cade Civil Society Alliances for Digital Empowerment

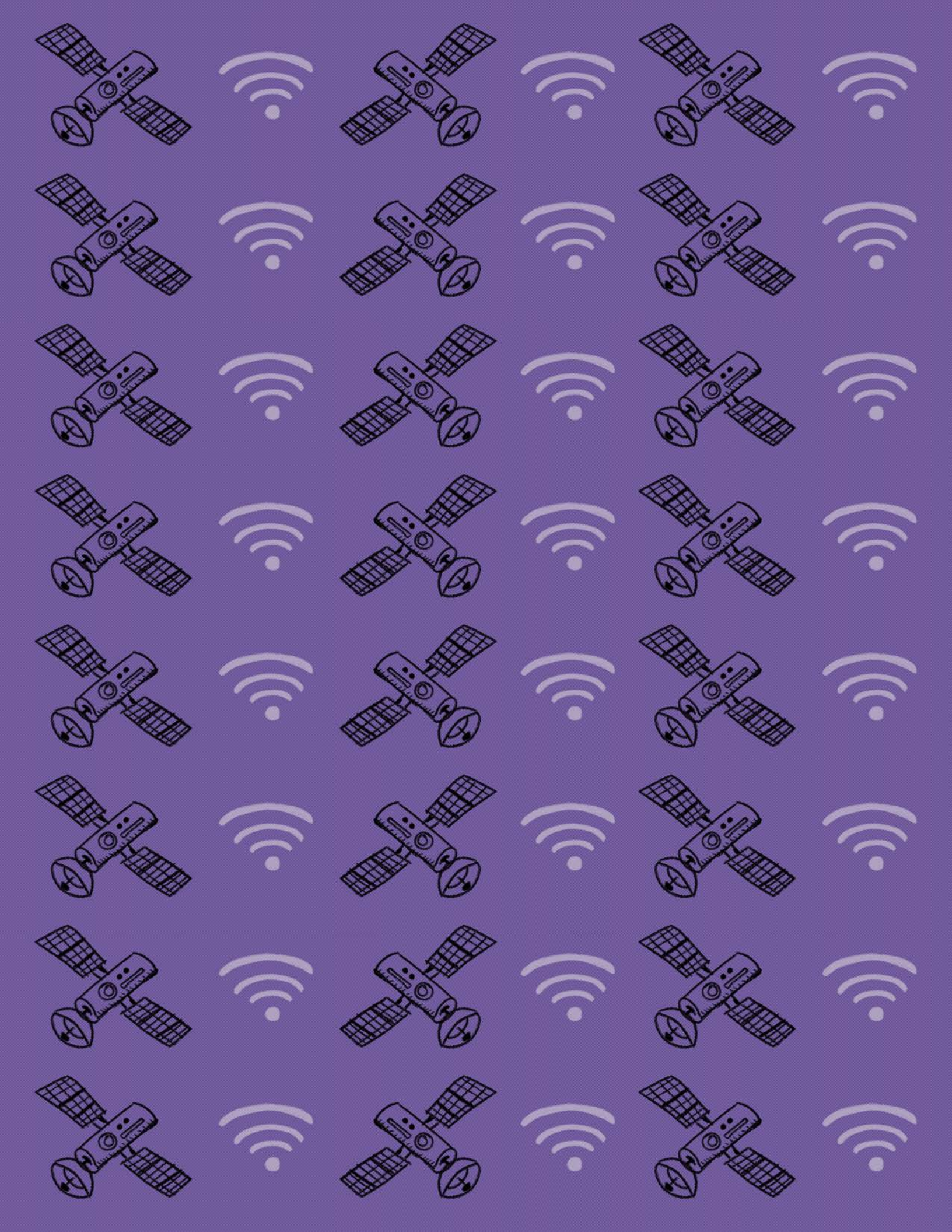
Co-funded by the European Union

NAVEGANTES DA INTERNET:

Ciclo de formação para a governança da internet e para a cidadania digital

Ciclo de formação sobre governança da internet

Fundación Karisma



Publicação: Setembro de 2025
Traduzido em maio de 2026

Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

NAVEGANTES DA INTERNET:

Ciclo de formação para a governança da internet e para a cidadania digital

Fundación Karisma
Fundação Karisma

Somos uma organização da sociedade civil que visa proteger e promover os direitos humanos e a justiça social no desenvolvimento e no uso das tecnologias digitais. Trabalhamos na promoção dos direitos humanos no mundo digital.
comunicaciones@karisma.org.co

Autoria e esquisa:

Módulo 1:
Michael Ruiz
Lorena Enciso
Camila Pardo.

Módulo 2:
Daniela Schnidrig
Edda Forero.

Módulo 3
Edda Forero.

Coordenação
Paula Rodríguez Badillo
Maria Camila Galvis

Revisão
Paula Rodríguez Badillo
Michael Ruiz
Pilar Saenz

Direção da Karisma
Catalina Moreno Arocha
Juan Diego Castañeda

Correção de estilo
Laura Grisales Silva

Design editorial
Daniela Ramírez Moreno

Coordenação editorial
Natalia Andrade Fajardo

Esta pesquisa foi realizada no âmbito do consórcio CADE. Veja mais em https://cadeproject.org/

Esta publicação é cofinanciada pela União Europeia. Seu conteúdo é de responsabilidade exclusiva da Fundación Karisma e não reflete necessariamente as opiniões da União Europeia.

INTRODUÇÃO AO CICLO DE FORMAÇÃO SOBRE GOVERNANÇA DA INTERNET

Este ciclo de formação visa aproximar jovens, docentes rurais, comunidades historicamente marginalizadas e interessados nos debates sobre a governança da internet, entendida não apenas como um tema técnico, mas sim como um campo político no qual são definidos direitos, oportunidades e formas de participação cidadã. A ideia central é que os espaços de governança não fiquem em conversas abstratas ou dominadas por atores com mais recursos, mas que integrem as perspectivas e experiências das nossas comunidades na América Latina e no Caribe.

Este ciclo de formação é realizado no marco do projeto Civil Society Alliances for Digital Empowerment (CADE), uma aliança que impulsiona projetos sobre governança da internet e acesso a espaços de incidência desde os países do Sul Global e conta com o apoio financeiro da União Europeia.

A proposta é estruturada em três módulos que são articulados da seguinte forma:

- **Como funciona a internet?**
  Apresenta as bases técnicas e sociais da internet para compreender o que está por trás da tela, como viajam as mensagens, o que é a infraestrutura digital e por que estas questões são chaves para falar de direitos e de participação.

- **Governança da internet: decisões que nos afetam**
  Explora quem toma as decisões sobre a internet, quais interesses estão em jogo e quais são os principais espaços e princípios de governança. A ênfase está em reconhecer o papel da sociedade civil e abrir oportunidades concretas de incidência.

- **Digitalização de serviços e direitos cidadãos**
  Convida a refletir criticamente sobre como os Estados promovem a digitalização dos serviços, quais são os seus impactos na vida cotidiana e como vincular estas discussões com a governança da internet, desde um enfoque de direitos, de inclusão e de soberania digital.

Em conjunto, estes três módulos oferecem um percurso que vai do técnico ao político e do global ao cotidiano: desde os cabos, servidores e protocolos que sustentam a rede, até as políticas públicas de digitalização que afetam o modo no qual temos acesso a saúde, a educação ou a justiça.

Objetivo geral do ciclo de formação

Fortalecer as capacidades de jovens, de docentes e de comunidades vulneráveis na América Latina e no Caribe para compreender e adquirir ferramentas de participação e de incidência nos debates e nas decisões da governança da internet, com o objeto de ampliar as suas capacidades e promover o reconhecimento das suas experiências locais na construção de um entorno digital mais justo, inclusivo e democrático.

Objetivos específicos

1. **Compreender** os fundamentos técnicos, sociais e políticos da internet, desde a sua infraestrutura até a sua governança multilateral.

2. **Analisar** os principais debates, atores e espaços de governança da internet, tornando visível as tensões de poder e as oportunidades de participação para a sociedade civil.

3. **Refletir** criticamente sobre os processos de digitalização impulsionados pelos Estados e a sua relação com os direitos humanos e as desigualdades territoriais.

4. **Promover** a participação significativa de comunidades rurais, de juventudes e de setores vulneráveis em espaços de governança da internet, vinculando experiências locais com debates regionais e globais.

5. **Fomentar** a incidência mediante propostas concretas que integrem perspectivas comunitárias na agenda da governança e da digitalização, contribuindo para que as tecnologias estejam a serviço das pessoas e dos territórios.

cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

COMO FUNCIONA A INTERNET?

O que está por trás da tela?

Decifremos isso que chamamos "Internet".

Módulo 1

Ciclo de formação sobre governança da internet

Fundación Karisma

CONTENIDO

INTRODUÇÃO

Na atualidade, a Internet é uma infraestrutura essencial que conecta milhões de pessoas, dispositivos e serviços em todo o mundo. Entretanto, além do seu uso cotidiano, entender o que é a Internet em termos técnicos, sociais, econômicos e políticos é fundamental para abordar a sua governança de maneira informada e efetiva.

Este módulo tem como objetivo oferecer uma visão clara e acessível sobre o que é a Internet: como funciona, como foi desenvolvida, quais são os seus principais componentes técnicos e quem intervém na sua operação. Também, apresentamos a natureza descentralizada da Internet, os seus princípios fundamentais como a interoperabilidade, a abertura e o acesso universal e como estes influenciam diretamente nos debates e nas decisões sobre a sua governança.

Ao finalizar este módulo você contará com mais ferramentas para compreender os desafios e as oportunidades que surgem ao gerenciar uma rede global, estas permitirão que você participe de maneira informada nas discussões sobre políticas públicas, regulação e direitos digitais que configuram o presente e o futuro da Internet.

OBJETIVOS DO MÓDULO

Objetivo geral:

Compreender de maneira autônoma e crítica o funcionamento técnico, social e político da Internet, mediante a análise das suas camadas, do trajeto da informação, usando como exemplo as mensagens instantâneas e as dinâmicas de controle e de bloqueios da Internet.

Objetivos específicos:

- Descrever e explicar as três camadas da Internet (infraestrutura física, padrões/serviços lógicos e conteúdos/aplicações) e o percurso de uma mensagem desde o dispositivo até o destinatário usando o WhatsApp como exemplo.
- Analisar os mecanismos e as causas de cortes, falhas e controles da Internet —incluindo a manipulação do DNS e a censura estatal— mediante o estudo de casos (p. ex., restrições ao WhatsApp na China).
- Apresentar algumas metodologias básicas de documentação e de análise de disrupções da Internet, utilizando ferramentas e recursos como o Observatório de Bloqueios da Internet (OBI) para registrar, interpretar e comunicar incidentes.

.

UNIDADE I: COMO FUNCIONA A INTERNET? VEJAMOS O EXEMPLO DO WHATSAPP

Com esta unidade procuramos dar um contexto sobre o que é e como funciona a Internet através do exemplo das mensagens instantâneas com o WhatsApp, uma ferramenta de uso massivo e cotidiano.

Aqui mostramos a infraestrutura da internet, a transmissão de dados e o funcionamento de alguns aspectos de segurança digital, elementos-chave para entender a Internet. Além disso, compartilhamos alguns dos desafios, dos riscos e das limitações do funcionamento atual desta grande rede que nos conecta a todos a nível global.

Objetivo general

Explicar o funcionamento básico da Internet para oferecer uma compreensão estratégica desde a prática, além da teoria, abordando a sua definição, como opera, as ferramentas que a mantém e os atores que participam no seu funcionamento.

Objetivos específicos

1. Compreender como são transmitidas as mensagens através das redes que compõem a Internet.
2. Introduzir o papel dos protocolos de comunicação, especialmente TCP/IP, no funcionamento da internet.
3. Analisar como o controle, as falhas técnicas e as quedas do serviço de internet podem afetar o acesso aos direitos e ao trabalho de incidência das organizações sociais.

Temas

1. O que é a internet?
2. Breve história da internet. Como começou? Qual foi a motivação para o seu início? Como foi o avanço e as etapas da internet?
3. Como viajam as mensagens: do dispositivo para o servidor e do servidor para o destinatário - espetro radioelétrico.
4. O papel dos operadores de serviços de internet.
5. Criptografia e privacidade.
6. Caso: restrições ao WhatsApp em distintos países.

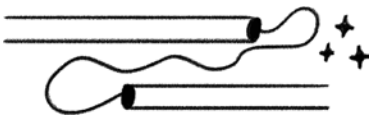
O QUE É A INTERNET?

A Internet é uma rede mundial de redes. Isto é, uma grande estrutura que conecta entre si milhões de computadores, servidores, cabos e outros dispositivos em todo o mundo. Esta conexão permite que possam comunicar-se e compartilhar informação.

Embora às vezes seja representa como uma nuvem, na realidade a Internet é baseada em uma infraestrutura física: cabos de fibra óptica, antenas, satélites e centros de dados que permitem que os dados viajem de um lugar para outro. Cada vez que enviamos uma mensagem, abrimos uma página web ou vemos um vídeo, estamos usando essa rede de redes para trocar informação.

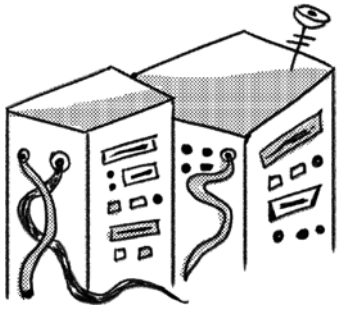
Internet: a Cidade Digital

Imaginemos que a Internet não é algo invisível e técnico, mas sim uma cidade enorme e complexa chamada Cidade Digital. Nesta cidade, tudo acontece através do fluxo constante de informação:



As ruas são as conexões

Existem diferentes tipos de ruas, algumas são como rodovias rápidas (fibra óptica) que permitem que os dados viajem muito rápido e com alta capacidade. Outras são como caminhos rurais ou estradas secundárias (satélite, cabo coaxial) que são mais lentas e têm menor largura de banda. Inclusive existem ruas cheias de semáforos e obstáculos (redes Wi-Fi congestionadas) que podem retardar o tráfego.



Os edifícios são os servidores

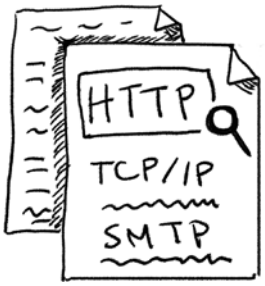
Estes edifícios abrigam a informação ou serviços de diferentes tipos: desde páginas web e vídeos até e-mails e arquivos. Alguns armazenam grandes volumes de dados (grandes centros de dados), outros são pequenas lojas com informação específica (servidores individuais). São semelhantes a bares, lojas, shoppings, parques, hospitais, etc.

As pessoas são os dispositivos e os usuários

Temos computadores, telefones inteligentes, tablets... Todos estes são cidadãos ou cidadãs que moram na Cidade Digital e se comunicam entre si. Alguns são apenas receptores de informação (dispositivos passivos), outros também são produtores (usuários que publicam conteúdo em redes sociais ou enviam e-mails).

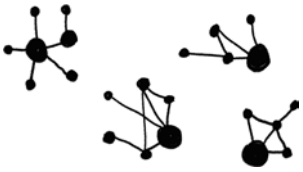
O tráfego é os datos

Cada mensagem, cada foto, cada vídeo é um veículo que viaja pelas ruas da cidade.



As regras e a ordem são os protocolos

Como em qualquer cidade precisamos de regras para que tudo funcione bem. Na Cidade Digital estas regras são os protocolos, como HTTP (para navegar por páginas web), TCP/IP (a base do sistema de endereços que identifica cada dispositivo) ou SMTP (para enviar e-mails). Estes protocolos garantem que os dados cheguem ao seu destino corretamente e que as diferentes partes da cidade possam comunicar-se entre si.



Os bairros são as redes

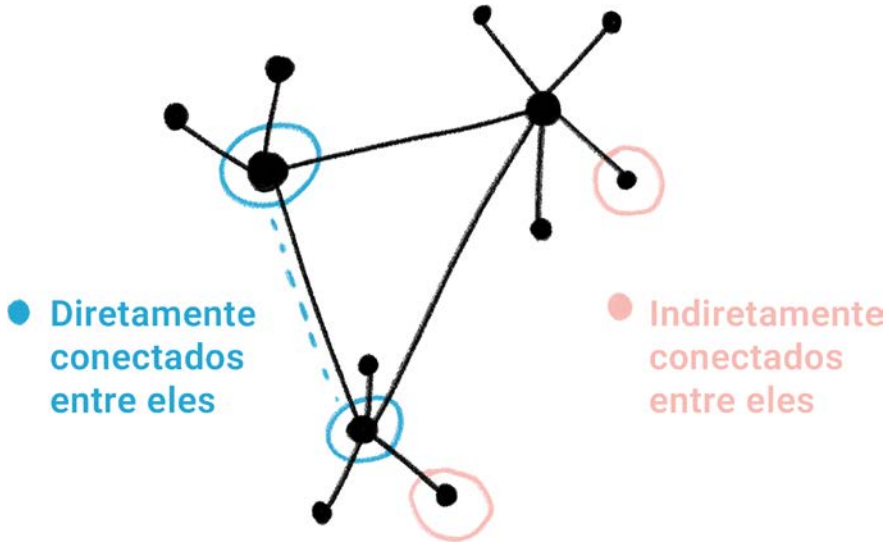
As ruas são agrupadas em bairros, cada bairro tem o seu próprio administrador e as suas próprias regras específicas. Por exemplo, a rede local da sua casa ou a rede social que você utiliza.

A polícia e os bombeiros são a segurança

Imagina que toque um alarme, a polícia (antivírus) tenta bloquear aos intrusos e rastreá-los; se o intruso entra e causa um incêndio chegam os bombeiros (equipes de resposta, cópias de segurança e recuperação), apagam o fogo, salvam o que podem e logo investigam como entrou o intruso para que a polícia possa fortalecer a vigilância.

Redes e nós

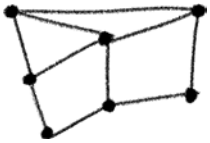
A Internet é definida como uma “rede de redes” composta por redes menores chamadas nós. Estes nós agem como centros de conexão, desde os quais outros nós são estendidos. Imagine que cada nó é um ponto em uma rede, onde alguns estão conectados diretamente entre si, enquanto que outros estão conectados de maneira indireta através de nós intermediários. No contexto da Internet, os nós são dispositivos que podem enviar e receber informação. Cada dispositivo tem um endereço único, conhecido como endereço IP, que permite localizá-lo na rede. A informação viaja de um nó para outro, passando por nós intermediários que retransmitem os dados até que chegam ao nó destinatário.



Então, entre os tipos de redes encontramos:

Redes centralizadas:
Quando os diferentes nós estão conectados através de um único nó.

Redes descentralizadas:
Quando muitos nós se conectam através de múltiplos nós, sem que um único aglomere todas as conexões. Isto quer dizer que existem múltiplos centros.

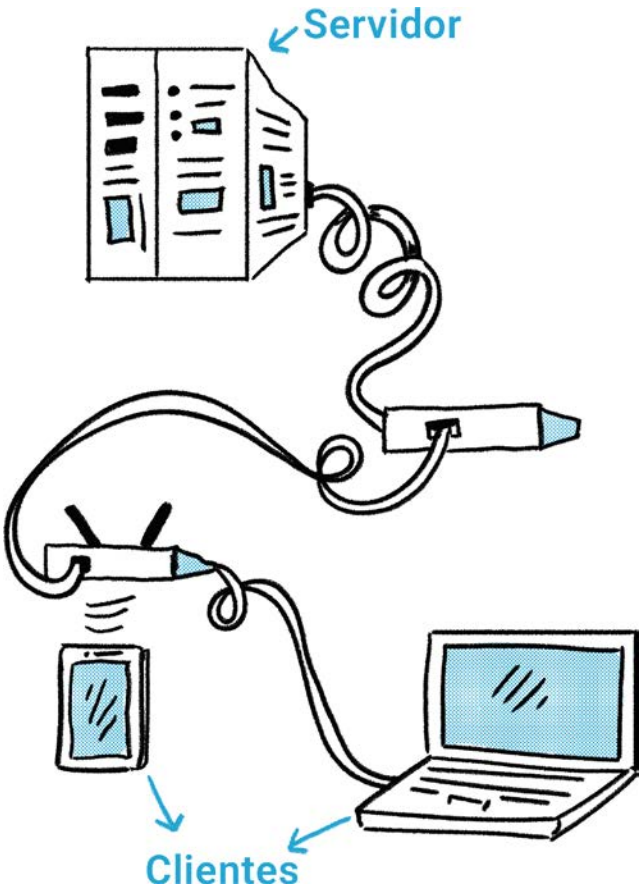


Redes distribuídas:
Quando cada nó está conectado de forma não hierárquica com os outros, já que não existem centros nem pequenos nem grandes.

Uma vez identificados, sabemos que embora todos estes tipos de redes coexistam na Internet, o tipo de estrutura que predomina é a descentralizada. Entretanto, quando abordemos as problemáticas da governança da Internet veremos que crescentemente alguns serviços marcam uma pauta centralizadora da Internet.

Tipos de nós: servidores, clientes e roteadores

Agora que sabemos que a Internet está composta por nós, é importante distinguir os tipos principais: **servidores, clientes e dispositivos de rede.**



Fonte: Adaptado e traduzido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021.

Servidores

Os servidores são nós que funcionam como computadores conectados a uma rede na qual proporcionam serviços e aceitam conexões desde outros dispositivos ou aplicações (aos que chamamos clientes). A sua tarefa principal é receber, processar e enviar informação de acordo com o solicitado por esses dispositivos. Por exemplo:

- Um servidor de e-mails recebe mensagens, armazena-as e entrega-as aos destinatários.
- Um servidor de vídeo games coordena jogos, mantém o estado do jogo e sincroniza os jogadores.
- Um servidor de mensagens (como o WhatsApp) encaminha e entrega mensagens entre usuários e guarda históricos quando é necessário.
-

Ao contrário de um computador pessoal, um servidor está otimizado para suportar muitas conexões simultâneas, funcionar continuamente e manejar grandes volumes de dados. Em poucas palavras: é um computador potente desenvolvido para gerenciar e distribuir informações pedidas por outros dispositivos.

Os servidores são nós conectados fisicamente a uma rede que oferecem serviços e podem aceitar conexões de outros nós. A sua função principal costuma ser enviar, receber ou processar informação. Alguns exemplos são os servidores de vídeo games, de e-mail ou de mensagens instantâneas (como o WhatsApp). Podemos imaginá-los como um potente computador desenvolvido para gerenciar a informação enviada mediante outros dispositivos.

Clientes

São aqueles nós que estabelecem conexões com os servidores, ou seja, aqueles que fazem uso dos serviços oferecidos por um ou vários servidores. Por exemplo, quando queremos ler o e-mail precisamos de uma aplicação cliente (como Outlook, Thunderbird ou Gmail) que está conectada ao servidor para autenticar a conta, sincronizar pastas e fazer downloads ou mostrar as mensagens. Este cliente usa um protocolo como IMAP/POP3, além de oferecer a interface para redigir, pesquisar, organizar mensagens e guardar uma cópia local temporária se for necessário.

O mesmo ocorre com as mensagens instantâneas: o WhatsApp precisa da aplicação cliente no telefone ou na área de trabalho para enviar ou receber mensagens do seu servidor e mostrar notificações. O cliente maneja a interface e a gestão de conversas, mas a entrega e o encaminhamento das mensagens passam pelos servidores do serviço.

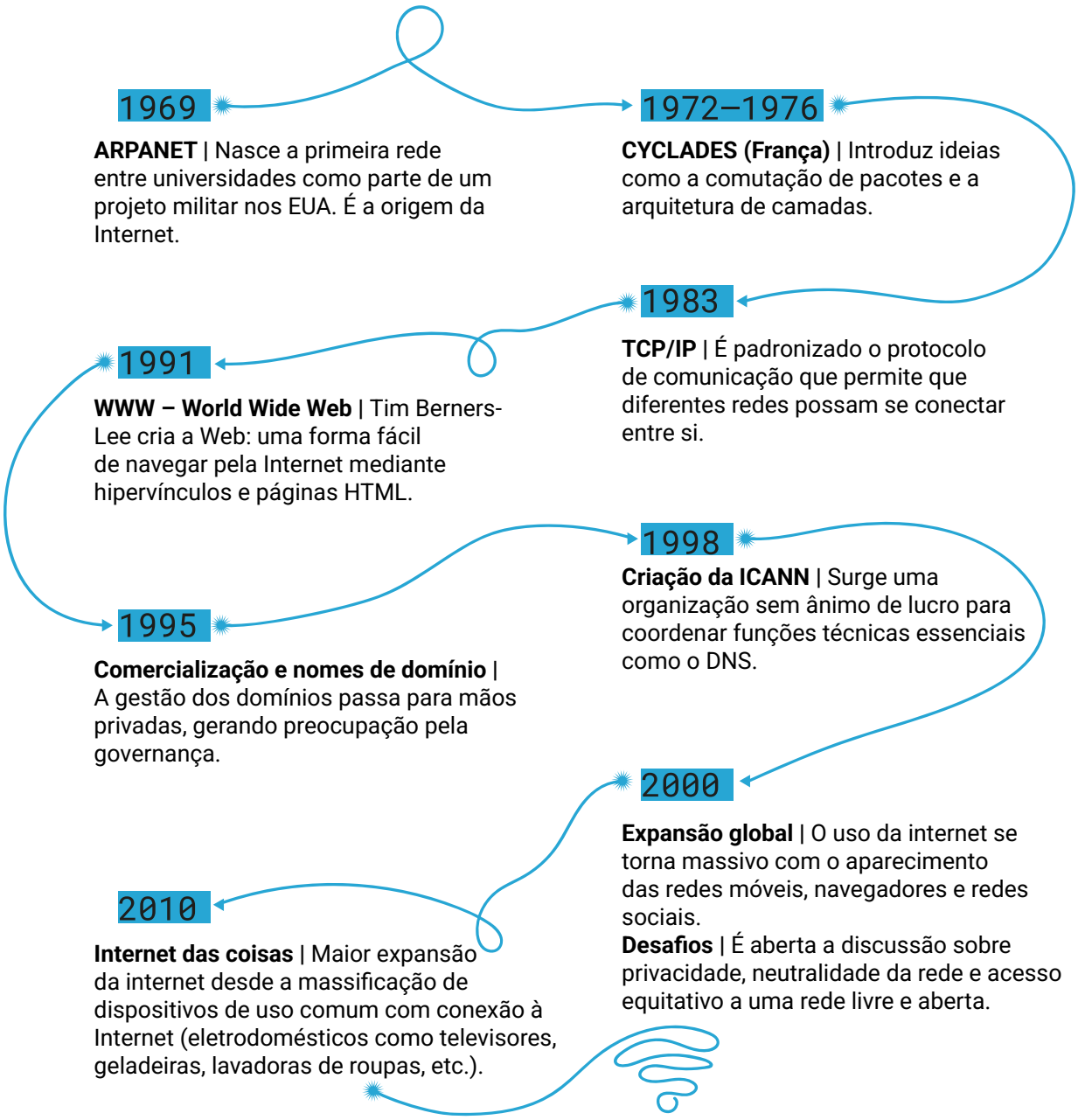
Dispositivos de rede

Os dispositivos de rede são de distintos tipos, capacidades, funções e alcances. Facilitam a interconexão entre clientes e servidores para permitir a troca de informação e o estabelecimento de conexões. Alguns exemplos cotidianos de dispositivos de rede são os roteadores, os pontos de acesso Wi-Fi ou os switches de rede1.

1 Um switch de rede pode ser entendido como um distribuidor inteligente dentro de um escritório ou casa conectada: recebe pacotes (dados) que chegam pelas suas portas e entrega-os exatamente para o destinatário correto, em vez de enviá-los para todos. Quando você precisa de um? Se você tiver vários dispositivos conectados por cabos e quiser conexões confiáveis e rápidas entre eles (ou para um roteador), um switch é a peça que os conecta e organiza o tráfego entre os distintos dispositivos.

COMO NASCE A INTERNET? PEQUENO PERCURSO.

Linha de tempo da história da Internet



A Internet não nasceu como um produto comercial, mas como um experimento colaborativo entre universidades, governos e empresas. A sua evolução mostra como uma infraestrutura pensada para compartilhar recursos entre pesquisadores se converteu em uma rede global crítica para a informação, os direitos e a participação cidadã.

Pelo exposto, gostaríamos de destacar quatro momentos-chave:

1. **Internet: inícios no setor defesa e acadêmico:** Tudo começou com um grupo de pessoas que sonhavam em conectar computadores para compartilhar informação, inclusive à distância. O primeiro experimento grande foi a ARPANET, uma rede criada pelo Departamento de Defesa dos Estados Unidos (através da agência DARPA) para que os computadores de distintas universidades e de centros de pesquisa pudessem "falar entre eles". O seu objetivo não era apenas compartilhar recursos e dados acadêmicos, mas também provar ideias de comunicações resilientes e distribuídas que permitissem manter a troca de informação, mesmo que partes da rede ficassem fora de serviço —uma preocupação estratégica do setor defesa durante a Guerra Fria. A DARPA financiou e coordenou a construção de nós e protocolos (como NCP e depois TCP/IP), promovendo a colaboração entre pesquisadores militares e acadêmicos e estabelecendo as bases técnicas e organizativas que logo permitiram a expansão da rede para usos civis e comerciais.

