOS DEL MÓDULO

Objetivo general:

Contribuir a la construcción de conocimiento sobre la gobernanza de Internet, promoviendo la participación activa y el pensamiento crítico en torno a su uso, regulación e infraestructura.

Objetivos específicos:

- Fortalecer el conocimiento entre jóvenes y comunidades rurales sobre el funcionamiento de Internet y los mecanismos de gobernanza que lo configuran.
- Ofrecer una visión general sobre los temas, espacios y procesos más relevantes del ecosistema de gobernanza de Internet.
- Abordar la gobernanza desde una perspectiva crítica que visibilice las dinámicas de poder y los intereses de distintos actores.
- Resaltar oportunidades concretas de participación para la sociedad civil en la toma de decisiones a nivel nacional, regional y global.

UNIDAD I:

TEMA I: INTRODUCCIÓN A LA GOBERNANZA DE INTERNET

Para comprender cómo y por qué Internet impacta nuestras vidas es fundamental entender quiénes toman las decisiones sobre su funcionamiento y desarrollo. Este primer tema ofrece una introducción a la gobernanza de Internet: qué significa, cómo surge, cómo se organiza y por qué importa especialmente para la sociedad civil en América Latina.

¿QUÉ ENTENDEMOS POR SOCIEDAD CIVIL?

Podemos entender sociedad civil como el conjunto de organizaciones, colectivos y espacios autónomos de la vida pública —no estatales ni empresariales— que actúan de manera organizada o informal para representar intereses ciudadanos, vigilar al poder, promover valores y proteger derechos. Incluye, entre otros:

- Organizaciones no gubernamentales (ONG) y asociaciones civiles dedicadas a derechos humanos.
- Movimientos sociales y colectivos comunitarios (p. ej., feministas, pueblos indígenas, LGBTIQ+, ambientalistas).
- Sindicatos, cooperativas y agrupaciones profesionales cuando defienden derechos públicos.
- Medios comunitarios, redes ciudadanas y plataformas de incidencia.
- Personas activistas, víctimas organizadas y defensoras/es de derechos humanos que actúan individual o colectivamente.



DEFINICIONES CLAVE: ¿QUÉ ES LA GOBERNANZA DE INTERNET?

¿Una definición ampliamente aceptada de la gobernanza de Internet se adoptó en la Cumbre Mundial sobre la Sociedad de la Información (Túnez, 2005) y es actualmente utilizada por el Foro de Gobernanza de Internet:

La gobernanza de Internet es el desarrollo y la aplicación por parte de gobiernos, sector privado y sociedad civil, en sus respectivos roles, de principios, normas, reglas, procedimientos de toma de decisiones y programas que dan forma a la evolución y uso de Internet.

Dicho de manera más simple: **la gobernanza de Internet se refiere a cómo se toman las decisiones que afectan el funcionamiento, desarrollo y uso de Internet.** Esto incluye:

- **Estándares**

Los estándares son globales, esto permite que puedan comunicarse, es decir, transferir datos entre dispositivos que estén en lugares geográficos distintos y hechos o fabricados por diversas empresas. Por ejemplo, cómo se conectan las redes de Internet o cómo se asignan las direcciones IP.

- **Políticas**

Las políticas constituyen las reglas que influyen en lo que vemos, compartimos o incluso en si podemos acceder o no a ciertos servicios. Estas pueden ser globales: acuerdos internacionales y/o multilaterales empresariales.

También pueden ser políticas locales que están creadas por gobiernos nacionales o reguladores regionales que buscan establecer normas propias para su territorio. Esto significa que conviven diferentes jurisdicciones y modelos de regulación: mientras una red social puede aplicar reglas iguales para todo el mundo, un país puede decidir imponer requisitos adicionales que afectan a las personas usuarias de esa región. Por ejemplo:

- Leyes de protección de datos, marcos de referencia o políticas para evitar la censura en línea.
- Los términos y condiciones que debes aceptar para crear una cuenta en alguna plataforma.
-
-

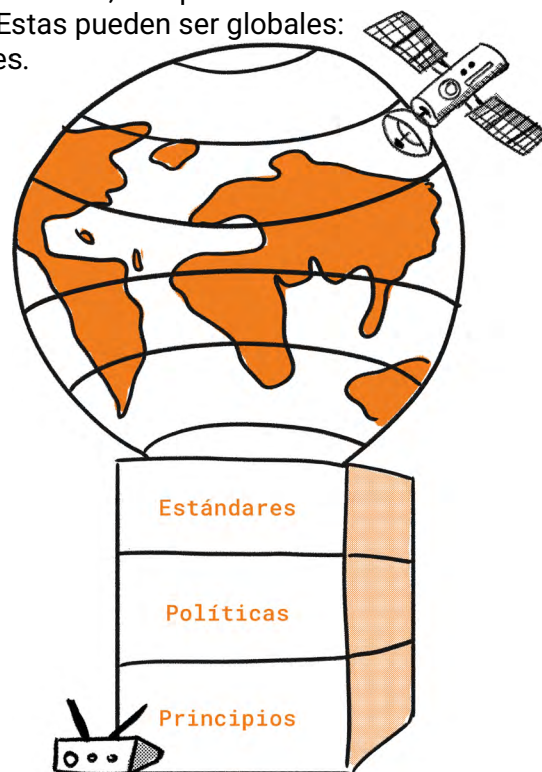


Figura 1. Gobernanza de Internet

- **Principios**

Son aquellas metas amplias que se busca sean transversales al uso y experiencia de Internet:

- Libertad, privacidad y derechos humanos
- Gobernanza democrática y colaborativa
- Universalidad
- Diversidad
- Innovación
- Neutralidad de la red
- Inimputabilidad de la red
- Funcionalidad, seguridad y estabilidad
- Estandarización e interoperabilidad
- Ambiente legal y reglamentario

Es importante tener en cuenta que la gobernanza de Internet no ocurre en un solo lugar, sino que es un proceso distribuido y descentralizado, que cambia y evoluciona todo el tiempo con la participación de muchos actores.

¿Recuerdan el modelo de capas que vimos en el primer módulo para explicar cómo funciona Internet? Allí nos enfocamos en los aspectos técnicos: desde los cables y señales físicas, pasando por los protocolos, hasta llegar a las aplicaciones y contenidos que usamos todos los días.

En este segundo módulo retomaremos esa idea de las capas, pero ahora la veremos desde otro ángulo: la gobernanza. Es decir, cómo diferentes actores Estados, empresas, organizaciones y ciudadanía influyen y toman decisiones sobre Internet. Aquí incluso añadimos una capa más, la capa social, porque Internet no es solo tecnología: es también un espacio humano, político y cultural, atravesado por derechos, disputas y formas de organización.

Se pueden identificar 4 capas en las que el entramado de la gobernanza de Internet puede proveer un entendimiento más acotado:

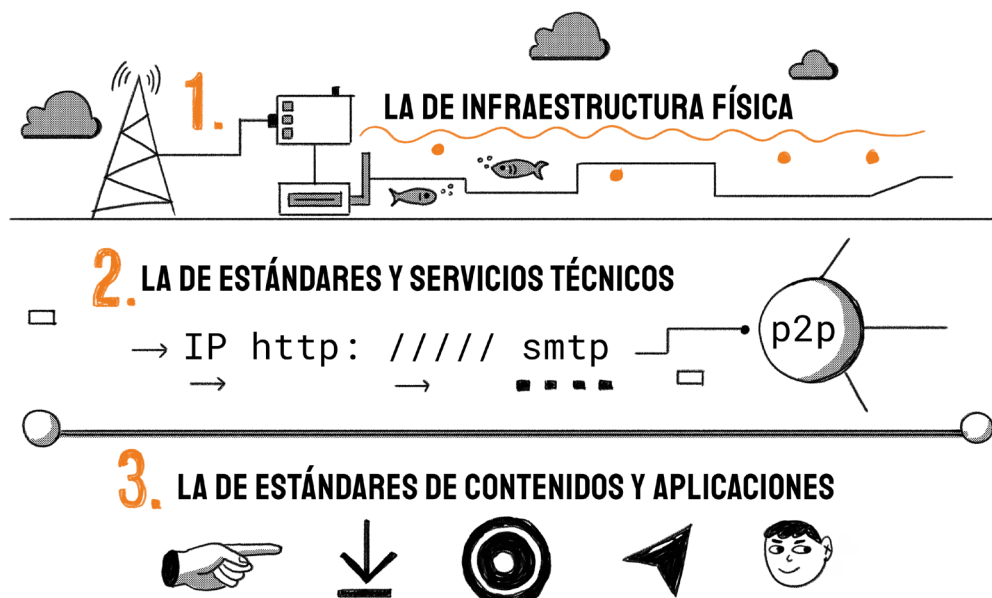


Figura 2. Capas del funcionamiento de Internet.

- **Capa social**

Internet es creada y utilizada por personas. Podemos incluir una capa social porque está integrada en la vida cotidiana de las personas de todo el mundo, incluso de aquellas que aún no están plenamente conectadas a ella. Esto incluye:

- Estados y gobiernos
- Organismos privados y empresas
- Organizaciones políticas
- Ciudadanos

- **Capa de contenido y aplicación**

Aquí está una gran parte del debate público y político de la gobernanza de Internet, incluyendo: privacidad, cifrado, libertad de expresión, derechos humanos y propiedad intelectual. Muchos de estos debates tienen lugar a través de instrumentos políticos tradicionales, como la regulación estatal o los acuerdos entre el sector público y el privado. Aquí es importante el papel del Foro de Gobernanza de Internet (IGF), del cual se hablará más adelante, puesto que sirve como foro global para que los gobiernos y sociedad civil discutan los temas que consideran más relevantes.

- **Capa lógica: estándares y servicios técnicos**

En este nivel se definen los lenguajes y protocolos facilitados por estándares y procedimientos como los que vimos en el módulo anterior (TCP/IP, estándares de redes Wi-Fi, DNS y direcciones IP). Una parte importante de esta coordinación recae en la Unión Internacional de Telecomunicaciones (UIT, por sus siglas en inglés ITU: International Telecommunication Union), organismo especializado de Naciones Unidas que establece estándares globales en telecomunicaciones.

Si bien la labor de la UIT ha sido clave para garantizar la interoperabilidad de las redes a nivel mundial, también ha sido cuestionada porque algunos Estados con regímenes autoritarios utilizan este espacio para influir en la normalización de tecnologías de nueva generación, incorporando funciones que faciliten la vigilancia, el rastreo y el control de la información. Por ejemplo, en discusiones recientes sobre estándares para redes móviles y gestión de tráfico, se han propuesto mecanismos que podrían limitar el anonimato, bloquear contenidos o reforzar la trazabilidad de los usuarios, lo que representa un riesgo para la libertad en Internet.

- **Capa de infraestructura física**

Está compuesta por satélites, cables submarinos y terrestres, sistemas inalámbricos, centros de datos, entre otros. En esta capa se encuentran organizaciones como IETF (Internet Engineering Task Force), IRTF (Internet Research Task Force) e IAB (Internet Architecture Board). Esta capa está usualmente vinculada al sector privado de telecomunicaciones. Sin embargo, quienes definen los protocolos de operación e interoperabilidad desde el desarrollo de estándares, protocolos y gobernanza entre las diferentes regiones del mundo son: ISOC (Internet Society), ICANN (Internet Corporation for Assigned Names and Numbers) e IEEE (Institute of Electrical and Electronics Engineers).

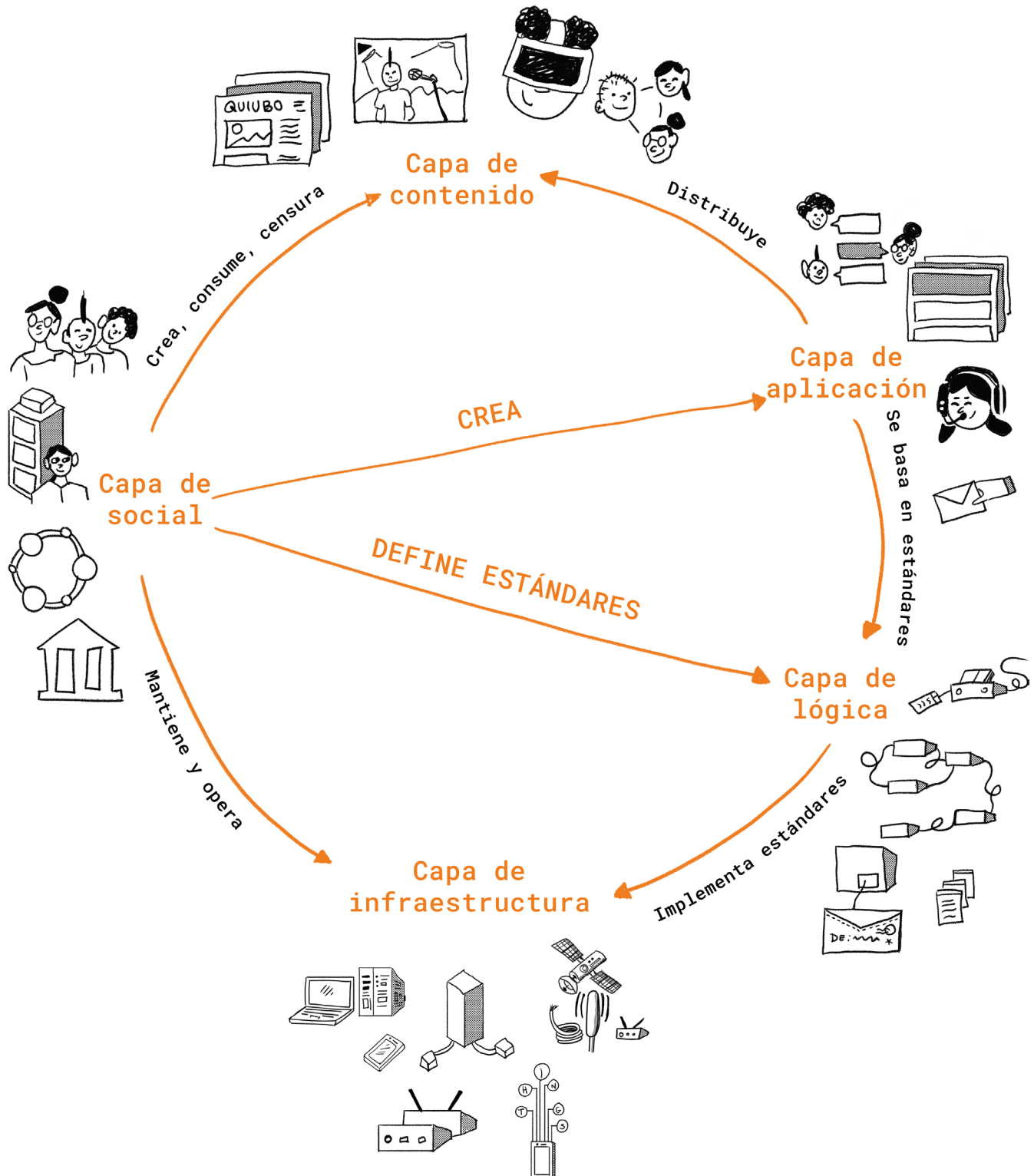


Figura 3. Capas del funcionamiento de Internet.
Adaptado y traducido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021

GOBERNANZA MULTILATERAL VS “MULTISTAKEHOLDER” (O DE MÚLTIPLES PARTES INTERESADAS)

A la hora de aplicar la gobernanza de Internet, debemos preguntarnos cómo se hace en la práctica, cómo se participa y se ejerce dicha gobernanza. En principio, existen distintos modelos de toma de decisiones sobre Internet, dos de ellos son:

- **Gobernanza multilateral**, en la que el control está en manos de Estados y organismos intergubernamentales (como la ONU o la UIT, vista anteriormente).
- **Gobernanza “multistakeholder”** (o de múltiples partes interesadas), en la que hay participación conjunta de gobiernos, empresas, comunidad técnica, academia y sociedad civil.

¿Por qué un modelo de múltiples partes interesadas y no otro?

El modelo de múltiples partes interesadas es promovido por la sociedad civil, ya que permite una participación más equitativa. Sin embargo, no está exento de tensiones: ¿tienen todas las voces el mismo peso? ¿Cómo se puede garantizar la representación de comunidades que históricamente han sido marginadas?

Por más que un proceso sea multilateral y llevado a cabo por gobiernos, y no un proceso de múltiples partes interesadas, es importante que haya participación robusta de distintos actores. Esto se debe a que en Internet (y las políticas públicas asociadas a este) no hay un solo actor que tenga todos los conocimientos ni todas las respuestas. El intercambio y la participación de distintos actores enriquece al proceso y genera políticas más robustas.

***Espacio de discusión:** ¿Qué condiciones son necesarias para una participación significativa? ¿Qué prácticas facilitan una participación efectiva en estos espacios?*

Figura 4. Discusión

PRINCIPIOS FUNDAMENTALES DE LA GOBERNANZA DE INTERNET

Aunque existen muchas formulaciones de principios de Internet y su gobernanza, hay un conjunto que, a lo largo de los años, sigue siendo común a las distintas comunidades y organizaciones que los han reflexionado. Estos principios orientan cómo debería funcionar y desarrollarse Internet para que sea un espacio equitativo, seguro y libre. En esta sección presentamos cuatro:

- **Apertura:** Internet abierta significa que cualquier persona puede usar, crear, y contribuir a Internet.

Ejemplo: Wikipedia. Cualquiera puede entrar, usarla y aportar contenido. No es un espacio cerrado, sino construido colectivamente.

- **Descentralización:** Internet no tiene un único punto de control. Su gestión se redistribuye entre distintos actores (organismos técnicos, gobiernos, empresas y sociedad civil), lo que evita concentrar el poder en una sola entidad y hace la red más resiliente y democrática. Sin embargo, esta distribución también puede generar falta de coordinación y procesos de decisión más lentos o fragmentados.

Ejemplo: El correo electrónico funciona de manera descentralizada: hay muchos proveedores (Gmail, ProtonMail, Riseup, etc.), pero todos se comunican entre sí sin depender de un único servidor central.

- **Participación:** es muy importante que múltiples actores puedan participar significativamente.

Ejemplo: En las comunidades de software libre, como la de Linux, distintas personas y organizaciones aportan ideas, discuten y contribuyen colectivamente, lo que fortalece la diversidad y la innovación

- **Neutralidad de la red:** los proveedores de Internet no deben bloquear ni priorizar contenidos según intereses comerciales o políticos.

Ejemplo: La sentencia C-206 de 2025 de la Corte Constitucional de Colombia declaró inexecutable el apartado del artículo 56 de la Ley 1450 (que habilitaba ofertas de “tarifa cero”/zero-rating), por considerar que permitir que los operadores (ISP) ofrezcan acceso gratuito y exclusivo a ciertas apps (WhatsApp, Facebook, TikTok, etc.) vulnera la neutralidad de la red y puede afectar pluralismo, competencia y libertad de elección.

Por su parte, **UNESCO** ha propuesto un marco de principios para promover una Internet universal e inclusiva (conocidos como **principios ROAM** por sus siglas en inglés). Estos son:

- **Derechos Humanos:** Internet debe apoyar y promover los derechos humanos, como la libertad de expresión, el acceso a la información, la privacidad, etc. Las políticas digitales deben estar alineadas con los marcos internacionales de derechos humanos.
- **Apertura:** La red debe ser abierta desde un punto técnico y legal. es decir, debe ser interoperable, basada en estándares abiertos, y libre de censura o barreras a la expresión.
- **Accesibilidad:** El acceso a Internet debe ser equitativo, asequible y seguro para todas las personas, incluidas comunidades rurales, personas con discapacidad, juventudes, etc.
- **Participación de múltiples partes interesadas:** Las políticas sobre Internet deben desarrollarse con la participación significativa de todos los sectores.

Test: ¿Qué principio o principios se están afectando en cada una de estas situaciones hipotéticas?

1. Acceso lento a ciertos servicios

a. Una empresa proveedora de Internet comienza a reducir la velocidad de servicios de streaming gratuitos, mientras que prioriza a (y cobra extra por) otras plataformas asociadas.

Respuesta: *neutralidad de la red, apertura.*

2. Concentración de infraestructura digital

a. Un solo proveedor controla la mayoría de las conexiones de fibra óptica de un país, lo que le permite definir precios, prioridades, y dejar ciertas zonas sin servicio.

Respuesta: *descentralización, apertura*

3. Bloqueo de contenido político

a. Un gobierno decide bloquear el acceso a un sitio web de noticias independientes durante un periodo de elecciones, argumentando que es contenido inapropiado.