2. **Regras comuns:** À medida que mais redes se incorporavam, era necessário que todas falassem o mesmo "idioma". Assim nasceram os protocolos TCP/IP, um conjunto de regras que permitem que redes muito distintas se conectem entre si.

3. **WWW:** Nos anos 90 chegaram os navegadores web (por exemplo Netscape Navigator e Internet Explorer) e com eles a Internet se tornou muito mais acessível e fácil de usar. Antes dos navegadores gráficos a maioria dos recursos na rede eram consultados mediante interfaces de texto, comandos ou programas especializados. Os navegadores introduziram várias transformações-chave: interface gráfica e hipervínculos, padrão HTML e URL, integração multimídia e scripts, pesquisa e diretórios, comercialização, desenvolvimeno web e adoção massiva.

4. **Governança colaborativa:** Desde o começo, as decisões sobre como devia funcionar a Internet foram tomadas de forma aberta e participativa através de grupos de trabalho e de documentos públicos como a Solicitud de Comentarios (RFC, pelas suas siglas em inglês de Request for Comments).

Hoje, o funcionamento da Internet continua dependendo de uma infraestrutura física robusta, de normas técnicas compartilhadas (como TCP/IP) e de uma governança colaborativa onde participam tanto atores técnicos como sociais, garantindo que siga sendo uma ferramenta pública, aberta e universal.

COMO VIAJAM AS MENSAGENS: DO DISPOSITIVO PARA O SERVIDOR E DO SERVIDOR PARA O DESTINATÁRIO - ESPECTRO RADIOELÉTRICO

AS CAMADAS DA INTERNET

Existem diferentes modelos que explicam como funciona a internet: um modelo de três camadas que facilita o entendimento prático e geral da Internet, o modelo TCP/IP de quatro camadas e o modelo OSI de 7 camadas. Embora este documento esteja enfocado no modelo das três camadas, aqui apresentamos uma tabela comparativa entre os diferentes modelos.

Modelo de três camadas	Modelo OSI	Modelo TCP/IP
Camada 1: Infraestrutura física	Camada 1: Física	Camada 1: Acesso ao meio
Camada 2: Padrões e serviços técnicos	Camada 2: Enlace de dados	
	Camada 3: Rede	Camada 2: Internet
	Camada 4: Transporte	Camada 3: Transporte
Camada 3: Padrões de conteú-dos e aplicações	Camada 5: Sessão	Camada 4: Aplicação
	Camada 6: Apresentação	
	Camada 7: Aplicação	

Modelo de 3 camadas

O modelo de 3 camadas é uma forma simplificada de entender como está organizada a Internet e como os seus diferentes elementos interagem para nos permitir conectar-nos, comunicar-nos e compartilhar informações. Este modelo nos ajuda a visualizar que a Internet não é uma única coisa, mas sim uma rede complexa composta por distintos níveis, cada um com funções específicas.

Neste modelo, as camadas que compõem a Internet são:

(1) camada de infraestrutura física
(2) camada de padrões e de serviços técnicos
(3) padrões de conteúdos e de aplicações

Imagem 1: extraído de Cómo funciona internet, Karisma

CAMADA I: INFRAESTRUTURA FÍSICA

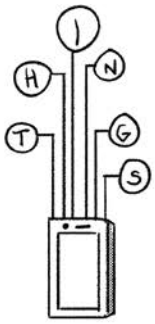
A camada física é a infraestrutura tangível pela qual viaja a Internet. Inclui antenas, satélites, cabos convencionais e de fibra óptica. Embora não a vejamos na tela, sem esta rede de equipamentos e cabos elétricos não poderíamos enviar mensagens nem fazer upload ou receber fotos. Em resumo: **é o conjunto de elementos físicos que transportam todos os dados que enviamos e recebemos.**

A camada física da Internet está composta por cabos e equipamentos como roteadores que conectam entre si a múltiplos Sistemas Autônomos (AS) em pontos-chave chamados Internet Exchange Points (IXP). Estes últimos permitem interconectar dados entre si e costumam estar localizados em grandes centros de dados que estão ligados todo o tempo.

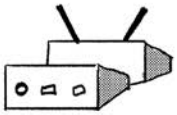
Está composta pelos seguintes elementos:

- Cabos submarinos e terrestres
- Antenas e torres
- Centros de dados
- Roteadores, switches
- Pontos de Interconexão de Internet (IXP)

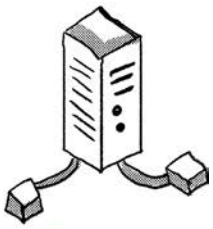
Computadores
(servidores, computadores pessoais, dispositivos móveis)



Internet das coisas
(IoT, em inglês Internet of Things.)



Dispositivos de rede
(roteadores, gateways,comutadores, repetidores, etc.)



Centros de dados
(em inglês, 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.

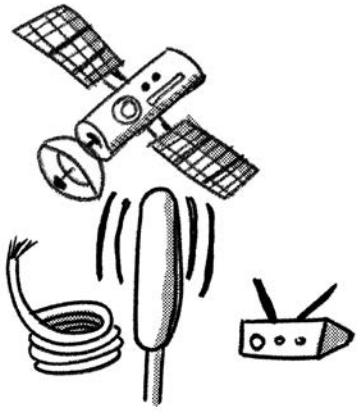
Para o que serve esta camada?

- Conecta todo o mundo em uma única rede.
- Transporta os dados de forma rápida e eficiente.
- Interconecta redes distintas, fazendo que as comunicações não tenham fronteiras.
- Suporta todos os outros níveis da Internet. Sem esta camada, nada funciona.
-

Um **Sistema Autônomo (AS)** é uma grande rede independente (por exemplo, um operador de Internet, uma universidade ou empresa grande) que controla o seu próprio tráfego interno.

Os IXP são lugares físicos onde muitos AS se interconectam e compartilham dados de forma direta, fazendo que a Internet seja mais rápida, estável e barata.

Os cabos físicos (especialmente de fibra óptica) transportam dados a grande velocidade entre continentes, países e cidades. Os roteadores e switches são encarregados de direcionar essa informação pela melhor rota possível, garantindo que os dados cheguem ao seu destino correto. São grandes redes independentes, de operadores de Internet, universidades ou empresas que gerenciam as suas próprias rotas internas de dados.



Cabos de telecomunicação, redes sem fio, redes satelitais

Elemento	O que faz?	Exemplo
Cabos de fibra óptica	Transportam dados a grande velocidade usando luz.	Cabo submarino entre continentes
Antenas e torres	Enviam dados pelo ar.	Torre de celular
Satélites	Permitem conexão em lugares remotos.	Internet em zonas rurais
Roteadores e switches	Redirecionam dados para o seu destino.	Roteador da sua casa ou empresa
Centros de dados	Lugares onde muitas redes se conectam.	Ponto de interconexão de tráfego (IXP)

CAMADA 2: PADRÕES E SERVIÇOS TÉCNICOS (OU CAMADA LÓGICA)

Esta camada é a encarregada pelo funcionamento correto da Internet a nível técnico. Se a camada anterior era semelhante às rodovias, ruas e pontes da nossa Cidade Digital, esta poderia ser traduzida como as regras de circulação das vias. Por exemplo, como operam os sinais de trânsito, por onde transitam os dados e como devem fazê-lo, as velocidades máximas e mínimas, entre outros aspectos. Esta camada precisa de uma grande participação de instituições privadas e de agrupações profissionais que determinam as condições técnicas e padrões que facilitam a interconexão de informação na Internet.

Como os nós se comunicam em uma rede?

A Internet precisa que distintos nós (clientes, servidores e dispositivos de rede) se comuniquem entre eles, para que isto ocorra é necessária uma linguagem comum que permita que os diferentes nós se entendam. Por isso foi criado um sistema de regras com uma sintaxe particular que permite dito entendimento. Dito sistema de regras responde às seguintes perguntas:

- Posso pôr um pacote de dados dentro de outro?
- O que acontece se um pacote não tem informação de endereço ou de destinatário?
- Como são enviados os dados através da Internet? É enviado um único pacote grande ou é dividido em partes menores?
- É possível modificar uma informação enquanto viaja pela Internet?
- O que acontece quando uma informação é perdida? É possível perder informação enquanto viaja pela cidade digital?
- De quais detalhes precisa um pacote de dados para viajar pela Internet?

O que são os pacotes?

Os pacotes são as unidades nas quais a informação é dividida para viajar por uma rede. Ou seja, todo dado que pretende ser enviado através de uma rede é dividido em pacotes. Cada pacote contém duas partes principais:

- **Cabeçalho (header):** leva metadados necessários para que a rede entregue o pacote corretamente —por exemplo, endereços IP de origem, e de destino, números de porta, informação de fragmentação, controle de erros e de encaminhamento.
- **Carga útil (payload):** é o conteúdo real que está sendo enviado (fragmento do arquivo, parte de um correio, uma petição HTTP, etc.).

Características importantes

- **Fragmentação e reagrupação:** uma mensagem grande é dividida em vários pacotes; o receptor volta a reagrupá-los adequadamente.
- **Encaminhamento:** os roteadores leem o cabeçalho do pacote para decidir por qual caminho enviar cada paquete para o seu destinatário.
- **Confiabilidade vs. velocidade:** protocolos como TCP agregam controle de erros e confirmações para garantir a entrega; UDP prioriza rapidez sem garantias.
- **Tamanho limitado:** cada meio/rede impõe um tamanho máximo por pacote (MTU); pacotes muito grandes são fragmentados.

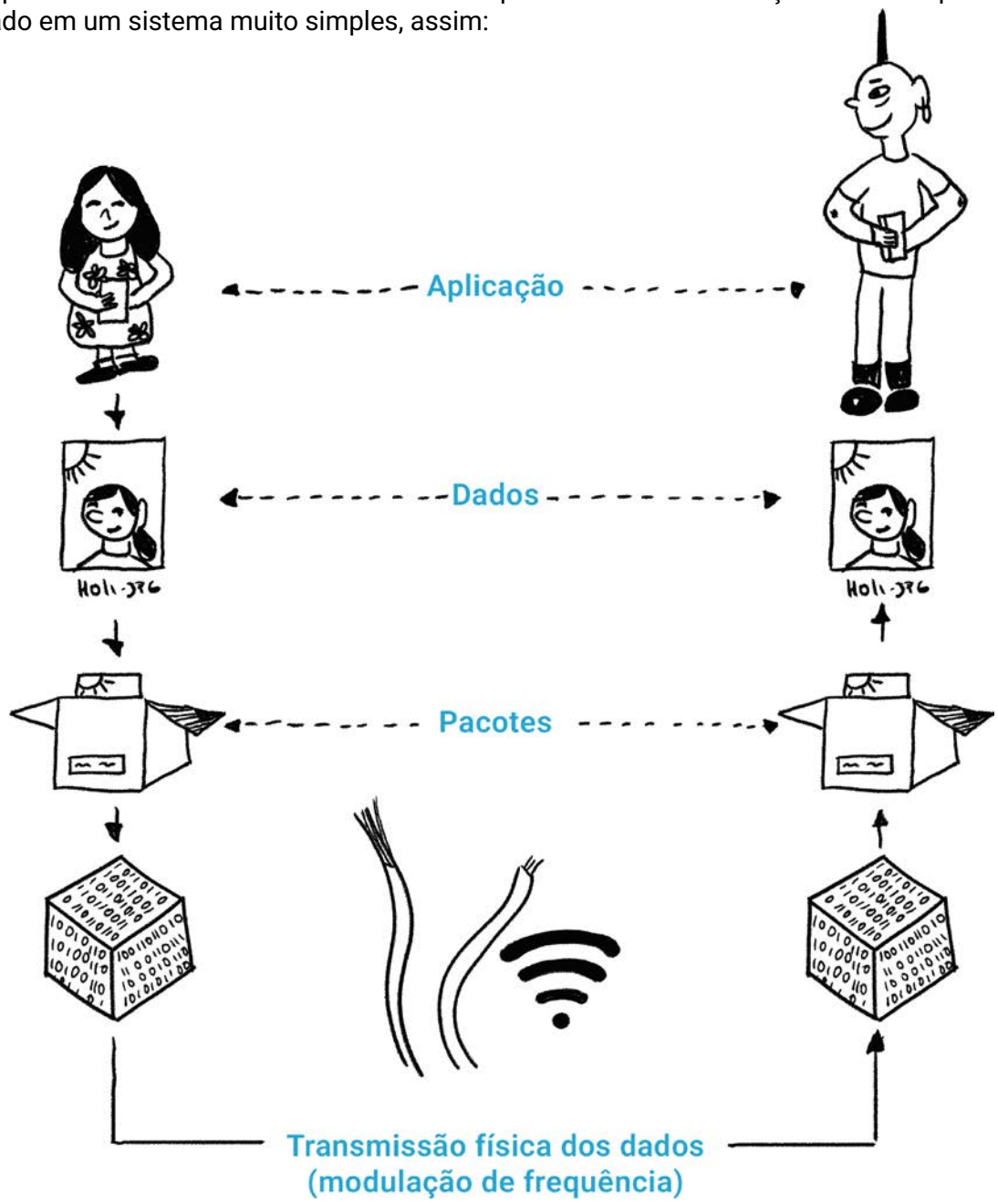
> Pense em um envio de mensagens. O cabeçalho equivale à etiqueta externa com o endereço, o remetente, as instruções de manejo e os dados de rastreamento; a carga útil equivale ao objeto dentro da caixa.

Damos o exemplo do envio de um vídeo ou de uma fotografia pelo WhatsApp ou por qualquer outro meio de envio de mensagens: dito elemento seria descomposto em vários pacotes que são enviados de forma independente. Isto é muito útil, pois imagine que sua foto for perdida completamente, ela teria que ser enviada novamente na íntegra, enquanto que se uma parte dessa foto for perdida, é muito mais fácil reenviar apenas essa parte.

Do que os pacotes estão compostos?

No mundo digital, os dados sempre são apresentados no seu nível mais básico desde um sistema binário, isto é, zeros (0) e uns (1). Este é o sistema de dados que podem ser processados pelos computadores. Dita codificação muda dependendo do meio, isto é, pode mudar se passar por ondas, cabo de cobre ou fibra óptica.

Desde o ponto de vista das camadas da Internet o processo de comunicação entre nós pode ser visualizado em um sistema muito simples, assim:



Fonte: Adaptado e traduzido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021.

O protocolo TCP/IP

Toda esta comunicação precisa de regras, as quais chamaremos protocolos. Embora existam diferentes tipos, o principal a nível da Internet é o Internet Protocol (IP). Este é o encarregado de definir o formato do cabeçalho dos paquetes que viajam pela Internet, isto é, entre os dispositivos da rede desde o seu emissor até o seu destinatário. Incluindo, é claro, a informação que leva o cabeçalho dos pacotes e o seu formato.

A principal virtude deste e de outros protocolos é que permitem enlaçar distintos tipos de dispositivos (por exemplo, um computador, um celular ou um servidor) que executam sistemas operativos distintos (Windows, Linux, Android ou MacOS) sobre distintos tipos de redes.

Como funciona?

Primeiro, é atribuído um endereço IP para todo dispositivo conectado a uma rede. Este aspecto é chave para comunicar-se através da Internet, sempre e quando o endereço respeitar o padrão. Existem dois tipos de **endereços IP:**

- **Públicos:** Aqueles que têm acesso direto à Internet.
- **Privados:** Aqueles que não têm acesso direto à Internet, mas são conectados a esta através de um intermediário. Por exemplo, o roteador de um escritório ou de uma casa.

O roteador, como dispositivo de rede, tem atribuído um endereço IP público, determinado pelo Operador de Serviço de Internet (abordaremos isto mais adiante) e, por sua vez, fornece para cada dispositivo conectado à sua rede local (LAN) um IP privado.

Uma condição importante para os IP públicos e privados é que todo endereço deve ser único dentro da rede. Isto quer dizer que ninguém na extensão da Internet pode ter o mesmo endereço IP que outro nó/dispositivo. Sempre existe um destinatário e um emissor com um endereço IP único que evita que haja confusões durante a comunicação. Imagine solicitar um delivery e que no seu mesmo bairro ou cidade tenha duas pessoas com o mesmo endereço. Que problema!

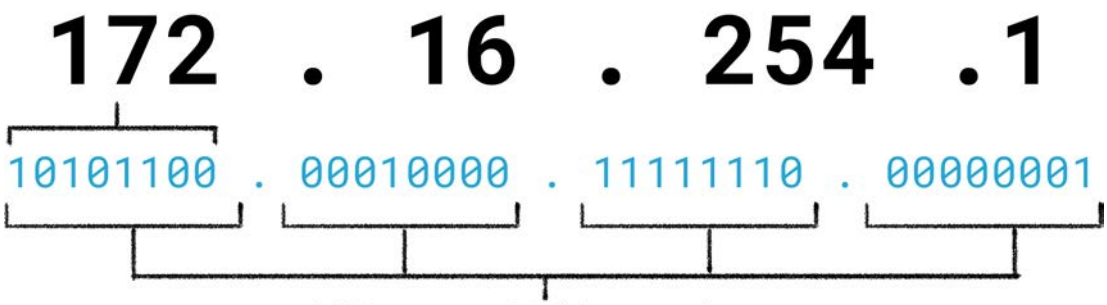
Como se veem os endereços IP?

Atualmente, existem duas versões de endereços IP, cada uma tem uma aparência diferente:

- **IPv4:** A versão mais usada na Internet, embora que não tenha tantos endereços disponíveis (dispõe apenas de 4.300 milhões) para todos os dispositivos e pessoas que agora se conectam à Internet.
  Está composta por quatro séries numéricas entre 0 e 256, separadas por pontos
- **IPv6:** A versão mais recente e eficiente, é capaz de cobrir a imensidão dos dispositivos conectados à Internet por muitíssimos anos. Não nos aprofundaremos na composição desta versão, mas só para matar a curiosidade, assim se ve:
  `2001:0DB8:0000:0001:0000:0000:0010:01FF`

Você se lembra que dissemos que tudo viaja na Internet com o sistema binário? A título de ilustração, assim se representa a seguinte IPv4 em número binário:

Estrutura de um endereço IP (Versão 4 ou "IPv4")



8 bits x 4 = 32 bits, ou 4 bytes

Extraído de Paz Peña (2013, p. 17)

Como são usados os endereços para enviar os pacotes por Internet?

Cada pacote leva no seu cabeçalho o endereço IP de origem e o endereço IP de destino. Esses endereços permitem que a rede saiba de onde vem o pacote e onde deve chegar. O envio funciona assim:

1. O dispositivo emissor cria o pacote com o endereço IP destino no cabeçalho e envia ao roteador local (por exemplo, o roteador de casa).
2. O roteador local examina o endereço destino e consulta a sua tabela de encaminhamento para decidir qual é o seguinte salto —normalmente envia o pacote ao roteador do operador de Internet (ISP)—.
3. Cada roteador intermediário repete o processo: lê a IP destino, consulta a sua tabela de rotas e reenvia o pacote para o seguinte roteador que o aproxima do destino.
4. O pacote avança por uma cadeia de roteadores e redes (backbones do ISP, roteadores regionais, etc.) até que chega a um roteador que está na mesma rede que o dispositivo destino.
5. Este último roteador entrega o pacote para o dispositivo receptor para a entrega final.
6. No destino, o pacote é substituído por outros pacotes (se a mensagem foi fragmentada) e a camada de transporte (p. ex. TCP) verifica integridade e ordem; se faltar algum pacote, o receptor solicita reenvio.

DNS: Sistemas de Nomes de Domínio

O que é um servidor?

Os conteúdos e serviços da internet estão armazenados em computadores da rede. Os sites, por exemplo, estão hospedados nestes tipos de computadores que chamamos servidores. Um servidor é um computador especializado que armazena dados e serviços disponíveis na internet. Diferentemente de um computador pessoal, um servidor está projetado para responder de forma contínua e eficiente a múltiplas solicitações de outros computadores (como a sua) que tentam acessar aos sites, aos e-mails, aos arquivos ou às plataformas.

Normalmente, em vez de usar um endereço IP para acessar os conteúdos, eles são encontrados através do seu **nome de domínio**. Este nome permite acessar aos sites e aos serviços na Internet sem ter que lembrar do endereço IP e, para isso é usado o serviço **DNS** (Domain Name System, pelas suas siglas em inglês) que funciona de forma parecida a um catálogo telefônico, permitindo encontrar um endereço IP a partir do nome de domínio. Por exemplo, o domínio karisma.org.co é resolvido pelo endereço IP 5.9.111.213.

Os servidores web podem estar em qualquer parte do mundo e um único IP pode hospedar muitas páginas distintas. Por exemplo, uma empresa pode ter várias páginas hospedadas em um mesmo servidor. O lugar físico onde está um servidor (isto é, em qual país ou região está hospedado) determina quais leis são aplicáveis. Por exemplo, na Europa, os servidores devem cumprir com o Regulamento Geral de Proteção.

Os nomes de domínio funcionam como um tradutor de endereços IP para nomes que podemos lembrar mais facilmente. Aqui é importante saber como funcionam as páginas web e o cache, mas antes de aprofundar no tema, voltemos para a nossa Cidade Digital.

Cada casa ou edifício precisa de um endereço claro para que outras pessoas possam chegar a ela sem dificuldades. Entretanto, quando se trata de sites, teríamos que consultá-los sabendo o endereço IP do site. Imagine que sempre que você quiser entrar à sua rede social favorita ou ao site da sua universidade ou do seu colégio você tivesse que escrever um endereço IPv4 como **172.16.254.1** ou, pior, em IPv6 algo como **2001:0DB8:0000:0001:0000:0000:0010:01FF**. Seria difícil, verdade? Pois imagine que os DNS são semelhantes a um catálogo telefônico que evita que tenhamos que lembrar dos endereços IP de todos os sites. Isto significa que, daqui em diante, você só terá que lembrar do nome do site que quer visitar e o navegador ou a aplicação que você usa resolverá o endereço do site que você está querendo consultar —muito mais fácil—. Isto implica que não podem existir dois nomes exatamente iguais.

Os nomes de domínio são uma base de dados pública e descentralizada que associa um nome único a um endereço IP junto a outros dados. Da mesma forma que outros protocolos na Internet, os nomes de domínio têm algumas regras, aqui apresentamos as principais:

- **Subdomínio:** o dono de um domínio registrado pode criar os subdomínios que desejar, inclusive sub-subdomínios, sub-sub-subdomínios e assim consecutivamente. Ninguém pode registrar ou comprar um subdomínio de outro domínio de forma separada.
- **Domínio:** Qualquer pessoa ou organização pode comprar um nome de domínio a uma organização ou empresa aprovada pela ICANN.
- **TLD (top level domain):** Existem mais de 300 TLD comuns.
- Raiz: São os servidores DNS que protegem no nível mais alto os registros de todos os TLD e é mantido pela ICANN.

Isto em conjunto se vê, por exemplo, assim:

Quando você faz a pesquisa no navegador da sua preferência, é feita uma solicitação nos servidores DNS para encontrar o endereço IP que você está solicitando.

> Se você desejar aprender mais e de forma interativa sobre os DNS, recomendamos este recurso:
>
> Cómo funciona DNS

Aspectos comerciais da infraestrutura da Internet: os ISP

Para ter acesso à Internet desde qualquer dispositivo é necessário contar com as condições técnicas —que já vimos ao longo do curso— mas também com as condições comerciais de obter acesso à Internet. Aqui devemos acrescentar as organizações intermediárias que investem em condições técnicas e físicas para dar cobertura de Internet e obter uma retribuição econômica em troca. Eles serão chamados operadores de serviço de internet (ISP, pela sua sigla em inglês: Internet Service Provider). Empresas como Claro, Movistar e Tigo na Colômbia, ou internacionais como AT&T e Verizon.

Os ISP são os intermediários entre as pessoas usuárias e a infraestrutura da Internet. É importante ter presentes características como cobertura, tecnologia (cabo, fibra óptica, banda larga, etc.) e velocidade. Os ISP cumprem um rol fundamental no funcionamento da internet porque permitem que as pessoas e as organizações se conectem com o resto da rede.

Entre as suas funções e capacidades estão:

- Atribuir endereços IP aos dispositivos.
- Encaminhar o tráfego, isto é, decidir por onde viajam os dados para chegar ao seu destino.
- Administrar a infraestrutura técnica que torna possível a conexão.
- Filtrar, bloquear ou priorizar certos conteúdos ou serviços, o que lhes dá um grande poder sobre o tipo de acesso que as pessoas têm.
- Oferecer planos diferenciados que afetam a velocidade ou disponibilidade de aplicações específicas.

O acesso à internet pode ocorrer de distintas formas dependendo da tecnologia disponível, da localização geográfica e das decisões dos operadores. Cada tipo de acesso tem implicações na velocidade, qualidade, preço e estabilidade da conexão e pode influenciar diretamente quem acessa, como o faz e para que.

Estes são os tipos mais comuns de acesso à internet:

- **Banda larga:** Fornece internet através de cabos ou linhas telefônicas. É comum em serviços de televisão por cabo. Tem boa velocidade, mas é menos estável que a fibra. Muitos lares em cidades ainda acessam à Internet desta maneira.
- **Fibra óptica:** É uma das conexões mais rápidas e estáveis. Usa cabos especiais que transmitem dados através da luz. Costuma estar disponível em zonas urbanas, é cara de instalar em zonas rurais. Os ISPs que oferecem este serviço costumam ser grandes operadores.
- **DSL:** funciona através de linhas telefônicas. É mais lenta e está sendo substituída por tecnologias mais modernas. Ainda é usada em zonas com infraestrutura limitada.
- **Sem fio:** Redes satelitais ou móveis (comuns em zonas rurais).
- **Internet móvel (3G, 4G, 5G):** Utiliza redes celulares. É muito comum em setores onde não existem conexões fixas ou quando o acesso é feito desde celulares. Depende da cobertura das antenas instaladas pelas empresas de telecomunicações.

Quais instituições regulam e se envolvem diretamente nestes padrões?

ICANN: Coordena nomes de domínio e endereços IP com participação global e aberta. As decisões são tomadas por consenso. Um exemplo de gestão deste espaço são as Políticas sobre datos de registro e transferencia de dominios

IETF (Internet Engineering Task Force): Organismo que estabelece padrões técnicos TCP/IP através de consensos abertos. Estes padrões são adotados por pessoas usuárias, redes e fabricantes para construir a Internet que usamos. Embora seja um espaço técnico, as organizações da sociedade poderiam aliar-se para gerar uma participação através de equipes técnicas e não técnicas que possam incidir em considerações de segurança e de privacidade neste espaço. Porém, a influência prática costuma precisar de contribuições técnicas (propostas, implementação, testes). A IETF não é um fórum político amplo; a sua linguagem e os seus processos são técnicos, por isso que a entrada efetiva para atores não técnicos costuma precisar de apoio.

IANA (Autoridade para Atribuição de Números da Internet): É uma organização membro da ICANN, responsável por coordenar com registros regionais da Internet (RIRs, por exemplo, LACNIC para América Latina e o Caribe) os operadores de serviços, os operadores de redes e a comunidade técnica para garantir que os identificadores da Internet sejam únicos e estejam bem coordenados. As suas funções cobrem: atribuição e gestão de espaço de endereços IP e a gestão de nomes de domínio de alto nível.

LACNIC: Registro Regional de Endereços IP da América Latina: É a organização regional (RIR) responsável pela atribuição e administração de recursos numéricos da Internet (IP) na América Latina e no Caribe.

CAMADA 3: CONTEÚDOS E APLICAÇÕES

A camada de conteúdos e de aplicações é a que usamos diretamente quando navegamos pela Internet. É o que vemos, tocamos e com o que interagimos: páginas web, e-mails, aplicações de mensagens, redes sociais, vídeos, entre outros.

Normalmente, nós a associamos com a "Internet", porque é a mais visível e cotidiana. Mas, como já vimos, debaixo existem outras camadas que fazem possível que tudo isto funcione.

Uma metáfora para entendê-lo

Se seguimos com a comparação viária, esta camada estaria composta pelos veículos que circulam pelas ruas:

- Graças a ela podemos mover-nos, comunicar-nos e transportar informação.
- Aqui estão os espaços onde nós nos expressamos, compartimos saberes, construímos comunidade e exercemos cidadania.

Todas as nossas ações na Internet ocorrem aqui: pesquisar no Google, mandar um e-mail, bater papo no WhatsApp, fazer uma videochamada ou fazer upload de um vídeo. Nela os dados circulam e permitem a conexão com outras pessoas em questão de segundos.

E quando dizemos que "aqui estão os espaços onde nos expressamos, compartilhamos saberes, construímos comunidade e exercemos cidadania", indicamos que a Internet não é apenas tecnologia: também é um espaço social e político. Na Internet nós nos organizamos, denunciamos, compartilhamos aprendizados, fazemos campanhas ou comemoramos. Em outras palavras, esta camada pode ser entendida como uma praça pública digital onde ocorre a nossa vida on-line e onde estão em jogo direitos como a liberdade de expressão e o acesso à informação.