Respuesta: *apertura, neutralidad*

4. Consulta pública sin participación real

a. El gobierno abre una consulta sobre una nueva ley de ciberseguridad, pero el formulario está sólo en inglés, está abierto por solo 48 horas, y no hay devolución a los comentarios recibidos.

Respuesta: *participación*

Anexo 1. Respuestas.

Figura 5. Ejercicio

Recursos:

- ISOC. (s.f.) [Gobernanza de Internet](#)
- ISOC. (s.f.) [Curso en línea de Gobernanza de Internet](#)
- ISOC. (s.f.) [Glosario de términos de Internet](#)
- ISOC. (s.f.) [Ecosistema para la Gobernanza de Internet](#)
- [Género y Gobernanza de Internet](#)
- ISOC, Policy [brief](#) sobre gobernanza de Internet (inglés)
- ISOC, [Línea de tiempo](#) (inglés)
- Fundación Karisma y RedPaTodos, [Video](#) sobre gobernanza de Internet
- [Glosario](#) de UNESCO sobre términos de gobernanza de Internet (inglés)
- [Indicadores](#) de UNESCO sobre la universalidad de Internet (indicadores ROAM)
- [Principios para la gobernanza y el uso de Internet](#)

Figura 6. Recursos.

TEMA 2: ACTORES Y ESPACIOS DE TOMA DE DECISIÓN

Internet no se gobierna desde un solo lugar ni por un solo grupo o actor: su gobernanza es el resultado de decisiones tomadas por múltiples actores como lo son entidades técnicas, gobiernos, sector privado, organizaciones de la sociedad civil, etc. En este tema cubriremos: quiénes son estos actores clave en la gobernanza de Internet, cómo se relacionan entre sí y cuáles son los espacios clave de toma de decisiones para la gobernanza de Internet. Además, exploraremos el contexto institucional latinoamericano y los diferentes espacios de participación a nivel local y global como lo son el **LACIGF** y el **Youth LACIGF**.

MAPEO DE ACTORES CLAVE EN LA GOBERNANZA DE INTERNET

A continuación presentaremos los principales grupos de actores involucrados en la gobernanza de Internet. Cada grupo tiene distintos niveles de involucramiento, poder e influencia.

- **Sector técnico:** son organizaciones que desarrollan, mantienen y promueven los estándares técnicos de Internet:
 - **ICANN (Internet Corporation for Assigned Names and Numbers):** administra los nombres de dominio (como “.org” o “.lat”)
 - **IANA (Internet Assigned Numbers Authority):** es la organización responsable de la coordinación global de la zona raíz del Sistema de Nombres de Dominio (DNS), la asignación de direcciones Internet Protocol (IP) y otros recursos críticos de protocolos de internet.
 - **IETF (Internet Engineering Task Force):** desarrolla protocolos técnicos (como HTTP o el TCP-IP) que hacen posible el funcionamiento de Internet.
 - **ISOC (Internet Society):** promueve la coordinación global para el desarrollo de protocolos y estándares compatibles, lleva a cabo tareas educativas, y contribuye a políticas públicas.
 - **UIT (Unión Internacional de Telecomunicaciones):** la agencia de la ONU encargada de coordinar temas técnicos y de regulación de telecomunicaciones.

- **IEEE (Institute of Electrical and Electronics Engineers):** asociación profesional global para la tecnología y la ingeniería con una estructura organizacional distribuida. Está abierta a sugerencias sobre nuevas tecnologías e incluso puede establecerse la formación de grupos de trabajo.
 - **IRTF (Internet Research Task Force):** fomenta la investigación sobre la evolución del Internet mediante la creación de grupos de investigación enfocados y a largo plazo que estudian temas relacionados con protocolos, aplicaciones, arquitectura y tecnologías del Internet.
 - **IAB (Internet Architecture Board):** supervisa el desarrollo técnico y de ingeniería tanto del Grupo de Trabajo sobre Protocolos de Internet (IETF) como la Fuerza de Tarea para Investigación en Internet (IRTF).
-
- **Gobiernos:** desarrollan políticas públicas nacionales a nivel local, y además participan en procesos internacionales y negociaciones multilaterales.
 - **Sector privado:** incluye a empresas que proveen infraestructura digital (por ejemplo, empresas de telecomunicaciones como Cloudflare, CISCO, Juniper, Claro, etc.), así como plataformas digitales (como Google o Meta). Tienen un gran poder económico.
 - **Sociedad civil:** organizaciones, redes, y activistas que defienden los derechos humanos, el acceso equitativo a Internet y promueven la participación significativa en la toma de decisiones sobre la gobernanza de Internet.
 - **Academia:** centros de investigación, universidades, y personas expertas que contribuyen con experticia e investigación.
 - **Organismos y espacios internacionales:** espacios intergubernamentales (como la ONU) o multiactor que promueven el diálogo (por ejemplo, a través del Foro de Gobernanza de Internet) o el desarrollo de normas globales (como el Pacto Digital Mundial).

INTERACCIONES, TENSIONES Y ASIMETRÍA DE PODER

Todos esos actores —gobiernos, empresas, sociedad civil y otros— pueden participar en la gobernanza de Internet, pero no llegan en igualdad de condiciones.

No todos tienen el mismo poder

- Las empresas suelen tener mucho dinero y contactos que les permiten presionar la toma de decisiones.
- Los gobiernos pueden crear leyes y políticas porque tienen autoridad legal, pero a veces no saben suficiente de tecnología o no priorizan los derechos humanos.
- La sociedad civil aporta experiencia en derechos humanos y una mirada crítica, pero tiene menos recursos y enfrenta barreras para participar plenamente (idioma, dinero y trámites).

Barreras prácticas para la sociedad civil

- Muchos procesos globales se hacen en inglés.
- Participar cuesta tiempo y dinero (viajes, honorarios, traducción).
- Conseguir visas o acceder a reuniones presenciales puede ser difícil.

Conflictos de interés

- Una empresa puede defender políticas que favorezcan sus ganancias aunque afecten la privacidad.
- Algunos Estados pueden usar la regulación para restringir la libertad de expresión.

MAPEO DE ESPACIOS CLAVE EN LA GOBERNANZA DE INTERNET

La gobernanza de Internet ocurre en múltiples niveles: espacios globales, regionales y nacionales. Estos espacios definen marcos normativos, técnicos y políticos que son clave porque afectan el ejercicio de nuestros derechos. Entender qué espacios existen (y que tan abiertos son a la sociedad civil) es clave para poder planear nuestras estrategias de incidencia.

A continuación te presentamos algunos de los espacios principales de toma de decisiones respecto de la gobernanza e Internet:

ESPACIOS GLOBALES				
Espacio	Descripción	Apertura	Relevancia para sociedad civil	Participación de Latam
Foro de Gobernanza de Internet (IGF)	Espacio de diálogo multiactor organizado por la ONU. No toma decisiones vinculantes, pero genera consensos y visibiliza debates clave.	Alto Cualquier persona puede asistir, proponer sesiones, participar en talleres y unirse a distintas coaliciones temáticas.	Ideal para promover agendas como sociedad civil y para generar o reforzar relaciones con otros actores.	Como sociedad civil podemos participar de este IGF global para visibilizar temas de relevancia para nuestra región.
Pacto Digital Mundial (Global Digital Compact)	Una iniciativa impulsada por la Secretaría General de la ONU, que busca establecer principios comunes sobre el futuro digital global.	Medio Las negociaciones fueron solamente entre Estados, y si bien hubo procesos de consulta, algunos sectores de la sociedad civil consideran que no fueron lo suficientemente robustos.	El pacto cubre cuestiones como regulación de plataformas, inteligencia artificial, entre otros temas vinculados directamente a los derechos humanos.	Mediante la participación en negociaciones a través de sus Estados, y aportando desde sociedad civil, academia y sector privado en las consultas y espacios multiactor vinculados al proceso
Cumbre mundial sobre la Sociedad de la Información (WSIS)	Es un proceso iniciado por la ONU en dos partes, en 2003 y 2005, que culminó en una definición de gobernanza de Internet que consagra la necesidad de involucrar a múltiples partes interesadas, y la creación del IGF. Después de 20 años de su creación se está haciendo la revisión de su impacto y la pertinencia del modelo de múltiples partes interesadas en la coyuntura actual. Puedes ver más en nuestro último informe: Perspectiva de Colombia en la revisión a 20 años de la Cumbre Mundial de la Sociedad de la Información.	Medio Las negociaciones son intergubernamentales, con distintas instancias de participación multistakeholder.	La revisión de los 20 años de WSIS es fundamental en nuestro contexto, donde un grupo reducido de actores busca imponer visiones autoritarias de Internet. Además, este proceso definirá si se renueva el mandato del IGF.	Las organizaciones de sociedad civil pueden participar en las consultas globales y además hacer incidencia con gobiernos de la región para influenciar sus posiciones en la negociación.

Figura 7. Espacios globales de Gobernanza de Internet.

ESPACIOS REGIONALES			
Espacio	Descripción	Apertura	Relevancia para sociedad civil
Foro de Gobernanza de América Latina y el Caribe (LACIGF)	La versión de Latinoamérica y el Caribe del IGF. Reúne a todos los sectores para discutir temas de gobernanza de Internet desde una perspectiva regional.	Muy alto Se organiza de forma abierta y con participación de múltiples partes interesadas.	Las discusiones del LACIGF alimentan las discusiones del IGF global, por ende, es uno de los principales espacios para visibilizar temas urgentes de nuestra región.
Registro de Direcciones de Internet para América Latina y Caribe (LACNIC)	LACNIC es una organización técnica que gestiona la asignación de direcciones IP y otros recursos críticos de Internet en la región.	Medio Si bien su foco es técnico, hay distintas instancias de participación de actores no gubernamentales, por ejemplo a través de foros y procesos abiertos de desarrollo de políticas.	Es un espacio clave para entender cómo funciona Internet técnicamente y para incidir en decisiones sobre infraestructura (temas en los que es necesaria más involucramiento de organizaciones de sociedad civil).
Agenda digital de América Latina y el Caribe (eLAC)	Iniciativa intergubernamental organizada por la CEPAL para promover una agenda común sobre desarrollo digital	Bajo a moderado La participación directa está limitada a Estados, aunque hay mecanismos de consulta y espacios de diálogo con actores no gubernamentales.	Las discusiones en este espacio influyen en discusiones nacionales sobre política pública de transformación digital.

Figura 8. Espacios regionales de Gobernanza de Internet.

ESPACIOS NACIONALES Y LOCALES

Cada país tiene distintos canales de toma de decisiones en temas digitales y de tecnología, ya sean formales o informales. Algunos ejemplos son consultas públicas sobre proyectos de ley relacionados con temas de Internet (por ejemplo, iniciativas sobre protección de datos, ciberseguridad, inteligencia artificial o regulación de plataformas); mesas o comités consultivos en organismos regulatorios (por ejemplo, en entes regulatorios de telecomunicaciones); y foros multiactor nacionales como el [Foro Colombiano de Gobernanza de Internet t.co/](https://www.t.co/).

Espacio de discusión:

- ¿Tienes experiencia previa de incidencia o involucramiento en algunos de los espacios presentados en este módulo? ¿Cuáles? ¿Estarías interesada en participar?
- ¿Conoces ejemplos de temas relevantes para América Latina que se hayan discutido en foros globales?

Figura 9. Preguntas

El contexto en Latinoamérica

En Latinoamérica, las decisiones sobre Internet están marcadas por desigualdades que vienen de lejos: económicas, sociales y culturales. Muchas comunidades —especialmente en zonas rurales y territorios indígenas— todavía tienen menos acceso a conexiones, dispositivos y contenidos en su lengua. Por eso, garantizar acceso digno y políticas de conectividad debe ser una prioridad regional.

También hay un problema con las leyes y normas que se están aprobando: muchas veces se diseñan sin considerar los derechos humanos ni las realidades y necesidades locales. Eso puede poner en riesgo la privacidad, la libertad de expresión y el derecho a comunicarse en la propia lengua o según las propias prácticas comunitarias.

¿Qué significa esto para las comunidades?

- Si no hay conectividad real, las políticas públicas no sirven: hace falta infraestructura, formación y contenidos en idiomas locales.
- Si las leyes no se construyen considerando la salvaguarda de derechos fundamentales, las comunidades y las personas defensoras pueden quedar más expuestas a vigilancia, censura o exclusión.
- Las soluciones deben contemplar el contexto y de las organizaciones sociales, porque son ellas las que mejor conocen sus necesidades y riesgos.

Para que Internet sea verdaderamente útil y seguro en la región, las políticas deben construirse con quienes viven y defienden los territorios: comunidades indígenas, pueblos rurales y activistas. No estamos pidiendo permiso para participar; exigimos que se nos escuche y que las decisiones respeten nuestras lenguas, modos de vida y derechos.

Recursos:

- *Global Partners Digital*, [blog](#) “Everything you need to know about the WSIS+20 review” (inglés)
- *APC*, [blog](#) “The feminist principles for including gender in the Global Digital Compact” (inglés)
- *Foro Global de Justicia Digital*, [blog](#) “Justicia digital, ¡ya! Un llamado a la acción hacia la CMSI+20 y más allá”.
- *Sociedad civil en ICANN*

<https://www.icann.org/resources/pages/civil-society>

Figura 10. Recursos.

TEMA 3:

GOBERNANZA DE INTERNET Y DERECHOS HUMANOS

Internet es un espacio donde se ejercen (y a veces se vulneran) derechos fundamentales. Es difícil pensar en aspectos de nuestra vida cotidiana que no estén relacionados de una u otra forma por la tecnología. Nos comunicamos a través de apps de mensajería, chequeamos nuestro balance bancario a través de apps, pedimos comida o compramos productos a través de aplicaciones digitales o incluso la atención a salud está mediada por el registro en bases de datos digitales.

En esta sección vamos a explorar cómo las decisiones sobre Internet afectan directamente, de formas positivas y negativas, al ejercicio de los derechos humanos. Es importante que como sociedad civil tengamos claras estas intersecciones para reconocer posibles amenazas emergentes a nuestros derechos y así, hacer incidencia que sea más informada y estratégica.

GOBERNANZA DE INTERNET Y DERECHOS HUMANOS - UN VÍNCULO CLAVE

La gobernanza de Internet (entendida, como “las decisiones que afectan el funcionamiento, desarrollo y uso de Internet”) tiene efectos concretos sobre distintos derechos:

- **El derecho a la privacidad:**

Las decisiones sobre qué datos se recogen, quien los controla, y con qué fines pueden utilizarse tienen un vínculo directo con el derecho a la privacidad. Marcos legislativos sobre protección de datos pueden contribuir al ejercicio de este derecho, mientras que decisiones sobre vigilancia o eliminación del cifrado lo pueden vulnerar.

Ejemplo: Cuando aceptamos los términos y condiciones de WhatsApp, estamos autorizando que ciertos datos sean recolectados (como nuestra lista de contactos). Si una empresa decide vender esos datos a terceros, nuestra privacidad puede verse comprometida.

- **El derecho a la libertad de expresión**

Internet puede ofrecer un espacio en el que expresarnos, pero también hay políticas que limitan el ejercicio de este derecho. Por ejemplo, ciertas políticas de moderación de contenidos como el bloqueo de ciertos sitios web pueden afectar directamente nuestra libertad de expresarnos

Ejemplo: Si una red social eliminó una publicación sobre derechos sexuales y reproductivos alegando que “viola las normas de la comunidad”, se está afectando nuestra capacidad de expresarnos.

- **El acceso a la información**

Las políticas públicas de Internet tienen un efecto directo sobre quienes pueden tener acceso y quiénes no, qué contenidos están disponibles y en qué idiomas y que barreras económicas existen. Sin acceso significativo a Internet (no solo conectividad sino apropiación y educación digital), este derecho se ve afectado.

Ejemplo: En comunidades rurales donde el Internet es lento y costoso, las niñas y mujeres tienen menos acceso a información educativa o de salud.

- **Derecho a la no discriminación**

Ciertas tecnologías (por ejemplo, sistemas de inteligencia artificial) pueden reproducir sesgos y estereotipos de género, raza, nivel socioeconómico y otros.

Ejemplo: sistemas de reconocimiento facial que funcionan peor para mujeres y personas racializadas, lo que puede derivar en exclusiones o acusaciones injustas.

Ejemplo 1: Moderación de contenidos y censura

Las plataformas digitales —donde nos hablamos, contamos nuestras historias y debatimos sobre lo que nos importa— no siempre respetan los derechos fundamentales. Sus reglas para decidir qué se publica y qué se borra frecuentemente no coinciden con estándares internacionales de derechos humanos.

Algunos problemas concretos:

- Muchas decisiones se toman con sistemas automáticos, sin revisión humana ni una forma clara de apelar las decisiones de las plataformas.
- Las reglas de moderación suelen diseñarse con lógicas comerciales o con normas culturales de países del Norte Global, que no siempre entienden nuestras realidades ni nuestras lenguas.
- Se aplica la moderación de forma desigual: discursos que defienden derechos (por ejemplo, feministas o a favor del aborto) a veces son silenciados, mientras que discursos de odio o desinformación quedan en la plataforma.

Ejemplos:

- Colectivos proaborto en México y Colombia han denunciado bloqueos de cuentas en WhatsApp y censura en redes sociales al intentar organizarse o difundir información.
- La mayor campaña de censura en redes sociales contra las violaciones de derechos humanos al pueblo palestino, orquestada y patrocinada por Israel ([Israel & Meta, The Greatest Global Mass Censorship Campaign to Ever Exist](#))

Ejemplo 2: Vigilancia estatal y privada

Las tecnologías de vigilancia —que abarcan desde herramientas de interceptación de comunicaciones hasta sistemas de reconocimiento facial o de geolocalización— pueden ser utilizadas de formas muy distintas según el contexto, el marco legal y los actores involucrados. En algunos casos, se emplean con fines legítimos de seguridad pública; sin embargo, también se han documentado usos abusivos que ponen en riesgo la vida privada y la seguridad de periodistas, defensores y activistas. En varios países de Latinoamérica, por ejemplo, estas herramientas han sido utilizadas para espiar a quienes investigan o defienden los derechos humanos. En México, entre abril y mayo de 2019, [al menos 456 personas fueron vigiladas con el software Pegasus](#).

Por eso es importante pedir controles claros y transparencia: investigaciones independientes cuando haya denuncias, leyes que limiten el uso de estas herramientas, medidas de reparación para las víctimas y formación en seguridad digital para comunidades y movimientos.

Ejemplo 3: Discriminación y exclusión en entornos digitales

La tecnología no es neutral, puede reproducir y en muchos casos mantener y amplificar las desigualdades. Algunos ejemplos de impactos diferenciados en ciertas comunidades son:

- Las mujeres y personas LGBTIQ+ experimentan más violencia digital.
- Los pueblos originarios enfrentan falta de acceso y barreras lingüísticas para su participación en espacios de gobernanza.

Espacio de discusión:

- a) ¿Qué barrera concreta enfrenta tu comunidad para usar Internet de forma equitativa? (ej.: conectividad, idioma, amenazas, censura, costo, falta de formación).
- b) ¿Qué derechos se ven afectados? (privacidad, libertad de expresión, acceso a la información, derecho colectivo).
- c) ¿Quiénes tienen poder para cambiar eso y qué necesitan para hacerlo? (gobierno, empresa, organizaciones locales).

Redacta 3 propuestas accionables y sencillas (máx. 2 líneas cada una), priorizando:

- Una medida de política pública (ej.: fondos de conectividad comunitaria con control local).
- Una medida operativa o de solidaridad (ej.: red de traductores voluntarios para procesos de gobernanza).
- Una medida de protección (ej.: apoyo legal o protocolos de seguridad digital para defensoras).

Figura 11. Espacio de discusión.

Recursos:

- Luchadoras, [Guia sobre Violencia Digital](#)
- Fundacion Karisma, [K+Lab](#)
- EFF, [Principios](#) de Manila sobre Responsabilidad de Intermediarios
- APC, [Principios](#) Feministas para Internet
- Amnesty International, [El proyecto Pegasus](#)
- Al Sur, [informe](#) La moderación de contenidos desde una perspectiva interamericana
- R3D, [Informe](#) "El Estado de la Vigilancia"

Figura 12. Recursos.