Por que esta camada é importante?

A camada de conteúdos e de aplicações é onde realmente vivemos a Internet: é o espaço visível e tangível que nós usamos para comunicar-nos, aprender, entreter-nos e organizar-nos. Aqui convergem páginas web, mensagens, redes sociais, plataformas de vídeo, e-mails e diversas aplicações; são os espaços de encontro onde ocorrem as nossas conversas, conhecimentos e experiências sociais. Ao interagir com um app ou abrir uma página não vemos os cabos nem os protocolos, mas sim sentimos de imediato a experiência —a rapidez, a interface, a possibilidade de compartilhar— que define como nos relacionamos on-line.

Além disso, esta camada também é um espaço social e político: nela exercemos direitos digitais como a liberdade de expressão, o acesso à informação e à associação. É a praça pública digital onde construímos comunidade, denunciamos injustiças, difundimos aprendizados e organizamos iniciativas coletivas. Uma praça pública digital? Sim, mas diferentemente de uma praça física que pertence a todas as pessoas, esta praça digital está em grande parte gerenciada por plataformas privadas como Meta, Google, X, TikTok, etc., que decidem o que pode ser mostrado, o que deve ser ocultado e o que deve ser eliminado. Por isso, o seu desenvolvimento, governança e acessibilidade importam tanto como a infraestrutura técnica que a sustenta: limitar, censurar ou dificultar o acesso a estes conteúdos equivale a restringir a vida pública e democrática que hoje circula na Internet.

Para que serve esta camada?

Serve para muito mais que “bater papo” ou “ver vídeos”. Aqui as nossas interações digitais são organizadas e ganham forma. Nela são definidas muitas regras invisíveis:

- O que aparece primeiro em uma pesquisa.
- Qual conteúdo é recomendado no nosso muro.
- Quais publicações são eliminadas por descumprimento das normas da comunidade.
- Quais mensagens ou vídeos se tornam virais e quais ficam escondidas.

Em outras palavras, esta camada não apenas conecta pessoas, também influencia em qual informação circula e como é distribuída.

Alguns protocolos por trás da cena

Dentro desta camada estão contidas regras técnicas que fazem que tudo funcione:

Extraído da Fundação Karisma (2024)

HTTP e HTTPS

Quando você entra em uma página web e escreve algo como `www.fundacionkarisma.org` o seu navegador precisa de um protocolo para pedir para o servidor que mostre essa página para você. Esse protocolo se chama HTTP (Hypertext Transfer Protocol).

- **HTTP (Hypertext Transfer Protocol)**
  É o protocolo mais antigo e tradicional para navegar pela Internet.
    - Funciona como se você mandasse um cartão postal sem envelope: a informação viaja "à vista".
    - Qualquer pessoa que interceptar a comunicação poderia ler o que você faz, por exemplo se você usa uma rede Wi-Fi pública ou se alguém está espiando o tráfego.
    - Isso significa que os seus dados (como o que escreve em um formulário) podem ser vistos ou modificados.

- **HTTPS (Hypertext Transfer Protocol Secure)**
  É a versão segura do HTTP.
    - Aqui o cartão postal viaja dentro de um envelope fechado com cadeado. Esse cadeado é a criptografia que protege a comunicação usando um sistema chamado TLS (Transport Layer Security).
    - Com o HTTPS, embora alguém intercepte a conexão, não poderá ler o que você envia nem o que recebe (como senhas, mensagens ou números de cartão).
    - Os navegadores costumam mostrar um cadeado ao lado do endereço web para indicar que a conexão é segura.

Em poucas palavras: se você vir HTTP, desconfie para coisas sensíveis; se você vir HTTPS, tem uma camada extra de segurança.

> Se você deseja aprender mais e de forma interativa sobre os DNS, recomendamos este recurso:
>
> Cómo funciona HTTPS

SMTP: o carteiro dos e-mails

O e-mail também precisa de um protocolo para funcionar. Quando você escreve uma mensagem e clica em **"enviar"**, a sua aplicação de e-mail (Gmail, Outlook, Thunderbird, etc.) usa **SMTP (Simple Mail Transfer Protocol).**

- Pense em SMTP como o **carteiro digital**: recolhe o seu e-mail e entrega-o ao servidor de destino.
- Importante: SMTP **só envia e-mails**, não os recebe.
- Para recebê-los, são usados outros protocolos chamados **POP3** ou **IMAP**.
    - **POP3** faz o download dos e-mails para o seu dispositivo.
    - **IMAP** permite vê-los desde vários dispositivos porque os mantêm sincronizados no servidor.

Embora muitas vezes vemos apenas a interface do Gmail ou do Outlook, no fundo são estes protocolos que tornam possível que as suas mensagens viajem de um lugar para outro.

Conhecer estes protocolos não é apenas “tecnicismo”, mas nos dá ferramentas para tomar decisões mais seguras. Por exemplo, saber que o HTTPS protege os nossos dados ou que o IMAP permite manter sincronizada a bandeja de e-mail no celular e no computador.

Vejamos como funciona a camada de transportes nos dois cenários cotidianos:

PARTE I - COMO ACESSAMOS AOS CONTEÚDOS NA INTERNET?

Quando entramos ao nosso navegador da Internet para pesquisar algo —por exemplo, “segurança digital”, uma notícia ou um vídeo de música— normalmente não sabemos em qual lugar do mundo está essa informação nem em qual computador está guardado. Pode estar na Colômbia, nos Estados Unidos ou em um servidor em outro continente.

O surpreendente é que, embora fisicamente possa estar muito longe, chegamos a ela em segundos. Isso é possível graças a uma série de passos que ocorrem em segundo plano que permitem que a informação viaje desde onde está armazenada até a sua tela.

Paso 1: usamos um navegador

Quase sempre, o primeiro que fazemos para ingressar na Internet é abrir um navegador como Google, DuckDuckGo ou Bing. Escrevemos uma palavra ou uma pergunta (“o que é phishing”, “receitas de arroz com coco”, “como proteger a minha senha”), e em milésimos de segundo aparece uma lista de páginas relacionadas.

Mas atenção: os navegadores não são neutros. Eles decidem o que mostrar primeiro e o que esconder mais abaixo.

- Fatores como quantas pessoas visita uma página, que tão confiável parece, se tem enlaces de outros sites ou inclusive se está pagando publicidade influenciam na ordem dos resultados.
- Em outras palavras, o navegador não nos ajuda apenas: também filtra, organiza e prioriza o que podemos ver.

Pensemos em um exemplo cotidiano, pergunte no seu bairro onde vendem bom pão. Cada pessoa recomendará algo distinto para você: a padaria mais famosa, a que está mais perto ou do seu primo. O navegador faz algo parecido, mas a grande escala.
Atividade rápida: Ingresse na mesma palavra no Google e no DuckDuckGo. Quais diferenças você encontra nos primeiros resultados que aparecem?

Passo 2: Abrimos uma página web utilizando uma URL

Quando clicamos em um resultado, estamos entrando em uma página web que tem um endereço como www.karisma.org.co ou www.wikipedia.org.

Passo 3: o domínio se converte em um endereço IP (DNS)

Aqui entra em ação o **DNS (Sistema de Nomes de Domínio)**, o qual traduz o nome da página para o endereço IP que indica exatamente onde está hospedado e disponível o site ou serviço que estamos solicitando (sempre que, de fato, exista).

Pensemos em outro exemplo simples: quando você marca "Mãe" no seu celular, não está escrevendo o número completo, mas o seu telefone o procura na sua agenda e marca o número correto. O DNS faz o mesmo, mas em escala global.

Passo 4: o servidor responde

Quando você visita uma página, o seu computador envia uma solicitação para o servidor onde está guardada esta página, utilizando o endereço IP. Este servidor é esse grande computador que armazena todos os arquivos: textos, imagens, vídeos, etc. Se o servidor estiver disponível, responde enviando-lhe o conteúdo pedido.

Exemplo: Você pede uma pizza por delivery. Você telefona (faz a solicitação), a pizzaria prepara e envia o seu pedido (o servidor responde), e finalmente você saboreia a sua pizza em casa (o seu navegador mostra a página).

PARTE 2 COMO VIAJA UMA MENSAGEM DE WHATSAPP OU POR MENSAGEM INSTANTÂNEA?

Agora pensemos em algo mais cotidiano: enviar uma mensagem pelo WhatsApp.

Passo 1:
Você escreve uma mensagem (“vou em caminho”) e oprime **enviar**

Passo 2:
O seu celular a converte em uma linguagem que a rede entende: **zeros e uns (bits)**.

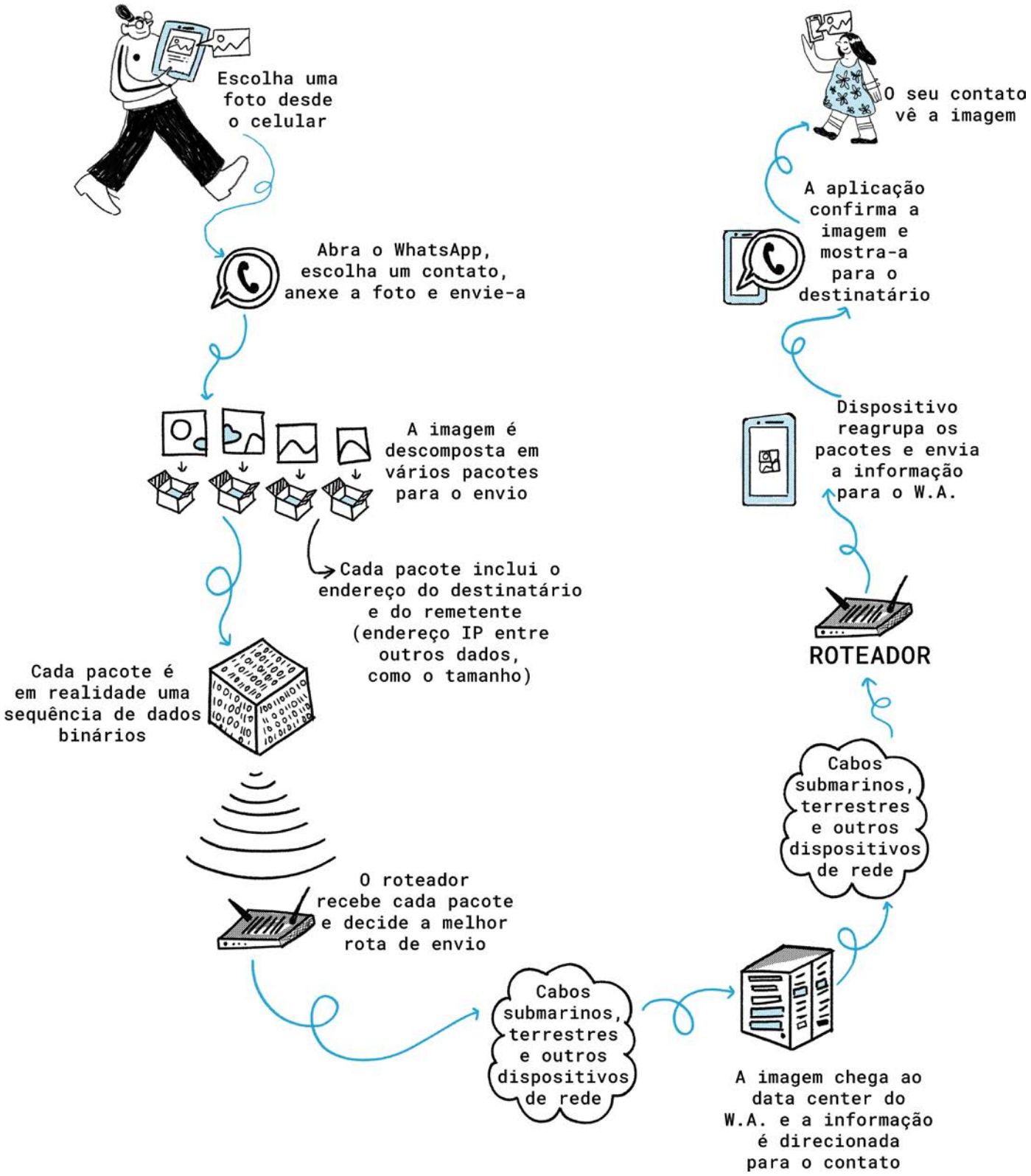
Passo 3: De acordo com a sua conexão:
- Se você estiver em Wi-Fi esses bits viajam como ondas de rádio até o seu roteador.
- Se você estiver em rede móvel (4G/5G) viajam como ondas até a antena celular mais próxima.

Passo 4:
Logo, o seu roteador ou antena as manda por cabos de fibra óptica até a rede do seu operador de Internet.

Passo 5:
Esse sinal chega aos servidores do WhatsApp (na nuvem). Lá acontece algo chave:
- A mensagem é criptografada para protegê-la.
- O sistema identifica quem é o destinatário e prepara o caminho de volta.

Passo 6:
Finalmente, a mensagem faz o percurso inverso até chegar ao celular da sua amiga ou do seu amigo.

> **Imagine que é como enviar uma carta** muito rápido. O envelope (criptografado) garante que ninguém a leia no caminho, o carteiro (servidor) decide para onde deve ir, e a carta passa por várias ruas e agências de correio (roteadores, antenas, operadores) até chegar à casa correta.


Escolha uma foto desde o celular
Abra o WhatsApp, escolha um contato, anexe a foto e envie-a
A imagem é descomposta em vários pacotes para o envio
Cada pacote inclui o endereço do destinatário e do remetente (endereço IP entre outros dados, como o tamanho)
Cada pacote é em realidade uma sequência de dados binários
O roteador recebe cada pacote e decide a melhor rota de envio
Cabos submarinos, terrestres e outros dispositivos de rede
A imagem chega ao data center do W.A. e a informação é direcionada para o contato
Cabos submarinos, terrestres e outros dispositivos de rede
ROTEADOR
Dispositivo reagrupa os pacotes e envia a informação para o W.A.
A aplicação confirma a imagem e mostra-a para o destinatário
O seu contato vê a imagem

Criptografia e privacidade: Também, se você for uma pessoa usuária do WhatsApp terá percebido que na parte superior dos chats aparece o texto criptografado de ponta a ponta. Isto é muito importante, já que significa que a mensagem é “coberta”/“ocultada” no seu celular e só o outro celular pode lê-lo. Nem o WhatsApp pode fazê-lo.

Se enviamos uma mensagem em uma caixa fechada, apenas você e a outra pessoa teriam a chave para abri-la. Isto tem sentido por várias razões, entre elas porque na internet também temos direito à intimidade. A informação que compartilhamos, enviamos e recebemos deve permanecer entre as pessoas que nós decidirmos.

REFERÊNCIAS

- 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: Fundação Karisma

UNIDADE 2: MANIPULAÇÕES DA INTERNET E O DNS

Como já foi explicado na unidade anterior, a Internet opera através de um vasto sistema de protocolos interconectados e de estruturas de governança. Nesta unidade abordaremos o fenômeno das manipulações da Internet, entendidas como os bloqueios, quedas e cortes da Internet.

Além disso, vamos aproveitar o conhecimento que já obtivemos sobre o DNS e veremos como pode ser usado para evadir certo tipo de cortes da Internet, enquanto somamos privacidade e segurança ao nosso uso da Internet.

Compreender como funciona a filtragem, o bloqueio e os DNS alternativos é essencial para quem participa na governança da Internet, especialmente para as organizações sociais que trabalham pelos diretos humanos, pela liberdade digital e pelo acesso equitativo à informação.

Objetivo geral

Introduzir os conhecimentos-chave em torno das dinâmicas de controle, falhas e manipulação da Internet, mostrando como ocorrem os bloqueios, as estratégias e técnicas empregadas, e as medidas básicas para evitar ou contornar esses bloqueios (como o uso de DNS alternativos).

Objetivos específicos

1. Identificar as diferenças entre falhas, cortes e bloqueios da Internet e reconhecer as estratégias e as técnicas mais comuns de restrição a nível conceitual.
2. Examinar, mediante o caso da China e do WhatsApp, como são aplicadas estas técnicas na prática e quais efeitos têm sobre a comunicação e os direitos digitais.
3. Guiar em passos simples para configurar DNS alternativos e entender os seus benefícios e as suas limitações como medida introdutória de evasão de censura.

CONTROLE, FALHAS E QUEDAS DA INTERNET

Lembre-se que as redes podem entregar pacotes sempre que estes tiverem cabeçalhos corretos, independentemente do seu conteúdo, desde que os pacotes forem encaminhados; ou seja, que tiverem claro o seu remetente e o seu destino. Isto é o que chamamos de **neutralidade da rede**. Porém, às vezes, os Estados, as instituições ou outras autoridades querem impedir que as pessoas tenham acesso a determinados conteúdos na Internet. Estas medidas podem ter graves consequências para os direitos humanos e para as liberdades civis.

A nível nacional, os ISP poderiam ser obrigados a implementar medidas que incluam bloqueios e filtros em todo o tráfego que entra e sai do país. No que se refere ao controle regional de conteúdo, múltiplos nós da rede podem colaborar em vez de depender de sistemas centralizados. Além disso, as entidades como bibliotecas, universidades, lugares de trabalho e lan houses têm a capacidade de estabelecer os seus próprios controles de bloqueio e de filtragem de conteúdos, adaptando-se às suas necessidades específicas.

COMO FUNCIONAM OS CORTES DA INTERNET E O QUE IMPLICAM?

Existem pelo menos três estratégias:

Bloqueio

Torna um site ou serviço inacessível para um conjunto específico de usuários, com frequência funciona com a cooperação dos ISP locais. O bloqueio é uma forma mais direta de impedir o acesso a conteúdos, serviços ou plataformas on-line. A diferença da filtragem, que pode ser seletiva ou parcial, o bloqueio costuma ser total e impedir o acesso completo a um site ou a um serviço, com o objetivo de evitar que as pessoas usuárias cheguem a determinados sites ou aplicações. O bloqueio pode:

- Limitar o **direito à informação e à liberdade de expressão**.
- Ser aplicado de forma **arbitrária**, sem transparência nem justificativa clara.
- Dificultar o acesso a **serviços digitais essenciais**, como serviços públicos, serviços de saúde, canais de comunicação e de expressão on-line (por exemplo, redes sociais e aplicações de mensagens instantâneas seguras) ou serviços de armazenamento na nuvem.
- Gerar **efeitos colaterais:** ao bloquear um servidor completo, podem ser afetados outros sites não relacionados.

Filtragem

É um enfoque mais geral que trata de impedir o acesso ao conteúdo com base em características definidas, como o uso de determinadas palavras ou de conteúdo de imagens. A filtragem pode ter consequências diretas sobre os direitos digitais:

- Pode afetar a **liberdade de expressão e o acesso à informação.**
- Pode ser arbitrária ou desproporcional se não for feita com critérios claros e mecanismos de prestação de contas.
- Em contextos autoritários, é uma forma de censura que silencia vozes críticas ou torna invisível temas sociais e políticos.

Estrangulamento (ou degradação)

É utilizado para fazer que o acesso a alguns serviços ou sites seja muito difícil, lento ou praticamente impossível para algumas pessoas.

Técnicas

Bloqueio do IP
São bloqueios do endereço IP de origem e de destino. Pode ser usado para bloquear faixas de endereços IP.

Filtragem do conteúdo
Quem administra ou tem o controle de um roteador é capaz de ver o tráfego que passa através deste. Podem ler os cabeçalhos com informação dos sites que estamos visitando. Se uma conexão não está criptografada, o conteúdo da mesma poderá ser visto. Isto permite filtrar, por exemplo, sites que contêm determinadas palavras.

Filtragem da URL
Esta forma de filtragem escaneia as URL pesquisando palavras determinadas para bloquear o acesso.

Bloqueio do DNS
O bloqueio do DNS é um método que impede o funcionamento normal do sistema DNS, o qual dificulta a resolução de certos nomes de domínio. Os ISP aplicam estes bloqueios nos resolvedores de DNS sob o seu controle, geralmente predeterminados ao assinar o seu serviço da Internet. Se for implementado um bloqueio de DNS, ao tentar acessar a um site, o resolvedor de DNS do ISP pode simular que não encontra o servidor correspondente ou proporciona um endereço IP diferente, como mensagens de advertência. Este tipo de bloqueio afeta a todos os protocolos que dependem do sistema DNS, incluindo HTTP(S), FTP, POP e SSH.

Filtragens de pacotes
Os roteadores implementam na leitura dos pacotes alguns filtros com a finalidade de procurar descumprimentos de protocolos, vírus, spam ou intrusões, bloqueando ditos pacotes como consequência. Estes filtros também podem proteger as redes de ataques cibernéticos.

Inspeção profunda de pacotes (DPI: Deep Packet Inspection)
Similar à filtragem de pacotes, em vez de limitar-se a olhar os cabeçalhos dos pacotes, também lê os dados que contêm. A DPI é um software de processamento de dados que pode ser útil para ver o interior dos pacotes com a finalidade de identificar, supervisionar e solucionar anomalias na rede, mas os encaminhadores e servidores também podem utilizá-la para a extração de dados, para a escuta clandestina e para a censura na Internet. Esta tecnologia pode redirecionar, etiquetar, bloquear, limitar a velocidade e informar, ou pode descartar silenciosamente os pacotes que marque como suspeitos.

Apagões da Internet
Os Estados podem facilmente fechar uma rede inteira manipulando o protocolo que traça o mapa da Internet (BGP: Border Gateway Protocol). Além disso, podem ser produzidos cortes pela desconexão ou dano físico à infraestrutura da Internet.

Conteúdo e remoção de resultados de pesquisa
As técnicas de censura podem ser aplicadas na fonte do conteúdo, não apenas através da rede. Os editores, autores e operadores de serviços têm que cumprir os pedidos legítimos ou as leis aplicáveis para retirar, anular a publicação, suprimir da lista ou ocultar conteúdos quando assim for exigido pela lei ou pelos pedidos governamentais.

Bloqueio por porta ou protocolo
Interrompe certos serviços (como o WhatsApp ou o Tor) ao impedir a comunicação nos canais que usam.

Caso: restrições ao WhatsApp em distintos países.

Os governos ou operadores de internet (ISPs) não precisam “hackear” o WhatsApp. O que sim podem fazer é bloquear o acesso ao nível de rede. Isto impede que o WhatsApp funcione no seu celular ou no seu computador. Isto pode acontecer durante protestos sociais, eleições ou crises políticas para evitar que as pessoas se comuniquem ou compartilhem informação.

Método	O que fazem?	O que você percebe?
Bloqueio do IPs	Bloqueiam os servidores do WhatsApp.	As mensagens não podem ser enviadas nem recebidas.
Manipulação do DNS	Mudam ou bloqueiam o nome “whatsapp.com”.	Aparece “operador não encontrado”.
Throttling (limitação da largura de banda)	Reduz a velocidade só para o WhatsApp.	O texto chega lento. Áudios, vídeos ou ligações não funcionam.
Bloqueio de protocolos	Filtram e bloqueiam ligações e mensagens criptografadas.	Não é possível fazer ligações.
Bloqueio da versão web	Cortam o acesso ao WhatsApp desde os navegadores.	Funciona no celular, mas não no computador.

O CASO DO WHATSAPP NA CHINA: CENSURA E CONTROLE

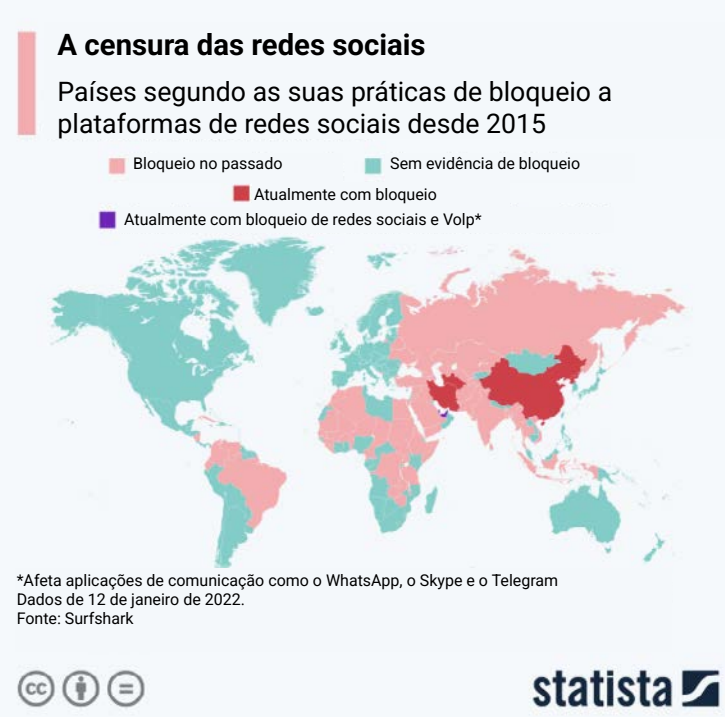
A China mantém um dos sistemas de censura da internet mais estritos do mundo, conhecido como o "Grande Firewall". Plataformas estrangeiras como o Facebook, o Twitter, o Google e o WhatsApp estão bloqueadas porque o governo não pode controlá-las facilmente nem acessar os dados que circulam por elas.

Por que o WhatsApp está bloqueado?

Criptografia de ponta a ponta: O WhatsApp criptografa as mensagens de ponta a ponta, o que impede que o governo chinês possa interceptar ou monitorar as conversas, diferentemente de aplicações como o WeChat.

Controle da informação: O governo chinês promove o uso de plataformas nacionais que cooperam com as autoridades e permitem o monitoramento e a censura, como o WeChat (propriedade da Tencent).

Sensibilidade política: Aplicações como o WhatsApp têm sido usadas para organizar protestos ou difundir informação crítica para o regime, o que é considerado uma ameaça pelas autoridades chinesas.



Cronologia:

- Em 2017, o acesso ao WhatsApp começou a ser restringido: primeiro as videochamadas e o envio de arquivos.
- Ao final de 2017, o WhatsApp foi bloqueado completamente na China.
- Atualmente, apenas é possível acessar ao WhatsApp na China usando VPNs, que também estão cada vez mais restringidas pelo governo.

Implicações:

- Este caso mostra a tensão entre a comunicação digital criptografada e o controle autoritário da informação.
- Também evidencia como as políticas nacionais podem redefinir o acesso às tecnologias globais, afetando a liberdade de expressão e a privacidade.

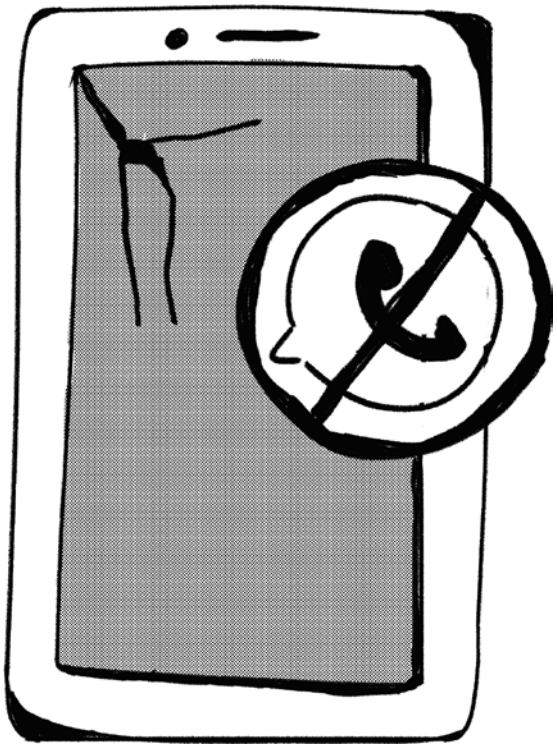
Além das práticas técnicas de censura e de controle, o bloqueio do WhatsApp na China está inscrito em dinâmicas geopolíticas e de soberania tecnológica. Os Estados —não apenas a China— tomam decisões sobre quais plataformas permitir ou restringir com base em considerações de segurança nacional, autonomia tecnológica, proteção de dados e controle do fluxo de informação. Nesse marco, promover plataformas locais (como o WeChat) forma parte de uma estratégia mais ampla para reduzir dependência de operadores estrangeiros, fortalecer indústrias nacionais e exercer capacidade de regulação sobre dados e conteúdos.

Entretanto, desde a perspectiva de direitos humanos a chave é a responsabilidade do Estado em garantir que as medidas que afetam o acesso à informação e à livre expressão sejam necessárias, proporcionadas e submetidas a normas e vias de reparação. O bloqueio do WhatsApp ilustra como políticas orientadas à soberania tecnológica podem ser traduzidas em restrições concretas para a comunicação privada e pública: a criptografia de extremo a extremo protege a privacidade e a liberdade de expressão das pessoas usuárias, mas também dificulta a vigilância exigida pelo Estado; a resposta estatal —bloquear a aplicação ou limitar funções— restringe direitos sem processos transparentes nem recursos efetivos para as pessoas afetadas.