TEMA 4: PARTICIPACIÓN DE LA SOCIEDAD CIVIL

La sociedad civil tiene un rol fundamental en la defensa de los derechos humanos en procesos de gobernanza de Internet, pero ¿qué tan abiertos son realmente los espacios de decisión? ¿Cuáles son los desafíos, oportunidades y estrategias de participación desde nuestras realidades en Latinoamérica? Este tema busca visibilizar las vías de participación disponibles, así como las barreras estructurales que impiden una participación significativa, plena y efectiva. Además, compartimos algunos ejemplos concretos de incidencia.

¿PUEDE LA SOCIEDAD CIVIL PARTICIPAR EN LA GOBERNANZA DE INTERNET?

La gobernanza de Internet se define, en parte, por su enfoque multistakeholder (de múltiples partes interesadas), lo que significa que distintos sectores —incluida la sociedad civil— deben tener voz en las discusiones. Sin embargo, la apertura formal no siempre se traduce en participación significativa.

¿CUÁLES SON LAS BARRERAS DE ACCESO?

Aunque en teoría muchos espacios sean “abiertos”, existen obstáculos reales que dificultan la participación de las organizaciones de sociedad civil, especialmente aquellas del Sur Global. Por ejemplo:

- **Idioma y jerga técnica:** la mayoría de los procesos se llevan a cabo en inglés y con terminología técnica especializada.
- **Falta de recursos financieros:** a diferencia de, por ejemplo, el sector privado, muchas organizaciones de sociedad civil a menudo no cuentan con financiamiento, tiempo, o personal capacitado para seguir procesos largos y complejos.
- **Exclusión estructural:** ciertas organizaciones enfrentan mayores obstáculos, por ejemplo, organizaciones de pueblos originarios y comunidades rurales.
- **Falta de transparencia y acceso a la información:** muchos procesos son opacos, sin información pública sobre instancias de participación.
- **Participación simbólica o no significativa:** muchas veces se realizan consultas como una forma de cumplir con un requisito formal, pero sin mecanismos reales para integrar esas perspectivas de forma significativa en los procesos.

Actividad “Mapa de barreras y pequeñas acciones”

Objetivo: Identificar barreras concretas que impiden a tu comunidad participar en la gobernanza de Internet y diseñar acciones pequeñas y viables para empezarlas a resolver.

Materiales: hoja de papel o documento digital.

Pasos

1. Contexto

Escribe en una línea cuál es tu comunidad (ej.: comunidad indígena, barrio rural, colectivo feminista, grupo estudiantil).

2. Mapa rápido de barreras

Haz una lista de hasta 6 barreras que impiden la participación en decisiones sobre Internet (una por línea). Piensa en: conectividad, costo, idioma, trámites/visados, falta de información, violencia digital, falta de representación, falta de financiamiento, formatos inaccesibles, etc. Junto a cada barrera apunta en 3–5 palabras por qué existe (causa).

3. Prioriza

Marca la barrera más urgente o la que creas más fácil de atacar a corto plazo.

4. Pequeñas acciones

Para la barrera priorizada, diseña 3 acciones concretas y muy factibles que puedas impulsar tú solo/a o con pocas personas. Deben ser realizables en 1–3 meses. Ejemplos: taller local de seguridad digital de 2 horas, traducir y compartir un resumen en lengua local, recoger firmas para solicitar internet comunitario, grabar audio explicativo y distribuirlo por WhatsApp. Para cada acción escribe:

- Qué se hará (1 línea).
- Primer paso inmediato (1 línea).
- Recurso mínimo necesario (persona, tiempo, dinero).

5. Riesgos y mitigaciones

Escribe 2 posibles riesgos o obstáculos para la acción elegida (ej.: represalias, falta de interés, costo) y una breve idea para reducir cada riesgo.

6. Compromiso personal

Escribe qué harás esta semana (acción concreta y día) para avanzar en la primera acción.

Figura 13. Recursos.

¿Por qué es importante que las organizaciones de sociedad civil participen en el modelo de múltiples partes interesadas de gobernanza de Internet?

El modelo de múltiples partes interesadas permite que las organizaciones de sociedad civil no solo observen, sino que formen parte activa de las decisiones sobre cómo se gobierna Internet. Esta participación es clave por varias razones:

1. Defender los derechos humanos en los espacios digitales

Las ONG trabajan por los derechos humanos como la libertad de expresión, la privacidad y el acceso a la información. Estos derechos también se ejercen y se vulneran en Internet. Participar en la gobernanza permite protegerlos desde el diseño mismo de las normas e infraestructuras digitales.

2. Llevar las voces del territorio y comunidades a los espacios globales

Las decisiones sobre Internet afectan a todas las personas, en todos los países. Las ONG aportan experiencias y perspectivas de comunidades locales, ayudando a que el Internet sea una plataforma para la inclusión.

3. Incidir antes de que las políticas estén definidas

En el modelo de múltiples partes interesadas las decisiones se toman por consenso. Esto le da a las ONG la oportunidad de participar en la construcción de políticas desde el inicio. Entendiendo que es un espacio en el que cada vez es más necesario integrarnos y colaborar para incidir desde las organizaciones de la sociedad civil.

4. Rendición de cuentas o Accountability

Como gran parte del control de Internet está en manos de gobiernos y empresas privadas, la presencia de las ONG ayuda a fomentar la transparencia, el control social y la rendición de cuentas.

5. Colaborar con otros sectores

Estar en estos espacios permite que las ONG trabajen junto a comunidades técnicas, empresas y responsables de políticas, construyendo soluciones conjuntas para los desafíos digitales actuales. El trabajo articulado con otros sectores y organizaciones es una oportunidad para el trabajo en red y generación de confianza entre las partes interesadas.

Estrategias de participación desde sociedad civil

- **Campañas públicas** a través de movilización en redes, campañas visuales, o de sensibilización ciudadana. Ejemplos: [KeepItOn campaign](#), Access Now
- **Litigio estratégico:** uso del sistema judicial para impugnar leyes o políticas que violan derechos. Ejemplos: [Incidencia judicial](#) de nuestra organización que permite motivar cambios locales, nacionales e internacionales.
- **Incidencia directa:** participación en consultas públicas, reuniones con personas tomadoras de decisiones, presentación de informes o recomendaciones. Ejemplos: [input conjunto](#) de organizaciones de sociedad civil en el proceso de desarrollo del Pacto Digital Global
- **Alianzas:** construcción de redes de sociedad civil y redes multiactor (con periodistas, sector privado, academia). Ejemplos: [consorcio AlSur](#)
- **Participación en espacios técnicos:** involucrarse en espacios como ICANN o ITU, desde la perspectiva de derechos. Ejemplos: [participación](#) de sociedad civil en el Study Group 13 de la UIT.

Actividad:

Objetivo: Transformar las barreras identificadas en el ejercicio individual en un plan colectivo de incidencia con estrategias y actividades concretas.

Materiales: documento compartido o tablero digital, si las personas están en el mismo lugar, un tablero o papelógrafo, donde puedan escribir todas las personas.

Pasos:

1. Compartir

Cada persona dice brevemente la barrera que priorizó en el ejercicio individual.

2. Elegir un proceso de gobernanza

El grupo elige un proceso trabajado en el módulo (ej.: protección de datos, conectividad, moderación de contenidos, nombres de dominio).

3. Definir 2-3 estrategias de incidencia

Conecten la barrera elegida con el proceso seleccionado. Ejemplo de estrategias: visibilización, alianzas, incidencia en políticas públicas, producción de conocimiento local.

4. Diseñar actividades concretas

Para cada estrategia, propongan una actividad simple y realista (ej.: campaña en redes, taller comunitario, traducción de un recurso, carta a una autoridad, alianza con otra organización).

Pueden usar este modelo o crear el propio:

Estrategia de incidencia	Ejemplo de actividad	Quiénes se comprometen	Recurso mínimo
--------------------------	----------------------	------------------------	----------------

Figura 14. Actividad.

Incidencia exitosa

Promoción de ciber normas inclusivas - Fundación Karisma (Puedes acceder al documento completo [aquí](#)).

¿Qué pasó?

En 2022, participamos de un espacio multistakeholder para enfrentar la violencia contra las mujeres en política, buscando asegurar que cualquier futura ley tuviera en cuenta derechos humanos como el derecho a la libertad de expresión y la privacidad.

¿Qué hicieron?

- Aportaron perspectiva digital al diseño de indicadores sobre violencia online.
- Colaboraron en un texto alternativo para una ley basada en el modelo de la OEA.
- Advirtieron sobre propuestas problemáticas como el bloqueo de contenido sin garantías.

¿Qué dificultades hubo?

- Tensiones entre derechos (protección frente a la violencia y libertad de expresión).
- Procesos legislativos rápidos, sin suficiente consulta pública.
- Desacuerdos sobre quién debe tener poder para eliminar contenidos.

¿Qué lograron?

- Visibilizar los derechos digitales en el debate sobre violencia política.
- Promover el diálogo entre actores diversos.
- Generar recomendaciones para políticas más equilibradas y participativas.

Es un ejemplo claro de cómo la sociedad civil puede incidir críticamente en procesos legislativos para proteger derechos en el entorno digital.

Recursos:

- *Al Sur, articulación regional.* <https://www.alsur.lat/>
- *Global Partners Digital y Fundación Karisma, Promoción de ciber normas inclusivas. Estudio de caso*
- *Derechos Digitales, Promoción de ciber normas inclusivas. Estudio de caso.*
- *Access Now, Digital ID Toolkit.* <https://www.accessnow.org/guide/digital-id-toolkit/>

Figura 15. Recursos.

UNIDAD 2

TEMA 5: TENDENCIAS Y DEBATES ACTUALES

Las tecnologías emergentes, los conflictos geopolíticos y la expansión de las plataformas digitales (entre otros factores) han generado nuevos desafíos y tensiones en cuanto a la gobernanza de Internet. En este tema te ofrecemos un panorama de las principales tendencias y debates que afectan la evolución de Internet.

Fragmentación de Internet

¿Qué es el *splinternet*?

El término se refiere a la fragmentación de la capa técnica de Internet en múltiples “Internet nacionales” o regionales controladas por Estados u otros actores. En el primer módulo hablamos del caso de China en torno al gran muro de fuego. Como parte de este fenómeno, China mantiene una red fuertemente controlada, con acceso restringido a plataformas globales. Por otra parte, Rusia ha probado sistemas para desconectarse del Internet global en situaciones de crisis.

Si bien algunos actores defienden estas medidas como defensa frente al colonialismo tecnológico¹ (que ocurre cuando unos pocos países o empresas -generalmente del norte global- controlan la tecnología y hacen que otros dependan de ellos para usarla o desarrollarla) también **pueden utilizarse para justificar medidas de censura, control y aislamiento.**

Veamos un [ejemplo en Brasil](#) en torno a la soberanía digital. En distintas discusiones políticas y legislativas en Brasil se ha promovido el planteamiento de qué datos deben almacenarse dentro del país para proteger la autonomía y la protección de datos. Organizaciones de la sociedad civil, como la Associação Brasileira de Imprensa y grupos de derechos digitales, han señalado que sin garantías fuertes de derechos humanos estas medidas pueden facilitar el acceso estatal a datos y concentrar poder, especialmente si no existen salvaguardias judiciales y transparencia en las solicitudes de información.

1. El colonialismo tecnológico se puede observar cuando empresas, países o plataformas externas dominan y controlan infraestructuras, datos, normas y servicios digitales en otra región, imponiendo tecnologías, modelos de negocio y prácticas que benefician a los proveedores extranjeros y reducen la autonomía local; esto puede debilitar economías locales, limitar la diversidad cultural y poner en riesgo la soberanía digital.

Regulación de inteligencia artificial y algoritmos

¿Por qué importa? porque cada **vez más decisiones son tomadas o influenciadas por algoritmos y sistemas de Inteligencia Artificial (IA)**, por ejemplo: quien accede a un crédito, qué noticias vemos, qué contenidos se censuran.

Estas decisiones no siempre son transparentes, y como se alimentan de datos e información, pueden **reproducir sesgos discriminatorios** que ya existen en nuestra sociedad. Por ejemplo, al utilizar voces femeninas para asistentes de IA, se refuerza el estereotipo de que las mujeres deben llevar a cabo tareas de servicio. Además, se han documentado casos en los que sistemas de identificación facial han tenido dificultades para identificar adecuadamente a las mujeres, en particular, a mujeres de color. En Latinoamérica, países como Colombia, Brasil, Chile y Costa Rica han comenzado a desarrollar marcos legales o estrategias nacionales de IA.

Ciberseguridad

¿Qué es la ciberseguridad? Muchas veces se la define como un conjunto de políticas y medidas técnicas destinadas a proteger redes, dispositivos e infraestructuras digitales frente a ataques. Sin embargo, es importante entender que **no se busca proteger sistemas porque sí, sino porque están para servir a las personas y, por extensión, sus derechos**. La ciberseguridad es necesaria para ejercer nuestros derechos y, a su vez, la ausencia de ciberseguridad puede tener consecuencias trágicas y vulnerar nuestros derechos (por ejemplo, si un ciber ataque filtra información sobre la orientación sexual de una persona en un país en el que la homosexualidad está criminalizada).

Una definición que incluye este factor es la de la Freedom Online Coalition, que define la ciberseguridad como *“La preservación –a través de políticas, tecnología y educación– de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, a fin de mejorar la seguridad de las personas tanto online como offline”*.

¿Qué pasa cuando se usan leyes de ciberseguridad como herramienta o excusa para restringir derechos? Leyes de ciberdelito o ciberseguridad mal diseñadas pueden justificar la vigilancia masiva, criminalizar protesta social o activismo digital, perseguir periodistas o bloquear páginas de forma arbitraria. Es por esto que como organizaciones de sociedad civil debemos exigir marcos de ciberseguridad con enfoques de derechos humanos y participación ciudadana.

Plataformas y economía digital

¿Qué está en juego? Las plataformas digitales como Google, Meta o Amazon concentran un gran poder económico, social y político. Estas controlan el flujo y acceso a la información (a través de buscadores y redes sociales) y así como algunos aspectos del trabajo (a través de apps de delivery o comercio en línea). Estas plataformas definen sus propias reglas, muchas veces sin transparencia ni responsabilidad ante los Estados o las personas.

Algunos de los problemas clave desde una perspectiva de derechos humanos son los monopolios digitales que dificultan la competencia, aumentan la precarización laboral en plataformas y los modelos extractivistas que se basan en la explotación de nuestros datos personales.

Actividad:

Objetivo: Analizar cómo las tendencias actuales en inteligencia artificial, soberanía digital y ciberseguridad en América Latina (con foco en Colombia) impactan los derechos humanos, y generar ideas de respuesta desde la sociedad civil.

Materiales: documento digital compartido o tablero digital ([Excalidraw](#))

1: Identificación de tendencias

- Cada participante lee al menos un recurso sugerido (ej.: el blog de ONU Mujeres sobre IA y sesgos, el ensayo de Pohle y Thiel sobre soberanía digital, o el informe de Derechos Digitales sobre ciberseguridad).
- En el mural digital, cada persona escribe en un post-it virtual:
 - Una tendencia observada en Colombia o la región (ej.: uso creciente de IA en educación).
 - El derecho que puede verse afectado.

2: Conexión de ideas

- El grupo organiza los post-its en 3 grandes áreas:
 - **IA y sesgos**
 - **Soberanía digital**
 - **Ciberseguridad**
- Entre los post-its, dibujen flechas o conexiones que muestren cómo las tendencias se relacionan o se refuerzan (ej.: "uso de IA en salud" afecta privacidad también conecta con falta de soberanía en gestión de datos).

3: Respuesta colectiva

- A partir del mapa visual, el grupo escribe en el mural un “cartel de acción colectiva” con:
 - Un problema central (ej.: “Falta de transparencia en sistemas de IA”).
 - Una propuesta de respuesta desde la sociedad civil (ej.: “Campaña para exigir auditorías con enfoque de género en algoritmos públicos”).
- El cartel puede ser un cuadro de texto destacado, un dibujo sencillo o un ícono con frase breve.

Resultado esperado

Un **mapa visual** que incluya

Tendencias identificadas por el grupo.

Derechos en juego conectados.

Una propuesta colectiva de respuesta clara y visible.

- **Lluvia de ideas** sobre tendencias que las participantes observan en Colombia y discusión grupal sobre qué derechos se pueden ver afectados y cómo podríamos responder desde la sociedad civil.
- En grupos, **analizar titulares de diarios** recientes sobre IA, filtraciones de datos, plataformas sociales. ¿Qué actores están involucrados? ¿Qué derechos están en juego? ¿Cómo podemos responder como sociedad civil?

Figura 16. Actividad

Recursos:

- Derechos Digitales, [Artículo](#) "América Latina ante la inteligencia artificial: mapeo de iniciativas regulatorias en la región"
- Julia Pohle y Thorsten Thiel, Revista Latinoamericana de Economía y Sociedad Digital, [Ensayo](#) "Soberanía Digital"
- Internet Society, [paper](#) "Soberanía digital y su impacto en Internet."
- UN Women, [Blog](#) "Como la inteligencia artificial refuerza los sesgos de género y que podemos hacer al respecto."
- New York Times, [Artículo](#) "Many facial-recognition systems are biased, says US study"
- Freedom Online Coalition, [definición](#) de ciberseguridad.
- Derechos Digitales, [Informe](#) "Ciberseguridad en América Latina: Estrategias nacionales en 2024"
- TEDIC, [Trabajo y Economía Digital](#)
- Derechos Digitales, [artículo](#) "Transformaciones y desafíos en los derechos digitales en América Latina: un balance de 2024"

Figura 17. Recursos.

TEMA 6: ACCESO Y CONECTIVIDAD

Internet tiene el potencial de contribuir al **desarrollo sostenible, la participación democrática y el ejercicio de derechos**, pero ese potencial sólo puede cumplirse si todas las personas pueden acceder a Internet de forma segura, significativa y equitativa. Este tema explora las múltiples dimensiones del acceso a tecnologías, no sólo técnicas o económicas, sino también culturales, sociales y políticas. Visibilizaremos las brechas que afectan especialmente a juventudes, mujeres, personas racializadas, pueblos originarios y habitantes de zonas rurales.

DIGITALIZACIÓN, DESARROLLO SOSTENIBLE E INCLUSIÓN

La digitalización puede ayudar a la vida comunitaria —acceso a salud, educación y mercados— pero sólo si llega de forma justa. Si las políticas digitales replican las mismas desigualdades de antes, entonces la tecnología termina excluyendo en vez de ayudar.

La Agenda para el Desarrollo Sostenible 2030² reúne 17 objetivos que buscan precisamente reducir esas brechas. Tres de ellos están muy relacionadas con lo digital y con las comunidades: educación de calidad (ODS 4), infraestructura y conectividad que incluyan a todos (ODS 9), y la reducción de las desigualdades (ODS 10). Pensar en tecnología desde estos objetivos significa priorizar acceso real, contenidos en nuestras lenguas y decisiones donde las comunidades tengan voz y control.

BRECHAS DIGITALES: ¿QUIÉN ACCEDE Y QUIÉN NO?

No todas las personas tienen el mismo acceso a Internet. Las brechas digitales no se refieren solo a estar conectadas, sino también a cómo accedemos, con qué calidad, para qué y con qué derechos. Algunos ejemplos de brechas digitales son:

- **Geográficas:** hay zonas rurales o alejadas que tienen baja cobertura o cobertura inestable.
- **Socioeconómicas:** los costos de los dispositivos, de la electricidad o de los planes de datos móviles influyen en quienes pueden acceder a ellos.
- **De género:** las mujeres tienen menos acceso y más probabilidad de recibir violencia digital
- **Intergeneracionales:** mientras que las juventudes tienen más exposición a Internet, las personas mayores quedan rezagadas.
- **Culturales y lingüísticas:** falta de contenidos en lenguas originarias, o falta de contenidos que estén adaptados a contextos y necesidades diversas.

2. Es un plan de acción adoptado en 2015 por los Estados miembros de Naciones Unidas. Su objetivo es erradicar la pobreza, proteger el planeta y garantizar que todas las personas gocen de paz y prosperidad para 2030.

CONECTIVIDAD BÁSICA VS. ACCESO SIGNIFICATIVO

Tener conexión es un mero pre-requisito, pero no garantiza la inclusión. Tener conectividad significativa implica que las personas podamos acceder y usar Internet de forma:

- **Asequible** (a un precio accesible)
- **Segura** (sin vigilancia o exposición a violencia)
- **Con contenidos relevantes** (información útil y en nuestro lenguaje)
- **Participativa** (que tengamos la capacidad de crear y no solamente consumir contenidos, que podamos aprender, compartir y transformar).