O caso mostra três tensões centrais:

- **Soberania tecnológica vs. direitos individuais e coletivos**
  A busca de autonomia e de controle pode entrar em conflito com a proteção da privacidade, da liberdade de expressão e de outros direitos humanos conexos.
- **Segurança nacional e ordem pública vs. proporcionalidade e transparência**
  As medidas de bloqueio costumam ser justificadas em segurança, mas com frequência carecem de controles independentes e de avaliação de impactos.
- **Dependência tecnológica global vs. governança local**
  A infraestrutura e os serviços globais não operam em um vácuo político; as decisões regulatórias nacionais reconfiguram o acesso às tecnologias e aos mercados.

Enfocar a discussão desde os direitos humanos permite avaliar as medidas além do juízo geopolítico: trata-se de perguntar se as restrições são legais, necessárias, proporcionadas e sujeitas a supervisão independente; se existem canais para a reparação; e como afetam a grupos vulneráveis. Manter esse enfoque evita simplificações que associem automaticamente modelos tecnológicos com valores culturais ou civis, e põe o centro na proteção de liberdades fundamentais e na responsabilidade estatal em qualquer contexto político.



SERVIÇOS ALTERNATIVOS DNS

Um dos princípios-chave da governança da Internet é que a rede deve ser aberta, interoperável e acessível para todas as pessoas. Os bloqueios costumam ser realizados através do DNS. Diante desta situação, surgiram serviços alternativos de DNS como uma ferramenta técnica que permite às pessoas usuárias e às organizações sortear bloqueios injustificados, melhorar a sua privacidade e garantir uma experiência de navegação mais livre.

Os serviços DNS alternativos permitem substituir o servidor DNS padrão fornecido pelo seu operador da Internet por outro mais rápido, mais privado ou menos propenso a aplicar bloqueios. Quando o DNS do seu operador filtra ou bloqueia conteúdo, você pode mudar para um serviço DNS alternativo para ter acesso mais livre e seguro.

Exemplos dos DNS alternativos

`1.1.1.1` – Cloudflare (rápido e com enfoque em privacidade).
`8.8.8.8 y 8.8.4.4` – Google Public DNS.
`9.9.9.9` – Quad9 (com proteção contra malware).

A nossa recomendação:

- **Quad9** (excepcional para a filtragem de malware)
- **Mullvad DNS** (útil para maximizar a privacidade)
- **NextDNS** (para quem quer ter muito mais controle da sua informação, dos seus filtros e da sua segurança)

Tenha presente que embora seja uma ferramenta útil, **não protege contra bloqueios mais sofisticados**, como os feitos por IP ou inspeção profunda de pacotes.

Também, em alguns países, **trocar o DNS poderia ser monitorado ou restringido**, embora na maioria de contextos seja legal.

DNS over HTTPS

DNS over HTTPS (DoH) é uma tecnologia que criptografa as solicitações DNS que o seu navegador ou dispositivo faz, e envia-as através do protocolo HTTPS, o mesmo que é usado para conexões seguras a sites. Isto significa que ninguém entre você e o servidor DNS pode ver quais sites você está pesquisando.

Normalmente, quando você visita um site, o seu dispositivo pregunta para um servidor DNS “Onde está www.organizacion.org?”. Essa solicitação, na maioria dos casos, não está criptografada. Qualquer pessoa que interceptar o seu tráfego (operador de Internet, rede pública, inclusive governos) pode ver quais sites você está tentando visitar - inclusive se depois o conteúdo da página estiver protegido por HTTPS.

ATIVIDADE PRÁTICA:

no celular troque o DNS para Quad9

Objetivo: Aprender a mudar os servidores DNS predeterminados para melhorar a privacidade, velocidade de navegação e enganar bloqueios.

Quais benefícios traz mudar o DNS no seu dispositivo?

- **Privacidade:** criptografa as consultas DNS entre o seu dispositivo e o resolvedor, evitando que terceiros na rede (por exemplo, o operador de Internet, redes públicas Wi-Fi ou hackers na mesma rede) vejam quais domínios você consulta.
- **Integridade e segurança:** ao usar DoT (DNS over TLS) o risco de manipulação por atores intermediários das respostas DNS é reduzido.
- **Proteção em redes abertas:** em Wi-Fi públicas ou redes não confiáveis, evita que um atacante intercepte ou reescreva as respostas DNS.
- **Compatibilidade com posturas de segurança e de privacidade:** permite implementar um serviço de DNS que filtra sites maliciosos assim como rastreadores invasivos com a privacidade.
- **Evita filtragem passiva e a censura por DNS:** dificulta que operadores realizem análise passiva do tráfego DNS para perfis ou segmentação de usuários e bloqueio de serviços na Internet.

Quais efeitos negativos poderia chegar a ter de mudar o DNS?

Dependendo da qualidade, da estabilidade e da distância geográfica do servidor DNS que você configurar, poderia experimentar latência, algo que em termos práticos significa que alguns sites demoram em carregar um pouco mais, desde o imperceptível até o significativo. Entretanto, também é possível que você experimente o contrário: sites que carregam muito mais rápido que com o DNS predeterminado. Não se preocupe, sempre é possível experimentar que o servidor que melhor funcione na sua situação, recomendamos que você prove com Quad9, Mullvad DNS, NextDNS e Cloudflare DNS (este último é, normalmente, a opção mais rápida disponível, mas com menos enfoque na privacidade).

Do que você precisa?
De um celular com acesso à Internet Android ou iOS.

Dados de configuração para Quad9
Quando você configurar o seu DNS terá que pôr alguns dos seguintes dados. Dependendo do seu dispositivo, poderia precisar pôr o endereço IPv4, o endereço HTTPS ou o endereço TLS (este para os casos de Android). Esta é a forma na qual o seu dispositivo saberá para quem está fazendo a consulta DNS e utilizando qual protocolo.

```
IPv4
9.9.9.9
149.112.112.112

HTTPS (DoH)
https://dns.quad9.net/dns-query

TLS (DoT)
dns.quad9.net
```

Siga as instruções oficiais:
Guía para configurar el DNS em Android
Guía para configurar el DNS en iOS

Para verificar que ficou configurado corretamente, visite
https://on.quad9.net/

VOCÊ QUER APRENDER A DOCUMENTAR E ANALISAR CASOS DE DISRUPÇÕES DA INTERNET?

Apresentamos o Observatório de Bloqueios da Internet OBI

Acreditamos em uma Internet livre de censura e de bloqueios arbitrários. Por isso, o OBI põe à disposição ferramentas, guias e passos simples para que você se una a esta causa. A seguir, explicamos como usar o passo a passo. O Observatório de Bloqueios da Internet (OBI) é uma iniciativa da Karisma para que qualquer pessoa possa identificar, documentar e denunciar bloqueios na rede. Acreditamos em uma Internet livre de censura e de bloqueios arbitrários. Por isso, OBI põe à disposição ferramentas, guias e passos simples para que você se una a esta causa. A seguir, explicamos como usá-lo de forma geral.

1. Entre ao site oficial

Vá a https://obi.karisma.org.co/guia/. Lá encontrará informação-chave, tutoriais e enlaces que podem ser úteis.

2. Faça o download do guia "Está bloqueado?"

Clique no botão do enlace que diz " Faça o download do guia" ou "Está bloqueado?"
Este guia gratuito está pensado para qualquer pessoa, sem a necessidade de ser especialista.
O que ensina:

- Detectar um possível bloqueio
- Confirmar se é um erro ou um bloqueio real
- Documentar o que você encontrou
- Denunciá-lo para que outras pessoas saibam

3. Use ferramentas recomendadas pelo OBI

Dentro do guia ou do site você encontrará ferramentas como:

- OONI Probe: app gratuito que você pode instalar no seu celular ou PC. E realiza provas automáticas para detectar se uma página web está sendo bloqueada desde a sua rede.
- VPN: para saltar restrições geográficas ou de rede.

Nos guias do site OBI, você encontrará como usá-las passo a passo.

4. Documente o bloqueio

Quando você detectar um bloqueio:

- Anote qual é o site ou o serviço afetado
- Desde qual rede (Wi-Fi, dados móveis)
- Data e hora
- Qual mensagem de erro aparece (se houver)
- Você também pode fazer uma captura de tela

5. Denuncie o caso

Você pode enviar a sua denúncia para o OBI de maneira confidencial.
No site há formulários ou correios de contato.
Assim, a sua experiência se soma a uma base de dados coletiva que ajuda a:

- Visibilizar padrões de censura
- Promover a transparência
- Defender uma Internet livre para todas as pessoas

CONCLUSÕES

Ao longo deste módulo, exploramos as camadas fundamentais que permitem que a Internet funcione: desde como os nomes de domínio são traduzidos em endereços IP mediante o sistema DNS, até como este sistema pode ser manipulado para bloquear, filtrar ou restringir o acesso a certos conteúdos.

Aprendemos que tecnologias como HTTPS e DNS sobre HTTPS (DoH) não fazem apenas a navegação mais segura, mas que também se converteram em ferramentas de resistência diante da censura, da vigilância e dos bloqueios injustificados. Também vimos que mudar o servidor DNS é uma ação simples, mas poderosa que pode melhorar a privacidade e o acesso à informação.

Agora que já entendemos como a Internet funciona nas suas camadas técnicas e como a informação circula, podemos nos perguntar: quem decide as regras desse funcionamento? Quem controla o que acontece nesta grande rede? Veremos tudo isto no nosso seguinte módulo sobre Governança da Internet.

REFERENCIAS

- Asociación para el Progreso de las Comunicaciones. (n.d.). The (Internet) shutdown game. Consultado em 3 de Setembro de 2025 em https://shutdowngame.apc.org/
- Cute, B. (23 de Dezembro de 2019). 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
- Fundação Karisma. (2024). Cómo funciona Internet. Fundação Karisma. https://web.karisma.org.co/wp-content/uploads/2024/01/Como_funciona_internet. pdf
- Fundação Karisma & K+Lab. (n.d.-a). Guía para investigar bloqueos de Internet. Observatório de Bloqueios da Internet. Consultado em 3 de Setembro de 2025 em https://obi.karisma.org.co/guia/
- Fundação Karisma & K+Lab. (n.d.-b). Observatorio de Bloqueos de Internet. OBI. Consultado em 3 de Setembro de 2025 em https://obi.karisma.org.co/
- Fundação 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. (Setembro de 2024,). 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. Consultado em 3 Setembro de 2025 em https://www.ripe.net/community/internet-governance/internet-technical-community/iana/iana-stewardship-transition/3-what-is-iana/

MATERIAL ADICIONAL DE CONSULTA

1. Infraestrutura e Funcionamento da 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. Governança da Internet e DNS

- **ICANN Learn Platform:** Cursos gratuitos sobre governança e políticas da Internet ICANN for Beginners
- **¿Qué es el Internet de las cosas (IoT)?** - ¿Qué es el Internet de las cosas (IoT)? | IBM

3. Políticas de Acesso e Brechas Digitais

- ITU Report on Internet Accessibility in Developing Countries Facts and Figures 2024 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

cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

A INTERNET TEM REGRAS?

Falemos sobre a Governança da Internet

O que está em jogo para a sociedade civil?

Módulo 2

Ciclo de formação sobre governança da internet

Fundación Karisma

CONTENIDO

INTRODUÇÃO

A Internet é fundamental para a transformação da vida das pessoas e das sociedades através da digitalização, entendida não apenas como a adoção de tecnologias, mas também como a criação de novas formas de interação social, acesso ao conhecimento, inovação nos modelos produtivos e ampliação de oportunidades para a participação cidadã. Entretanto, para que esta transformação seja inclusiva e democrática é necessário compreender não só como funciona a web, mas também os diferentes mecanismos que determinam o acesso, o uso e o desenvolvimento da Internet na nossa região.

Este módulo oferece uma visão geral do que está em jogo para a sociedade civil, em particular, para a juventude, para as pessoas que vivem em contextos rurais e para as comunidades com pouca representação, em relação com a governança da Internet. Analisaremos como as decisões técnicas e as políticas sobre a Internet impactam os direitos humanos, a participação democrática e o desenvolvimento sustentável.

OBJETIVOS DO MÓDULO

Objetivo geral:

Contribuir para a construção de conhecimento sobre a governança da Internet, promovendo a participação ativa e o pensamento crítico sobre o seu uso, a sua regulação e a sua infraestrutura.

Objetivos específicos:

- Fortalecer o conhecimento entre os jovens e as comunidades rurais sobre o funcionamento da Internet e os mecanismos de governança que o configuram.
- Oferecer uma visão geral sobre os temas, os espaços e os processos mais relevantes do ecossistema da governança da Internet.
- Abordar a governança desde uma perspectiva crítica que torne visível as dinâmicas de poder e os interesses de distintos atores.
- Destacar oportunidades concretas de participação para a sociedade civil na tomada de decisões a nível nacional, regional e global.

UNIDADE I:

TEMA I: INTRODUÇÃO À GOVERNANÇA DA INTERNET

Para compreender como e por que a Internet impacta as nossas vidas é fundamental entender quem toma as decisões sobre o seu funcionamento e desenvolvimento. Este primeiro tema oferece uma introdução à governança da Internet: o que significa, como surge, como se organiza e por que importa especialmente para a sociedade civil na América Latina.

O QUE ENTENDEMOS POR SOCIEDADE CIVIL?

Podemos entender a sociedade civil como o conjunto de organizações, de coletivos e de espaços autônomos da vida pública —nem estatais nem empresariais— que agem de maneira organizada ou informal para representar interesses cidadãos, vigiar ao poder, promover valores e proteger direitos. Inclui, entre outros:

- Organizações não governamentais (ONGs) e associações civis dedicadas aos direitos humanos.
- Movimentos sociais e coletivos comunitários (p. ex., feministas, povos indígenas, LGBTIQ+, ambientalistas).
- Sindicatos, cooperativas e agrupações profissionais quando defendem direitos públicos.
- Meios comunitários, redes cidadãs e plataformas de incidência.
- Pessoas ativistas, vítimas organizadas e defensoras/es de direitos humanos que agem individual ou coletivamente.

DEFINIÇÕES-CHAVE: O QUE É A GOVERNANÇA DA INTERNET?

Uma definição amplamente aceita da governança da Internet foi adotada na Cúpula Mundial sobre a Sociedade da Informação (Tunísia, 2005) e é atualmente utilizada pelo Fórum de Governança da Internet:

> A governança da Internet é o desenvolvimento e a aplicação por parte de governos, do setor privado e da sociedade civil, nos seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisões e programas que dão forma à evolução e ao uso da Internet.

Dito de maneira mais simples: **a governança da Internet se refere a como são tomadas as decisões que afetam o funcionamento, o desenvolvimento e o uso da Internet. Isto inclui:**

- **Padrões**

Os padrões são globais, isto permite que possam se comunicar, isto é, transferir dados entre dispositivos que estão em lugares geográficos distintos e feitos ou fabricados por diversas empresas. Por exemplo, como se conectam às redes de Internet ou como são atribuídos os endereços IP.

- **Políticas**

As políticas constituem as regras que influenciam no que vemos, compartilhamos ou inclusive em se podemos acessar ou não a certos serviços. Estas podem ser globais: acordos internacionais e/ou multilaterais empresariais.

Também podem ser políticas locais que são criadas por governos nacionais ou por reguladores regionais que visam estabelecer normas próprias para o seu território. Isto significa que diferentes jurisdições e modelos de regulação convivem: enquanto uma rede social pode aplicar regras iguais para todo o mundo, um país pode decidir impor requisitos adicionais que afetam as pessoas usuárias dessa região. Por exemplo:

- Leis de proteção de dados, marcos de referência ou políticas para evitar a censura on-line.
- Os termos e condições que você deve aceitar para criar uma conta em alguma plataforma.

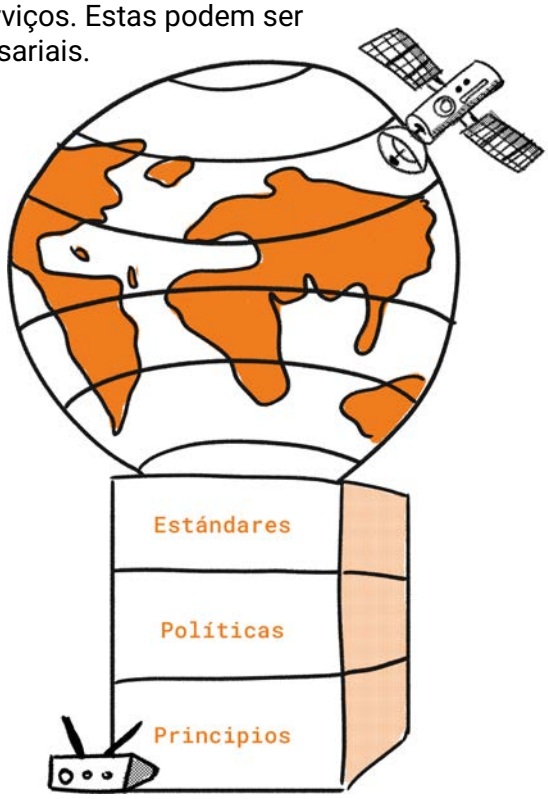


Figura 1. Governança da Internet

- **Princípios**
  São aquelas metas amplas que se busca sejam transversais para o uso e para a experiência da Internet:

  - Liberdade, privacidade e direitos humanos
  - Governança democrática e colaborativa
  - Universalidade
  - Diversidade
  - Inovação
  - Neutralidade da rede
  - Imputabilidade da rede
  - Funcionalidade, segurança e estabilidade
  - Padronização e interoperabilidade
  - Ambiente legal e regulamento

É importante ter em conta que a governança da Internet não ocorre em um só lugar, mas que é um processo distribuído e descentralizado, que muda e evolui todo o tempo com a participação de muitos atores.

Lembram-se do modelo de camadas que vimos no primeiro módulo para explicar como funciona a Internet? Lá nos enfocamos nos aspectos técnicos: desde os cabos e sinais físicos, passando pelos protocolos, até chegar às aplicações e aos conteúdos que usamos todos os dias.

Neste segundo módulo retomaremos essa ideia das camadas, mas agora a veremos desde outro ângulo: a governança. Isto é, como diferentes atores estatais, empresas, organizações e cidadania influenciam e tomam decisões sobre a Internet. Aqui inclusive acrescentamos mais uma camada, a **camada social**, porque a Internet não é só tecnologia: é também um espaço humano, político e cultural, atravessado por direitos, disputas e formas de organização.

Podem ser identificadas 4 camadas nas quais a estrutura da governança da Internet pode fornecer um entendimento mais delimitado:

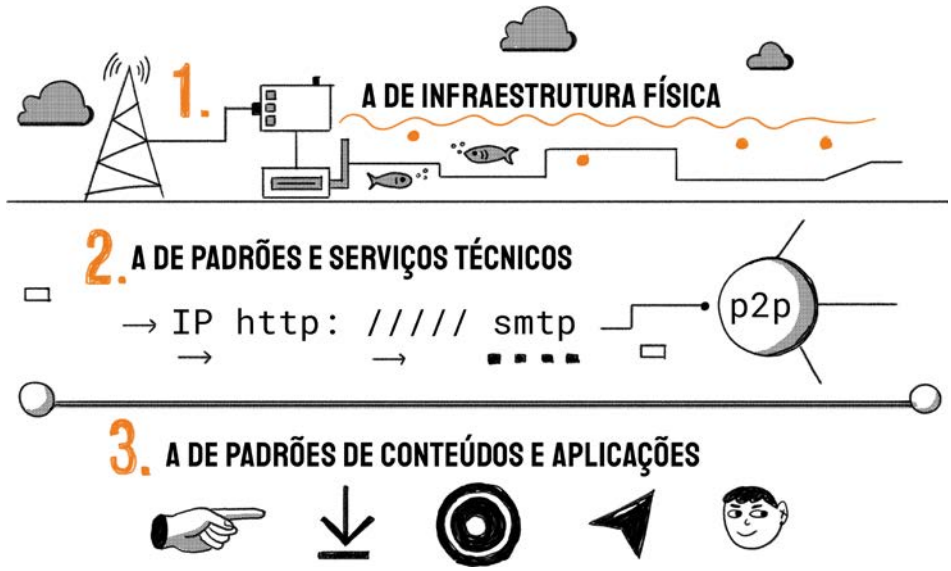


Figura 2. Capas del funcionamiento de Internet.

- **Camada social**
  A Internet é criada e utilizada por personas. Podemos incluir uma camada social porque está integrada na vida cotidiana das pessoas de todo o mundo, inclusive daquelas que ainda não estão plenamente conectadas a ela. Isto inclui:

  - Estados e governos
  - Organismos privados e empresas
  - Organizações políticas
  - Cidadãos

- **Camada de conteúdo e de aplicação**
  Aqui está uma grande parte do debate público e político da governança da Internet, incluindo: privacidade, criptografia, liberdade de expressão, direitos humanos e propriedade intelectual. Muitos destes debates têm lugar através de instrumentos políticos tradicionais, como a regulação estatal ou os acordos entre o sector público e o privado. Aqui é importante o papel do Fórum de Governança da Internet (IGF), sobre o qual será falado mais adiante, uma vez que serve como fórum global para que os governos e a sociedade civil discutam os temas que consideram mais relevantes.

- **Camada lógica: padrões e serviços técnicos**
  Neste nível são definidas as linguagens e protocolos facilitados por padrões e por procedimentos como os que vimos no módulo anterior (TCP/IP, padrões de redes Wi-Fi, DNS e endereços IP). Uma parte importante desta coordenação recai na União Internacional de Telecomunicações (UIT, pelas suas siglas em inglês ITU: International Telecommunication Union), organismo especializado das Nações Unidas que estabelece padrões globais em telecomunicações.

  Embora o trabalho da UIT tenha sido chave para garantir a interoperabilidade das redes a nível mundial, também foi questionada porque alguns Estados com regimes autoritários utilizam este espaço para influenciar na normalização de tecnologias de nova geração, incorporando funções que facilitam a vigilância, o rastreamento e o controle da informação. Por exemplo, em discussões recentes sobre padrões para redes móveis e gestão de tráfego, foram propostos mecanismos que poderiam limitar o anonimato, bloquear conteúdos ou reforçar a rastreabilidade dos usuários, o que representa um risco para a liberdade na Internet.

- **Camada de infraestrutura física**
  Está composta por satélites, cabos submarinos e terrestres, sistemas sem fio, centros de dados, entre outros. Nesta camada estão organizações como IETF (Internet Engineering Task Force), IRTF (Internet Research Task Force) e IAB (Internet Architecture Board). Esta camada está normalmente vinculada ao setor privado de telecomunicações. Porém, quem define os protocolos de operação e interoperabilidade desde o desenvolvimento de padrões, protocolos e governança entre as diferentes regiões do mundo são: ISOC (Internet Society), ICANN (Internet Corporation for Assigned Names and Numbers) e IEEE (Institute of Electrical and Electronics Engineers).

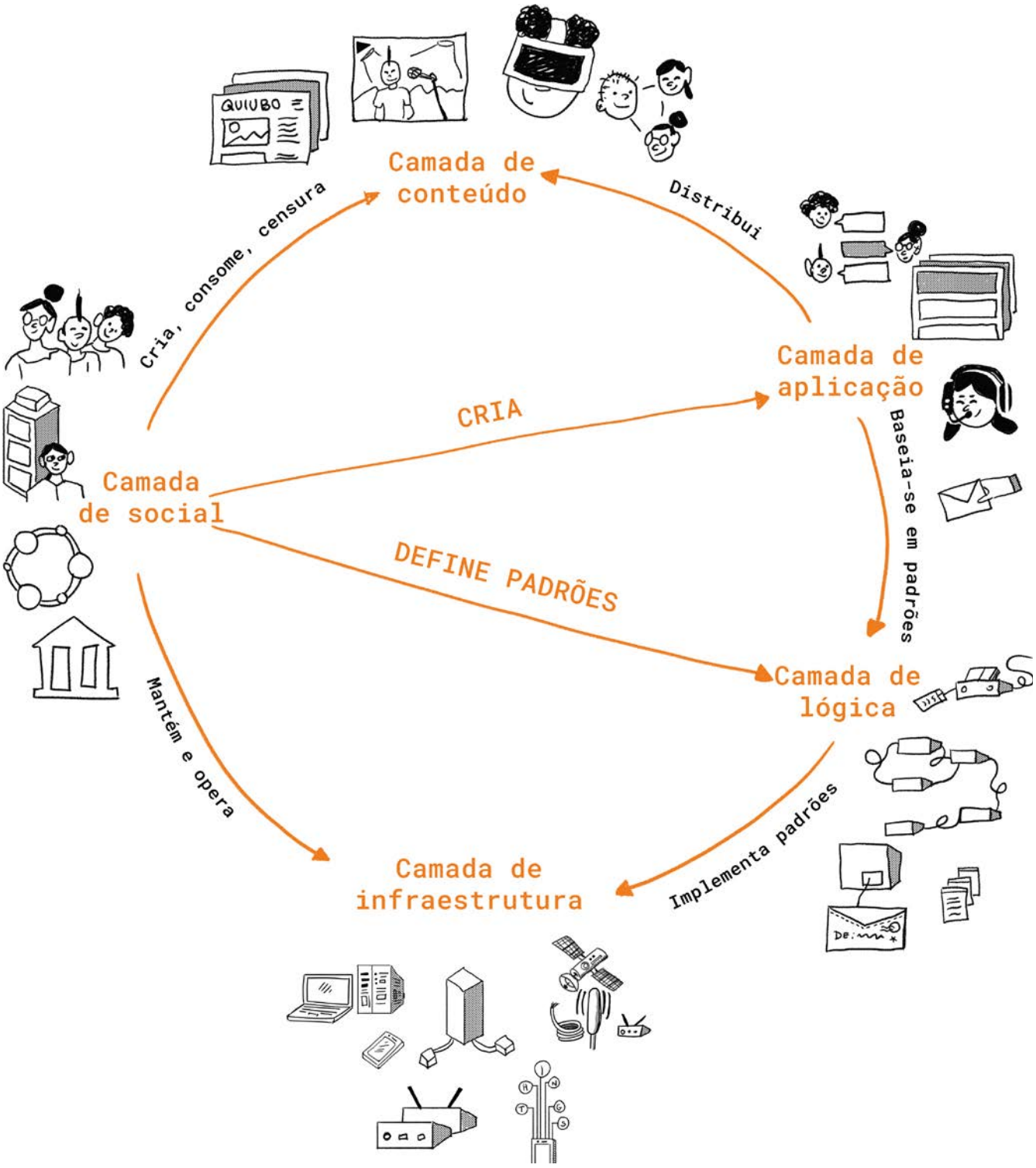


Figura 3. Camadas do funcionamento da Internet.
Adaptado e traduzido de How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance, por ARTICLE 19, 2021

GOVERNANÇA MULTILATERAL VS "MULTISTAKEHOLDER" (OU MULTISSETORIAL)

Na hora de aplicar a governança da Internet, devemos nos perguntar como isso é feito na prática, como é realizada a participação e como é exercida dita governança. Em princípio, existem distintos modelos de tomada de decisões sobre a Internet, dois deles são:

- **Governança multilateral,** na qual o controle está nas mãos de Estados e organismos intergovernamentais (como a ONU ou a UIT, visto anteriormente).
- **Governança "multistakeholder" (ou multissetorial),** na qual há participação conjunta de governos, de empresas, da comunidade técnica, da comunidade acadêmica e da sociedade civil.

Por que um modelo multissetorial e não outro?

O modelo multissetorial é promovido pela sociedade civil, uma vez que permite uma participação mais equitativa. Contudo, não está isento de tensões: todas as vozes têm o mesmo peso? Como é possível garantir a representação de comunidades que historicamente foram marginalizadas?

Por mais que um processo seja multilateral e realizado por governos, e não um processo multissetorial, é importante que tenha participação robusta de distintos atores. Isto acontece porque na Internet (e nas políticas públicas associadas a esta) não existe um só ator que tenha todos os conhecimentos nem todas as respostas. O troca e a participação de distintos atores enriquece ao processo e gera políticas mais robustas.

Espaço de discussão: *Quais são as condições necessárias para uma participação significativa? Quais práticas facilitam uma participação efetiva nestes espaços?*

Figura 4. Discussão

PRINCÍPIOS FUNDAMENTAIS DA GOVERNANÇA DA INTERNET

Embora existam muitas formulações de princípios da Internet e da sua governança, há um conjunto que, ao longo dos anos, continua sendo comum às diferentes comunidades e organizações que refletiram sobre ele. Estes princípios orientam como deveria funcionar e ser desenvolvida a Internet para que seja um espaço equitativo, seguro e livre. Nesta seção apresentamos quatro:

- **Abertura:** A internet aberta significa que qualquer pessoa pode usar, criar e contribuir para a Internet.

Exemplo: *Wikipedia.* Qualquer pessoa pode entrar, usá-la e contribuir com conteúdo. Não é um espaço fechado, mas sim construído coletivamente.

- **Descentralização:** 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.

Exemplo: *O correio eletrônico funciona de maneira descentralizada: existem muitos provedores (Gmail, ProtonMail, Riseup, etc.), mas todos se comunicam entre si sem depender de um único servidor central.*

- **Participação:** é muito importante que múltiplos atores possam participar significativamente.