REDES COMUNITARIAS Y MODELOS ALTERNATIVOS DE CONECTIVIDAD

Las redes comunitarias surgen, en muchos casos, como respuesta a la ausencia o limitaciones de los planes del Estado para garantizar la conectividad. Los programas estatales suelen enfocarse en grandes infraestructuras y contratos con empresas de telecomunicaciones, priorizando criterios de rentabilidad y cobertura masiva. Esto deja por fuera a comunidades rurales, indígenas o periféricas, donde el costo de llevar infraestructura es alto y los beneficios económicos, bajos.

Ahí es donde entran las redes comunitarias: no buscan reemplazar al Estado, sino complementar sus esfuerzos, demostrando que existen modelos alternativos de conectividad que parten de la organización local y de tecnologías apropiadas.

¿Qué las distingue?

- **Operadas por la comunidad:** son las vecinas, personas de la comunidad y organizaciones locales que mantienen la red y deciden sobre su funcionamiento .
- **Tecnologías apropiadas:** Usan lo que mejor se ajusta a cada territorio y comunidad, como frecuencias libres, equipos de bajo costo e incluso software abierto o infraestructuras compartidas.
- **No son solo tecnología:** la conectividad se integra con la vida comunitaria, es un apoyo a la educación en la lengua propia, difusión de saberes tradicionales, coordinación de actividades culturales y defensa de derechos.

GOBERNANZA EN LAS REDES COMUNITARIAS

Aunque no siempre se le llame así, en estas redes también hay gobernanza: la comunidad define sus propias reglas, decide colectivamente cómo se usa la red, quién la administra, qué se prioriza y cómo se cuidan los recursos.

Esto significa que las decisiones no vienen de una empresa o de un gobierno central, sino de la propia comunidad, de acuerdo con sus necesidades y valores.

En pocas palabras, las redes comunitarias permiten que las comunidades tomen control de su conectividad, protejan su privacidad y aseguran que Internet responda a sus realidades locales.

Ejemplo: Kimera - historia, propósito y cómo funciona

Origen y evolución

- Entre 1985 y 2006 el proyecto KIMERA desarrolló títulos educativos y multimedia en distintos formatos.
- En 2016 nuestra organización retomó el proyecto con el objetivo inicial de poner a disposición de los títulos multimedia y el software educativo desarrollado.
- Desde 2018 el foco se orientó al desarrollo de la Red Local Kimera.
- En 2024 el desarrollo del proyecto pasó a la Corporación Frutos de Utopía.

Qué es la Red Local Kimera

- Es una herramienta (programa) que permite crear un servidor local con contenidos y herramientas accesibles por red inalámbrica.
- Se instala en un computador personal o institucional con sistema operativo Windows.
- Puede ser accedida desde computadores, celulares, tabletas y cualquier dispositivo con conexión inalámbrica o mediante cable a la red.

Funcionalidad y beneficios principales

- Provisión local de contenidos y herramientas: aloja recursos (textos, multimedia, aplicaciones educativas) directamente en el equipo servidor.
- Acceso multiplataforma: cualquier dispositivo con conexión de red puede usar los recursos sin depender de Internet.
- Intercambio de archivos digitales: al permitir intercambio, cada Red Local Kimera deja de ser una isla estática; puede ofrecer nuevas opciones a sus usuarios y compartir contenidos.
- Actualización y colaboración: las redes locales pueden conectarse entre sí para intercambiar contenidos, sincronizarse y actualizarse.

Casos de uso típicos

- *Aulas y escuelas con conectividad limitada: acceso a materiales educativos locales sin consumo de datos.*
- *Bibliotecas y centros comunitarios: ofrecer catálogo digital, video, herramientas y servicios locales.*
- *Instituciones rurales o eventos temporales: crear una red accesible rápidamente para múltiples usuarios.*
- *Laboratorios y proyectos colaborativos: compartir archivos, herramientas y recursos entre participantes.*

Ventajas prácticas

- *Funciona sin dependencia constante de Internet.*
- *Usa hardware común (un PC con Windows) y dispositivos de uso cotidiano (teléfonos, tablets, laptops).*
- *Facilita acceso inclusivo a recursos digitales en contextos con conectividad débil o costosa.*
- *Facilita autonomía local y colaboración entre redes.*

Figura 18. Evolución de la red Kimera.

Juventudes y acceso: entre la oportunidad y la exclusión

Las juventudes suelen estar al centro de la cultura digital, pero eso no significa necesariamente que tengan acceso equitativo o participación en las decisiones.

Muchas veces las juventudes usan Internet sin alfabetización crítica, enfrentan vigilancia, son excluidas de políticas públicas digitales o sufren violencia digital (particularmente mujeres y personas LGBTQ+).

Es por ello que debemos exigir educación digital integral, participación en la formulación de políticas y acceso a tecnologías seguras y culturalmente relevantes.

Actividad: Mapeo de brechas digitales locales

Objetivo: Reflexionar sobre cómo las juventudes de tu entorno viven la tecnología, identificar barreras concretas y proponer soluciones locales y políticas sencillas.

Materiales: hoja de papel o documento digital.

Pasos

1. Contexto

Escribe en una línea quiénes son “las juventudes” en tu comunidad (edad aproximada, grupo: estudiantes, jóvenes indígenas, colectivos LGBTIQ+, jóvenes rurales, etc.).

2. Observación rápida

Responde en una tabla o lista breve:

- ¿Cómo acceden normalmente a Internet? (lugar, dispositivos, costo)
- Menciona 4 barreras que afectan ese acceso, una por categoría: económica, lingüística/cultural, educativa (alfabetización digital), y de género/seguridad (violencia, vigilancia). Para cada barrera añade 1 frase sobre cómo la percibes en tu entorno.

3. Impacto en la vida juvenil

Escribe 3 ejemplos concretos (2-3 líneas cada uno) de oportunidades perdidas o daños por esas brechas (ej.: no poder estudiar en línea, exposición a violencia en redes, exclusión de procesos de decisión).

Figura 19. Actividad.

Recursos:

- Naciones Unidas [Agenda 2030](#) para el desarrollo sostenible.
- [Redes Comunitarias Colombia](#)
- APC, [Inclusion Digital](#)
- Al Sur, [Informe](#) “Ampliando la conectividad a Internet”
- APC, [Informe](#) “Communal Internet Infrastructure”
- Colnodo, [Blog](#) “Redes comunitarias y acceso al espectro: Una alternativa sostenible para la inclusión digital en Colombia”.
- TEDIC, [Informe](#) “Conectividad y apropiación digital para la resiliencia climática en zonas rurales”
- Derechos Digitales, [Informe](#) “Conectividad en Amazonia: Recomendaciones para combatir la brecha digital”

Figura 20. Recursos.

MEDIOS ALTERNATIVOS DE PARTICIPACIÓN

Mastodon

Como ejemplo de digitalización colaborativa y participativa, Mastodon representa una alternativa al modelo centralizado de redes sociales. Su arquitectura federada y autogobernada muestra cómo las comunidades pueden gestionar sus espacios digitales manteniendo interoperabilidad, transparencia y autonomía. Esto contrasta con las plataformas centralizadas y abre un camino para pensar en gobiernos digitales que dialoguen con ciudadanía desde una perspectiva de soberanía tecnológica.

Aquí podría ir un video tutorial introductorio, en lugar de texto.

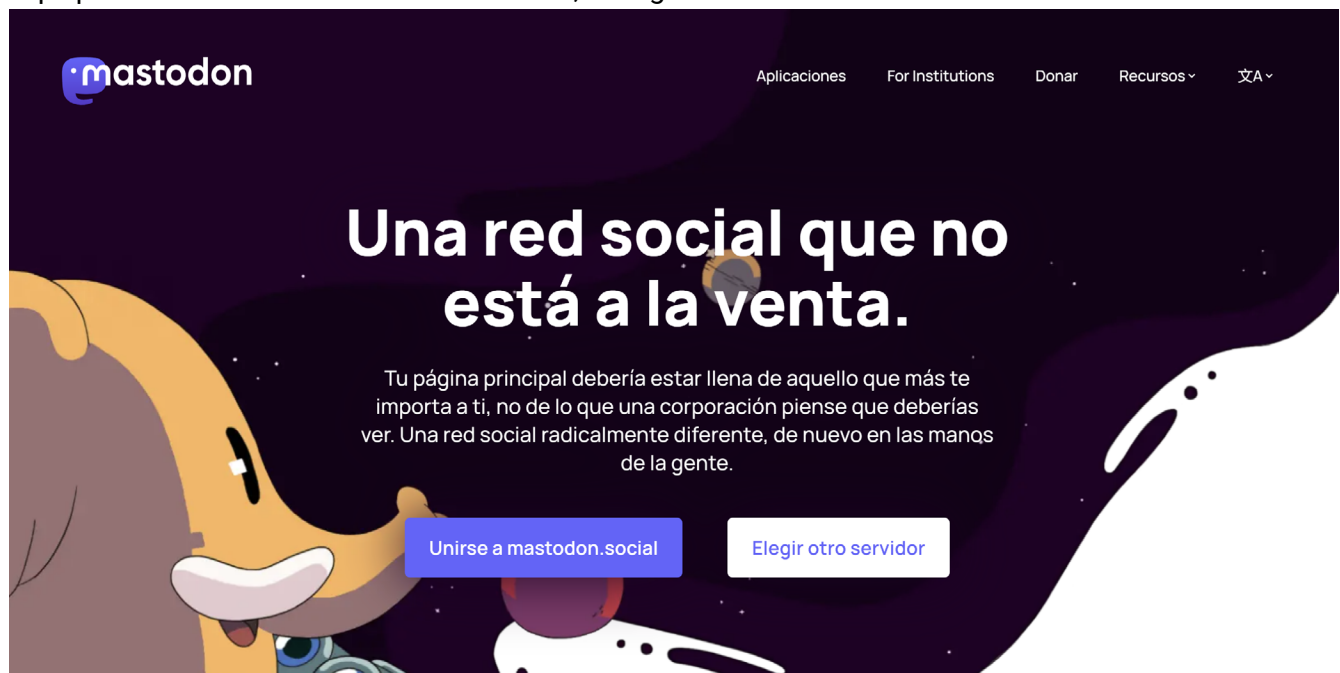


Figura 21. Interfaz de Mastodon.

Al igual que los blogs consisten en publicar actualizaciones en un sitio web, el microblogging consiste en publicar pequeñas actualizaciones en un flujo de actualizaciones en tu perfil. Puedes publicar entradas de texto y, opcionalmente, adjuntar archivos multimedia como imágenes, audio, vídeo o encuestas.

Al igual que en un sitio web tradicional, las personas usuarias se registran, publican mensajes, suben fotos y conversan entre ellas. A diferencia de un sitio web tradicional, los sitios web de Mastodon pueden interoperar, lo que permite a sus usuarios comunicarse entre sí; al igual que puedes enviar un correo electrónico desde tu cuenta de Gmail a alguien que utilice Outlook, Fastmail, Protonmail o cualquier otro proveedor de correo electrónico, siempre que conozcas su dirección de correo electrónico, puedes mencionar o enviar mensajes a cualquier persona en cualquier sitio web utilizando su dirección.

¿Por qué Mastodon?

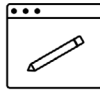
 Descentralizado La comunicación global instantánea es demasiado importante para pertenecer a una empresa. Cada servidor Mastodon es una entidad totalmente independiente, capaz de interactuar con otras para formar una red social global.	 Código abierto Mastodon es software gratuito y de código abierto. Creemos en su derecho a usar, copiar, estudiar y cambiar Mastodon como usted considere oportuno, y nos beneficiamos de las contribuciones de la comunidad.	 No a la venta Respetamos su independencia. Su página principal está supervisada y creada por usted. Nunca publicaremos anuncios ni anunciaremos perfiles para que pueda verlos, lo que significa que sus datos y su tiempo son suyos y solamente suyos.	 Interoperable Basado en protocolos web abiertos, Mastodon puede hablar con cualquier otra plataforma que implemente ActivityPub. Con una cuenta obtendrá acceso a todo un universo de aplicaciones sociales: el fediverso.
--	---	---	---

Figura 22. ¿Por qué usar Mastodon?

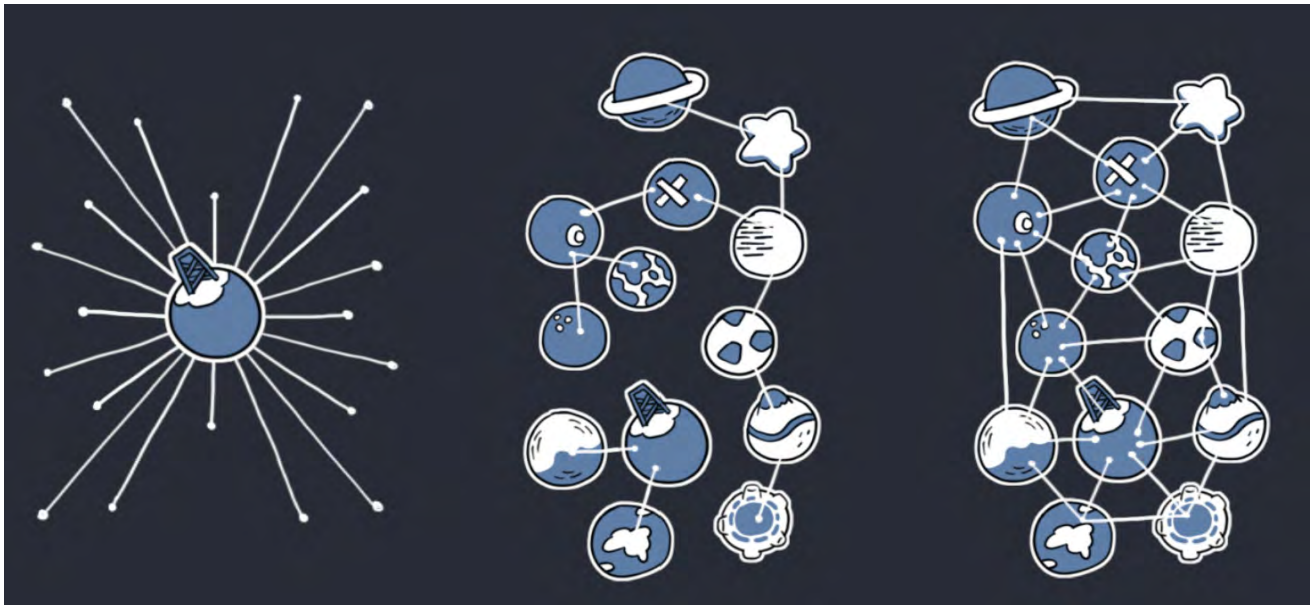


Figura 23. De izquierda a derecha: Centralizado, Federado, Distribuido. Tomado de: <https://docs.joinmastodon.org/>

Cuentas sugeridas en Mastodon social:

<https://mastodon.social/@derechosdigital>

<https://mastodon.social/@tedicpy>

<https://mastodon.social/@interferencias@social.interferencias.tech>

También puedes explorar mastodon.la

Fuente de profundización:

[Guía para comenzar a usar Mastodon - Laintersección](#)

TEMA 7: GOBERNANZA DE INTERNET Y JUSTICIA MEDIOAMBIENTAL

Internet y las tecnologías digitales no son neutras ni “inmateriales”: dependen de recursos naturales, energía, infraestructuras críticas y circuitos de producción que tienen impactos directos y concretos sobre los territorios. Este tema propone vincular la gobernanza de Internet con las luchas por la justicia medioambiental, visibilizando sus impactos ecológicos, formas de extractivismo digital³ y barreras que enfrentan pueblos originarios y comunidades rurales para participar en debates globales.

CAMBIO CLIMÁTICO Y TECNOLOGÍAS DIGITALES

Aunque muchas veces se vincula a Internet con soluciones sostenibles (como contribuir a la eficiencia energética o monitoreo ambiental), las tecnologías digitales tienen importantes costos ecológicos.

Los impactos medioambientales incluyen:

- Gran consumo energético de centros de datos y redes globales.
- La producción de dispositivos electrónicos que requieren minerales como el litio, cobalto y coltán, extraídos muchas veces en condiciones de explotación laboral y afectación ambiental
- La generación de residuos (“e-waste”), que en muchos casos son exportados a países del Sur Global, convirtiendo a ciertos territorios en vertederos tecnológicos.
- Infraestructuras como cables, antenas, o satélites, que afectan ecosistemas y territorios.

***Espacio de discusión:** ¿Cómo puede Internet formar parte de la solución climática sin reproducir las lógicas del extractivismo?*

Figura 24. Discusión

3. Extractivismo: modelo económico basado en la extracción intensiva de recursos naturales (minerales, petróleo, gas, madera, agrocommodities) para la exportación, con escasa transformación local y baja reinversión en comunidades. Suele generar ganancias concentradas, degradación ambiental, desplazamiento social y dependencia económica, al priorizar la extracción a corto plazo sobre la sostenibilidad y los derechos de poblaciones locales.

Extractivismo digital: transferencia del mismo patrón al mundo digital: recolección masiva y prolongada de datos, extracción de valor de la atención y comportamiento de las personas, y explotación de infraestructuras digitales sin compartir beneficios con las comunidades productoras. Produce dependencia tecnológica y económica, pérdida de soberanía sobre datos y plataformas, externalidades sociales (vigilancia, polarización) y erosión de capacidades locales para agregar valor.

EXTRACTIVISMO DIGITAL Y EXTRACCIÓN DE DATOS

Así como el extractivismo tradicional explota recursos naturales sin respeto por la vida o la autodeterminación de los pueblos, el extractivismo digital explota datos en formas problemáticas.

¿Qué es el extractivismo digital? Es un modelo basado en la recolección masiva de datos personales culturales y territoriales sin consentimiento ni beneficio para las comunidades. Son prácticas que afectan especialmente a pueblos originarios, comunidades rurales y activistas medioambientales.

Algunos ejemplos son:

- El uso de imágenes satelitales o drones para mapear territorios sin consulta previa
- Plataformas que se instalan con incentivos fiscales y alta demanda de recursos naturales (como agua y energía), especialmente en zonas empobrecidas.

PUEBLOS ORIGINARIOS: PARTICIPACIÓN E INCIDENCIA EN LA GOBERNANZA

A pesar de los fuertes impactos que las tecnologías tienen sobre sus territorios y culturas, los pueblos originarios enfrentan múltiples barreras para participar en procesos de gobernanza de Internet.

Algunas barreras comunes son:

- **Idioma y representación cultural**
- **Falta de acceso a conectividad** adecuada y significativa
- **Exclusión sistemática** de espacios técnicos o diplomáticos
- **Falta de consulta** libre, previa e informada sobre infraestructura digital.

Algunos ejemplos de estrategias y resistencias:

- **Alianzas con colectivos ecodigitales, feministas y de derechos humanos**

Existen colaboraciones entre movimientos feministas y pueblos indígenas para promover la igualdad de género y los derechos colectivos. Por ejemplo, en la Convención Constitucional de Chile de 2022, se **evidenció** la importancia del trabajo en red entre representantes de pueblos indígenas y movimientos feministas para plasmar un texto constitucional inclusivo. Sin embargo, se señaló la necesidad de una mayor interseccionalidad para integrar plenamente los derechos de las mujeres indígenas.

- **Redes comunitarias indígenas**

Telecomunicaciones Indígenas Comunitarias (**TIC-AC**) es una asociación civil mexicana conformada por comunidades indígenas y rurales. Desde 2016, han obtenido concesiones sociales para operar redes de telecomunicaciones autónomas en estados como Oaxaca, Guerrero, Puebla, Chiapas y Veracruz. Estas redes permiten a las comunidades gestionar su propia infraestructura de telefonía móvil e Internet, promoviendo la autonomía tecnológica y la preservación cultural.

- **Participación en foros de gobernanza**

Las comunidades indígenas han aumentado paulatinamente su participación en espacios de gobernanza de Internet, como el Foro de Gobernanza de Internet y su capítulo regional.

Recursos:

- Paz Peña Ochoa, [Libro](#) "Tecnologías para un planeta en llamas" y [keynote](#) "Hacer que la digitalización funcione para un desarrollo inclusivo y sostenible"
- ALAI y APC, [investigación](#) "Tecnología y medio ambiente: respuestas desde el Sur Global"
- [Telecomunicaciones Indígenas Comunitarias](#)
- Colnodo, Documental ["Redes Comunitarias"](#)
- APC, [Tecnología, justicia ambiental y sustentabilidad](#)
- APC, [artículo](#) "Sembrando cambios en 2023: El gran impacto comunitario de la red de APC"
- APC, [artículo](#) "Sembrando cambios: Sostenibilidad ambiental y la importancia de potenciar el liderazgo de las mujeres".
- Jess Ciacchi, Sursiendo, [artículo](#) "Imaginar un principio feminista para Internet que ponga en el centro a la justicia ambiental"

Figura 25. Recursos.