Exemplo: *Nas comunidades de software livre, como a do Linux, distintas pessoas e organizações contribuem com ideias, discutem e contribuem coletivamente, o que fortalece a diversidade e a inovação.*

- **Neutralidade da rede:** Os provedores de Internet não devem bloquear nem priorizar conteúdos de acordo com interesses comerciais ou políticos.

Exemplo: *A sentença C-206 de 2025 da Corte Constitucional de Colômbia declarou inexequível a seção do artigo 56 da Lei 1450 (que habilitava ofertas de "tarifa zero"/ zero-rating), por considerar que permitir que os operadores (ISP) ofereçam acesso gratuito e exclusivo a certos apps (o WhatsApp, o Facebook, o TikTok, etc.) vulnera a neutralidade da rede e pode afetar pluralismo, competência e liberdade de escolha.*

Pela sua parte, a **UNESCO** propôs um marco de princípios para promover uma Internet universal e inclusiva (conhecidos como **princípios ROAM** pelas suas siglas em inglês). Estes são:

- **Direitos Humanos:** A internet deve apoiar e promover os direitos humanos, como a liberdade de expressão, o acesso à informação, a privacidade, etc. As políticas digitais devem estar alinhadas com os marcos internacionais de direitos humanos.
- **Abertura:** A rede deve ser aberta desde um ponto técnico e legal, isto é, deve ser interoperável, baseada em padrões abertos e livre de censura ou de barreiras à expressão.
- **Acessibilidade:** O acesso à Internet deve ser equitativo, acessível e seguro para todas as pessoas, incluídas comunidades rurais, pessoas com deficiência, juventude, etc.
- **Participação multissetorial:** As políticas sobre a Internet devem ser desenvolvidas com a participação significativa de todos os setores.

Teste: Qual princípio ou princípios estão sendo afetados em cada uma destas situações hipotéticas?

1. Acesso lento a certos serviços

a. Uma empresa operadora de Internet começa a reduzir a velocidade de serviços de streaming gratuitos, enquanto prioriza (e cobra extra por) outras plataformas associadas.
Resposta: neutralidade da rede, abertura.

2. Concentração de infraestrutura digital

a. Um único operador controla a maioria das conexões de fibra óptica de um país, o que lhe permite definir preços, prioridades e deixar certas zonas sem serviço.
Resposta: descentralização, abertura

3. Bloqueio de conteúdo político

a. Um governo decide bloquear o acesso a um site de notícias independentes durante um período de eleições, argumentando que é conteúdo inapropriado
Resposta: abertura, neutralidade

4. Consulta pública sem participação real

a. O governo abre uma consulta sobre uma nova lei de cibersegurança, mas o formulário está só em inglês, está aberto por só 48 horas, e não há devolução aos comentários recebidos.
Resposta: participação

Anexo 1. Respostas.

Figura 5. Exercício

Recursos:

- *ISOC. (s.f.) Gobernanza de Internet*
- *ISCO. (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 governança da Internet (inglês)*
- *ISOC, Línea de tiempo (inglés)*
- *Fundación Karisma y RedPaTodos, Video sobre governança da Internet*
- *Glosario da UNESCO sobre termos de governança da Internet (inglês)*
- *Indicadores da UNESCO sobre a universalidade da Internet (indicadores ROAM)*
- *Principios para la gobernanza y el uso de Internet*

Figura 6. Recursos.

TEMA 2: ATORES E ESPAÇOS DE TOMADA DE DECISÃO

A internet não é governada desde um único lugar nem por um só grupo ou ator: a sua governança é o resultado de decisões tomadas por múltiplos atores como são as entidades técnicas, os governos, o setor privado, as organizações da sociedade civil, etc. Neste tema cobriremos: quem são estes atores-chave na governança da Internet, como se relacionam entre si e quais são os espaços-chave de tomada de decisões para a governança da Internet. Além disso, exploraremos o contexto institucional latino-americano e os diferentes espaços de participação a nível local e global como são o **LACIGF** e o Youth **LACIGF**.

MAPEAMENTO DE ATORES-CLAVE NA GOVERNANÇA DA INTERNET

A seguir apresentaremos os principais grupos de atores envolvidos na governança da Internet. Cada grupo tem diferentes níveis de envolvimento, de poder e de influência.

- **Setor técnico:** são organizações que desenvolvem, mantêm e promovem os padrões técnicos da Internet:
-
    - **ICICANN (Internet Corporation for Assigned Names and Numbers):** administra os nomes de domínio (como ".org" ou ".lat")
    - **IANA (Internet Assigned Numbers Authority):** é a organização responsável pela coordenação global da zona raiz do Sistema de Nomes de Domínio (DNS), pela atribuição de endereços Internet Protocol (IP) e por outros recursos críticos de protocolos da internet.
    - **IETF (Internet Engineering Task Force):** desenvolve protocolos técnicos (como HTTP ou o TCP-IP) que tornam possível o funcionamento da Internet.
    - **ISOC (Internet Society):** promove a coordenação global para o desenvolvimento de protocolos e de padrões compatíveis, realiza tarefas educativas e contribui para políticas públicas.
    - **UIT (União Internacional de Telecomunicações):** a agência da ONU encarregada por coordenar temas técnicos e de regulação de telecomunicações.

    - **IEEE (Institute of Electrical and Electronics Engineers):** associação profissional global para a tecnologia e para a engenharia com uma estrutura organizacional distribuída. Está aberta a sugestões sobre novas tecnologias e inclusive pode se estabelecer para a formação de grupos de trabalho.
    - **IRTF (Internet Research Task Force):** fomenta a pesquisa sobre a evolução da Internet mediante a criação de grupos de pesquisa enfocados e a longo prazo que estudam temas relacionados com protocolos, aplicações, arquitetura e tecnologias da Internet.
    - **IAB (Internet Architecture Board):** supervisiona o desenvolvimento técnico e de engenharia tanto do Grupo de Trabalho sobre Protocolos da Internet (IETF) como da Força de Tarefa para Pesquisa na Internet (IRTF).

- **Governos:** desenvolvem políticas públicas nacionais a nível local e, além disso, participam em processos internacionais e negociações multilaterais.

- **Setor privado:** inclui as empresas que fornecem infraestrutura digital (por exemplo, empresas de telecomunicações como a Cloudflare, a CISCO, a Juniper, a Claro, etc.), e, também, as plataformas digitais (como o Google ou a Meta). Têm um grande poder econômico.

- **Sociedade civil:** organizações, redes e ativistas que defendem os direitos humanos, o acesso equitativo à Internet e promovem a participação significativa na tomada de decisões sobre a governança da Internet.

- **Setor acadêmico:** centros de pesquisa, universidades e especialistas que contribuem com perícia e pesquisa.

- **Organismos e espaços internacionais:** espaços intergovernamentais (como a ONU) ou multilaterais que promovem o diálogo (por exemplo, através do Fórum de Governança da Internet) ou o desenvolvimento de normas globais (como o Pacto Digital Mundial).

INTERAÇÕES, TENSÕES E ASSIMETRIA DE PODER

Todos estes atores —governos, empresas, sociedade civil e outros— podem participar na governança da Internet, mas não chegam em igualdade de condições.

Nem todos têm o mesmo poder

- As empresas costumam ter muito dinheiro e contatos que lhes permitem pressionar a tomada de decisões.

- Os governos podem criar leis e políticas porque têm autoridade legal, mas às vezes não sabem o suficiente de tecnologia ou não priorizam os direitos humanos.

- A sociedade civil contribui com experiência em direitos humanos e um olhar crítico, mas tem menos recursos e enfrenta barreiras para participar plenamente (idioma, dinheiro e processos).

Barreiras práticas para a sociedade civil

- Muitos processos globais são realizados em inglês.

- Participar custa tempo e dinheiro (viagens, honorários, tradução).

- Conseguir vistos ou acessar a reuniões presenciais pode ser difícil.

Conflitos de interesse

- Uma empresa pode defender políticas que favoreçam o seu lucro embora afetem à privacidade.

- Alguns Estados podem usar a regulação para restringir a liberdade de expressão.

MAPEAMENTO DE ESPAÇOS-CHAVE NA GOVERNANÇA DA INTERNET

A governança da Internet ocorre em múltiplos níveis: espaços globais, regionais e nacionais. Estes espaços definem marcos normativos, técnicos e políticos que são chave porque afetam o exercício dos nossos direitos. Entender quais espaços existem (e que tão abertos são para a sociedade civil) é chave para poder planejar as nossas estratégias de incidência.

A seguir apresentamos alguns dos espaços principais de tomada de decisões com relação à governança da Internet:

ESPAÇOS GLOBAIS				
Espaço	**Descrição**	**Abertura**	**Relevância para a sociedade civil**	**Participação da Latam**
Fórum de Governança da Internet (IGF)	Espaço de diálogo multilateral organizado pela ONU. Não toma decisões vinculantes, mas gera consensos e torna visível debates-chave.	**Alta** Qualquer pessoa pode assistir, propor sessões, participar em oficinas e unir-se a distintas coalizões temáticas.	Ideal para promover agendas como sociedade civil e para gerar ou reforçar relações com outros atores.	Como sociedade civil podemos participar deste IGF global para tornar visível temas de relevância para a nossa região.
Pacto Digital Mundial (Global Digital Compact)	Uma iniciativa impulsionada pela Secretaria Geral da ONU, que visa estabelecer princípios comuns sobre o futuro digital global.	**Média** As negociações foram somente entre os Estados, e embora houve processos de consulta, alguns setores da sociedade civil consideram que não foram o suficientemente robustos.	O pacto cobre questões como regulação de plataformas, inteligência artificial, entre outros temas vinculados diretamente aos direitos humanos.	Mediante a participação em negociações através dos seus Estados, e contribuindo desde a sociedade civil, o setor acadêmico e o setor privado nas consultas e espaços multilaterais vinculados ao processo.
Cúpula mundial sobre a Sociedade da Informação (WSIS)	É um processo iniciado pela ONU em duas partes, em 2003 e 2005, que culminou em uma definição de governança da Internet que consagra a necessidade de envolver múltiplos setores e a criação do IGF. Depois de 20 anos da sua criação está sendo feita a revisão do seu impacto e da pertinência do modelo multissetorial na conjuntura atual. Veja mais no nosso último relatório: Perspectiva de Colombia en la revisión de los 20 años de la Cúpula Mundial de la Sociedade de Información.	**Média** As negociações são intergovernamentais, com diferentes instâncias de participação multistakeholder.	A revisão dos 20 anos da WSIS é fundamental no nosso contexto, onde um grupo reduzido de atores visa impor visões autoritárias da Internet. Além disso, este processo definirá se se renova o mandato do IGF.	As organizações da sociedade civil podem participar nas consultas globais e, além disso, fazer incidência com governos da região para influenciar as suas posições na negociação.

Figura 7. Espaços globais de Governança da Internet.

ESPAÇOS REGIONAIS			
Espaço	**Descrição**	**Abertura**	**Relevância para a sociedade civil**
Fórum de Governança da América Latina e o Caribe (LACIGF)	A versão da América Latina e o Caribe do IGF. Reúne todos os setores para discutir temas de governança da Internet desde uma perspectiva regional.	Muito alta É organizada de forma aberta e com a participação multissetorial.	As discussões do LACIGF alimentam as discussões do IGF global, portanto, é um dos principais espaços para tornar visível temas urgentes da nossa região.
Registro de Endereços da Internet para a América Latina e o Caribe (LACNIC)	O LACNIC é uma organização técnica que gerencia a atribuição de endereços IP e outros recursos críticos da Internet na região.	Média Embora o seu foco seja técnico, há distintas instâncias de participação de atores não governamentais, por exemplo através de fóruns e de processos abertos de desenvolvimento de políticas.	É um espaço-chave para entender como funciona a Internet tecnicamente e para incidir em decisões sobre a infraestrutura (temas nos quais é necessário mais envolvimento de organizações da sociedade civil).
Agenda digital da América Latina e do Caribe (eLAC)	Iniciativa intergovernamental organizada pela CEPAL para promover uma agenda comum sobre desenvolvimento digital.	Baixa a moderada A participação direta está limitada a Estados, embora existem mecanismos de consulta e espaços de diálogo com atores não governamentais.	As discussões neste espaço influenciam nas discussões nacionais sobre a política pública de transformação digital.

Figura 8. Espaços regionais de Governança da Internet.

ESPAÇOS NACIONAIS E LOCAIS

Cada país tem distintos canais de tomada de decisões em temas digitais e de tecnologia, sejam formais ou informais. Alguns exemplos são as consultas públicas sobre projetos de lei relacionados com temas da Internet (por exemplo, iniciativas sobre proteção de dados, cibersegurança, inteligência artificial ou regulação de plataformas); mesas ou comitês consultivos em organismos regulatórios (por exemplo, em entidades regulatórias de telecomunicações); e fóruns multilaterais nacionais como o Foro Colombiano de Gobernanza de Internet t.co/.

Espaço de discussão::

- *Você tem experiência prévia de incidência ou envolvimento em alguns dos espaços apresentados neste módulo? Quais? Você estaria interessado(a) em participar?*
- *Você conhece exemplos de temas relevantes para a América Latina que tenham sido discutidos em fóruns globais?*

Figura 9. Perguntas

O contexto na América Latina

Na América Latina, as decisões sobre a Internet estão marcadas por desigualdades que vêm de longe: econômicas, sociais e culturais. Muitas comunidades —especialmente nas zonas rurais e nos territórios indígenas— têm ainda menos acesso às conexões, dispositivos e conteúdos na sua língua. Por isso, garantir acesso digno e políticas de conectividade deve ser uma prioridade regional.

Também, há um problema com as leis e com as normas que estão sendo aprovadas: muitas vezes são elaboradas sem considerar os direitos humanos nem as realidades e as necessidades locais. Isto pode pôr em risco a privacidade, a liberdade de expressão e o direito a se comunicarem na própria língua ou de acordo com as próprias práticas comunitárias.

O que significa isto para as comunidades?

- Se não houver conectividade real as políticas públicas não servem: faz falta infraestrutura, formação e conteúdos em idiomas locais.
- Se as leis não são construídas considerando a salvaguarda de direitos fundamentais, as comunidades e as pessoas defensoras podem ficar mais expostas à vigilância, à censura e à exclusão.
- As soluções devem contemplar o contexto e as organizações sociais, porque são elas as que melhor conhecem as suas necessidades e riscos.

Para que a Internet seja verdadeiramente útil e segura na região, as políticas devem ser construídas com quem vive e defende os territórios: comunidades indígenas, povos rurais e ativistas. Não estamos pedindo permissão para participar; exigimos ser escutados e que as decisões respeitem as nossas línguas, modos de vida e direitos.

Recursos:

- *Global Partners Digital, blog "Everything you need to know about the WSIS+20 review" (inglês)*
- *APC, blog "The feminist principles for including gender in the Global Digital Compact" (inglês)*
- *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: GOVERNANÇA DA INTERNET E DIREITOS HUMANOSS

A Internet é um espaço onde são exercidos (e, às vezes, são vulnerados) os direitos fundamentais. É difícil pensar em aspectos da nossa vida cotidiana que não estejam relacionados de uma ou de outra forma com a tecnologia. Nós nos comunicamos através de apps de mensagens, verificamos o nosso saldo bancário através de apps, pedimos comida ou compramos produtos através de aplicações digitais e, inclusive, o atendimento de saúde está mediado pelo registro nas bases de dados digitais.

Nesta seção vamos explorar como as decisões sobre a Internet afetam diretamente, de formas positivas e negativas, o exercício dos direitos humanos. É importante que como sociedade civil tenhamos presente estas interseções para reconhecer possíveis ameaças emergentes aos nossos direitos e, assim, poder incidir de forma mais informada e estratégica

GOVERNANÇA DA INTERNET E DIREITOS HUMANOS - UM VÍNCULO-CHAVE

A governança da Internet (entendida, como “as decisões que afetam o funcionamento, o desenvolvimento e o uso da Internet”) tem efeitos concretos sobre distintos direitos:

- **EO direito à privacidade:**

As decisões sobre as quais dados são coletados, quem os controla e com que fins podem ser utilizados têm um vínculo direto com o direito à privacidade. Marcos legislativos sobre proteção de dados podem contribuir para o exercício deste direito, enquanto decisões sobre a vigilância ou a eliminação da criptografia pode deixa-la vulnerável.

Exemplo: Quando aceitamos os termos e condições do WhatsApp, estamos autorizando que certos dados sejam coletados (como a nossa lista de contatos). Se uma empresa decide vender estes dados a terceiros, a nossa privacidade pode ficar comprometida.

- **O direito à liberdade de expressão:**

A Internet pode oferecer um espaço no qual nos expressamos, mas também existem políticas que limitam o exercício deste direito. Por exemplo, certas políticas de moderação de conteúdos como o bloqueio de certos sites podem afetar diretamente a nossa liberdade de expressão.

Exemplo: Se uma rede social eliminou uma publicação sobre direitos sexuais e reprodutivos alegando que "viola as normas da comunidade", a nossa capacidade de expressão está sendo afetada.

- **O acesso à informação**

As políticas públicas da Internet têm um efeito direto sobre quem pode ter acesso e quem não, quais conteúdos estão disponíveis e em quais idiomas e quais barreiras econômicas existem. Sem acesso significativo à Internet (não apenas a conectividade, mas também a apropriação e a educação digital), este direito é afetado.

Exemplo: Em comunidades rurais onde a Internet é lenta e cara, as meninas e as mulheres têm menos acesso à informação educativa ou de saúde.

- **Direito à não discriminação**

Certas tecnologias (por exemplo, sistemas de inteligência artificial) podem reproduzir preconceitos e estereótipos de gênero, raça, nível socioeconômico e outros.

Exemplo: sistemas de reconhecimento facial que funcionam pior para as mulheres e para pessoas racializadas, o que pode derivar em exclusões ou acusações injustas.

Exemplo 1: Moderação de conteúdos e censura

As plataformas digitais —onde falamos, contamos as nossas histórias e debatemos sobre o que nos importa— nem sempre respeitam os direitos fundamentais. As suas regras para decidir o que é publicado e o que é eliminado, frequentemente, não coincidem com padrões internacionais de direitos humanos.

Alguns problemas concretos:

- Muitas decisões são tomadas com sistemas automáticos, sem revisão humana nem uma forma clara de apelar das decisões das plataformas.
- As regras de moderação costumam ser desenvolvidas com lógicas comerciais ou com normas culturais dos países do Norte Global, que nem sempre entendem as nossas realidades nem as nossas línguas.
- A moderação é aplicada de forma desigual: discursos que defendem direitos (por exemplo, feministas ou a favor do aborto) às vezes são silenciados, enquanto discursos de ódio ou desinformação ficam na plataforma.

Exemplos:

- Coletivos pró-aborto no México e na Colômbia denunciaram bloqueios de contas no WhatsApp e a censura em redes sociais ao tentarem se organizar ou difundir informação.
- A maior campanha de censura nas redes sociais contra as violações de direitos humanos do povo palestino, articulada e patrocinada por Israel
- (Israel & Meta, The Greatest Global Mass Censorship Campaign to Ever Exist)

Exemplo 2: Vigilância estatal e privada

As tecnologias de vigilância —que abrangem desde ferramentas de interceptação de comunicações até sistemas de reconhecimento facial ou de geolocalização— podem ser utilizadas de formas muito diferentes de acordo com o contexto, com o marco legal e com os atores envolvidos. Em alguns casos, são empregados com fins legítimos de segurança pública; entretanto, também foram documentados usos abusivos que põem em risco a vida privada e a segurança de jornalistas, de defensores e de ativistas. Em vários países da América Latina, por exemplo, estas ferramentas foram utilizadas para espiar pessoas que investigam ou defendem os direitos humanos. No México, entre abril e maio de 2019 pelo menos 456 pessoas foram vigiadas com o software Pegasus.

Por isso é importante pedir controles claros e transparência: investigações independentes quando houver denúncias, leis que limitam o uso destas ferramentas, medidas de reparação para as vítimas e formação em segurança digital para comunidades e movimentos.

Exemplo 3: Discriminação e exclusão em entornos digitais

A tecnologia não é neutra, pode reproduzir e em muitos casos manter e amplificar as desigualdades. Alguns exemplos de impactos diferenciados em certas comunidades são:

- As mulheres e as pessoas LGBTIQ+ experimentam mais violência digital.
- Os povos originários enfrentam falta de acesso e de barreiras linguísticas para a sua participação em espaços de governança.

Espaço de discussão:

a) Qual barreira concreta a sua comunidade enfrenta para usar a Internet de forma equitativa? (ex.: conectividade, idioma, ameaças, censura, custo, falta de formação).
b) Quais direitos são afetados? (privacidade, liberdade de expressão, acesso à informação, direito coletivo).
c) Quem tem poder para mudar isto e do que precisam para fazê-lo? (governo, empresa, organizações locais).

Redija 3 propostas acionáveis e simples (máx. 2 linhas cada uma), priorizando:

- *Uma medida de política pública (ex.: fundos de conectividade comunitária com controle local).*
- *Uma medida operativa ou de solidariedade (ex.: rede de tradutores voluntários para processos de governança).*
- *Uma medida de proteção (ex.: apoio legal ou protocolos de segurança digital para defensoras).*

Figura 11. Espaço de discussão.

Recursos:

- *Lutadoras, 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*
- *Ao Sul, informe La moderación de contenidos desde una perspectiva interamericana*
- *R3D, Informe "El Estado de la Vigilancia"*

Figura 12. Recursos.

TEMA 4: PARTICIPAÇÃO DA SOCIEDADE CIVIL

A sociedade civil tem um papel fundamental na defensa dos direitos humanos em processos de governança da Internet, mas que tão abertos são realmente os espaços de decisão? Quais são os desafios, as oportunidades e as estratégias de participação desde as nossas realidades na América Latina? Este tema visa tornar visível as vias de participação disponíveis, assim como as barreiras estruturais que impedem uma participação significativa, plena e efetiva. Além disso, compartilhamos alguns exemplos concretos de incidência.

A SOCIEDADE CIVIL PODE PARTICIPAR NA GOVERNANÇA DA INTERNET?

A governança da Internet é definida, em parte, pelo seu enfoque multistakeholder (multissetorial), o que significa que distintos setores —incluída a sociedade civil— devem ter voz nas discussões. Entretanto, a abertura formal nem sempre é traduzida em participação significativa.

QUAIS SÃO AS BARREIRAS DE ACESSO?

Embora em teoria muitos espaços sejam “abertos”, existem obstáculos reais que dificultam a participação das organizações da sociedade civil, especialmente aquelas do Sul Global. Por exemplo:

- **Idioma e jargão técnico:** a maioria dos processos são realizados em inglês e com terminologia técnica especializada.
- **Falta de recursos financeiros:** diferentemente, por exemplo, do setor privado, muitas organizações da sociedade civil com frequência não contam com financiamento, tempo, ou pessoal capacitado para seguir processos longos e complexos.
- **Exclusão estrutural:** certas organizações enfrentam maiores obstáculos, por exemplo, organizações de povos originários e comunidades rurais.
- **Falta de transparência e acesso à informação:** muitos processos são turvos, sem informação pública sobre instâncias de participação.
- **Participação simbólica ou não significativa:** muitas vezes são realizadas consultas como uma forma de cumprir com um requisito formal, mas sem mecanismos reais para integrar essas perspectivas de forma significativa nos processos.

Atividade "Mapa de barreiras e pequenas ações"

Objetivo: *Identificar barreiras concretas que impedem a sua comunidade de participar na governança da Internet e desenvolver ações pequenas e viáveis para começar a resolvê-las.*

Materiais:*folha de papel ou documento digital.*

Passos

1. Contexto
Escreva em uma linha qual é a sua comunidade (ex.: comunidade indígena, bairro rural, coletivo feminista, grupo estudantil).

2. Mapa rápido de barreiras
Faça uma lista de até 6 barreiras que impedem a participação em decisões sobre a Internet (uma por linha). Pense em: conectividade, custo, idioma, processos/vistos, falta de informação, violência digital, falta de representação, falta de financiamento, formatos inacessíveis, etc. Junto a cada barreira anote em 3–5 palavras por que existe (causa).

3. Prioriza
Marca a barreira mais urgente ou a que você acredita mais fácil de atacar a curto prazo.

4. Pequenas ações
Para a barreira priorizada, desenvolva 3 ações concretas e muito viáveis que você possa impulsionar sozinho/a ou com poucas pessoas. Devem ser realizáveis em 1–3 meses. Exemplos: oficina local de segurança digital de 2 horas, traduzir e compartilhar um resumo em língua local, abaixo-assinado para solicitar a internet comunitária, gravar áudio explicativo e distribui-lo pelo WhatsApp. Para cada ação escreva:

- *O que será feito (1 linha).*
- *Primeiro passo imediato (1 linha).*
- *Recurso mínimo necessário (pessoa, tempo, dinheiro).*

5. Riscos e mitigações
Escreva 2 possíveis riscos ou obstáculos para a ação escolhida (ex.: represálias, falta de interesse, custo) e uma breve ideia para reduzir cada risco.

6. Compromisso pessoal
Escreva o que você fará esta semana (ação concreta e dia) para avançar na primeira ação.

Figura 13. Recursos.

Por que é importante que as organizações da sociedade civil participem no modelo multissetorial pela governança da Internet?

O modelo multissetorial permite que as organizações da sociedade civil não apenas observem, mas que **formem parte ativa das decisões sobre como a Internet é governada.** Esta participação é chave por várias razões:

1. **Defender os direitos humanos nos espaços digitais**
   As ONGs trabalham pelos direitos humanos como a liberdade de expressão, a privacidade e o acesso à informação. Estes direitos também são exercidos e vulnerados na Internet. Participar na governança permite protegê-los desde o desenvolvimento mesmo das normas e das infraestruturas digitais.
2. **Levar as vozes do território e das comunidades para os espaços globais**
   As decisões sobre a Internet afetam todas as pessoas, em todos os países. As ONGs proporcionam experiências e perspectivas de comunidades locais, ajudando a que a Internet seja uma plataforma para a inclusão.
3. **Incidir antes de que as políticas estejam definidas**
   No modelo multissetorial, as decisões são tomadas por consenso. Isto dá às ONGs a oportunidade de participar na construção de políticas desde o início. Entendendo que é um espaço no qual cada vez é mais necessário que nos integremos e colaboremos para incidir desde as organizações da sociedade civil.
4. **Prestação de contas ou Accountability**
   Como grande parte do controle da Internet está nas mãos de governos e de empresas privadas, a presença das ONGs ajuda a fomentar a transparência, o controle social e a prestação de contas.
5. **Colaborar com outros setores**
   Estar nestes espaços permite que as ONGs trabalhem junto a comunidades técnicas, a empresas e a responsáveis pelas políticas, construindo soluções conjuntas para os desafios digitais atuais. O trabalho articulado com outros setores e organizações é uma oportunidade para o trabalho em rede e para a geração de confiança entre os setores interessados.

Estratégias de participação desde a sociedade civil

- **Campanhas públicas** através de mobilização nas redes, campanhas visuais, ou de sensibilização cidadã. Exemplos: KeepItOn campaign, Access Now

- **Litígio estratégico:** uso do sistema judicial para impugnar leis ou políticas que violam direitos. Exemplos: Incidencia judicial da nossa organização que permite motivar mudanças locais, nacionais e internacionais.

- **Incidência direta:** participação em consultas públicas, reuniões com pessoas tomadoras de decisões, apresentação de relatórios ou recomendações. Exemplos: input conjunto de organizações da sociedade civil no processo de desenvolvimento do Pacto Digital Global.

- **Alianças:** construção de redes da sociedade civil e de redes multilaterais (com jornalistas, setor privado, setor acadêmico). Exemplos: consorcio AlSur

- **Participação em espaços técnicos:** envolver-se em espaços como a ICANN ou a ITU, desde a perspectiva de direitos. Exemplos: participación da sociedade civil no Study Group 13 da UIT.

Atividade:

Objetivo: *Transformar as barreiras identificadas no exercício individual em um plano coletivo de incidência com estratégias e atividades concretas.*

Materiais: *documento compartilhado ou painel digital, se as pessoas estão no mesmo lugar, um quadro onde possam escrever todas as pessoas.*

Passos:

1. Compartilhar
Cada pessoa diz brevemente qual barreira priorizou no exercício individual.

2. Escolher um processo de governança
O grupo escolhe um processo trabalhado no módulo (ex.: proteção de dados, conectividade, moderação de conteúdos, nomes de domínio).

3. Definir 2–3 estratégias de incidência
Conectam a barreira escolhida com o processo selecionado.
Exemplo de estratégias: visibilização, alianças, incidência em políticas públicas, produção de conhecimento local.

4. Desenvolver atividades concretas
Para cada estratégia, proponham uma atividade simples e realista (ex.: campanha nas redes, oficina comunitária, tradução de um recurso, carta para uma autoridade, aliança com outra organização).

Podem usar este modelo ou criar o próprio:

Estratégia de incidência	Exemplo de atividade	Quem se compromete	Recurso mínim

Figura 14. Actividad.

Incidência de sucesso

Promoção de ciber normas inclusivas - Fundación Karisma (Acessar ao documento completo aqui).

O que aconteceu?

Em 2022, participamos de um espaço multistakeholder para enfrentar a violência contra as mulheres na política, visando garantir que qualquer lei futura considere tanto os direitos humanos como o direito à liberdade de expressão e à privacidade.

O que fizeram?

- Proporcionaram perspectiva digital para a elaboração de indicadores sobre a violência on-line.
- Colaboraram em um texto alternativo para uma lei baseada no modelo da OEA.
- Advertiram sobre propostas problemáticas como o bloqueio de conteúdo sem garantias.

Quais dificuldades houve?

- Tensões entre direitos (proteção frente à violência e à liberdade de expressão).
- Processos legislativos rápidos, sem suficiente consulta pública.
- Desacordos sobre quem deve ter poder para eliminar conteúdos.

O que conseguiram?

- Tornar visível os direitos digitais no debate sobre violência política.
- Promover o diálogo entre atores diversos.
- Gerar recomendações para políticas mais equilibradas e participativas.

É um exemplo claro de como a sociedade civil pode incidir criticamente em processos legislativos para proteger direitos no 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.

UNIDADE 2

TEMA 5: TENDÊNCIAS E DEBATES ATUAIS

As tecnologias emergentes, os conflitos geopolíticos e a expansão das plataformas digitais (entre outros fatores) geraram novos desafios e tensões em relação à governança da Internet. Neste tema oferecemos um panorama das principais tendências e debates que afetam a evolução da Internet.

Fragmentação da Internet

O que é o splinternet?

O término se refere à fragmentação da camada técnica da Internet em múltiplas "Internet nacionais" ou regionais controladas pelos Estados ou outros atores. No primeiro módulo falamos sobre o caso da China em torno do firewall. Como parte deste fenômeno, a China mantém uma rede fortemente controlada, com acesso restringido às plataformas globais. Por outra parte, a Rússia aprovou sistemas para se desconectar da Internet global em situações de crise.

Embora alguns atores defendem estas medidas como defesa contra o colonialismo tecnológico[1] (que ocorre quando uns poucos países ou empresas -geralmente do norte global- controlam a tecnologia e fazem que outros dependam deles para usá-la ou desenvolvê-la) também **podem ser utilizadas para justificar medidas de censura, controle e isolamento.**

Vejamos um exemplo no Brasil em torno da soberania digital. Em distintas discussões políticas e legislativas no Brasil foi promovida a abordagem de quais dados devem ser armazenados dentro do país para proteger a autonomia e a proteção de dados. Organizações da sociedade civil, como a Associação Brasileira de Imprensa e grupos de direitos digitais, indicaram que sem garantias fortes de direitos humanos estas medidas podem facilitar o acesso estatal a dados e concentrar poder, especialmente se não existem salvaguardas judiciais e transparência nas solicitações de informação.

1. O colonialismo tecnológico pode ser observado quando empresas, países ou plataformas externas dominam e controlam infraestruturas, dados, normas e serviços digitais em outra região, impondo tecnologias, modelos de negócio e práticas que beneficiam aos provedores estrangeiros e reduzem a autonomia local; isto pode debilitar economias locais, limitar a diversidade cultural e pôr em risco a soberania digital.

Regulação da inteligência artificial e dos algoritmos

Por que é importante? porque cada **vez mais decisões são tomadas ou influenciadas por algoritmos e por sistemas de Inteligência Artificial (IA)**, por exemplo: quem acessa a um crédito, quais notícias vemos, quais conteúdos são censurados.

Estas decisões nem sempre são transparentes, e como se alimentam de dados e de informação, podem reproduzir tendências discriminatórias que já existem na nossa sociedade. Por exemplo, ao utilizar vozes femininas para assistentes de IA, é reforçado o estereótipo de que as mulheres devem realizar tarefas de serviço. Além disso, foram documentados casos nos quais sistemas de identificação facial têm tido dificuldades para identificar adequadamente às mulheres, em particular, às mulheres negras. Na América Latina, países como a Colômbia, o Brasil, o Chile e a Costa Rica começaram a desenvolver marcos legais ou estratégias nacionais de IA.

Cibersegurança

O que é a cibersegurança? Muitas vezes é definida como um conjunto de políticas e de medidas técnicas destinadas a proteger redes, dispositivos e infraestruturas digitais contra ataques. Entretanto, é importante entender que **não se visa proteger sistemas porque sim, mas porque estão para servir às pessoas e, por extensão, os seus direitos.** A cibersegurança é necessária para exercer os nossos direitos e, ao mesmo tempo, a ausência da cibersegurança pode ter consequências trágicas e vulnerar os nossos direitos (por exemplo, se um ciberataque filtrar informação sobre a orientação sexual de uma pessoa em um país no qual a homossexualidade está criminalizada).

Uma definição que inclui este fator é a da Freedom Online Coalition, que define a cibersegurança como *"A preservação –através de políticas, de tecnologia e de educação– da disponibilidade, da confidencialidade e da integridade da informação e da sua infraestrutura subjacente, com o fim de melhorar a segurança das pessoas tanto on-line como off-line"*.

O que acontece quando são usadas leis de ciberseguraça como ferramenta ou desculpa para restringir direitos? Leis de cibercrime ou de cibersegurança mal elaboradas podem justificar a vigilância massiva, criminalizar protesto social ou ativismo digital, perseguir jornalistas ou bloquear páginas de forma arbitrária. É por isto que como organizações da sociedade civil devemos exigir marcos de cibersegurança com enfoques de direitos humanos e de participação cidadã.

Plataformas e economia digital

O que está em jogo? As plataformas digitais como o Google, o Meta ou a Amazon concentram um grande poder econômico, social e político. Estas controlam o fluxo e o acesso à informação (através de navegadores e de redes sociais) e assim como alguns aspectos do trabalho (através de apps de delivery ou de comércio on-line). Estas plataformas definem as suas próprias regras, muitas vezes sem transparência nem responsabilidade diante dos Estados ou das pessoas.

Alguns dos problemas-chave desde uma perspectiva de direitos humanos são os monopólios digitais que dificultam a concorrência, aumentam a precarização do trabalho em plataformas e os modelos extrativistas que são baseados na exploração dos nossos dados pessoais.

Atividade:

Objetivo: Analisar como as tendências atuais em inteligência artificial, soberania digital e cibersegurança na América Latina (com foco na Colômbia) impactam os direitos humanos e geram ideias de resposta desde a sociedade civil.

Materiais: **documento digital compartilhado ou painel digital** *(Excalidraw)*

1: Identificação de tendências

- *Cada participante lê pelo menos um recurso sugerido (ex.: o blogue da ONU Mulheres sobre IA e preconceitos, o ensaio de Pohle e Thiel sobre soberania digital, e o relatório de Direitos Digitais sobre cibersegurança).*
- *No mural digital, cada pessoa escreve em um post-it virtual:*
  - *Uma tendência observada na Colômbia ou na região (ex.: uso crescente da IA na educação).*
  - *O direito que pode ser afetado.*

2: Conexão de ideias

- *O grupo organiza os post-its em 3 grandes áreas:*
  - ***IA e preconceitos***
  - ***Soberania digital***
  - ***Cibersegurança***
- *Entre os post-its, desenhem setas ou conexões que mostram como as tendências se relacionam ou se reforçam (ex.: "uso da IA em saúde" afeta privacidade também conecta com falta de soberania na gestão de dados).*

3: Resposta coletiva

- *A partir del mapa visual, el grupo escribe en el mural un "cartel de acción colectiva" con:*
  - *Um problema central (ex.: "Falta de transparência em sistemas da IA").*
  - *Uma proposta de resposta desde a sociedade civil (ex.: "Campanha para exigir auditorias com enfoque de gênero em algoritmos públicos").*
- *O cartaz pode ser um quadro de texto destacado, um desenho simples ou um ícone com frase breve.*

Resultado esperado

*Um **mapa visual** que inclua*

1. *Tendências identificadas pelo grupo.*
2. *Direitos em jogo conectados.*
3. *Uma proposta coletiva de resposta clara e visível.*

- ***Chuva de ideias*** sobre as tendências que as participantes observam na Colômbia e discussão grupal sobre quais direitos podem ser afetados e como poderíamos responder desde a sociedade civil.
- Em grupos, ***analisar manchetes de jornais*** recentes sobre a IA, filtragens de dados, plataformas sociais. Quais atores estão envolvidos? Quais direitos estão em jogo? Como podemos responder como sociedade civil?

Figura 16. Atividade.

Recursos:

- *Direitos Digitais, Artigo “América Latina ante dl inteligencia artificial: mapeo de iniciativas regulatorias en la región”*
- *Julia Pohle e Thorsten Thiel, Revista Latinoamericana de Economía y Sociedad Digital, Ensaio “Soberanía Digital”*
- *Internet Society, paper “Soberanía digital y su impacto en Internet.”*
- *UN Women, Blogue “Como la inteligencia artificial refuerza los sesgos de género y que podemos hacer al respecto.”*
- *New York Times, Artigo “Many facial-recognition systems are biased, says US study”*
- *Freedom Online Coalition, definição de cibersegurança.*
- *Direitos Digitais, Relatório “Ciberseguridad en América Latina: Estrategias nacionales en 2024”*
- *TEDIC, Trabajo y Economía Digital*
- *Direitos Digitais, artigo “Transformaciones y desafíos en los derechos digitales en América Latina: un balance de 2024”*

Figura 17. Recursos.

TEMA 6: ACESSO E CONECTIVIDADE

A Internet tem o potencial de contribuir para o **desenvolvimento sustentável, para a participação democrática e para o exercício de direitos**, mas esse potencial só pode ser cumprido se todas as pessoas puderem acessar à Internet de forma segura, significativa e equitativa. Este tema explora as múltiplas dimensões do acesso às tecnologias, não apenas técnicas ou econômicas, mas também culturais, sociais e políticas. Vamos dar visibilidade às brechas que afetam especialmente à juventude, às mulheres, às pessoas racializadas, aos povos originários e aos habitantes de zonas rurais.

DIGITALIZAÇÃO, DESENVOLVIMENTO SUSTENTÁVEL E INCLUSÃO

A digitalização pode ajudar a vida comunitária —acesso à saúde, à educação e aos mercados— mas só se chega de forma justa. Se as políticas digitais replicam as mesmas desigualdades de antes, então a tecnologia termina excluindo em vez de ajudar.

A Agenda para o Desenvolvimento Sustentável 2030[2] reúne 17 objetivos que visam precisamente reduzir essas brechas. Três deles estão muito relacionadas com o digital e com as comunidades: educação de qualidade (ODS 4), infraestrutura e conectividade que incluam a todos (ODS 9), e a redução das desigualdades (ODS 10). Pensar em tecnologia desde estes objetivos significa priorizar acesso real, conteúdos nas nossas línguas e decisões onde as comunidades tenham voz e controle.

BRECHAS DIGITAIS: QUEM ACESSA E QUEM NÃO?

Nem todas as pessoas têm o mesmo acesso à Internet. As brechas digitais não se referem apenas a estar conectados, mas também a como acessamos, com que qualidade, para que e com quais direitos. Alguns exemplos de brechas digitais são:

- **Geográficas:** há zonas rurais ou afastadas que têm baixa cobertura ou cobertura instável.
- **Socioeconômicas:** os custos dos dispositivos, da eletricidade ou dos planos de dados móveis influenciam em quem pode ter acesso a eles.
- **De gênero:** as mulheres têm menos acesso e mais probabilidade de receber violência digital.
- **Intergeracionais:** enquanto a juventude está mais exposta à Internet, as pessoas mais velhas ficam para trás.
- **Culturais e linguísticas:** falta de conteúdos em línguas originárias ou falta de conteúdos que estejam adaptados a contextos e necessidades diversas.

2 É um plano de ação adotado em 2015 pelos Estados membros das Nações Unidas. O seu objetivo é erradicar a pobreza, proteger o planeta e garantir que todas as pessoas gozem de paz e de prosperidade para 2030.

CONECTIVIDADE BÁSICA VS. ACESSO SIGNIFICATIVO

Ter conexão é um mero prerrequisito, mas não garante a inclusão. Ter conectividade significativa implica que as pessoas podem acessar e usar a Internet de forma:

- **Acessível** (a um preço acessível).
- **Segura** (sem vigilância ou sem exposição à violência).
- **Com conteúdos relevantes** (informação útil e na nossa língua).
- **Participativa** (que tenhamos a capacidade de criar e não somente consumir conteúdos, que possamos aprender, compartilhar e transformar).

REDES COMUNITÁRIAS E MODELOS ALTERNATIVOS DE CONECTIVIDADE

As redes comunitárias surgem, em muitos casos, como resposta à ausência ou às limitações dos planos do Estado para garantir a conectividade. Os programas estatais costumam se enfocar em grandes infraestruturas e contratos com empresas de telecomunicações, priorizando critérios de rentabilidade e de cobertura massiva. Isto deixa de fora as comunidades rurais, indígenas ou periféricas, onde o custo de levar infraestrutura é alto e os benefícios econômicos são baixos.

Aqui é onde entram as redes comunitárias: não visam substituir o Estado, mas sim complementar os seus esforços, demonstrando que existem modelos alternativos de conectividade que partem da organização local e de tecnologias apropriadas.

O que as distingue?

- **Operadas pela comunidade:** são as vizinhas, as pessoas da comunidade e as organizações locais que mantêm a rede e decidem sobre o seu funcionamento.
- **Tecnologias apropriadas:** Usam o que melhor se ajusta a cada território e comunidade, como frequências livres, equipamentos de baixo custo e inclusive software aberto ou infraestruturas compartilhadas.
- **Não são apenas tecnologia:** a conectividade se integra com a vida comunitária, é um apoio para a educação na língua própria, difusão de saberes tradicionais, coordenação de atividades culturais e defesa de direitos.

GOVERNANÇA NAS REDES COMUNITÁRIAS

Embora nem sempre seja chamada assim, nestas redes também existe governança: a comunidade define as suas próprias regras, decide coletivamente como a rede é usada, quem a administra, o que é priorizado e como são cuidados os recursos.

Isto significa que as decisões não vêm de uma empresa ou de um governo central, mas sim da própria comunidade, de acordo com as suas necessidades e os seus valores.

Em poucas palavras, as redes comunitárias permitem que as comunidades tomem controle da sua conectividade, protejam a sua privacidade e garantam que a Internet responda às suas realidades locais.

Exemplo: Kimera - história, propósito e como funciona

Origem e evolução

- *Entre 1985 e 2006 o projeto KIMERA desenvolveu títulos educativos e multimídia em distintos formatos.*
- *Em 2016 a nossa organização retomou o projeto com o objetivo inicial de pôr à disposição os títulos multimídia e o software educativo desenvolvido.*
- *Desde 2018 o foco foi orientado para o desenvolvimento da Red Local Kimera.*
- *Em 2024 o desenvolvimento do projeto passou para a Corporação Frutos de Utopia.*

O que é a Rede Local Kimera

- *É uma ferramenta (programa) que permite criar um servidor local com conteúdos e ferramentas acessíveis por rede sem fio.*
- *É instalada em um computador pessoal ou institucional com sistema operativo Windows.*
- *Pode ser acessada desde computadores, celulares, tablets e qualquer dispositivo com conexão sem fio ou mediante cabo de rede.*

Funcionalidade e benefícios principais

- *Provisão local de conteúdos e de ferramentas: hospeda recursos (textos, multimídia, aplicações educativas) diretamente no equipamento servidor.*
- *Acesso multiplataforma: qualquer dispositivo com conexão de rede pode usar os recursos sem depender da Internet.*
- *Troca de arquivos digitais: ao permitir a troca, cada Rede Local Kimera deixa de ser uma ilha estática; pode oferecer novas opções aos seus usuários e compartilhar conteúdos.*
- *Atualização e colaboração: as redes locais podem conectar-se entre si para trocar conteúdos, sincronizar-se e atualizar-se.*

Casos de uso típicos

- *Salas e escolas com conectividade limitada: acesso aos materiais educativos locais sem consumo de dados.*
- *Bibliotecas e centros comunitários: oferecer catálogo digital, vídeo, ferramentas e serviços locais.*
- *Instituições rurais ou eventos temporais: criar uma rede acessível rapidamente para múltiplos usuários.*
- *Laboratórios e projetos colaborativos: compartilhar arquivos, ferramentas e recursos entre participantes.*

Vantagens práticas

- *Funciona sem dependência constante da Internet.*
- *Usa hardware comum (um PC com Windows) e dispositivos de uso cotidiano (telefones, tablets, laptops).*
- *Facilita acesso inclusivo aos recursos digitais em contextos com conectividade débil ou cara.*
- *Facilita autonomia local e colaboração entre redes.*

Figura 18. Evolução da rede Kimera.

Juventudes e acesso: entre a oportunidade e a exclusão

As juventudes costumam estar no centro da cultura digital, mas isso não significa necessariamente que tenham acesso equitativo ou participação nas decisões.

Muitas vezes as juventudes usam a Internet sem alfabetização crítica, enfrentam vigilância, são excluídas das políticas públicas digitais ou sofrem violência digital (particularmente mulheres e pessoas LGBTQ+).

É por isso que devemos exigir educação digital integral, participação na formulação de políticas e acesso às tecnologias seguras e culturalmente relevantes.

Atividade: Mapeamento de brechas digitais locais

Objetivo: *Refletir sobre como as juventudes do seu entorno vivem a tecnologia, identificar barreiras concretas e propor soluções locais e políticas simples.*

Materiais: *folha de papel ou documento digital.*

Passos

1. Contexto

Escreva em uma linha quem são "as juventudes" na sua comunidade (idade aproximada, grupo: estudantes, jovens indígenas, coletivos LGBTIQ+, jovens rurais, etc.).

2. Observação rápida

Responda em uma tabela ou lista breve:

- *Como acessam normalmente à Internet? (lugar, dispositivos, custo).*
- *Menciona 4 barreiras que afetam esse acesso, uma por categoria: econômica, linguística/cultural, educativa (alfabetização digital) e de gênero/segurança (violência, vigilância). Para cada barreira acrescente 1 frase sobre como a mesma é percebida no seu entorno.*

3. Impacto na vida juvenil

Escreva 3 exemplos concretos (2–3 linhas cada um) de oportunidades perdidas ou danos por essas brechas (ex.: não poder estudar on-line, exposição à violência em redes, exclusão de processos de decisão).

Figura 19. Atividade.

Recursos:

- *Nações Unidas Agenda 2030 para o desenvolvimento sustentável.*
- *Redes Comunitarias Colombia*
- *APC, Inclusión Digital*
- *Ao Sul, Relatório "Ampliando la conectividad a Internet"*
- *APC, Relatório "Communal Internet Infrastructure"*
- *Colnodo, Blogue "Redes comunitarias e acceso al espectro: Una alternativa sostenible para la inclusión digital en Colombia".*
- *TEDIC, Relatório "Conectividad y apropiación digital para a resiliencia climatica en las zonas rurales"*
- *Derechos Digitales, Relatório "Conectividad en la Amazonia: Recomendaciones para combatir la brecha digital"*

Figura 20. Recursos.

MEIOS ALTERNATIVOS DE PARTICIPAÇÃO

Mastodon

Como exemplo de digitalização colaborativa e participativa, o Mastodon representa uma alternativa ao modelo centralizado de redes sociais. A sua arquitetura federada e autogovernada mostra como as comunidades podem gerenciar os seus espaços digitais mantendo interoperabilidade, transparência e autonomia. Isto contrasta com as plataformas centralizadas e abre um caminho para pensar em governos digitais que dialoguem com a cidadania desde uma perspectiva de soberania tecnológica.

Aqui poderia ir um vídeo tutorial introdutório, em vez de texto.

Figura 21. Interface do Mastodon

Da mesma forma que os blogues consistem em publicar atualizações em um site, o microblogging consiste em publicar pequenas atualizações em um fluxo de atualizações no seu perfil. Você pode publicar entradas de texto e, com a opção de anexar arquivos multimídia como imagens, áudio, vídeo ou enquetes.

Da mesma forma que em um site tradicional, os usuários se registram, publicam mensagens, fazem upload de fotos e conversam entre eles. Diferentemente de um site tradicional, o site Mastodon pode interoperar, o que permite aos seus usuários comunicar-se entre si; da mesma forma que você pode enviar um e-mail desde a sua conta de Gmail a alguém que utiliza Outlook, Fastmail, Protonmail ou qualquer outro servidor de e-mail, sempre que você souber o seu endereço de e-mail pode mencionar ou enviar mensagens a qualquer pessoa em qualquer site utilizando o seu endereço.

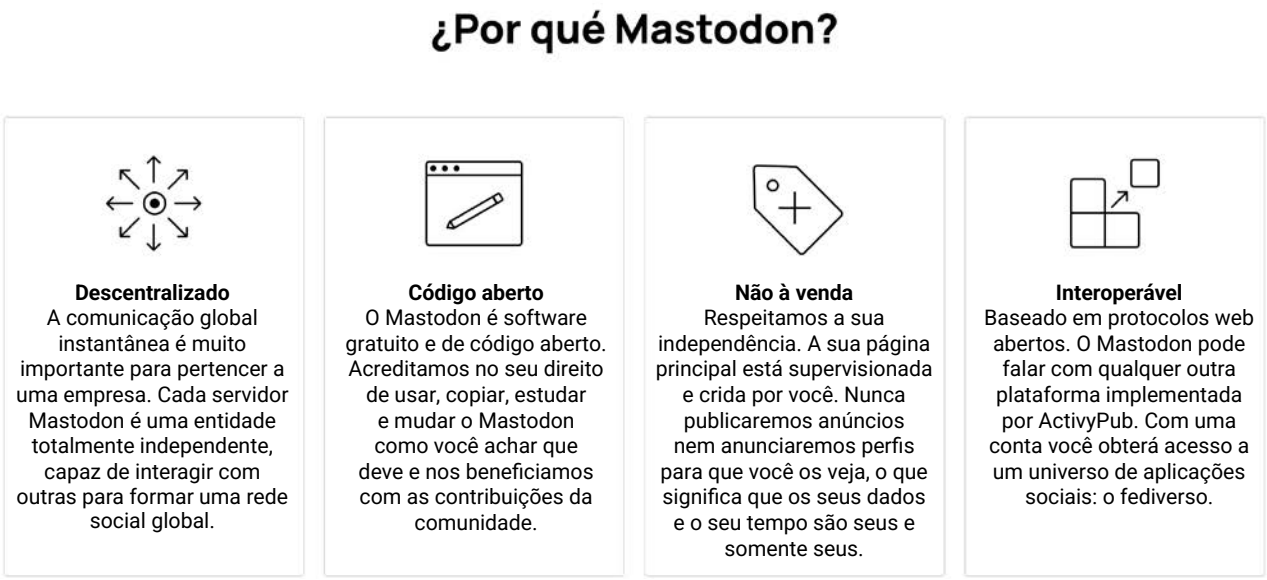


Figura 22. Por que usar o Mastodon?

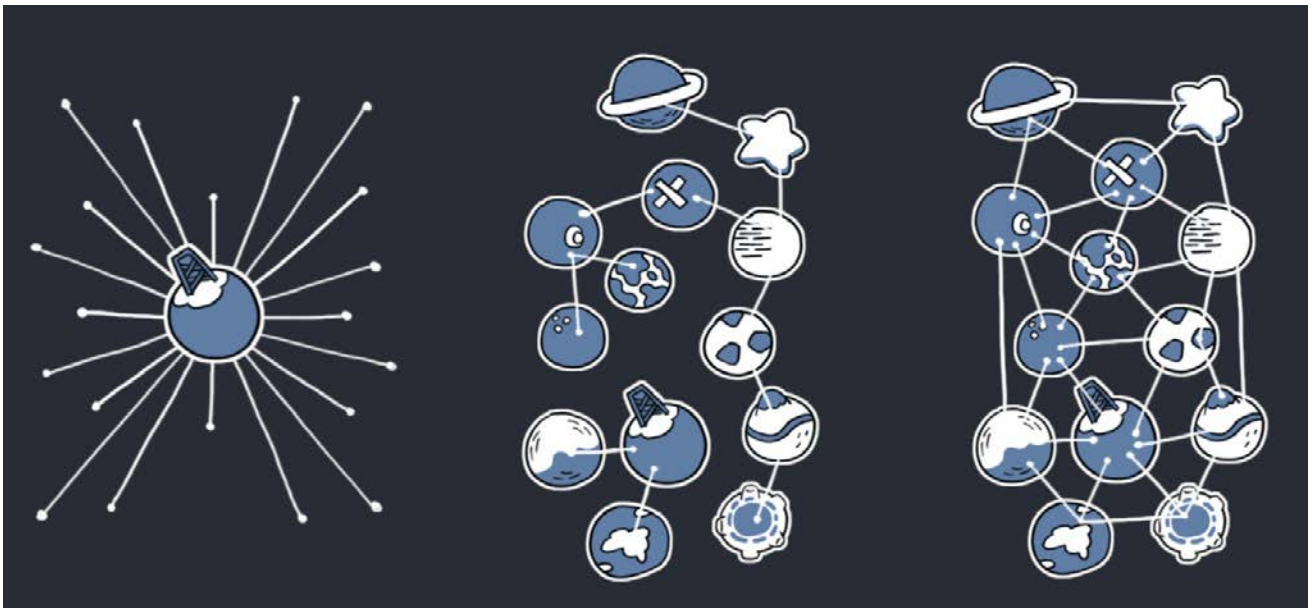


Figura 23. Da esquerda para a direita: Centralizado, Federado, Distribuído. Extraído de: https://docs.joinmastodon.org/

Contas sugeridas no Mastodon social:
https://mastodon.social/@derechosdigital
https://mastodon.social/@tedicpy
https://mastodon.social/@interferencias@social.interferencias.tech

Você também pode explorar mastodon.la

Fonte de aprofundamento:
Guía para comenzar a usar Mastodon - Laintersección

TEMA 7: GOVERNANÇA DA INTERNET E JUSTIÇA AMBIENTAL

A Internet e as tecnologias digitais não são neutras nem "imateriais": dependem de recursos naturais, de energia, de infraestruturas críticas e de circuitos de produção que têm impactos diretos e concretos sobre os territórios. Este tema propõe vincular a governança da Internet com as lutas pela justiça ambiental, tornando visível os seus impactos ecológicos, formas de extrativismo digital[3] e barreiras que enfrentam os povos originários e as comunidades rurais para participar em debates globais.

MUDANÇA CLIMÁTICA E TECNOLOGIAS DIGITAIS

Embora muitas vezes a Internet seja vinculada a soluções sustentáveis (como contribuir para a eficiência energética ou monitoramento ambiental), as tecnologias digitais têm importantes custos ecológicos.

Os impactos ambientais incluem:

- Grande consumo energético de centros de dados e de redes globais.
- A produção de dispositivos eletrônicos que precisam de minerais como o lítio, o cobalto e o coltan, muitas vezes extraídos em condições de exploração de mão de obra e afetação ambiental.
- A geração de resíduos ("e-waste"), que em muitos casos são exportados para países do Sul Global, convertendo certos territórios em aterros tecnológicos.
- Infraestruturas como cabos, antenas ou satélites que afetam ecossistemas e territórios.

Espaço de discussão: *Como a Internet pode formar parte da solução climática sem reproduzir as lógicas do extrativismo?*

Figura 24. Discusión

3. Extrativismo: modelo econômico baseado na extração intensiva de recursos naturais (minerais, petróleo, gás, madeira, commodities agrícolas) para a exportação, com escassa transformação local e baixo reinvestimento em comunidades. Costuma gerar lucros concentrados, degradação ambiental, deslocamento social e dependência econômica, ao priorizar a extração a curto prazo sobre a sustentabilidade e os direitos das populações locais.
Extrativismo digital: transferência do mesmo padrão para o mundo digital: coleta massiva e prolongada de dados, extração de valor da atenção e do comportamento das pessoas e exploração de infraestruturas digitais sem compartilhar benefícios com as comunidades produtoras. Produz dependência tecnológica e econômica, perda de soberania sobre dados e sobre plataformas, externalidades sociais (vigilância, polarização) e erosão das capacidades locais para agregar valor.

EXTRATIVISMO DIGITAL E EXTRAÇÃO DE DADOS

Da mesma forma como o extrativismo tradicional explora recursos naturais sem respeito pela vida ou pela autodeterminação dos povos, o extrativismo digital explora dados em formas problemáticas.

O que é o extrativismo digital? É um modelo baseado na coleta massiva de dados pessoais culturais e territoriais sem consentimento nem benefício para as comunidades. São práticas que afetam especialmente aos povos originários, às comunidades rurais e aos ativistas ambientais.

Alguns exemplos são:

- O uso de imagens satelitais ou drones para mapear territórios sem consulta prévia.
- Plataformas que são instaladas com incentivos fiscais e alta demanda de recursos naturais (como água e energia), especialmente em áreas empobrecidas.

POVOS ORIGINÁRIOS: PARTICIPAÇÃO E INCIDÊNCIA NA GOVERNANÇA

Apesar dos fortes impactos que as tecnologias têm sobre os seus territórios e culturas, os povos originários enfrentam múltiplas barreiras para participar em processos de governança da Internet.