TEMA 8: GOBERNANZA DE PLATAFORMAS DIGITALES E IGUALDAD DE GÉNERO

Las plataformas digitales (redes sociales, buscadores, apps, marketplace) son espacios clave hoy en día para la vida social, económica y política. Pero no son neutrales: tienen reglas propias, algoritmos opacos, y políticas que muchas veces reproducen desigualdades y violencias estructurales. Este tema explora cómo se gobiernan las plataformas, como afectan de manera específica a mujeres y personas LGBTQ+, y que alternativas feministas proponen una Internet más justa, inclusiva y transformadora.

¿QUÉ ES LA GOBERNANZA DE PLATAFORMAS DIGITALES?

Las plataformas digitales (como TikTok, Facebook, Youtube, Instagram) son actores privados que deciden qué contenido se muestra o se elimina, que se promociona, qué es permitido o cuándo, y cómo se recolectan datos y el uso que se les da.

Modelos de gobernanza actuales:

- **Autorregulación:** las empresas definen sus propias reglas sin intervención estatal;
- **Co-regulación:** colaboración entre Estado y plataformas para regular ciertos contenidos o comportamientos;
- **Regulación estatal:** leyes que obligan a las plataformas a cumplir normas sobre moderación, transparencia o responsabilidad legal.

Algunos problemas o desafíos comunes son la **falta de transparencia** sobre cómo se moderan contenidos, la **censura desigual** (contenidos sobre derechos sexuales y reproductivos vs. discursos de odio) y reglas y algoritmos creados desde el Norte Global con **poca perspectiva local o interseccional**.

VIOLENCIA DE GÉNERO DIGITAL: UNA EXPRESIÓN ESTRUCTURAL

Las mujeres y disidencias de género enfrentan violencias específicas y sistemáticas en el entorno digital que reflejan y amplifican las violencias que ya existen en el mundo *fuera de línea*.

Tipos de violencia digital

- Acoso, amenazas, doxxing (difusión de datos personales con intención de daño).
- Censura selectiva de contenidos feministas.
- Deepfakes, el uso de IA para crear y difundir imágenes íntimas sin consentimiento.
- Algoritmos segmentados, excluyentes y la invisibilización de contenidos por parte de plataformas.
- Vigilancia y control, especialmente contra activistas, periodistas, mujeres en política, o lideresas comunitarias.

Los impactos de la violencia de género digital son muy graves, e incluyen el silenciamiento de voces críticas, autocensura y retraimiento del espacio público digital, mayor exposición y revictimización y obstáculos para la participación política y el ejercicio de derechos.

Desde [Fundación Karisma](#) (Colombia) y organizaciones como [Luchadoras](#) (México) hemos documentado como mujeres indígenas, afrodescendientes, o trans enfrentan formas específicas y agravadas de violencia digital, que combinan racismo, clasismo, misoginia, y homofobia.

FEMINISMO Y TECNOLOGIA: HACIA UNA INTERNET FEMINISTA

Frente a estos desafíos, organizaciones feministas y de derechos digitales han desarrollado propuestas y principios para construir tecnologías más justas, participativas y transformadoras.

Los **Principios Feministas para Internet** fueron desarrollados por un grupo de activistas y organizaciones de la sociedad civil convocadas por la Association for Progressive Communications (APC) a partir de 2014, durante un encuentro en Malasia, y se han ido ampliando y consolidando en encuentros posteriores.

Algunos de los principios relevantes a este tema son:

- **Acceso a Internet:** Una Internet feminista comienza con posibilitar que más mujeres y personas queer puedan disfrutar de un acceso universal, satisfactorio, accesible, sin condiciones, abierto, significativo e igualitario a Internet
- **Acceso a la información:** Apoyamos y protegemos el acceso irrestricto a información relevante para las mujeres y personas +queer, en particular información sobre temas de salud y derechos sexuales y reproductivos, placer, aborto seguro, acceso a la justicia y temas LGBTIQ.
- **Toma de decisiones en la gobernanza de Internet:** Estamos a favor de desafiar los espacios y procesos patriarcales que controlan la gobernanza de Internet, y de incluir a más feministas y personas queer en la toma de decisiones.
- **Economías alternativas:** Tenemos el compromiso de cuestionar la lógica capitalista que empuja a la tecnología hacia una mayor privatización, lucro y control corporativo. Trabajamos para crear formas alternativas de poder económico basadas en principios de cooperación, solidaridad, bienes comunes, sostenibilidad ambiental y apertura.
- **Libertad de expresión:** Defendemos el derecho a expresarnos sexualmente como una cuestión de libertad de expresión y de no menos importancia que la expresión política o religiosa. Nos oponemos radicalmente a todo esfuerzo por parte de actores estatales y no estatales de controlar, vigilar, regular y restringir la expresión feminista queer en Internet a través de tecnología, legislación o violencia.
- **Pornografía y “contenidos ofensivos”:** Reconocemos que el tema de la pornografía en línea tiene que ver con la agencia, el consentimiento, el poder y el trabajo. Rechazamos todo vínculo causal simple entre el consumo de contenidos pornográficos y la violencia contra las mujeres. También rechazamos la abarcadora expresión “contenido dañino” como etiqueta aplicable a la expresión de la sexualidad femenina y transgénero. Estamos a favor de reivindicar y crear contenido erótico alternativo que se oponga a la visión patriarcal dominante y que coloque los deseos de las mujeres y las personas queer en el centro.
- **Violencia en línea:** Llamamos a todas las partes interesadas de Internet, incluyendo usuarios/as, diseñadores/as de políticas y el sector privado, a abordar la cuestión del acoso en línea y la violencia relacionada con la tecnología. Los ataques, amenazas, intimidación y vigilancia que experimentan las mujeres y las personas queer son reales, dañinos y alarmantes, y son parte del problema más amplio de la violencia basada en el género. Es nuestra responsabilidad colectiva abordar y terminar con dicha violencia.

Actividad:

Identificar un problema concreto de la gobernanza de Internet que afecta a la comunidad (ej.: sesgos en IA, falta de conectividad, censura de contenidos feministas) y, desde una lógica feminista y de justicia de género, diseñar propuestas de reglas, prácticas y decisiones para enfrentarlo.

1. Elegir una problemática

A partir de lo trabajado en las actividades previas, selecciona un problema específico que quieras abordar. Ejemplos: violencia de género digital, censura de contenidos sobre derechos sexuales y reproductivos, sesgos de IA, vigilancia estatal.

2. Analizar el problema

Responda brevemente:

- ¿A quién afecta más y por qué?
- ¿Qué actores tienen poder en esta situación (gobierno, empresas, sociedad civil)?
- ¿Qué derechos están en juego?

3. Imaginar desde la justicia de género

Ahora van a diseñar cómo serían las reglas y las prácticas justas para enfrentar ese problema:

- **Reglas:** ¿Qué normas se necesitan (ej.: transparencia en algoritmos, reglas claras contra violencia digital)?
- **Prioridades:** ¿Qué se pondría en el centro (ej.: cuidado, inclusión, lenguas locales)?
- **Decisiones:** ¿Cómo se tomarían colectivamente (ej.: participación comunitaria, consultas abiertas)?
- **Tecnología:** si se usa, ¿qué criterios feministas debería cumplir (ej.: accesible, auditable, sin sesgos)?

4. Acción colectiva

Escribe una propuesta de incidencia realizable (ej.: campaña de sensibilización, alianza con una ONG, participación en una consulta pública).

Figura 26. Actividad

Recursos:

- [Principios Feministas para Internet](#)
- TEDIC, [Podcast](#) Libres y seguras en Internet, episodio 10, Violencia de género en línea
- TEDIC, [Informe](#) "Violencia de género facilitada por la tecnología a mujeres políticas en Paraguay"
- Luchadoras, [Guía](#) sobre violencia digital
- Fundación Karisma, [Artículo](#) "La participación política de las mujeres pasa por evitar la violencia digital"
- APC, [Informe](#) "Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género".
- Fundación Karisma, [Artículo](#) "Pueden las plataformas digitales ser aliados en la lucha contra la violencia digital?"
- APC, [Red](#) de Investigación por una Internet Feminista.

Figura 27. Recursos

CONCLUSIONES

Internet no es solo una herramienta: es un espacio donde se juegan poder, derechos y oportunidades. Su gobernanza no ocurre en un solo lugar ni la define un único actor; es el resultado de negociaciones y tensiones entre gobiernos, empresas, comunidades técnicas, sociedad civil y academia. Entender este entramado nos permite ver que las reglas de Internet no son neutrales y que la participación ciudadana es indispensable para que las decisiones no se concentren en unos pocos, sino que reflejen las necesidades y aspiraciones de la diversidad de comunidades que la habitan.

Lo que está en juego va mucho más allá de la dimensión técnica; cada política de conectividad, cada decisión sobre datos personales o cada norma sobre moderación de contenidos tiene un impacto directo en nuestras vidas. Allí se definen condiciones que afectan derechos fundamentales como la privacidad, la libertad de expresión, el acceso a la información y la no discriminación. Así que dejar estos debates únicamente en manos de actores poderosos, como gobiernos o empresas, puede reforzar desigualdades o legitimar prácticas de control. Por ende, participar en la gobernanza de Internet es una forma concreta de defender nuestros derechos en el entorno digital y garantizar que este espacio sirva al bien común.

En América Latina, los retos son aún mayores por las desigualdades estructurales que arrastramos desde hace siglos: las brechas de conectividad, el costo del acceso, la carencia de contenidos en lenguas locales y la exclusión de comunidades rurales e indígenas, evitan que Internet sea una herramienta para la inclusión. Sin embargo, también existen experiencias que nos muestran otros caminos como las redes comunitarias que fortalecen la autonomía tecnológica, las luchas feministas que exigen una Internet libre de violencia de género y colectivos sociales que llevan sus voces a espacios globales de incidencia; dichas iniciativas demuestran que, incluso en condiciones adversas, es posible generar alternativas que hagan de Internet un recurso más justo y equitativo.

En suma, este módulo nos enseña que Internet no es un espacio neutral, sino un campo de disputa política, social y cultural. En ese orden de ideas, para que sea verdaderamente abierto, inclusivo y democrático, se necesitan reglas claras, procesos transparentes y participación efectiva de la sociedad civil en todos los niveles de gobernanza. Solo así lograremos que la red contribuya a ampliar derechos, fortalecer la democracia y proteger nuestras comunidades y territorios. Por ello, participar no es un privilegio, sino un derecho y una responsabilidad compartida.

DIGITALIZACIÓN, GOBERNANZA Y PARTICIPACIÓN



CONTENIDO

✱ Introducción	106
✱ Objetivo general	108
✱ Objetivos específicos	108
✱ Unidad 1: La relación entre tecnología, estado y DDHH	109
• Tecnología, Estado y Derechos Humanos	109
• Teléfonos móviles y computadores: infraestructura, cobertura y acceso	112
✱ Unidad 2: Conceptos clave	115
• Transformación Digital	115
• Gobierno Digital	116
◦ Del gobierno electrónico a gobierno digital	116
• Ciudadanía Digital	118
• Digitalización	118
◦ Conceptos claves para entender la digitalización	119
◦ Autenticación	119
◦ Interoperabilidad	200
◦ Datos	201
• Nuestros derechos	202

 Unidad 3: Identidad digital y gobernanza de internet: de lo local a lo regional	203
• Identidad digital o Digital ID	203
◦ ¿Qué es la identidad legal?	203
◦ El ciclo de vida de la identidad	205
◦ El reconocimiento biométrico	206
◦ ¿Cómo puede afectar la autenticación mediante biometría a nuestros derechos?	206
• Ejemplos de sistemas de identidad en la región	207
◦ Clave Única en Chile	207
◦ ¿Qué beneficios tiene la Clave Única?	208
◦ ID Digital en Brasil	208
◦ Renaper en Argentina	300
• Desafíos y riesgos principales de los sistemas de identificación en la región	301
• Identidad digital y gobernanza de Internet	301
• Espacios de participación regional: LACIGF and Youth LACIGF	302
• Formas de contribución ciudadana	304
• Cierre del módulo: gobernanza y participación	306
• Actividad	306
• Recursos adicionales	306
• Referencias	307



INTRODUCCIÓN

En la actualidad, el Estado moviliza recursos tanto económicos como humanos para desarrollar procesos que pretenden “facilitar” la prestación de servicios ciudadanos a través de la digitalización de los mismos.

No obstante, los procesos de transformación digital en la administración pública suelen desarrollarse sin los espacios de participación ciudadana necesarios para asegurar su implementación, acceso y aprovechamiento: estos deben responder satisfactoriamente a las necesidades reales de la ciudadanía y contemplar los contextos económicos y culturales de comunidades vulnerables. En muchos casos, estas iniciativas terminan reproduciendo desigualdades existentes, pues no consideran brechas digitales como el acceso a la conectividad, las diferencias territoriales, las limitaciones de alfabetización digital o las condiciones de accesibilidad para poblaciones diversas.





Además, tienden a presentarse principalmente como respuestas tecnocráticas a los problemas de (in)eficiencia estatal, más que como oportunidades para fortalecer el vínculo cívico entre ciudadanía y Estado. De esta manera, el énfasis suele ponerse en indicadores de cobertura y velocidad de trámites, en lugar de la calidad democrática de los procesos y la garantía de derechos.

Por ello, resulta fundamental promover espacios de diálogo y reflexión crítica que nos permitan cuestionar qué entendemos por transformación y gobierno digital, cuál es su impacto en la relación cotidiana con el Estado y cómo aseguramos que estas políticas no solo agilicen procesos administrativos, sino que amplíen la participación, fortalezcan la confianza ciudadana y reconozcan la diversidad de experiencias digitales en el país. También implica identificar y usar las herramientas que tenemos a la mano: legales, tecnológicas y organizativas, para exigir que la digitalización sea un verdadero instrumento de inclusión y garantía de derechos, en lugar de una nueva forma de exclusión.

Finalmente, la forma en que se diseñan, regulan y administran estas iniciativas digitales se enmarca dentro de la gobernanza de Internet: un entramado de normas, decisiones y actores que inciden en cómo se construye, se accede y se utiliza la red -cómo vimos en el anterior módulo-. Esto implica reconocer que las políticas de transformación digital no son neutras, sino que responden a visiones específicas sobre qué lugar debe ocupar la tecnología en la vida social. Por eso, resulta clave que los principios de la gobernanza de Internet (participación multiactor, transparencia, inclusión y enfoque de derechos) también orienten la manera en que se conciben y ejecutan los servicios digitales estatales, asegurando que sean herramientas al servicio de las personas y no mecanismos que profundicen la desigualdad o la concentración de poder.

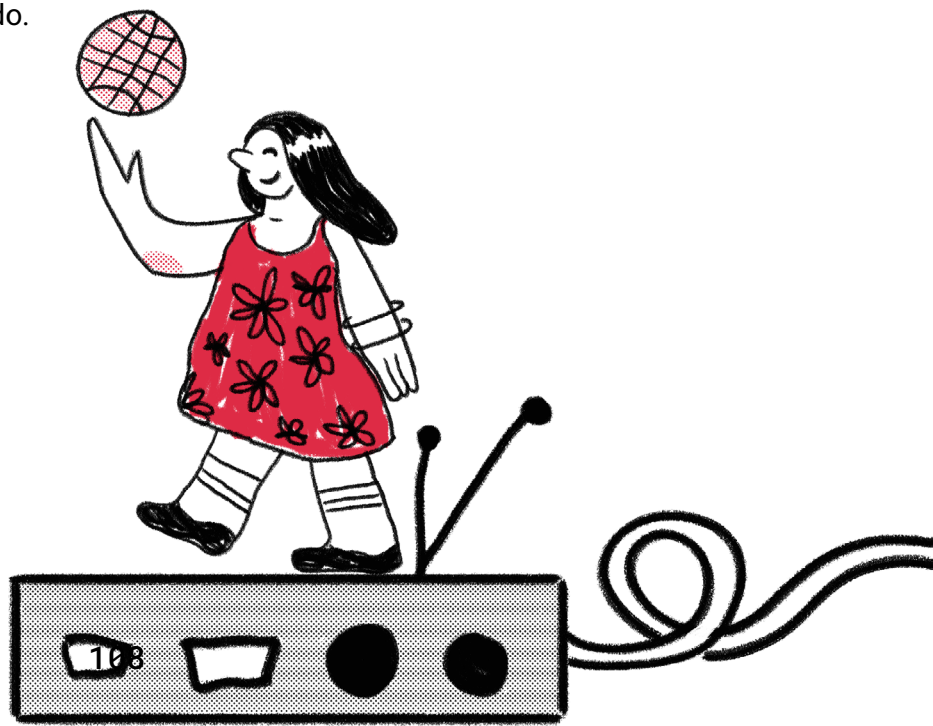
OBJETIVOS DEL MÓDULO

Objetivo general:

Fomentar la comprensión crítica y experiencial de la digitalización de trámites, información y servicios provistos por el Estado, promoviendo la garantía y el acceso a derechos.

Objetivos específicos:

- Comprender los conceptos clave y el contexto de la transformación y gobierno digital impulsada por los Estados.
- Identificar los principales desafíos y oportunidades que enfrentan los jóvenes, comunidades rurales y grupos en condición de vulnerabilidad en relación con la digitalización de los servicios ciudadanos.
- Relacionar los contextos de gobernanza de Internet con espacios de participación local y regional para promover los derechos humanos en contextos de digitalización de servicios provistos por el Estado.



UNIDAD I: LA RELACIÓN ENTRE TECNOLOGÍA, ESTADO Y DDHH

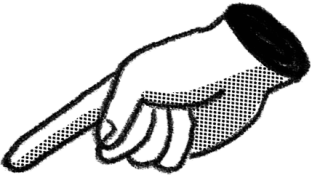
TECNOLOGÍA, ESTADO Y DERECHOS HUMANOS

La transformación digital ha cambiado la forma en que vivimos, trabajamos y nos relacionamos con el Estado. En Latinoamérica y el Caribe (de ahora en adelante LAC), el gobierno digital es una prioridad política desde hace casi 10 años, con avances desiguales entre países. Por ejemplo, la creación de la Estrategia Nacional de Gobierno Digital según cada país de la región:

País	Nombre de la estrategia (español)	Año
Argentina	Estrategia aplicada al Programa Federal de Transformación Pública Digital	2022
Barbados	Programa de Modernización del Sector	2019
Bolivia	Público Plan de implementación de gobierno electrónico 2017 -2025	2017
Brasil	Estrategia de Gobierno Digital / Estratégia de Governo Digital - 2020 a 2023*	2020
Chile	Estrategia de Transformación Digital del Estado	2019
Colombia	Política de Gobierno Digital (2022)	2022
Costa Rica	Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0	2018
República Dominicana	Agenda Digital 2030 - Eje de Gobierno Digital	2022
Ecuador	Plan Nacional de Gobierno Electronico 2018-2021	2018
México	Estrategia Digital Nacional 2021-2024 - Línea de acción: Política Digital en la Administración Pública Federal	2021
Panamá	Agenda Digital Nacional 2022 - Facilitadores Transversales del Gobierno Digital	2022
Paraguay	Agenda Digital - Componente: Gobierno Digital	2019
Perú	1. Política General del Gobierno 2021-2026 - Eje 8: Gobierno y transformación digital con equidad. 2. Reglamento de la Ley de Gobierno Digital	2018 y 2021
Trinidad y Tobago	Plan Estratégico de las TIC 2018 - 2022 - Estrategias de Gobierno Digital	2018
Uruguay	Plan de Gobierno Digital 2025	2021
Venezuela	Plan Nacional de Gobierno Electronico 2014-2019	2014

Figura 1. Estrategias Nacionales de Gobierno Digital (ENGD) en ALC (2022)

Nota. Tomado de Revisión del Gobierno Digital en América Latina y el Caribe: *Construyendo servicios públicos inclusivos y responsivos* (p. 48), por OECD/CAF, 2024, OECD Publishing. Recuperado el 8 de septiembre de 2025, de https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-america-latina-y-el-caribe_7a127615-es.html



La forma en que se diseñan, regulan y administran estas políticas se inserta en el marco de la **gobernanza de Internet**, ya que son un conjunto de procesos y reglas que determinan cómo usamos y gestionamos la red. Estas deben garantizar que la tecnología esté al servicio de las personas y no al revés.