Algumas barreiras comuns são:

- **Idioma e representação cultural**
- **Falta de acesso à conectividade adequada e significativa**
- **Exclusão sistemática dos espaços técnicos ou diplomáticos**
- **Falta de consulta livre, prévia e informada sobre infraestrutura digital.**

Alguns exemplos de estratégias e de resistências:

- **Alianças com coletivos ecodigitais, feministas e de direitos humanos**

Existem colaborações entre movimentos feministas e povos indígenas para promover a igualdade de gênero e os direitos coletivos. Por exemplo, na Convenção Constitucional do Chile de 2022, ficou evidenciada a importância do trabalho em rede entre representantes de povos indígenas e movimentos feministas para plasmar um texto constitucional inclusivo. Entretanto, foi indicada a necessidade de uma maior interseccionalidade para integrar plenamente os direitos das mulheres indígenas.

- **Redes comunitárias indígenas**

Telecomunicaciones Indígenas Comunitarias (TIC-AC) é uma associação civil mexicana formada por comunidades indígenas e rurais. Desde 2016, tem obtido concessões sociais para operar redes de telecomunicações autônomas em estados como Oaxaca, Guerrero, Puebla, Chiapas e Veracruz. Estas redes permitem às comunidades gerenciar a sua própria infraestrutura de telefonia móvel e de Internet, promovendo a autonomia tecnológica e a preservação cultural.

- **Participação em fóruns de governança**

As comunidades indígenas tem aumentado paulatinamente a sua participação em espaços de governança da Internet, como o Fórum de Governança da Internet e o seu capítulo regional.

Recursos:

- *Paz Peña Ochoa, Livro “Tecnologías para un planeta en llamas” e keynote “Hacer que la digitalización funcione para un desarrollo inclusivo y sostenible”*
- *ALAI e APC, pesquisa “Tecnologia y medio ambiente: respuestas desde el Sur Global”*
- *Telecomunicaciones Indígenas Comunitarias*
- *Colnodo, Documentário “Redes Comunitarias”*
- *APC, Tecnología, justicia ambiental y sostenibilidad*
- *APC, artigo “Sembrando cambios en 2023: El gran impacto comunitario de la red de APC”*
- *APC, artigo “Sembrando cambios: Sostenibilidad ambiental y la importancia de potenciar el liderazco de las mujeres”.*
- *Jess Ciacci, Sursiendo, artigo “Imaginar un principio feminista para Internet que ponga en el centro la justicia ambiental”*

Figura 25. Recursos.

TEMA 8: GOVERNANÇA DE PLATAFORMAS DIGITAIS E IGUALDADE DE GÊNERO

Atualmente, as plataformas digitais (redes sociais, buscadores, apps, marketplace) são espaços-chave para a vida social, econômica e política. Porém, não são neutros: têm regras próprias, algoritmos opacos e políticas que muitas vezes reproduzem desigualdades e violências estruturais. Este tema explora como são governadas as plataformas, como afetam de maneira específica tanto mulheres como pessoas LGBTQ+ e quais alternativas feministas propõem uma Internet mais justa, inclusiva e transformadora.

O QUE É A GOVERNANÇA DE PLATAFORMAS DIGITAIS?

As plataformas digitais (como o TikTok, o Facebook, o Youtube, o Instagram) são atores privados que decidem qual conteúdo é mostrado ou eliminado, qual é promovido, qual é permitido ou quando, e como são coletados dados e o uso dado a eles.

Modelos de governança atuais:

- **Autorregulação:** as empresas definem as suas próprias regras sem intervenção estatal;
- **Corregulação:** colaboração entre o Estado e as plataformas para regular certos conteúdos ou comportamentos;
- **Regulação estatal:** leis que obrigam às plataformas a cumprir normas sobre moderação, transparência ou responsabilidade legal.

Alguns problemas ou desafios comuns são a **falta de transparência** sobre como são moderados os conteúdos, a **censura desigua**l (conteúdos sobre direitos sexuais e reprodutivos vs. discursos de ódio) e regras e algoritmos criados desde o Norte Global com **pouca perspectiva local ou interseccional.**

VIOLÊNCIA DE GÊNERO DIGITAL: UMA EXPRESSÃO ESTRUTURAL

As mulheres e as dissidências de gênero enfrentam violências específicas e sistemáticas no entorno digital que refletem e ampliam as violências que já existem no mundo *off-line*.

Tipos de violência digital

- Assédio, ameaças, doxxing (difusão de dados pessoais com intenção de dano).
- Censura seletiva de conteúdos feministas.
- Deepfakes, o uso da IA para criar e difundir imagens íntimas sem consentimento.
- Algoritmos segmentados, excludentes e a invisibilidade de conteúdos por parte de plataformas.
- Vigilância e controle, especialmente contra ativistas, jornalistas, mulheres em política ou líderes comunitárias.

Os impactos da violência de gênero digital são muito graves e incluem o silenciamento de vozes críticas, autocensura e retraimento do espaço público digital, maior exposição e revitimização e

obstáculos para a participação política e para o exercício de direitos.
Desde a Fundación Karisma (Colômbia) e organizações como Luchadoras (México) temos documentado como mulheres indígenas, afrodescendentes, ou trans enfrentam formas específicas e agravadas de violência digital, que combinam racismo, classismo, misoginia e homofobia.

FEMINISMO E TECNOLOGIA: RUMO A UMA INTERNET FEMINISTA

Diante destes desafios, organizações feministas e de direitos digitais desenvolveram propostas e princípios para construir tecnologias mais justas, participativas e transformadoras.

Os **Princípios Feministas para a Internet** foram desenvolvidos por um grupo de ativistas e de organizações da sociedade civil convocados pela Association for Progressive Communications (APC) a partir de 2014, durante um encontro na Malásia foram se ampliando e consolidando em encontros posteriores.

Alguns dos princípios relevantes a este tema são:

- **Acesso à Internet:** Uma Internet feminista começa com possibilitar que mais mulheres e pessoas queer possam ter um acesso universal, satisfatório, acessível, sem condições, aberto, significativo e igualitário à Internet
- **Acesso à informação:** Apoiamos e protegemos o acesso irrestrito à informação relevante para as mulheres e para as pessoas +queer, em particular informação sobre temas de saúde e direitos sexuais e reprodutivos, prazer, aborto seguro, acesso à justiça e temas LGBTIQ.
- **Tomada de decisões na governança da Internet:** Estamos a favor de desafiar os espaços e os processos patriarcais que controlam a governança da Internet e de incluir a mais feministas e pessoas queer na tomada de decisões.
- **Economias alternativas:** Temos o compromisso de questionar a lógica capitalista que empurra a tecnologia para uma maior privatização, lucro e controle corporativo. Trabalhamos para criar formas alternativas de poder econômico baseadas em princípios de cooperação, solidariedade, bens comuns, sustentabilidade ambiental e apertura.
- **Liberdade de expressão:** Defendemos o direito a expressar-nos sexualmente como uma questão de liberdade de expressão e, não menos importante, que a expressão política ou religiosa. Nós nos opomos radicalmente a todo esforço por parte de atores estatais e não estatais de controlar, vigiar, regular e restringir a expressão feminista queer na Internet através da tecnologia, da legislação ou da violência.
- **Pornografia e "conteúdos ofensivos":** Reconhecemos que o tema da pornografia on-line tem que ver com o aliciamento, o consentimento, o poder e o trabalho. Recusamos todo vínculo causal simples entre o consumo de conteúdos pornográficos e a violência contra as mulheres. Também recusamos a abrangente expressão "conteúdo sensível" como etiqueta aplicável à expressão da sexualidade feminina e transgênero. Estamos a favor de reivindicar e de criar conteúdo erótico alternativo que se oponha à visão patriarcal dominante e que coloque os desejos das mulheres e das pessoas queer no centro.
- **Violência on-line:** Apelamos a todos os setores interessados da Internet, incluindo usuários/as, formuladores de políticas e do setor privado, para abordar a questão do assédio on-line e da violência relacionada com a tecnologia. Os ataques, ameaças, intimidação e vigilância que experimentam as mulheres e as pessoas queer são reais, prejudiciais e alarmantes e são parte do problema mais amplo da violência baseada no gênero. É a nossa responsabilidade coletiva abordar e terminar com dita violência.

- ***Actividad:***

Identificar um problema concreto de governança da Internet que afeta à comunidade (ex.: preconceitos na IA, falta de conectividade, censura de conteúdos feministas) e, desde uma lógica feminista e de justiça de gênero, desenvolver propostas de regras, de práticas e de decisões para enfrentá-lo.

1. Eleger uma problemática

A partir do trabalhado nas atividades prévias, selecione um problema específico que você queira abordar. Exemplos: violência de gênero digital, censura de conteúdos sobre direitos sexuais e reprodutivos, preconceitos na IA, vigilância estatal.

2. Analisar o problema

Responda brevemente:

- *A quem afeta mais e por quê?*
- *Quais atores têm poder nesta situação (governo, empresas, sociedade civil)?*
- *Quais direitos estão em jogo?*

3. Imaginar desde a justiça de gênero

Agora vão propor como seriam as regras e as práticas justas para enfrentar esse problema

- ***Regras:*** *Quais normas são necessárias (ex.: transparência em algoritmos, regras claras contra violência digital)?*
- ***Prioridades:*** *O que seria posto no centro (ex.: cuidado, inclusão, línguas locais)?*
- ***Decisões:*** *Como seriam tomadas coletivamente (ex.: participação comunitária, consultas abertas)?*
- ***Tecnologia:*** *se for usada, quais critérios feministas deveria cumprir (ex.: acessível, auditável, sem preconceito)?*

4. Ação coletiva

Escreva uma proposta de incidência realizável (ex.: campanha de sensibilização, aliança com uma ONG, participação em uma consulta pública)

Figura 26. Atividade

Recursos:

- *Principios Feministas para Internet*
- *TEDIC, Podcast Libres y segures en Internet, episodio 10, Violencia de género en línea*
- *TEDIC, Informe "Violencia de género facilitada por la tecnología a mujeres políticas en Paraguay"*
- *Luchadoras, Guia 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 Investigacion por una Internet Feminista.*

Figura 27. Recursos

CONCLUSÕES

A Internet não é apenas uma ferramenta: é um espaço onde estão em jogo poder, direitos e oportunidades. A sua governança não ocorre em um só lugar nem é definida em um único ator; é o resultado de negociações e de tensões entre governos, empresas, comunidades técnicas, sociedade civil e setor acadêmico. Entender esta estrutura nos permite ver que as regras da Internet não são neutras e que a participação cidadã é indispensável para que as decisões não estejam concentradas em uns poucos, mas sim que reflitam as necessidades e as aspirações da diversidade de comunidades que a habitam.

O que está em jogo vai muito além da dimensão técnica; cada política de conectividade, cada decisão sobre dados pessoais ou cada norma sobre moderação de conteúdos tem um impacto direto nas nossas vidas. Nela são definidas condições que afetam os direitos fundamentais como a privacidade, a liberdade de expressão, o acesso à informação e a não discriminação. Assim que deixar estes debates unicamente nas mãos de atores poderosos, como governos ou empresas, pode reforçar desigualdades ou legitimar práticas de controle. Portanto, participar na governança da Internet é uma forma concreta de defender os nossos direitos no entorno digital e garantir que este espaço sirva para o bem comum.

Na América Latina, os desafios são ainda maiores pelas desigualdades estruturais que arrastamos desde séculos: as brechas de conectividade, o custo do acesso, a carência de conteúdos em línguas locais e a exclusão de comunidades rurais e indígenas, evitam que a Internet seja uma ferramenta para a inclusão. Entretanto, também existem experiências que nos mostram outros caminhos como as redes comunitárias que fortalecem a autonomia tecnológica, as lutas feministas que exigem uma Internet livre de violência de gênero e de coletivos sociais que levam as suas vozes para espaços globais de incidência; ditas iniciativas demonstram que, inclusive em condições adversas, é possível gerar alternativas que façam da Internet um recurso mais justo e equitativo.

Resumidamente, este módulo nos ensina que a Internet não é um espaço neutro, mas sim um campo de disputa política, social e cultural. Nesta ordem de ideias, para que seja verdadeiramente aberto, inclusivo e democrático, são necessárias regras claras, processos transparentes e participação efetiva da sociedade civil em todos os níveis de governança. Somente assim conseguiremos que a rede contribua para ampliar direitos, fortalecer a democracia e proteger as nossas comunidades e territórios. Por isso, participar não é um privilégio, mas sim um direito e uma responsabilidade compartilhada.

cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

DIGITALIZAÇÃO, GOVERNANÇA E PARTICIPAÇÃO

Módulo 3

Ciclo de formação sobre governança da internet

Fundación Karisma

CONTENIDO

INTRODUÇÃO

Na atualidade, o Estado mobiliza recursos tanto econômicos como humanos para desenvolver processos que pretendem “facilitar” a prestação de serviços cidadãos através da digitalização dos mesmos.

Entretanto, os processos de transformação digital na administração pública costumam ser desenvolvidos sem os espaços de participação cidadã necessários para garantir a sua implementação, acesso e aproveitamento: estes devem responder satisfatoriamente às necessidades reais da cidadania e contemplar os contextos econômicos e culturais de comunidades vulneráveis. Em muitos casos, estas iniciativas terminam reproduzindo desigualdades existentes, pois não consideram brechas digitais como o acesso à conectividade, às diferenças territoriais, às limitações de alfabetização digital ou às condições de acessibilidade para populações diversas.

Além disso, tendem a apresentar-se principalmente como respostas tecnocráticas aos problemas de (in)eficiência estatal, mais do que como oportunidades para fortalecer o vínculo cívico entre cidadania e Estado. Desta maneira, a ênfase é geralmente colocada em indicadores de cobertura e velocidade dos procedimentos, em vez de qualidade democrática dos processos e da garantia de direitos.

Por isso, é fundamental promover espaços de diálogo e reflexão crítica que nos permitam questionar o que entendemos por transformação e governo digital, qual é o seu impacto na relação cotidiana com o Estado e como garantimos que estas políticas não apenas agilizem processos administrativos, mas que ampliem a participação, fortaleçam a confiança cidadã e reconheçam a diversidade de experiências digitais no país. Também, implica identificar e usar as ferramentas que temos à mão: legais, tecnológicas e organizativas, para exigir que a digitalização seja um verdadeiro instrumento de inclusão e de garantia de direitos, em vez de uma nova forma de exclusão.

Finalmente, a forma na qual são desenvolvidas, regulamentadas e administradas estas iniciativas digitais enquadra-se dentro da governança da Internet: uma estrutura de normas, decisões e atores que incidem em como é construída, acessada e utilizada a rede -como vimos no módulo anterior-. Isto implica reconhecer que as políticas de transformação digital não são neutras, mas sim que respondem a visões específicas sobre qual lugar deve ocupar a tecnologia na vida social. Por isso, resulta chave que os princípios da governança da Internet (participação multilateral, transparência, inclusão e enfoque de direitos) também orientem a maneira na qual são concebidos e executados os serviços digitais estatais, garantindo que sejam ferramentas ao serviço das pessoas e não mecanismos que aprofundem a desigualdade ou a concentração de poder.

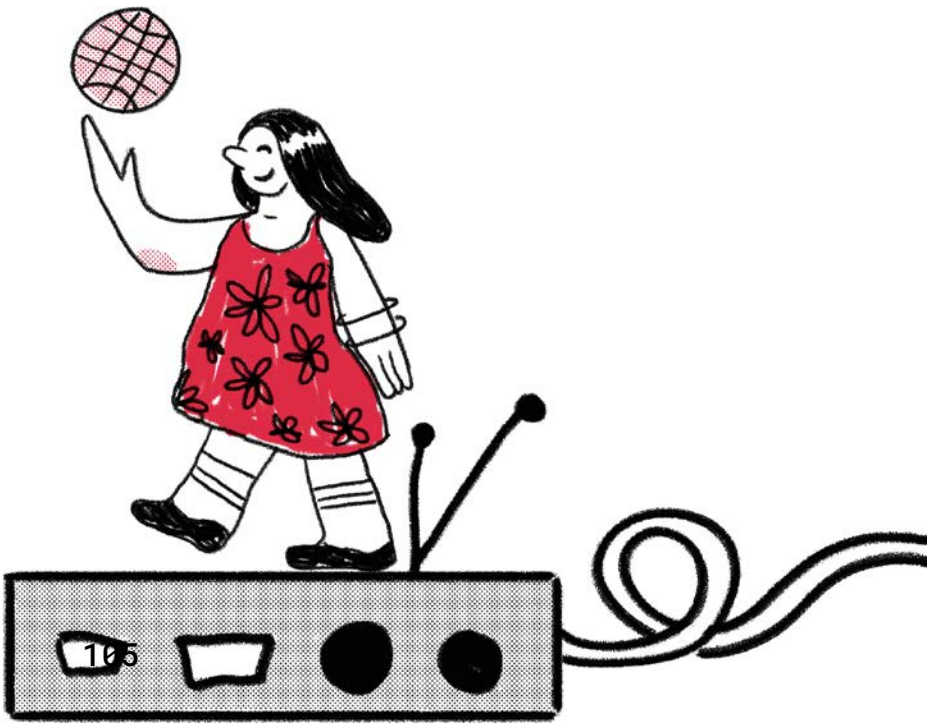
OBJETIVO GENERAL

Objetivo general:

Fomentar a compreensão crítica e experiencial da digitalização de processos, de informação e de serviços prestados pelo Estado, promovendo a garantia e o acesso a direitos.

Objetivo específicos

- Compreender os conceitos-chave e o contexto da transformação e do governo digital impulsionada pelos Estados.
- Identificar os principais desafios e oportunidades que enfrentam os jovens, as comunidades rurais e os grupos em condição de vulnerabilidade em relação com a digitalização dos serviços cidadãos.
- Relacionar os contextos de governança da Internet com espaços de participação local e regional para promover os direitos humanos em contextos de digitalização de serviços prestados pelo Estado.



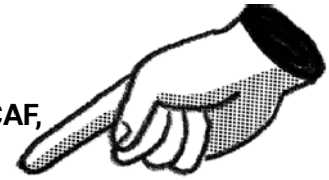
UNIDADE I: A RELAÇÃO ENTRE TECNOLOGIA, ESTADO E DH

TECNOLOGIA, ESTADO E DIREITOS HUMANOS

A transformação digital mudou a forma em que vivemos, trabalhamos e nos relacionamos com o Estado. Na América Latina e no Caribe (doravante LAC), a governança digital é uma prioridade política há quase 10 anos, com avanços desiguais entre países. Por exemplo, a criação da Estratégia Nacional de Governança Digital de acordo com cada país da região:

País	Nome da estratégia (português)	Ano
Argentina	Estratégia aplicada ao Programa Federal de Transformação Pública Digital	2022
Barbados	Programa de Modernização do Setor	2019
Bolívia	Plano Público de implementação de governo eletrônico 2017-2025	2017
Brasil	Estratégia de Governo Digital / Estratégia de Governo Digital – 2020 a 2023*	2020
Chile	Estrategia de Transformación Digital del Estado	2019
Colômbia	Política de Governo Digital (2022)	2022
Costa Rica	Estratégia de Transformação Digital do Estado rumo à Costa Rica do Bicentenário 4.0	2018
República Dominicana	Agenda Digital 2030 – Eixo de Governo Digital	2022
Ecuador	Plano Nacional de Governo Eletrônico 2018-2021	2018
México	Estratégia Digital Nacional 2021-2024 – Linha de ação: Política Digital na Administração Pública Federal	2021
Panamá	Agenda Digital Nacional 2022 – Facilitadores Transversais do Governo Digital	2022
Paraguai	Agenda Digital – Componente: Governo Digital	2019
Peru	1. Política Geral do Governo 2021-2026 – Eixo 8: Governo e transformação digital com equidade 2. Regulamento da Lei de Governo Digital	2018 y 2021
Trinidade e Tobago	Plano Estratégico das TIC 2018-2022 – Estratégias de Governo Digital	2018
Uruguai	Plano de Governo Digital 2025	2021
Venezuela	Plano Nacional de Governo Eletrônico 2014-2019	2014

Figura 1. Estratégias Nacionais de Governo Digital (ENGD) na LAC (2022)



Nota. Extraído 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. Consultado em 8 de setembro de 2025, em** https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-america-latina-y-el-caribe_7a127615-es.html

A forma na qual são desenvolvidas, regulamentadas e administradas estas políticas estão inseridas no marco da **governança da Internet**, já que são um conjunto de processos e regras que determinam como usamos e gerenciamos a rede. Estas devem garantir que a tecnologia esteja ao serviço das pessoas e não ao contrário.

A relação entre tecnologias (neste caso digitais) e o Estado começa com um movimento global de **transformação digital**, resultado da consolidação dos sistemas de informação e da implementação de processos de digitalização nas entidades públicas e privadas, com o interesse de melhorar processos tornando-os mais eficientes.

Este conceito —que é desenvolvido na unidade de conceitos-chave— significa também um momento de transição que permite pensar qual é a maneira na qual queremos que esses processos ocorram e se realmente estão garantindo a nossa autonomia e os nossos direitos.

Por isto, a integração de tecnologias digitais a processos de gestão estatal e digitalização de serviços prestados pelo Estado precisa considerar marcos internacionais de direitos humanos, os quais são obrigações assumidas por cada Estado sob os instrumentos internacionais.

Isto implica incorporar à legislação interna, de maneira clara e efetiva, os direitos e deveres reconhecidos em tratados internacionais como a **Convenção Americana sobre Direitos Humanos (CADH), o Protocolo de San Salvador** e a jurisprudência da **Corte Interamericana de Direitos Humanos**, os quais estabelecem que as políticas públicas —incluindo o uso de tecnologias como a inteligência artificial— devem respeitar os princípios de **legalidade, de necessidade e de proporcionalidade.**

LEGALIDADE:	**NECESSIDADE:**	**PROPORCIONALIDAE:**
Significa que toda ação deve estar fundamentada nas leis e normas vigentes.	Deve ser usado apenas quando realmente proporciona um benefício que não pode ser conseguido de outra maneira mais simples ou acessível.	Deve estar equilibrado: não deve causar mais problemas que benefícios.

Figura 2. Princípios de legalidade, de necessidade e de proporcionalidade.

Estes critérios são **essenciais** para garantir que a adoção de ferramentas digitais e automatizadas não vulnere os nossos direitos.

Neste sentido, documentos como a **Resolução A/HRC/RES/48/4 do Conselho de Direitos Humanos** reforçam a necessidade de que os Estados integrem ditos princípios no desenvolvimento e implementação dos seus marcos normativos e políticas tecnológicas.

MATERIAL ADICIONAL OU DE APROFUNDAMENTO:

- Convención Americana sobre Derechos Humanos. Interpretada e ilustrada por e para crianças e adolescentes da América Latina e do Caribe.
- ¿Qué es el Protocolo de San Salvador?
- ¿Qué es la Corte IDH?
- A/HRC/RES/48/4 Asamblea General

Para compreender a relação entre tecnologia, Estado e direitos humanos é importante considerar os seguintes aspectos: :

1. **Características sociodemográficas e tecnológicas** do país onde estão sendo implementadas e/ou geradas. Por exemplo: a distribuição da população, o acesso às tecnologias e às condições socioeconómicas que o determinam.
2. **Contexto regulatório e institucional** de cada país, em particular, leis de proteção de dados pessoais e acesso à informação pública.
3. **Infraestrutura e características técnicas e funcionais** que permitem o uso de tecnologias específicas na região.
4. **Processos de participação** que permitam às pessoas envolvidas ser escutadas não só na construção, mas também nas ações e nos planos que as afetem direta ou indiretamente.

Além disso, existem desafios permanentes em relação ao Estado como regulador em aspectos relacionados com: a proteção de dados, o acesso à informação, as regulamentações sobre cibersegurança, vigilância das comunicações, identificação e interoperabilidade, entre outros temas. Por exemplo, na Colômbia é habitual a dependência do Estado em relação a empresas estrangeiras como IDEMIA, multinacional francesa dedicada ao desenvolvimento de tecnologias para a identificação oficial. Também, existem desafios que provêm de tecnologias disruptivas e de um modelo de inovação não regulamentado como por exemplo, o serviço de verificação de identidade por parte do Worldcoin no México, no Chile e em outros países da região.

Na LAC existem vários espaços de discussão sobre a relação entre Estado, direitos humanos e tecnologia que vão de mãos dadas com a governança da Internet, como foi visto no módulo anterior.

PERGUNTA ATIVADORA: Como você vê a relação entre tecnologia, estado e direitos humanos no seu país?

CELULARES[1] E COMPUTADORES: INFRAESTRUTURA, COBERTURA E ACESSO

Os celulares e os computadores não servem apenas para comunicar-nos por meio de apps de mensagens e de redes sociais, são as ferramentas físicas através das quais exercemos, também, a cidadania digital; isto é, quando usamos estes dispositivos podemos, também, exercer e promover a garantia dos nossos direitos. Embora os dispositivos sejam essenciais para que possam funcionar e desenvolver todo o seu potencial precisam de infraestrutura: redes elétricas, redes de conectividade, centros de dados, antenas e pontos de interconexão. A implementação desta tecnologia é um meio para medir que tão sólida é a infraestrutura, a cobertura e o acesso à Internet.

Por exemplo:

Este é um mapa de calor que mostra a cobertura móvel 5G da Movistar[2] em Bogotá, Colômbia:

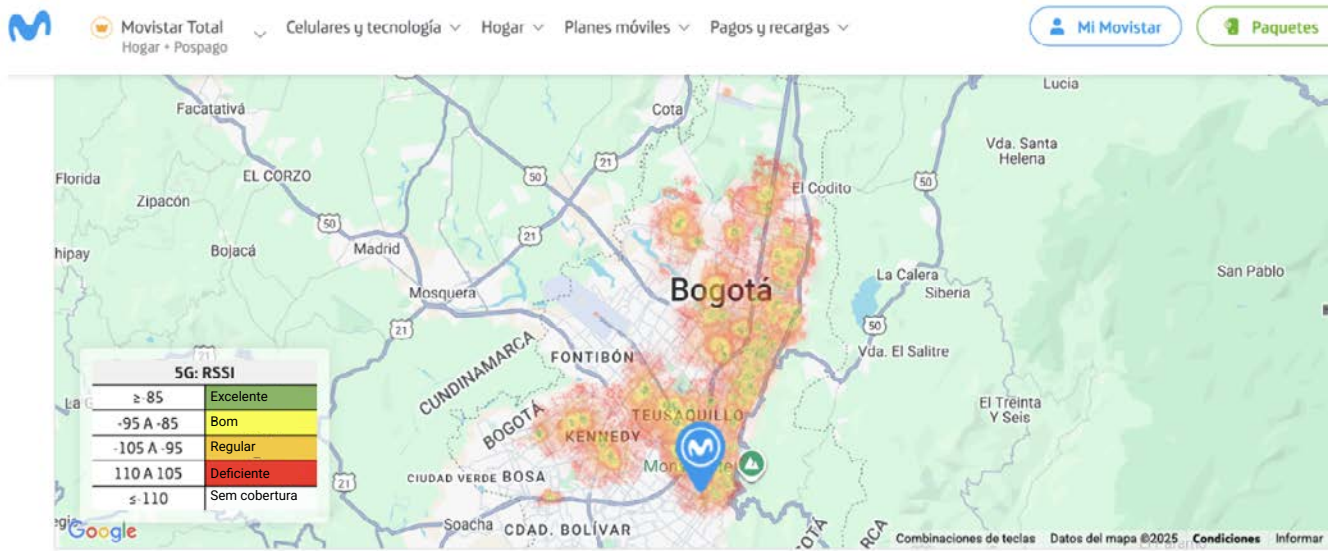


Figura 3. Cobertura móvel 5G da Movistar em Bogotá

Extraído de Movistar. (s.f.). Mapa de Cobertura Móvel 5G. movistar. https://www.movistar.com.co/mapa-de-cobertura-movil

1. Celular en Colombia, Móvil en Argentina, etc.
2. A qual é uma aproximação teórica da cobertura à realidade pois depende da zona, tráfego, topologia do terreno.