La relación entre tecnologías (en este caso digitales) y el Estado empieza con un movimiento global de **transformación digital**, resultado de la consolidación de los sistemas de información y la implementación de procesos digitalización en las entidades públicas y privadas, con el interés de mejorar procesos haciéndolos más eficientes.

Este concepto —que se desarrolla en la unidad de conceptos clave— significa también un momento de transición que permite pensar cuál es la manera en la que queremos que esos procesos se den y si realmente están garantizando nuestra autonomía y derechos.

Por eso, la integración de tecnologías digitales a procesos de gestión estatal y digitalización de servicios provistos por el Estado necesita considerar marcos internacionales de derechos humanos, los cuales son obligaciones asumidas por cada Estado bajo los instrumentos internacionales.

Esto implica incorporar de manera clara y efectiva, a la legislación interna, los derechos y deberes reconocidos en tratados internacionales como la **Convención Americana sobre Derechos Humanos (CADH)**, el **Protocolo de San Salvador** y la jurisprudencia de la **Corte Interamericana de Derechos Humanos**, los cuales establecen que las políticas públicas —incluyendo el uso de tecnologías como la inteligencia artificial— deben respetar los principios de **legalidad, necesidad y proporcionalidad**.

LEGALIDAD: Significa que toda acción debe estar respaldada por las leyes y normativas vigentes.	NECESIDAD: Debe usarse solo cuando realmente aporta un beneficio que no se puede conseguir de otra manera más sencilla o accesible.	PROPORCIONALIDAD: Debe estar equilibrado: no debe causar más problemas que beneficios.
---	---	--

Figura 2. Principios de legalidad, necesidad y proporcionalidad.

Estos criterios son **esenciales** para garantizar que la adopción de herramientas digitales y automatizadas no vulnere nuestros derechos.

En este sentido, documentos como la **Resolución A/HRC/RES/48/4 del Consejo de Derechos Humanos** refuerzan la necesidad de que los Estados integren dichos principios en el diseño e implementación de sus marcos normativos y políticas tecnológicas.

MATERIAL DE ADICIONAL O DE PROFUNDIZACIÓN:

- ✱ [Convención Americana sobre Derechos Humanos](#). Interpretada e ilustrada por y para niños, niñas y adolescentes de América Latina y el Caribe.
- ✱ [¿Qué es el Protocolo de San Salvador?](#)
- ✱ [¿Qué es la Corte IDH?](#)
- ✱ [A/HRC/RES/48/4 Asamblea General](#)



Para comprender la relación entre tecnología, Estado y derechos humanos es importante considerar los siguientes aspectos:

1. **Características sociodemográficas y tecnológicas** del país donde se están implementando y/o generando. Por ejemplo: la distribución de la población, el acceso a las tecnologías y las condiciones socioeconómicas que lo determinan.
2. **Contexto regulatorio e institucional** de cada país, en particular, leyes de protección de datos personales y acceso a la información pública.
3. **Infraestructura y características técnicas y funcionales** que permiten el uso de tecnologías específicas en la región.
4. **Procesos de participación** que permitan a las personas involucradas ser escuchadas no solo en la construcción, sino también en las acciones y planes que las afecten directa o indirectamente.

Además, hay desafíos permanentes en relación al Estado como regulador en aspectos relacionados con: la protección de datos, el acceso a la información, las regulaciones sobre ciberseguridad, vigilancia de las comunicaciones, identificación e interoperabilidad, entre otros temas. Por ejemplo, en Colombia es habitual la dependencia del Estado a empresas extranjeras como IDEMIA, multinacional francesa dedicada al desarrollo de tecnologías para la identificación oficial. También hay desafíos que provienen de tecnologías disruptivas y un modelo de innovación no regulado como por ejemplo, el servicio de verificación de identidad por parte de Worldcoin en [México](#), [Chile](#) y [otros países de la región](#).

En LAC hay varios espacios de discusión sobre la relación entre Estado, derechos humanos y tecnología que va de la mano con la gobernanza de Internet, como se vio en el módulo anterior.

PREGUNTA ACTIVADORA:

¿Cómo ves la relación entre tecnología, estado y derechos humanos en tu país?

TELÉFONOS MÓVILES¹ Y COMPUTADORES: INFRAESTRUCTURA, COBERTURA Y ACCESO

Los teléfonos móviles y computadores no sólo sirven para comunicarnos por medio de apps de mensajería y redes sociales, son las herramientas físicas a través de las cuáles también ejercemos la ciudadanía digital; es decir, cuando usamos estos dispositivos podemos también ejercer y promover la garantía de nuestros derechos. Si bien los dispositivos son esenciales, para que puedan funcionar y desarrollar todo su potencial requieren de infraestructura: redes eléctricas, redes de conectividad, centros de datos, antenas y puntos de intercambio. El despliegue de esta tecnología es un medio para medir qué tan sólida es la infraestructura, la cobertura y el acceso a Internet.

Por ejemplo:

Este es un mapa de calor que muestra la cobertura móvil 5G de Movistar² en Bogotá, Colombia:

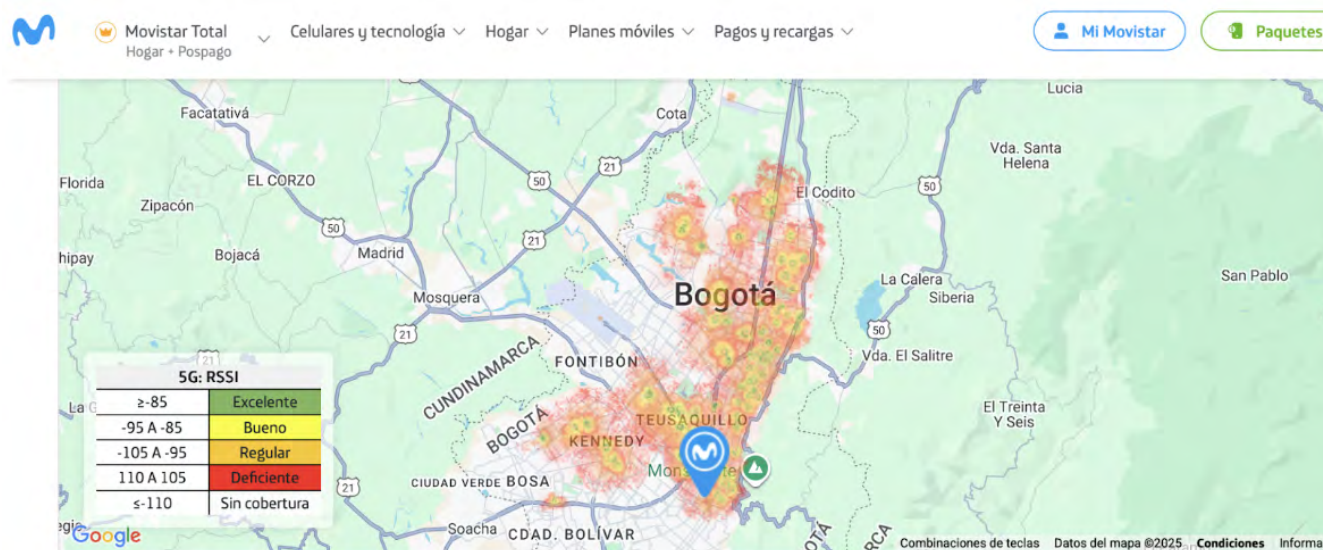


Figura 3. Cobertura móvil 5G de Movistar en Bogotá

Tomado de Movistar. (s.f.). Mapa de Cobertura Móvil 5G. movistar.
<https://www.movistar.com.co/mapa-de-cobertura-movil>

1. Celular en Colombia, Móvil en Argentina, etc.

2. La cual es una aproximación teórica de la cobertura a la realidad pues depende de la zona, tráfico, topología del terreno.

Y, esta es en Montería, Colombia, del mismo operador y red:

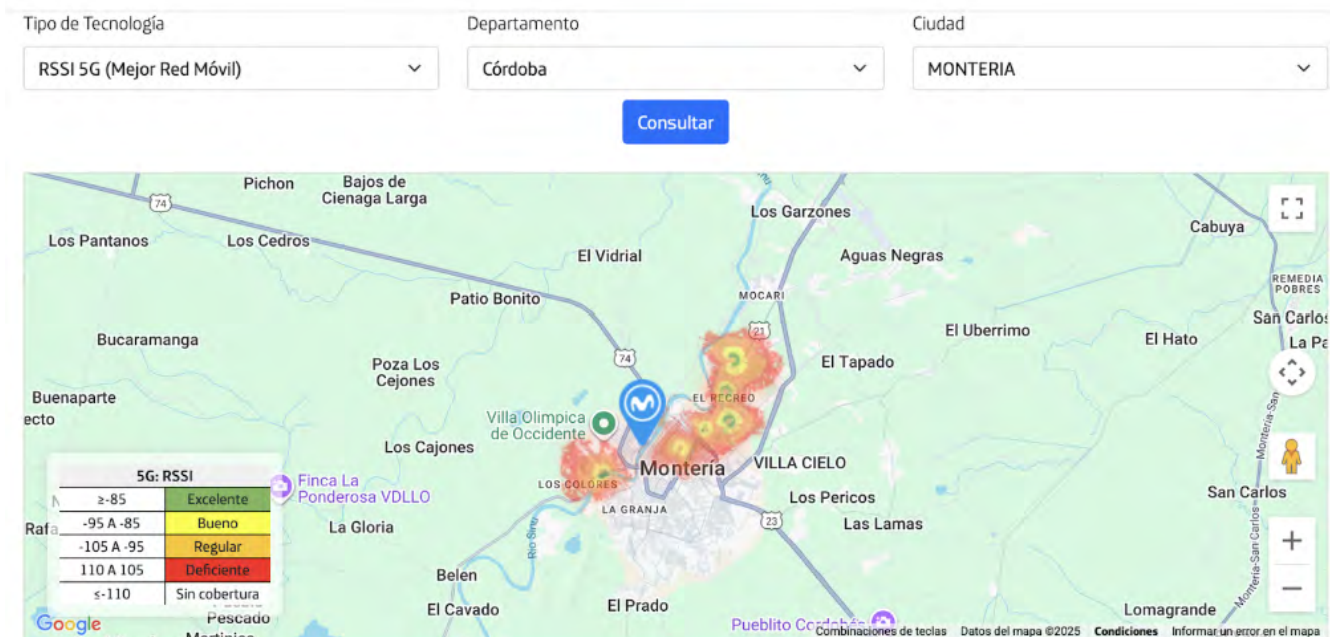


Figura 4. Cobertura móvil 5G de Movistar Montería, Córdoba.

Tomado de Movistar. (s.f.). Mapa de Cobertura Móvil 5G. Movistar.
<https://www.movistar.com.co/mapa-de-cobertura-movil>

La forma en que se decide dónde instalar infraestructura depende de cuánta gente vive en el lugar, las características del territorio y de si a las empresas les resulta rentable invertir allí. Por eso, para que se pueda llegar más lejos, es necesario que el Estado participe ofreciendo reglas claras e incentivos. Aun así, la realidad es que las redes en zonas rurales o marginadas no tienen la misma calidad que las de las ciudades con mejores condiciones económicas.

Si bien Movistar solo tiene cobertura del 55,4% en Colombia, el informe³ sobre el estado de la infraestructura y cobertura de los servicios móviles en el país (para junio del 2024) evidencia cómo puede variar el acceso y la infraestructura según el lugar donde nos encontremos.

En ese sentido, las telecomunicaciones desempeñan un papel fundamental para ejercer espacios de participación y gobernanza de Internet. En muchas zonas de los países de LAC el celular/teléfono móvil es el principal, por no decir que el único, medio de conexión a Internet. Este dispositivo puede presentar limitaciones técnicas (algunos dispositivos tienen baja capacidad de almacenamiento y limitadas actualizaciones) y situaciones de vulnerabilidad en términos de seguridad digital, sin embargo, es una herramienta que permite amplificar y consolidar también la comunidad y conexión entre causas.

3. <https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-analisis-sobre-infraestructura-y-cobertura-movil-en>

Mencionado esto, también es importante indicar que tener acceso a la tecnología (por ejemplo a celulares) no significa que automáticamente se produzca una transformación si las personas no saben usarla para ejercer sus derechos. A esto se suman otros problemas que plantea la digitalización, por ejemplo:

Falta de competencias digitales: Muchas personas usan la tecnología solo para entretenimiento, no saben cómo proteger sus datos, acceder a información pública, o hacer trámites en línea. Esto limita el uso de la digitalización como herramienta de empoderamiento.

Desigualdades de género y edad: En muchos contextos, las mujeres, personas mayores o con discapacidad enfrentan barreras adicionales en el acceso y uso de lo digital. Esto refuerza desigualdades ya existentes en vez de reducirlas.

Precarización laboral: La digitalización y automatización pueden desplazar empleos tradicionales sin que existan suficientes políticas de transición. Además, el trabajo en plataformas digitales muchas veces se caracteriza por la falta de derechos laborales.

En la práctica, cualquier debate sobre acceso universal o inclusión digital en la gobernanza de Internet depende de la disponibilidad, asequibilidad y capacidad de uso de estos dispositivos. Son el canal por el que se materializan las decisiones sobre acceso, neutralidad, seguridad y derechos digitales.

DISPONIBILIDAD: Se refiere a la existencia física y técnica de la infraestructura y dispositivos necesarios para conectarse a Internet.	ASEQUIBILIDAD: Se relaciona con la capacidad económica de las personas para costear el acceso.	CAPACIDAD: Es la habilidad efectiva de las personas para utilizar los dispositivos y servicios digitales de manera significativa.
---	--	---

Figura 5. Definición de disponibilidad, asequibilidad y capacidad.



UNIDAD 2: CONCEPTOS CLAVE

TRANSFORMACIÓN DIGITAL

Puede entenderse como el proceso de transición de la manera en la que realizamos trámites y gestionamos procesos en distintos ámbitos de la vida en sociedad. Implica pasar de prácticas físicas o en papel, a soluciones digitales, incorporando herramientas tecnológicas, mejorando la conectividad, modernizando la infraestructura de telecomunicaciones y fomentando la innovación en personas, empresas y gobiernos.

Sin embargo, este proceso puede excluir a: personas adultas mayores que no manejan medios digitales, comunidades rurales sin conectividad, mujeres en situación de pobreza que dependen de equipos heredados, entre otros sectores. Todas ellas suelen quedar fuera de los beneficios que promete la digitalización.

Un caso de América Latina

En varios países de la región, los sistemas de salud han incorporado historias clínicas electrónicas y citas en línea. Un hospital público, por ejemplo, puede reemplazar los expedientes en papel por un sistema digital en el que el médico consulta antecedentes desde una tablet mientras el paciente agenda su cita a través de una aplicación y recibe recordatorios por SMS. Esto agiliza la atención, evita la pérdida de información y abre la posibilidad de teleconsultas, especialmente útiles para comunidades rurales con conectividad mejorada.

En ese sentido, cada país cuenta con su propia estrategia de transformación digital.

Aquí puedes encontrar algunos ejemplos de la región:



México
[IDDE 2023.](#)



Uruguay
[Uruguay Digital.](#)



Perú
[Política Nacional de Transformación Digital.](#)



Colombia
[Estrategia Nacional Digital de Colombia.](#)

Con la pandemia de COVID-19 se aceleró la adopción de servicios digitales y la transformación digital se convirtió en el lema de diferentes apuestas de política pública para generar un modelo de gobierno más accesible y eficiente.

GOBIERNO DIGITAL

Cuando hablamos de **gobierno digital** nos referimos a una serie de políticas, iniciativas, estrategias, procesos y narrativas que se refieren a la prestación de servicios por parte de las entidades del Estado a través del uso y aprovechamiento de las Tecnologías de la información y la Comunicación (TIC). Esto incluye un marco de gobernanza para la adecuada gestión de servicios digitales, identidad digital, interoperabilidad y seguridad digital.

Para el caso de Latinoamérica

Un ejemplo de gobierno digital es la ventanilla única en línea, donde los ciudadanos pueden realizar trámites como pago de impuestos o registro de negocios, entre otros servicios. A través de una página web o una aplicación, las personas presentan sus solicitudes y realizan pagos, autenticándose con su identidad digital. Además, sistemas interoperables comparten información entre la secretaría de hacienda y urbanismo para validar datos sin que el ciudadano tenga que presentar papeles. Esto podría reducir las visitas presenciales, acelerar procesos y mejorar la transparencia, pero también puede crear inconvenientes, barreras y dificultades.

Para comprender mejor el ejemplo anterior creemos importante aclarar las diferencias entre **gobierno electrónico** y **gobierno digital a continuación**.



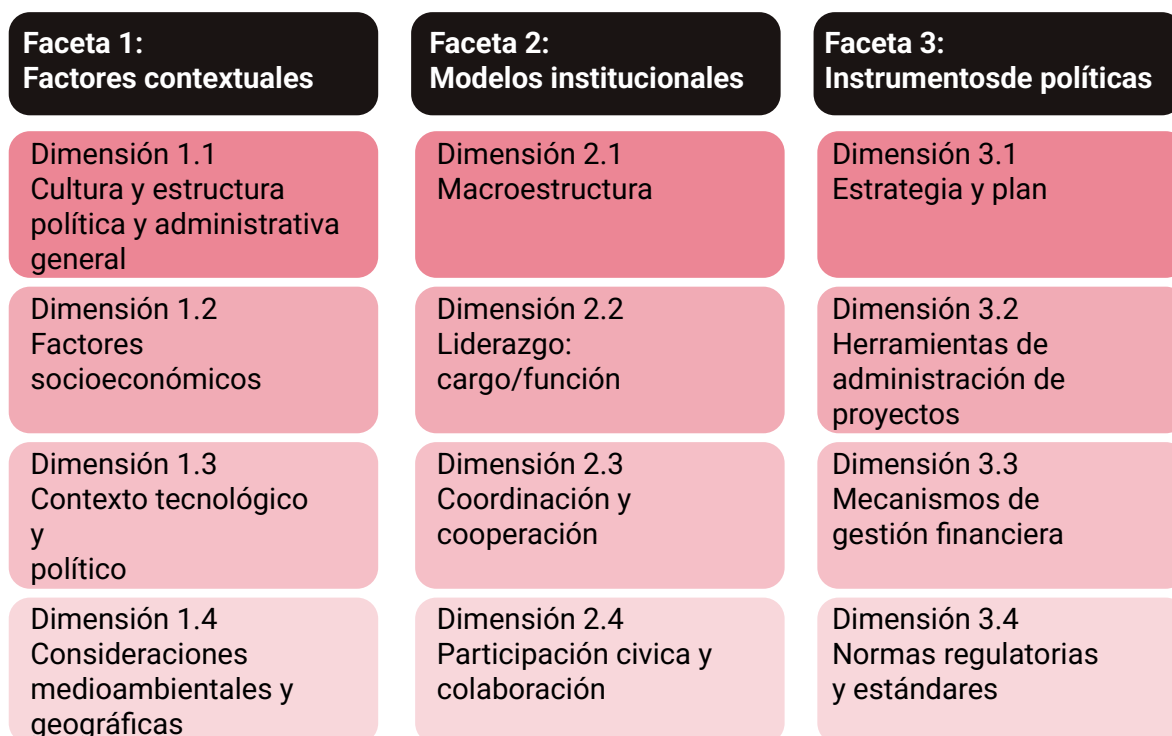
DEL GOBIERNO ELECTRÓNICO A GOBIERNO DIGITAL

El **gobierno electrónico** y el **gobierno digital** están estrechamente relacionados, pero representan etapas y enfoques distintos. El primero se centra en **digitalizar procesos existentes**, trasladando trámites y servicios tradicionales a canales en línea para ganar eficiencia, transparencia y rapidez, sin alterar sustancialmente la lógica administrativa que los sustenta.

En cambio, el **gobierno digital** implica un **cambio más profundo y estratégico**: utiliza tecnologías y datos para rediseñar las políticas, los servicios y las interacciones con la ciudadanía, priorizando un enfoque centrado en las personas, la proactividad, la integración entre instituciones y el uso ético de la información. Mientras el gobierno electrónico es, en gran medida, una “traducción digital” de lo analógico, el gobierno digital es **una reinención del Estado en la era digital**, donde la tecnología no es un fin en sí mismo, sino un medio para construir servicios inclusivos, coherentes e innovadores⁴.

Fuente: OCDE (2021[3]), The E-Leaders Handbook on the Governance of Digital Government,

4. <https://biblioguias.cepal.org/gobierno-digital/definiciones>



<https://doi.org/10.1787/ac7f2531-en>

Figura 6. Marco de la OCDE para la gobernanza del gobierno digital
Tomado de Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo servicios públicos inclusivos y responsivos (p. 29), por OECD/CAF, 2024, OECD Publishing. Recuperado el 8 de septiembre de 2025, de https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-america-latina-y-el-caribe_7a127615-es.html

CIUDADANÍA DIGITAL

Es el conjunto de **derechos, responsabilidades y prácticas** que permiten a las personas participar en la vida pública, social, económica y cultural a través de medios digitales.

En el contexto del informe Revisión del Gobierno Digital en América Latina y el Caribe de la OCDE/CAF (2024)⁵, la ciudadanía digital está vinculada a la capacidad de cada persona para:

- **Acceder** a las tecnologías e Internet de forma equitativa y continua.
- **Usar** servicios públicos digitales (como identidad digital, portales de trámites o datos abiertos) para ejercer derechos y cumplir obligaciones.
- **Participar** en procesos democráticos y de toma de decisiones en línea (consultas, presupuestos participativos, plataformas ciudadanas).
- **Protegerse** y actuar con responsabilidad en entornos digitales, cuidando la privacidad, la seguridad y la libertad de expresión.
- **Contribuir** a los servicios, políticas y soluciones digitales que respondan a necesidades colectivas.

En resumen, ser ciudadano digital no es solo **tener acceso a Internet**, sino **poder ejercer la ciudadanía plena** en el espacio digital con las habilidades, el conocimiento y las condiciones que garanticen inclusión, seguridad y participación efectiva.

APRENDE MÁS DE CIUDADANÍA DIGITAL CON ESTE VIDEO:

[¿Qué es la Ciudadanía Digital?](#)

DIGITALIZACIÓN

La digitalización se refiere al proceso de desarrollar o convertir información en formato digital, es decir, transformar datos, documentos y procesos que antes eran analógicos en formatos digitales accesibles y manejables.

La **digitalización en el Estado** implica que las instituciones públicas cuenten con **métodos seguros de identificación (autenticación)**, puedan **compartir información entre ellas sin barreras (interoperabilidad)** y gestionen los **datos de forma ética y estratégica**.

5. OECD/CAF (2024), Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos, OECD Publishing, Paris, <https://doi.org/10.1787/7a127615-es>.

CONCEPTOS CLAVES PARA ENTENDER LA DIGITALIZACIÓN

Autenticación

Es el conjunto de mecanismos que permiten verificar la identidad de una persona cuando accede a un servicio digital del Estado. Generalmente, la autenticación se realiza a través de tres posibles factores: **algo que conozco** (por ejemplo, una contraseña o PIN), **algo que poseo** (como un token, tarjeta o celular) o **una característica física** (huella digital, reconocimiento facial u otra forma de biometría).

Objetivo: garantizar que quien accede es realmente quien dice ser, protegiendo la privacidad del ciudadano.

Beneficios: evita fraudes y permite que trámites y servicios se realicen de forma segura en línea.

Barreras y retos:

1. No todos los sistemas de las distintas entidades estatales utilizan los mismos estándares, lo que dificulta la integración de mecanismos de autenticación unificados.
2. Los factores de autenticación basados en algo que se posee (celular, token, tarjeta) requieren que las personas dispongan de esos medios, lo que puede excluir a personas sin acceso a determinados dispositivos.
3. Personas con discapacidad visual, motriz o auditiva pueden enfrentar dificultades si las soluciones no contemplan medidas de accesibilidad.
4. Adquirir dispositivos compatibles o mantener conexión a Internet puede ser una carga económica para algunas personas.

Interoperabilidad

Significa que los sistemas y bases de datos de distintas instituciones públicas pueden “hablar” entre sí y compartir información de forma segura y estandarizada. Por ejemplo, que el Sistema de Registro Civil, la autoridad tributaria y el Ministerio de Salud puedan intercambiar datos sin que el ciudadano tenga que aportar varias veces la misma información.

Objetivo: mejorar la eficiencia administrativa, reducir duplicidades y agilizar los trámites.

Beneficio: menos burocracia para las personas y mejor coordinación entre organismos.

Barreras/retos:

1. Muchos servicios en LAC se diseñan pensando en mantener la burocracia y no son optimizados para el usuario. Falta investigación para conocer necesidades reales.
2. Cada institución puede usar diferentes formatos, lenguajes de programación y protocolos, lo que dificulta la integración.
3. No siempre existe un marco legal claro que habilite compartir datos entre organismos.
4. Se deben garantizar procesos de anonimización⁶ de la información cuando se comparta información entre entidades.

Tipos de interoperabilidad

Interoperabilidad técnica: significa que los sistemas de distintas instituciones pueden conectarse porque usan herramientas compatibles.

- API (interfaz de programación de aplicaciones): son los “traductores” que permiten que un programa hable con otro aunque estén hechos de forma distinta.
- Plataformas comunes: son espacios o sistemas compartidos donde varias instituciones pueden trabajar y usar la misma información.

Interoperabilidad semántica: definiciones, metadatos y esquemas de clasificación comunes para que los datos tengan el mismo significado en todos los contextos.

Interoperabilidad organizacional: roles, responsabilidades y flujos de trabajo alineados para el intercambio de datos.

Interoperabilidad legal: marcos normativos armonizados que permitan compartir datos de forma segura y conforme a la ley.

6. La anonimización puede entenderse como “ponerle máscara a los datos”, se ve la información, pero no la identidad. Es el proceso de quitar o cambiar los datos personales (nombre, dirección, foto, etc.) para que no se pueda identificar a una persona.

Datos

Se refiere a cómo el Estado genera, almacena, gestiona, comparte y utiliza la información que recoge en el ejercicio de sus funciones.

Incluye:

- **Gobernanza de datos:** normas y roles para administrarlos.
- **Datos abiertos:** información pública disponible para ciudadanos y empresas.
- **Protección de datos personales:** garantías para mantener el derecho a la privacidad.

Objetivo: usar los datos como recurso estratégico para diseñar políticas, evaluar servicios y tomar decisiones basadas en evidencia.

Beneficio: políticas públicas más efectivas y servicios más adaptados a las necesidades reales.

Barreras/retos:

1. Fragmentación institucional: diferentes entidades almacenan datos en sistemas no compatibles o aislados.
2. Calidad y actualización: información incompleta, duplicada o desactualizada reduce la confianza y utilidad de los datos.
3. Capacidades limitadas: falta de formación técnica en servidores públicos para gestionar y analizar grandes volúmenes de datos.
4. Resistencia cultural: miedo a compartir información entre instituciones o temor a perder control sobre ella.
5. Brechas tecnológicas: infraestructura digital insuficiente o desigual entre regiones.
6. Protección y confianza ciudadana: riesgos de mal uso o filtración de datos personales que generan desconfianza en los servicios digitales del Estado.

NUESTROS DERECHOS

En los últimos años, muchos trámites y servicios públicos como solicitar un documento de identidad, inscribirse a programas sociales o pagar impuestos han pasado de ser presenciales a gestionarse en línea. Esto ha mejorado la eficiencia y ha facilitado el acceso para millones de personas, pero también ha traído nuevos desafíos.

Piensa en una persona que intenta registrarse en un servicio público digital, pero el sistema no reconoce su documento por un error en la base de datos. O en un algoritmo que aprueba o rechaza solicitudes de forma automática, sin que la persona sepa cómo se tomó esa decisión.

Cuando digitalizamos servicios ciudadanos, debemos asegurarnos de que se respeten derechos fundamentales como:

- **Privacidad:** proteger los datos personales y evitar usos indebidos.

Ejemplo: cuando un sistema de salud en línea almacena la historia clínica de un paciente, debe garantizar que solo médicos autorizados puedan acceder y que no se utilice para discriminarlo en otras circunstancias como al momento de adquirir un seguro u obtener un empleo.

- **Acceso** a la información: garantizar transparencia y rendición de cuentas.

Ejemplo: una persona natural debería poder consultar en un portal oficial cuánto presupuesto se asigna a un programa social y en qué se gasta, sin barreras técnicas ni burocráticas.

- **No discriminación:** prevenir sesgos en sistemas y algoritmos.

Ejemplo: si un algoritmo que asigna becas universitarias da prioridad a ciertos perfiles por sesgos en los datos (como género o lugar de residencia), estaría reproduciendo desigualdades, en lugar de reducirlas.

- **Debido proceso:** ofrecer canales claros para impugnar decisiones automatizadas.

Ejemplo: si una persona es rechazada automáticamente en la inscripción a un subsidio, debe tener la posibilidad de apelar, entender la razón de la exclusión y que una persona funcionaria revise su caso de ser necesario.

La digitalización no es solo un cambio tecnológico, es un cambio social y político. Como jóvenes, ciudadanos y futuros profesionales tenemos un papel activo en exigir y construir un ecosistema digital que sea seguro, inclusivo y respetuoso con los derechos de todas las personas.



MATERIAL PARA PROFUNDIZAR:

✱ [Estándares de derechos humanos para el uso estatal de la IA en América Latina.](#)

UNIDAD 3: IDENTIDAD DIGITAL Y GOBERNANZA DE INTERNET: DE LO LOCAL A LO REGIONAL

IDENTIDAD DIGITAL O DIGITAL ID

Los sistemas de identidad son construcciones institucionalizadas que recogen características individuales predeterminadas por una autoridad para un fin concreto (puedes explorar más este tema en nuestro micrositio [ID Colombia](#)).

Las tecnologías digitales ofrecieron nuevas formas de construir esas identidades y nuevas posibilidades de conectar múltiples bases de datos a un individuo único. Aunque estos perfiles podrían utilizarse para garantizar los derechos humanos, estas herramientas también podrían utilizarse para discriminar sistemáticamente y ejercer violencia.

La creación de un sistema de identidad digital debe estar guiada por principios democráticos que permitan la inclusión social y la construcción de la confianza colectiva. Por ello, estos sistemas deben ser inclusivos, evitar la discriminación, proteger la privacidad, ser autosostenibles y estar diseñados con legalidad.

¿QUÉ ES LA IDENTIDAD LEGAL?

La identidad se refiere a una combinación de las características que hacen única a una persona en un contexto determinado. Específicamente, la identidad legal es el reconocimiento legal de una persona como sujeto de derechos y deberes por parte de un Estado.

La identidad legal es reconocida como un derecho humano por el artículo 6 de la Declaración Universal de los Derechos Humanos. Asimismo, las Naciones Unidas incluyeron en los Objetivos de Desarrollo Sostenible la meta 16:9 la cual busca “de aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos”.

Los sistemas de identidad tratan de recolectar y validar los atributos que hacen única a una persona siguiendo sus principales eventos vitales (nacimiento, adopción, matrimonio, muerte, etc.). En otras palabras, los **sistemas de identidad** son los que hacen **operable la identidad legal** de una persona.

Los sistemas de identidad tienen tres roles principales:

- **Identificación** - ¿Quién eres?: Proceso por el cual una autoridad establece la identidad de una persona recolectando y validando la información relevante de ella. Por ejemplo, la identificación en Colombia sucede con la recopilación de información para producir la tarjeta de identidad o la cédula. Los datos que se recogen son, entre otros, fotografía, características físicas y firma.
- **Autenticación** - ¿Eres quién dices ser?: Proceso mediante el que se comprueba que una persona que reclama una identidad es la misma inscrita en el sistema con la información recolectada en el proceso de identificación. Por ejemplo, las notarías en Colombia autentican con la huella digital, el método para validar la identidad de una persona que firma una escritura para vender una casa que está a su nombre. En Chile el Estado ofrece la Clave Única, una contraseña personal que permite autenticar a los ciudadanos para acceder a servicios públicos digitales como salud, educación y trámites legales. En Brasil, el sistema de Cadastro de Pessoas Físicas (CPF) se complementa con la autenticación biométrica (huella y reconocimiento facial) para acceder a servicios bancarios, votar de manera electrónica y validar trámites oficiales.
- **Autorización** - ¿eres elegible para este servicio? : Proceso por el cuál se determina si una persona puede acceder a un servicio y qué permisos tiene dentro de este. Por ejemplo, cuando para la entrega de subsidios la entidad que los administra comprueba que la persona esté inscrita y aparece como beneficiaria de los programas sociales.

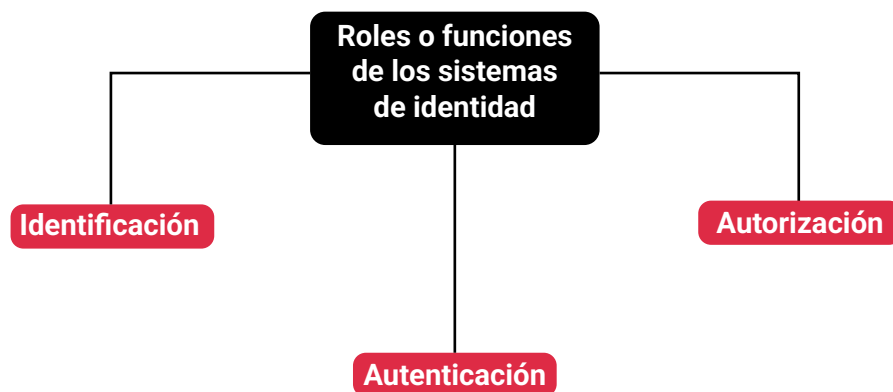


Figura 7. Roles o funciones de los sistemas de identidad
Tomado de Fundación Karisma. (2021, 7 de diciembre). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Recuperado el 8 de septiembre de 2025, de <https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id>

EL CICLO DE VIDA DE LA IDENTIDAD

En cada país hay instituciones que se encargan de identificar y autenticar a las personas. Por ejemplo, en Colombia lo hace la Registraduría Nacional del Estado Civil. Estas instituciones registran a la persona y le dan documentos o credenciales que luego sirven para acceder a distintos servicios del Estado. Este proceso se conoce como ciclo de vida de la identidad y tiene varias etapas:

Registro de la identidad

La persona entrega sus datos básicos (nombre, fecha de nacimiento, huella, etc.) a la autoridad que maneja el sistema de identidad.

Esos datos se revisan y validan con otras bases, como el registro civil, pasaportes o antecedentes.

Entrega de credenciales

Después del registro, se dan elementos que sirven para probar la identidad: por ejemplo, una cédula, un celular con aplicación, una clave o incluso datos biométricos (huella, iris, rostro).

Uso de credenciales

Cada vez que la persona necesita un servicio (como un trámite de salud, educación o apoyo social), presenta una de estas credenciales para demostrar que realmente es ella.

Administración del sistema

La institución mantiene actualizada la base de datos, guarda la información, renueva los documentos cuando es necesario y asegura que todo funcione de manera segura.

También se asegura de que haya interoperabilidad, es decir, que diferentes instituciones (salud, educación, impuestos, etc.) puedan usar la misma información sin pedirla varias veces.



Figura 8. Tipos de credenciales de identidad

Nota. Tomado de Fundación Karisma. (2021, 7 de diciembre). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Recuperado el 8 de septiembre de 2025, de <https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id>

EL RECONOCIMIENTO BIOMÉTRICO

La identificación biométrica funciona a partir de la recolección y abstracción de medidas o características corporales. Esta información se almacena en bases de datos que luego se integran en sistemas que comparan los registros guardados con los que registran sensores, por ejemplo, lectores de huellas o cámaras. Los resultados de estas comparaciones siempre se expresan en términos de probabilidad.

En la actualidad, existen siete elementos impulsados por la industria tecnológica: **las huellas, el rostro, el iris, la voz, el comportamiento, el ADN y los patrones vasculares**. El aumento de sensores en espacios tanto públicos como privados y las nuevas capacidades de estos dispositivos para recolectar, procesar y reconocer personas impone riesgos para los derechos fundamentales como la intimidad, la igualdad y no discriminación, la dignidad, la libertad de movimiento y la libre asociación.

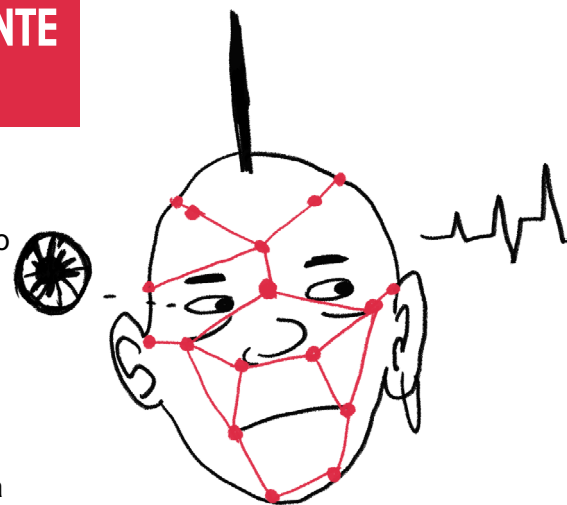
La biometría es una forma de identificar a una persona usando características físicas o de comportamiento que son únicas como la huella dactilar, el rostro, el iris o incluso la voz. Esta información se puede almacenar en bases de datos que luego se integran en sistemas que comparan los registros guardados con la información que se da en el momento.

En la vida cotidiana lo vemos cuando:

- Desbloqueamos un celular con la huella o el rostro.
- Pasamos por el control migratorio en aeropuertos con reconocimiento facial.
- Cobramos un subsidio o pensión usando huella digital en cajeros o entidades públicas.

¿CÓMO PUEDE AFECTAR LA AUTENTICACIÓN MEDIANTE BIOMETRÍA A NUESTROS DERECHOS?

- **Intimidad:** una cámara en la calle que te reconoce sin tu permiso.
- **Igualdad y no discriminación:** un sistema de reconocimiento facial que no identifica a personas con piel más oscura o a mujeres.
- **Dignidad:** tener que entregar tu huella o foto para trámites simples, sin alternativa.
- **Libertad de movimiento:** ser vigilada constantemente en espacios públicos con cámaras inteligentes.
- **Libre asociación:** cámaras que identifican quién está en una protesta.



EJEMPLOS DE SISTEMAS DE IDENTIDAD EN LA REGIÓN

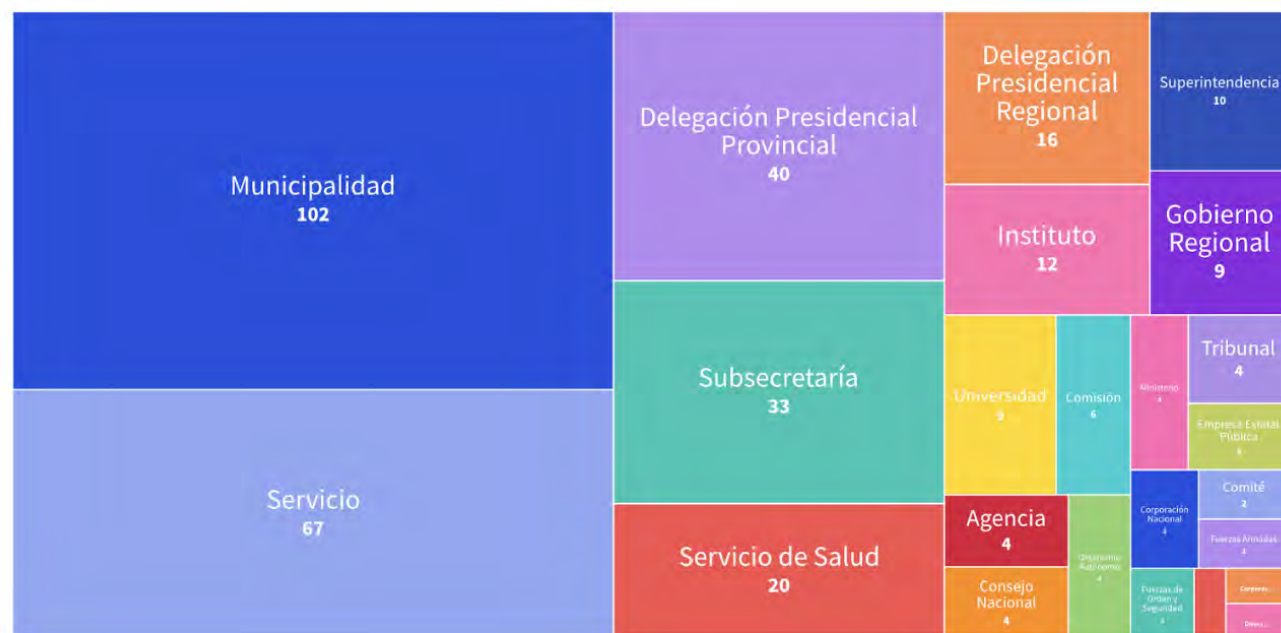
CLAVE ÚNICA EN CHILE

La Clave Única es la identidad digital que permite acceder a los servicios y beneficios del Estado de Chile por medio de Internet. Funciona como una contraseña única que valida de forma segura la identidad de una persona, facilitando su ingreso a todas las plataformas y trámites virtuales del Estado para chilenos y residentes mayores de 14 años.

“Esta herramienta de autenticación digital se ha convertido en la protagonista de la transformación digital del Estado chileno. La pandemia aceleró todos los procesos de digitalización y en 2024, 9 de cada 10 chilenos ya tienen su Clave Única activada”. (Esteban & Esteban, 2024).

Instituciones que utilizan Clave Única

Servicios ciudadanos que han habilitado la Clave Única en sus plataformas digitales a junio de 2024.



Fuente: Análisis y procesamiento de datos de Unholster en base a información de la Secretaría de Gobierno Digital, entre los años 2018 a junio de 2024.

Powered by
Unholster

Figura 9. Activaciones mensuales de Clave Única en Chile (2018–2024).
Elaborado por Unholster en base a información de la Secretaría de Gobierno Digital (s. f.), en CNN Chile Data by Unholster. Recuperado el 8 de septiembre de 2025, de <https://data.cnnchile.com/transformacion-digital/clave-unica/>

¿Qué beneficios tiene la Clave Única?

La Clave Única te permite acceder a una variedad de servicios públicos en línea, tales como:

- **Solicitar certificados del Registro Civil**, tales como nacimiento, matrimonio, defunción, antecedentes, etc.
- **Postular a beneficios sociales**, tales como el Ingreso Familiar de Emergencia, el Bono Covid, el Subsidio al Empleo, etc.
- **Realizar trámites tributarios**, tales como declarar renta, solicitar devolución de impuestos, emitir boletas de honorarios, etc.
- **Consultar tu historial clínico**, tus licencias médicas, tus cotizaciones previsionales, tus bonos de salud, etc.
- **Acceder a tu información académica**, tales como tus notas, tus becas, tus créditos, tus cursos, etc.
- **Participar en procesos electorales**, tales como cambiar tu domicilio, votar en plebiscitos, etc.

Un proyecto para echar una mirada:

Te invitamos a consultar el trabajo de la Organización de la Sociedad Civil Derechos Digitales. Trabajan “por la defensa de los derechos humanos en el entorno digital, combinando investigación, análisis de políticas públicas y tecnología, así como la divulgación y la capacitación en derechos y seguridad digital”.

PREGUNTA: ¿Cuáles son las ventajas y desventajas que podrías identificar en este sistema de identidad?

ID DIGITAL EN BRASIL

La plataforma GOV.BR reúne en un solo lugar los servicios de **identificación que demuestra en medios digitales** que “usted es usted”. En ella, los ciudadanos pueden identificarse de forma segura para acceder a servicios digitales. Es gratuita y está disponible para todos los ciudadanos brasileños.

Por otro lado existe la **Carteira de Identidade Nacional (CIN)**, es el nuevo documento de identificación que utiliza el CPF⁷ como número único y tiene un estándar nacional. La CIN aumenta la seguridad de la identificación de los brasileños, mejora los registros administrativos y contribuye a reducir el fraude en Brasil. La CIN también tiene una versión digital.

El objetivo de la Carteira de Identidade Nacional (CIN) es fortalecer y modernizar el sistema de identificación del país para que la prestación de servicios públicos y privados mejore continuamente. También busca reducir los fraudes millonarios, mitigar los problemas sociales y a delitos como el fraude de identidad, la falsificación de documentos y la estafa. Su objetivo es establecer la confianza y garantizar la integridad de los datos de identificación.

7. Cadastro de Pessoa Física o Registro de Contribuyente. Es el número que identifica a la persona ante la Receita Federal (o Ministerio de Hacienda).

La CIN integra los datos de identificación de los ciudadanos de forma segura y establece un flujo nacional en tiempo real para todos los organismos de identificación,

Sin embargo, la identificación civil presenta múltiples retos debido a la fragmentación e inseguridad de los sistemas de identificación, las diversas normativas legales y la falta de un estándar nacional para la verificación de la identidad de las personas. En ese sentido, CIN busca transformar la identificación de los ciudadanos, con la integración segura de datos y un flujo en tiempo real, lo que permitirá que diferentes áreas del gobierno actúen de manera integrada para satisfacer las necesidades de los ciudadanos.

La propuesta de la Carteira de Identidade Nacional (CIN) debe ser analizada también críticamente. Si bien busca integrar datos y ofrecer un flujo en tiempo real que facilite la coordinación estatal, su implementación debe garantizar:

- **No discriminación:** que ningún grupo (pueblos indígenas, comunidades rurales, personas sin acceso a tecnología) quede excluido del sistema.
- **Protección de la privacidad:** que la centralización de datos no derive en vigilancia masiva o uso indebido de la información personal.
- **Transparencia y participación:** que la ciudadanía conozca cómo se usan sus datos y pueda exigir rendición de cuentas.
- **Seguridad digital:** que existan salvaguardas efectivas contra filtraciones, abusos o manipulaciones.

Figura 10. Publicidad de la identificación digital en Brasil

Nota. Tomado de “Identificação do Cidadão e Carteira de Identidade Nacional”, por Governo Digital de Brasil (s. f.). Recuperado el 8 de septiembre de 2025, de <https://www.gov.br/governodigital/pt-br/identidade/>



identificacao-do-cidadao-e-carteira-de-identidade-nacional

Figura 11. Diferentes formatos y tipos de identificación en Brasil

Tomado de “Identificação do Cidadão e Carteira de Identidade Nacional”, por Governo Digital de Brasil (s. f.).

CIN Papel



Frete e verso

CIN Cartão



Frete e verso em cartão

CIN Digital



Versão digital no GOV.BR

Recuperado el 8 de septiembre de 2025, de

<https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional>

Un proyecto para echar una mirada:

data_labe es un “laboratorio de datos y narrativas en la favela Maré de Río de Janeiro. El equipo está formado por jóvenes residentes de comunidades populares que crean nuevas narrativas a través de datos.”

RENAPER EN ARGENTINA

Es una versión virtual del DNI que se usa a través de la aplicación Mi Argentina. Tiene las mismas funciones que el DNI tarjeta, excepto votar y viajar fuera del país.

Figura 12. Pantalla de Inicio del portal Mi Argentina



Tomado de Mi Argentina [Captura de pantalla], por Argentina. Presidencia de la Nación (s. f.). Recuperado el 8 de septiembre de 2025, de <https://www.argentina.gob.ar/miargentina/>

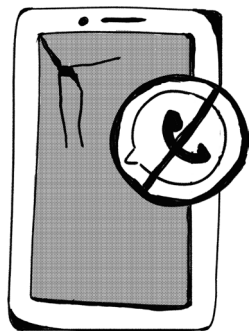
Un proyecto para echar una mirada:

[Reconoceme](#) es una campaña en Argentina que busca generar conciencia sobre los sistemas de reconocimiento facial (SRF), sus riesgos y las implicaciones para los derechos civiles y la privacidad. La iniciativa defiende el derecho de las personas a no ser identificadas sin garantías ni controles adecuados, promoviendo un debate público sobre su impacto en la democracia y las libertades individuales.

DESAFÍOS Y RIESGOS PRINCIPALES DE LOS SISTEMAS DE IDENTIFICACIÓN EN LA REGIÓN:

La identificación digital puede traer beneficios, pero también presenta riesgos que deben analizarse con cuidado: **exclusión, vigilancia, brechas de acceso y seguridad.**

Un punto crítico es la **protección de datos personales**, que en proyectos gubernamentales suele ser limitada. Existen dos problemas centrales:



1. **Falta de límites claros:** no siempre se define con precisión cómo, para qué y hasta dónde pueden los organismos públicos recolectar y usar la información personal.
2. **Escasos mecanismos de defensa:** las personas no cuentan con procesos accesibles y eficaces para apelar o reclamar si sienten que su información ha sido mal utilizada.

IDENTIDAD DIGITAL Y GOBERNANZA DE INTERNET

Desde una perspectiva de derechos y desarrollo inclusivo, la identidad digital es mucho más que una credencial tecnológica: es una puerta de acceso a oportunidades, servicios y participación ciudadana. Su relación con la gobernanza de Internet se refleja en tres ámbitos esenciales:

Seguridad y confianza

La identidad digital debe garantizar que cada individuo pueda autenticarse en línea de forma segura, protegiendo su información y evitando el fraude o la suplantación.

En la gobernanza de Internet, esto significa establecer marcos claros de protección de datos, auditorías transparentes y mecanismos de rendición de cuentas que fortalezcan la confianza de la ciudadanía.

Inclusión digital - Consultas previas

La identidad digital tiene que ser accesible para todas las personas, sin importar su ubicación geográfica, nivel socioeconómico o condición física.

La gobernanza de Internet responsable incluye promover conectividad asequible, alfabetización digital y diseño inclusivo de plataformas.

Además, las consultas previas con pueblos indígenas y comunidades locales son fundamentales para que las soluciones respeten la diversidad cultural, las lenguas y las visiones propias sobre privacidad y uso de datos.

Derechos humanos

La identidad digital debe proteger y promover derechos, no restringirlos. Esto implica:

- Defender el derecho a la privacidad frente a usos abusivos o vigilancia masiva.
- Garantizar la no discriminación en el acceso y uso de servicios digitales.
- Asegurar el derecho a la participación, permitiendo que más personas puedan ejercer ciudadanía plena a través de canales digitales seguros y transparentes.

ESPACIOS DE PARTICIPACIÓN REGIONAL: LACIGF AND YOUTH LACIGF

Conocer espacios de gobernanza de Internet, los temas que tratan y su importancia –ya vistos en el módulo anterior– permite analizar posibles oportunidades de incidencia y participación de cara a la digitalización de los servicios del Estado. Este no es un proceso puramente técnico: involucra decisiones políticas sobre cómo se diseñan, regulan y garantizan derechos en entornos digitales.

Justamente ahí la ciudadanía tiene un papel fundamental, pues puede señalar las brechas y riesgos que las políticas públicas suelen pasar por alto: desde la falta de conectividad en zonas rurales y la exclusión de poblaciones con menor alfabetización digital, hasta los riesgos de vigilancia, la ausencia de políticas de accesibilidad o el uso de tecnologías que no responden a necesidades locales.

Los espacios de gobernanza de Internet como el LACIGF y el Youth LACIGF ofrecen mecanismos concretos de participación, donde esas preocupaciones pueden convertirse en aportes que influyen en la agenda regional.

En este apartado nos centraremos en dos eventos de gobernanza de Internet abordados superficialmente en el módulo anterior. Tanto el LACIGF como el Youth LACIGF tienen lugar en nuestra región y se han consolidado como espacios valiosos para visibilizar problemáticas locales. Veremos los temas más usuales en estos espacios y una guía breve para aplicar al LACIGF. ¡Puedes proponer un espacio para dialogar sobre los problemas de la digitalización de servicios fundamentales en nuestra región!



Figura 13. Logo de LACIGF.

El Foro de Gobernanza de Internet de América Latina y el Caribe (LACIGF) se ha convertido a lo largo de sus ediciones en un espacio de encuentro regional para el diálogo político multisectorial en el que actores de gobiernos, sector privado, comunidad técnica, academia y organizaciones de la sociedad civil presentan y discuten sus perspectivas.

En los últimos años la región ha avanzado en la comprensión de los desafíos actuales de la gobernanza de Internet conformando un espacio propio para el debate y la identificación de las prioridades regionales, a la vez que se ha ampliado significativamente la participación y contribución de la región en los debates del [Foro de Gobernanza de Internet](#).



Figura 14. Logo del Youth LACIGF

Del LACIGF nace el Foro de la Gobernanza de Internet para las juventudes de América Latina y el Caribe ([Youth LACIGF](#)), dónde jóvenes de la región se articulan para discutir temas relacionados con la gobernanza del Internet.

Este encuentro multisectorial fue creado en el año 2016 en la ciudad de San José, Costa Rica; desde entonces ha itinerado por diferentes ciudades de LAC. Ha sido clave para la participación de las juventudes interesadas en la gobernanza de Internet en relación con la diversidad, el intercambio de experiencias, la perspectiva de abajo hacia arriba⁸, la creación de redes regionales y la garantía de espacios seguros y libres de violencias.

8. Bottom-up: significa que las decisiones, planes o soluciones nacen desde las personas, comunidades o actores locales, y no se imponen únicamente desde las autoridades o niveles centrales.

El Youth LACIGF ha abordado temas como el acceso a conectividad e infraestructura digital, privacidad, ciberseguridad, economía digital, derechos humanos y vigilancia. Todos estos temas inciden directamente en cómo se diseñan, implementan y perciben los servicios digitales del Estado.

También ha respondido a iniciativas globales como el Pacto Digital Global⁹ y desafíos que dejó la pandemia en torno al uso de la tecnología: marcos regulatorios que respeten la privacidad y autonomía de las personas usuarias, brechas de acceso y conectividad, exposición de datos personales, entre otros, que afectan la gobernanza y la inclusión digital.

FORMAS DE CONTRIBUCIÓN CIUDADANA

1. Intervenciones en plenarios y talleres.

La ciudadanía puede tomar la palabra para señalar problemas locales (ej. preocupaciones frente a la digitalización de servicios del Estado, falta de conectividad en comunidades rurales, riesgos de vigilancia, necesidad de políticas de accesibilidad).

2. Propuestas escritas o consultas previas.

LACIGF y Youth LACIGF suelen abrir períodos de consulta en línea donde cualquier persona u organización puede enviar aportes que luego se integran a la agenda de discusión.

3. Participación en grupos de trabajo.

Los foros generan mesas temáticas (como datos personales, servicios públicos digitales, inclusión de género, IA) donde la ciudadanía puede aportar insumos o sumarse como voluntaria.

4. Testimonios y experiencias.

Personas u organizaciones comparten casos de uso.

5. Construcción colectiva de recomendaciones

Al final de muchos foros, se elaboran síntesis o declaraciones que recogen las voces ciudadanas y se envían a instancias globales (como el IGF de la ONU).

Pasos para elaborar una contribución ciudadana:

Las contribuciones ciudadanas ayudan a incluir perspectivas locales y diversas en las discusiones regionales.

Primer paso: revisa los temas propuestos en la convocatoria anual (p.ej: conectividad, derechos digitales, ciberseguridad, gobernanza de datos o inclusión digital).

1. Escoge uno que sea relevante para tu comunidad o experiencia.
2. Incluye datos, casos y evidencias que muestren por qué tu aporte es importante.

9. busca establecer un marco mundial inclusivo para un futuro digital abierto, seguro y centrado en las personas, basado en los derechos humanos y los objetivos de desarrollo sostenible. Aquí esta disponible la vresión final: <https://docs.un.org/es/A/RES/79/1>

Puedes usar:

- Estadísticas oficiales y estudios (CEPAL, ONU, informes de ONGs).
- Experiencias y testimonios locales.
- Normativas o marcos legales relevantes.

Pregúntate:

- ¿Qué problema o necesidad quiero visibilizar?
- ¿Qué propuesta o solución sugiero?
- ¿Cómo se relaciona con la gobernanza de Internet y con los derechos humanos (privacidad, acceso, no discriminación, libertad de expresión)?

Formato.

Título: breve y descriptivo.

Contexto: explicar la situación actual y por qué es relevante.

Problema o desafío: detallar las barreras, riesgos o vulneraciones a derechos humanos, civiles o políticos.

Propuesta o recomendación: acciones concretas que el LACIGF y otros actores podrían considerar.

Impacto esperado: cómo tú propuesta mejoraría la situación.

Datos o ejemplos: evidencias que respalden tu aporte.

Si es posible, compártela con redes comunitarias, colectivos juveniles o personas expertas en el tema para recibir retroalimentación.

Segundo paso: verifica que cumpla con el formato y el plazo del LACIGF o Youth LACIGF.

- **Revisa en la convocatoria:**
 - Límite de palabras o páginas.
 - Idiomas aceptados.
 - Formato de envío (correo, formulario web).
- **Envía tu aporte antes de la fecha límite.**



CIERRE DEL MÓDULO : GOBERNANZA Y PARTICIPACIÓN

Comprender la digitalización no se trata solo de aprender a usar tecnologías, sino de entender cómo estas impactan nuestras vidas, nuestros derechos y nuestras comunidades.

ACTIVIDAD

- 1. Reflexión, preguntas y herramientas para construir una mirada crítica frente a la digitalización desde la soberanía ciudadana.**
 - ¿Qué barreras enfrenta mi comunidad para participar en estos procesos?
 - ¿Qué papel me gustaría asumir frente a esta transformación digital?
 - ¿Cómo me afecta (o no) la digitalización de servicios ciudadanos en mi vida diaria?
- 2. Redacta tu propio manifiesto**
 - ¿Qué principios deberían guiar la digitalización del Estado?
 - ¿Qué demandas te parecen urgentes desde tu rol como ciudadanx digital?

RECURSOS ADICIONALES

[ID Colombia](#) | Fundación Karisma

[Infraestructura y cobertura de redes de acceso móvil](#) | Postdata

[Soberanía y nacionalismo en entornos digitales: la llamativa ausencia de América Latina en el debate mundial](#) | Martín Becerra y Silvio Waisbord

[Soberanía Digital](#) | Julia Pohle y Thorsten Thiel

[Digitalización de Trámites y Servicios](#) | Ministerio TIC Colombia

[Política de Gobierno Digital](#) | Ministerio TIC Colombia

[Decreto 088 de 2022](#) | Función Pública

[Una transformación digital real y efectiva puede ayudar a América Latina y el Caribe a superar las trampas que impiden su desarrollo](#) | CEPAL

REFERENCIAS

OECD/CAF (2024), Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos, OECD Publishing, Paris, <https://doi.org/10.1787/7a127615-es>.

Garcia, J (2024). Inteligencia Artificial en el Estado: Estudio colectivo sobre experiencias y riesgos para los Derechos Humanos, Derechos Digitales.

Comisión Económica para América Latina y el Caribe. (s. f.). Definiciones [Biblioguías]. Biblioteca CEPAL. Recuperado el 8 de septiembre de 2025, de <https://biblioguias.cepal.org/gobierno-digital/definiciones>

Portal Gov.br. (s. f.). Checklist [Guía de edición de servicios]. Gobierno de Brasil. Recuperado el 8 de septiembre de 2025, de <https://www.gov.br/pt-br/guia-de-edicao-de-servicos-do-gov.br/o-que-e-um-servico/checklist>

Esteban, R., & Esteban, R. (2024, 13 septiembre). Menos de un tercio de los municipios de Chile tienen habilitado el uso de la Clave Única - CNN Chile Data by Unholster. CNN Chile Data by Unholster -. <https://data.cnnchile.com/transformation-digital/clave-unica//>

Ministerio de Gestión e Innovación en Servicios Públicos; Secretaría de Gobierno Digital. (s. f.). La plataforma brasileña de identidad digital [Presentación en PDF]. Red Interamericana de Gobierno Digital (Red GEALC). Recuperado el 8 de septiembre de 2025, de https://www.redgealc.org/site/assets/files/17944/brasil_-_taller_rg.pdf

Comisión de Regulación de Comunicaciones (CRC). (2024, 13 de diciembre). La CRC presenta el análisis sobre infraestructura y cobertura móvil en Colombia. CRC. Recuperado el 8 de septiembre de 2025, de la página CRC. <https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-analisis-sobre-infraestructura-y-cobertura-movil-en>

Fundación Karisma. (2021, 7 de diciembre). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Recuperado el 8 de septiembre de 2025, de <https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id>

Argentina. Presidencia de la Nación. (s. f.). Mi Argentina [Sitio web]. Recuperado el 8 de septiembre de 2025, de <https://www.argentina.gob.ar/miargentina/>

Youth LACIGF. (s. f.). Youth LACIGF: Foro de Gobernanza de Internet para las juventudes de América Latina y el Caribe [Sitio web]. Recuperado el 8 de septiembre de 2025, de <https://youthlacigf.lat/>

Internet Governance Forum. (s. f.). Internet Governance Forum [Sitio web]. Recuperado el 8 de septiembre de 2025, de <https://intgovforum.org/es/>

Fundación **Karisma**



karisma.org.co