E, esta é em Montería, Colômbia, do mesmo operador e rede:

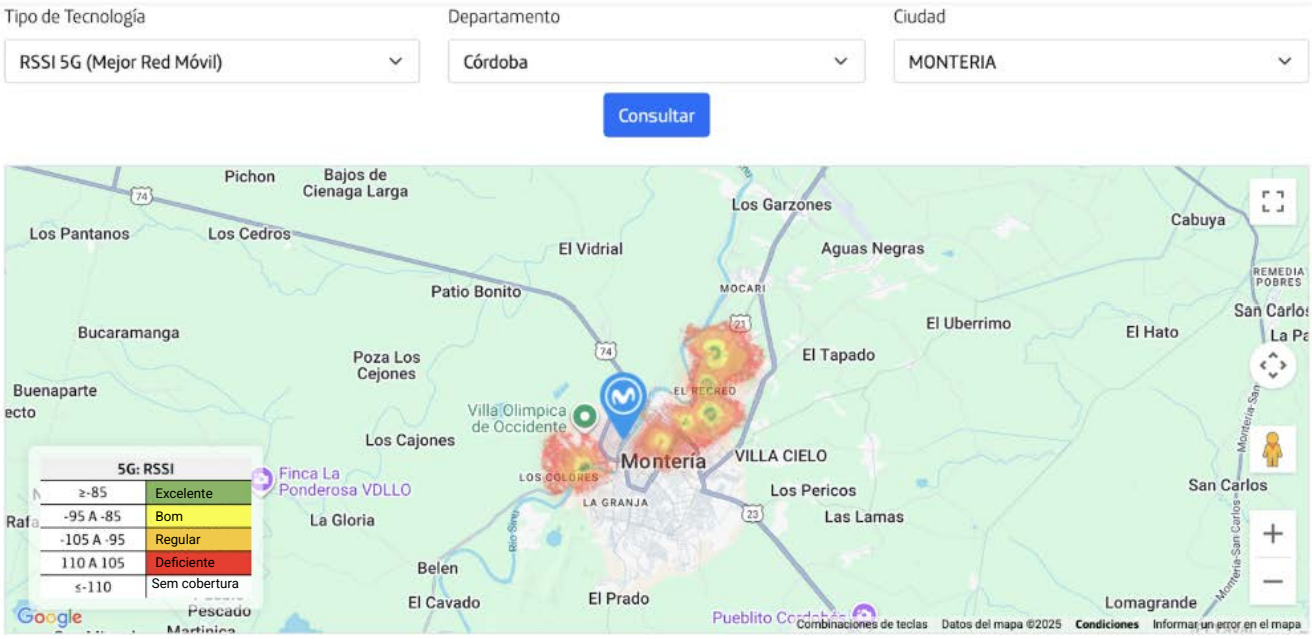


Figura 4. Cobertura móvel 5G da Movistar Montería, Córdoba.

Extraído de Movistar. (s.f.). Mapa de Cobertura Móvel 5G. Movistar. https://www.movistar.com.co/mapa-de-cobertura-movil

A forma na qual é decidido onde instalar infraestrutura depende de quantas pessoas vivem no lugar, das características do território e de se é rentável ou não para as empresas investir ali. Por isso, para que seja possível chegar mais longe, é necessário que o Estado participe oferecendo regras claras e incentivos. Mesmo assim, a realidade é que as redes nas zonas rurais ou marginalizadas não têm a mesma qualidade que as das cidades com melhores condições econômicas.

Embora a Movistar só tenha cobertura de 55,4% na Colômbia, o relatório[3] sobre o estado da infraestrutura e da cobertura dos serviços móveis no país (em junho de 2024) evidencia como pode variar o acesso e a infraestrutura de acordo com o lugar onde nos encontremos.

Neste sentido, as telecomunicações desempenham um papel fundamental para exercer espaços de participação e de governança da Internet. Em muitas regiões dos países da LAC o celular/telefone móvel é o principal, por não dizer que o único, meio de conexão à Internet. Este dispositivo pode apresentar limitações técnicas (alguns dispositivos têm baixa capacidade de armazenamento e atualizações limitadas) e situações de vulnerabilidade em termos de segurança digital, porém, é uma ferramenta que permite amplificar e consolidar também a comunidade e a conexão entre causas.

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

Mencionado isto, também é importante indicar que ter acesso à tecnologia (por exemplo a celulares) não significa que automaticamente é produzida uma transformação se as pessoas não sabem usá-la para exercer os seus direitos. A isto somemos outros problemas associados à digitalização, por exemplo:

- **Falta de competências digitais:** Muitas pessoas usam a tecnologia só para entretenimento, não sabem como proteger os seus dados, acessar à informação pública ou fazer processos on-line. Isto limita o uso da digitalização como ferramenta de empoderamento.

- **Desigualdades de gênero e de idade:** Em muitos contextos, as mulheres, as pessoas mais velhas ou com deficiência enfrentam barreiras adicionais no acesso e no uso do digital. Isto reforça desigualdades já existentes em vez de reduzi-las.

- **Precarização do trabalho:** A digitalização e a automatização podem deslocar empregos tradicionais sem que existam suficientes políticas de transição. Além disso, o trabalho em plataformas digitais muitas vezes se caracteriza pela falta de direitos trabalhistas.

Na prática, qualquer debate sobre acesso universal ou inclusão digital na governança da Internet depende da disponibilidade, da acessibilidade e da capacidade de uso destes dispositivos. São o canal pelo qual são materializadas as decisões sobre acesso, neutralidade, segurança e direitos digitais.

DISPONIBILIDADE:	ACESSIBILIDADE:	CAPACIDADE:
Refere-se à existência física e técnica da infraestrutura e dos dispositivos necessários para conectar-se à Internet.	Relaciona-se com a capacidade econômica das pessoas para financiar o acesso.	É a habilidade efetiva das pessoas para utilizar os dispositivos e os serviços digitais de maneira significativa.

Figura 5. Definição de disponibilidade, de acessibilidade e de capacidade.

UNIDADE 2: CONCEITOS-CHAVE

TRANSFORMAÇÃO DIGITAL

Pode ser entendida como o processo de transição da maneira na que realizamos trâmites e gerenciamos processos em distintos âmbitos da vida em sociedade. Implica passar de práticas físicas ou em papel, para soluções digitais, incorporando ferramentas tecnológicas, melhorando a conectividade, modernizando a infraestrutura de telecomunicações e fomentando a inovação em pessoas, em empresas e em governos.

Entretanto, este processo pode excluir a: pessoas adultas mais velhas que não usam meios digitais, comunidades rurais sem conectividade, mulheres em situação de pobreza que dependem de equipamentos herdados, entre outros setores. Todas elas costumam ficar de fora dos benefícios que promete a digitalização.

Um caso da América Latina

Em vários países da região, os sistemas de saúde incorporaram prontuários eletrônicos e consultas on-line. Um hospital público, por exemplo, pode substituir os prontuários em papel por um sistema digital no qual o médico consulta antecedentes desde um tablet enquanto o paciente agenda a sua consulta através de uma aplicação e recebe lembretes por SMS. Isto agiliza a atenção, evita a perda de informação e abre a possibilidade de teleconsultas, especialmente úteis para comunidades rurais com conectividade melhorada.

Neste sentido, cada país conta com a sua própria estratégia de transformação digital.

Aqui você pode encontrar alguns exemplos da região:

MÉXICO
IDDE 2023.

URUGUAI
Uruguay Digital.

PERU
Política Nacional de Transformación Digital.

COLÔMBIA
Estrategia Nacional Digital de Colombia.

Com a pandemia de COVID-19 acelerou-se a adoção de serviços digitais e a transformação digital converteu-se no lema de diferentes apostas de política pública para gerar um modelo de governo mais acessível e eficiente.

GOVERNO DIGITAL

Quando falamos de **governo digital** nos referimos a uma série de políticas, de iniciativas, de estratégias, de processos e de narrativas que se referem à prestação de serviços por parte das entidades do Estado através do uso e do aproveitamento das Tecnologias da informação e da Comunicação (TIC). Isto inclui um âmbito de governança para a adequada gestão de serviços digitais, de identidade digital, de interoperabilidade e de segurança digital.

Para o caso da América Latina

Um exemplo de governo digital é o guichê único virtual, onde os cidadãos podem realizar atividades como pagamento de impostos ou registro de negócios, entre outros serviços. Através de uma página web ou de uma aplicação, as pessoas apresentam as suas solicitações e realizam pagamentos, identificando-se com a sua identidade digital. Além disso, sistemas interoperáveis compartilham informação entre a secretaria de fazenda e urbanismo para validar dados sem a necessidade que o cidadão tenha que apresentar documentos. Isto poderia reduzir as visitas presenciais, acelerar processos e melhorar a transparência, mas também pode criar inconvenientes, barreiras e dificuldades.

Para compreender melhor o exemplo anterior acreditamos que é importante esclarecer as diferenças entre **governo eletrônico** e **governo digital** a seguir.

DO GOVERNO ELETRÔNICO AO GOVERNO DIGITAL

O governo eletrônico e o governo digital estão estreitamente relacionados, mas representam etapas e enfoques distintos. O primeiro se centra em digitalizar processos existentes, transferindo processos e serviços tradicionais para canais on-line para ganhar eficiência, transparência e rapidez, sem alterar substancialmente a lógica administrativa que os sustenta.

Ao contrário, o governo digital implica uma mudança mais profunda e estratégica: utiliza tecnologias e dados para reformular as políticas, os serviços e as interações com a cidadania, priorizando um enfoque centrado nas pessoas, na proatividade, na integração entre instituições e no uso ético da informação. Enquanto o governo eletrônico é, em grande medida, uma "tradução digital" do analógico, o governo digital é uma reinvenção do Estado na era digital, onde a tecnologia não é um fim em si mesmo, mas um meio para construir serviços inclusivos, coerentes e inovadores[4].

Fonte: OCDE (2021[3]), The E-Leaders Handbook on the Governance of Digital Government,, https://doi.org/10.1787/ac7f2531-en

4. https://biblioguias.cepal.org/gobierno-digital/defniciones

Faceta1: Fatores contextuais	Faceta 2: Modelos institucionais	Faceta 3: Instrumentos de políticas
Dimensão 1.1 Cultura e estrutura política e administrativa geral	Dimensão 2.1 Macroestrutura	Dimensão 1.3 Estratégia e plano
Dimensão 1.2 Fatores socioeconômicos	Dimensão 2.2 Liderança: cargo/função	Dimensão 3.2 Ferramentas de administração de projetos
Dimensão 1.3 Contexto tecnológico e político	Dimensão 2.3 Coordenação e cooperação	Dimensão 3.3 Mecanismos de gestão financeira
Dimensão 1.4 Considerações ambientais e geográficas	Dimensão 2.4 Participação cívica e colaboração	Dimensão 3.4 Normas regulatórias e padrões

Figura 6. Âmbito da OCDE para a governança do governo digital
Extraído 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. Consultado em 8 de setembro de 2025, em https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-america-latina-y-el-caribe_7a127615-es.html

CIDADANIA DIGITAL

É o conjunto de direitos, de responsabilidades e de práticas que permitem às pessoas participar na vida pública, social, econômica e cultural através de meios digitais.

No contexto do relatório Revisión del Gobierno Digital en América Latina y el Caribe por OCDE/CAF (2024)[5], a cidadania digital está vinculada à capacidade de cada pessoa para:

- **Acessar** às tecnologias e à Internet de forma equitativa e contínua.
- **Usar** serviços públicos digitais (como identidade digital, portais de processos ou dados abertos) para exercer direitos e cumprir obrigações.
- **Participar** em processos democráticos e de tomada de decisões on-line (consultas, orçamentos participativos, plataformas cidadãs).
- **Proteger-se** e agir com responsabilidade em entornos digitais, cuidando da privacidade, da segurança e da liberdade de expressão.
- **Contribuir** para os serviços, para as políticas e para as soluções digitais que respondam às necessidades coletivas.

Resumidamente, ser cidadão digital não é só **ter acesso à Internet**, mas **poder exercer a cidadania plena** no espaço digital com as habilidades, o conhecimento e as condições que garantam inclusão, segurança e participação efetiva.

APRENDA MAIS DE CIDADANIA DIGITAL COM ESTE VÍDEO:

¿Qué es la Ciudadanía Digital?

DIGITALIZAÇÃO

A digitalização se refere ao processo de desenvolver ou converter informação em formato digital, isto é, transformar dados, documentos e processos que antes eram analógicos em formatos digitais acessíveis e manejáveis.

A **digitalização no Estado** implica que as instituições públicas contem com **métodos seguros de identificação (autenticação)**, possam **compartilhar informação entre elas sem barreiras (interoperabilidade)** e gerenciem os **dados de forma ética e 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.

CONCEITOS- CHAVE PARA ENTENDER A DIGITALIZAÇÃO

Autenticação

É o conjunto de mecanismos que permitem verificar a identidade de uma pessoa quando acessa a um serviço digital do Estado. Geralmente, a autenticação é realizada através de três possíveis fatores: **algo que conheço** (por exemplo, uma senha ou PIN), **algo que possuo** (como um token, cartão ou celular) ou **uma característica física** (impressão digital, reconhecimento facial ou outra forma de biometria).

Objetivo: garantir que quem acessa é realmente quem diz ser, protegendo a privacidade do cidadão.

Benefícios: evita fraudes e permite que processos e serviços sejam realizados de forma segura on-line.
Barreiras e desafios:

1. Nem todos os sistemas das distintas entidades estatais utilizam os mesmos padrões, o que dificulta a integração de mecanismos de autenticação unificados.
2. Os fatores de autenticação baseados em algo possuído (celular, token, cartão) necessitam que as pessoas disponham destes meios, o que pode excluir pessoas sem acesso a determinados dispositivos.
3. Pessoas com deficiência visual, motora ou auditiva podem enfrentar dificuldades se as soluções não contemplarem medidas de acessibilidade.
4. Adquirir dispositivos compatíveis ou manter conexão à Internet pode ser uma carga econômica para algumas pessoas.

Interoperabilidade

Significa que **os sistemas e as bases de dados de distintas instituições públicas podem "falar" entre si** e compartilhar informação de forma segura e padronizada. Por exemplo, que o Sistema de Registro Civil, a autoridade tributária e o Ministério de Saúde possam interconectar dados sem que o cidadão tenha que proporcionar várias vezes a mesma informação.

Objetivo: melhorar a **eficiência administrativa**, reduzir duplicações e agilizar os processos.

Benefício: menos burocracia para as pessoas e melhor coordenação entre entidades.

Barreras/retos:

1. Muitos serviços na LAC são desenvolvidos pensando em manter a burocracia e não são otimizados para o usuário. Falta pesquisa para conhecer as necessidades reais.
2. Cada instituição pode usar diferentes formatos, linguagens de programação e de protocolos, o que dificulta a integração.
3. Nem sempre existe um marco legal claro que habilite compartilhar dados entre entidades.
4. Devem ser garantidos processos de anonimização[6] da informação quando esta é compartilhada entre entidades.

Tipos de interoperabilidade

Interoperabilidade técnica: significa que os sistemas de distintas instituições podem conectar-se porque usam ferramentas compatíveis.

- API (interface de programação de aplicações): são os "tradutores" que permitem que um programa fale com outro ainda que estejam feitos de forma distinta.
- Plataformas comuns: são espaços ou sistemas compartilhados onde várias instituições podem trabalhar e usar a mesma informação.

Interoperabilidade semântica: definições, metadados e esquemas de classificação comuns para que os dados tenham o mesmo significado em todos os contextos.

6. A anonimização pode ser entendida como "mascarar os dados", a informação é vista, mas não a identidade. É o processo de tirar ou trocar os dados pessoais (nome, endereço, foto, etc.) para que não seja possível identificar uma pessoa.

Interoperabilidade organizacional: papéis, responsabilidades e fluxos de trabalho alinhados para a troca de dados.

Interoperabilidade legal: marcos normativos harmonizados que permitam compartilhar dados de forma segura e de acordo com a lei.

Datos

Refere-se a como o Estado gera, armazena, gerencia, compartilha e utiliza a informação que coleta no exercício das suas funções.
Inclui:

- **Governança de dados:** normas e papéis para administrá-los.
- **Dados abertos:** informação pública disponível para cidadãos e para empresas.
- **Proteção de dados pessoais:** garantias para manter o direito à privacidade.

Objetivo: usar os dados como recurso estratégico para desenvolver políticas, avaliar serviços e tomar decisões baseadas em evidência.

Benefício: políticas públicas mais efetivas e serviços mais adaptados às necessidades reais.

Barreiras/desafios:

1. Fragmentação institucional: diferentes entidades armazenam dados em sistemas não compatíveis ou isolados.
2. Qualidade e atualização: informação incompleta, duplicada ou desatualizada reduz a confiança e a utilidade dos dados.
3. Capacidades limitadas: falta de formação técnica em servidores públicos para gerenciar e para analisar grandes volumes de dados.
4. Resistência cultural: medo a compartilhar informação entre instituições ou temor a perder controle sobre ela.
5. Brechas tecnológicas: infraestrutura digital insuficiente ou desigual entre regiões.
6. Proteção e confiança cidadã: riscos de mau uso ou filtragem de dados pessoais que geram desconfiança nos serviços digitais do Estado.
7. desigual entre regiones.
8. Protección y confianza ciudadana: riesgos de mal uso o filtración de datos personales que generan desconfianza en los servicios digitales del Estado.

OS NOSSOS DIREITOS

Nos últimos anos, muitos processos e serviços públicos como solicitar um documento de identidade, inscrever-se a programas sociais ou pagar impostos passaram de ser presenciais a ser on-line. Isto melhorou a eficiência e facilitou o acesso para milhões de pessoas, mas também trouxe novos desafios.

Pense em uma pessoa que tenta registrar-se em um serviço público digital, mas o sistema não reconhece o seu documento por um erro na base de dados. Ou em um algoritmo que aprova ou rejeita solicitações de forma automática, sem que a pessoa saiba como foi tomada essa decisão.

Quando digitalizamos serviços cidadãos, devemos garantir que sejam respeitados direitos fundamentais como:

- **Privacidade:** proteger os dados pessoais e evitar usos indevidos.

Exemplo: quando um sistema de saúde on-line armazena o prontuário de um paciente, deve garantir que só médicos autorizados possam acessar e que não seja utilizado para discriminá-lo em outras circunstâncias como ao momento de adquirir um seguro ou obter um emprego.

- **Acesso à informação:** garantir transparência e prestação de contas.

Exemplo: uma pessoa física deveria poder consultar em um portal oficial quanta verba foi atribuída a um programa social e em que será gasto, sem barreiras técnicas nem burocráticas.

- **Não discriminação:** prevenir preconceitos em sistemas e algoritmos.

Exemplo: se um algoritmo que atribui bolsas de estudo universitárias dá prioridade a certos perfis por tendenciosidade nos dados (como gênero ou lugar de residência), estaria reproduzindo desigualdades, em lugar de reduzi-las.

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

Exemplo: se uma pessoa é rejeitada automaticamente na inscrição a um subsídio, deve ter a possibilidade de apelar, entender a razão da exclusão e que um funcionário revise o seu caso se for necessário.

A digitalização não é apenas uma mudança tecnológica, é uma mudança social e política. Como jovens, cidadãos e futuros profissionais temos um papel ativo em exigir e em construir um ecossistema digital que seja seguro, inclusivo e respeitoso com os direitos de todas as pessoas.

MATERIAL PARA APROFUNDAR:

- Estándares de derechos humanos para el uso estatal de la IA en América Latina.

UNIDADE 3: IDENTIDADE DIGITAL E GOVERNANÇA DA INTERNET: DO LOCAL AO REGIONAL

IDENTIDADE DIGITAL OU DIGITAL ID

Os sistemas de identidade são construções institucionalizadas que coletam características individuais predeterminadas por uma autoridade para um fim concreto (você pode explorar mais sobre este tema no nosso microsite ID Colombia).

As tecnologias digitais ofereceram novas formas de construir essas identidades e novas possibilidades de conectar múltiplas bases de dados a um indivíduo único. Embora estes perfis poderiam ser utilizados para garantir os direitos humanos, estas ferramentas poderiam também ser utilizadas para discriminar sistematicamente e exercer violência.

A criação de um sistema de identidade digital deve estar guiada por princípios democráticos que permitam a inclusão social e a construção da confiança coletiva. Por isto, estes sistemas devem ser inclusivos, evitar a discriminação, proteger a privacidade, ser autossustentáveis e estar desenvolvidos com legalidade.

O QUE É A IDENTIDADE LEGAL??

A identidade se refere a uma combinação das características que tornam uma pessoa única em um contexto determinado. Especificamente, a identidade legal é o reconhecimento legal de uma pessoa como sujeito de direitos e de deveres por parte de um Estado.

A identidade legal é reconhecida como um direito humano pelo artigo 6 da Declaração Universal dos Direitos Humanos. Igualmente, as Nações Unidas incluíram nos Objetivos de Desenvolvimento Sustentável a meta 16:9 a qual visa “daqui a 2030, proporcionar acesso a uma identidade jurídica para todos, em particular mediante certidões de nascimentos”.

Os sistemas de identidade tratam de coletar e validar os atributos que tornam única a uma pessoa seguindo os seus principais eventos vitais (nascimento, adoção, matrimônio, morte, etc.). Em outras palavras, os **sistemas de identidade** são os que tornam **operável a identidade legal** de uma pessoa.

Os sistemas de identidade têm três papéis principais:

- **IDENTIFICAÇÃO** – QUEM É VOCÊ?: Processo pelo qual uma autoridade estabelece a identidade de uma pessoa coletando e validando a informação relevante dela. Por exemplo, a identificação na Colômbia ocorre com a coleta de informação para produzir a tarjeta de identidade ou a cédula. Os dados que são coletados são, entre outros, fotografia, características físicas e assinatura.
-
- **AUTENTICAÇÃO** – VOCÊ É QUEM DIZ SER?: Processo mediante o qual é comprovado que uma pessoa que reclama uma identidade é a mesma inscrita no sistema com a informação coletada no processo de identificação. Por exemplo, os cartórios na Colômbia fazem autenticação com a impressão digital, o método para validar a identidade de uma pessoa que assina uma escritura para vender uma casa que está no seu nome. No Chile o Estado oferece a Clave Única, uma senha pessoal que permite reconhecer aos cidadãos para acessar a serviços públicos digitais como saúde, educação e processos legais. No Brasil, o sistema de Cadastro de Pessoas Físicas (CPF) é complementado com a autenticação biométrica (impressão digital e reconhecimento facial) para acessar a serviços bancários, votar de maneira eletrônica e validar processos oficiais.
-
- **AUTORIZAÇÃO** – VOCÊ É ELEGÍVEL PARA ESTE SERVIÇO?: Processo pelo qual é determinado se uma pessoa pode acessar a um serviço e quais autorizações têm dentro deste. Por exemplo, quando para a entrega de subsídios a entidade que os administra comprova que a pessoa está inscrita e aparece como beneficiária dos programas sociais.

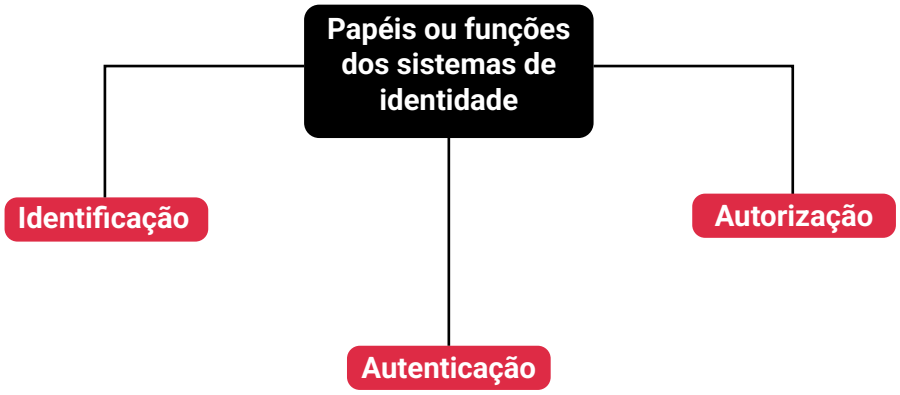


Figura 7. Papeles o funciones de los sistemas de identidad
Extraído de Fundación Karisma. (7 de dezembro de 2021). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Consultado em 8 de setembro de 2025, em https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id

O CICLO DE VIDA DA IDENTIDADE

Em cada país existem instituições encarregadas de identificar e reconhecer às pessoas. Por exemplo, na Colômbia isto é tarefa da Registraduría Nacional del Estado Civil. Estas instituições registram a pessoa e fornecem-lhe documentos ou credenciais que depois servem para acessar a distintos serviços do Estado. Este processo é conhecido como ciclo de vida da identidade e tem várias etapas:

1. Registro da identidade
A pessoa entrega os seus dados básicos (nome, data de nascimento, impressão digital, etc.) para a autoridade que maneja o sistema de identidade.
Estes dados são revisados e validados com outras bases, como a certidão de nascimento, passaportes ou antecedentes.

2. Entrega de credenciais
Depois do registro, são fornecidos elementos que servem para provar a identidade: por exemplo, um documento de identidade, um celular com aplicação, uma senha ou inclusive dados biométricos (impressão digital, íris, rosto).

3. Uso de credenciais
Cada vez que a pessoa precisa de um serviço (como um serviço de saúde, educação ou apoio social), apresenta uma destas credenciais para demostrar que realmente é ela.

4. Administração do sistema
A instituição mantém atualizada a base de dados, guarda a informação, renova os documentos quando é necessário e garante que tudo funcione de maneira segura.
- Também garante que haja interoperabilidade, isto é, que diferentes instituições (saúde, educação, impostos, etc.) possam usar a mesma informação sem pedi-la várias vezes.

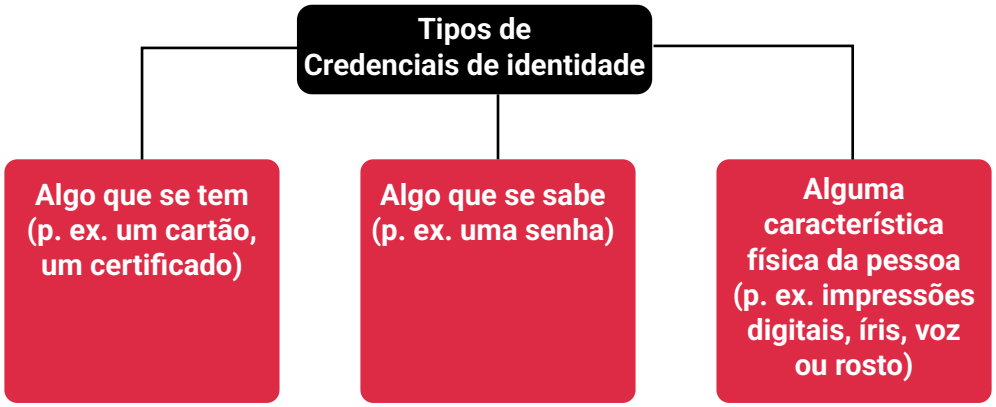


Figura 8. Tipos de credenciais de identidade
Observação. Extraído de Fundación Karisma. (7 de dezembro de 2021). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Consultado em 8 de setembro de 2025, em https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id

O RECONHECIMENTO BIOMÉTRICO

A identificação biométrica funciona a partir da coleta e da abstração de medidas ou de características corporais. Esta informação é armazenada em bases de dados que logo são integradas em sistemas que comparam os registros guardados com os registrados pelos sensores, por exemplo, leitores de impressões digitais ou câmeras. Os resultados destas comparações sempre são expressados em termos de probabilidade.

Na atualidade, existem sete elementos impulsionados pela indústria tecnológica: as impressões digitais, o rosto, a íris, a voz, o comportamento, o DNA e os padrões vasculares. O aumento de sensores em espaços tanto públicos como privados e as novas capacidades destes dispositivos para coletar, processar e reconhecer pessoas impõe riscos para os direitos fundamentais como a intimidade, a igualdade e não discriminação, a dignidade, a liberdade de movimento e a livre associação.

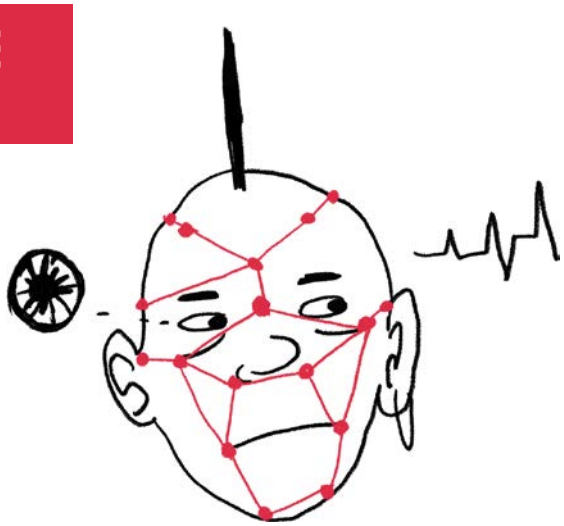
A biometria é uma forma de identificar a uma pessoa usando características físicas ou de comportamento que são únicas como a impressão digital, o rosto, a íris ou inclusive a voz. Esta informação pode ser armazenada em bases de dados que logo são integradas em sistemas que comparam os registros guardados com a informação fornecida no momento.

Na vida cotidiana vemos isso quando:

- Desbloqueamos um celular com a impressão digital ou o rosto.
- Passamos pelo controle migratório em aeroportos com reconhecimento facial.
- Cobramos um subsídio ou aposentadoria usando impressão digital em caixas ou entidades públicas.

COMO A IDENTIFICAÇÃO MEDIANTE BIOMETRIA PODE AFETAR OS NOSSOS DIREITOS?

- **Intimidade:** uma câmera na rua que o reconhece sem a sua autorização.
- **Igualdade e não discriminação:** um sistema de reconhecimento facial que não identifica as pessoas com pele mais escura ou as mulheres.
- **Dignidade:** ter que entregar a sua impressão digital ou foto para processos simples, sem alternativa.
- **Liberdade de movimento:** ser vigilada constantemente em espaços públicos com câmeras inteligentes.
- **Livre associação:** câmeras que identificam quem está em um protesto.



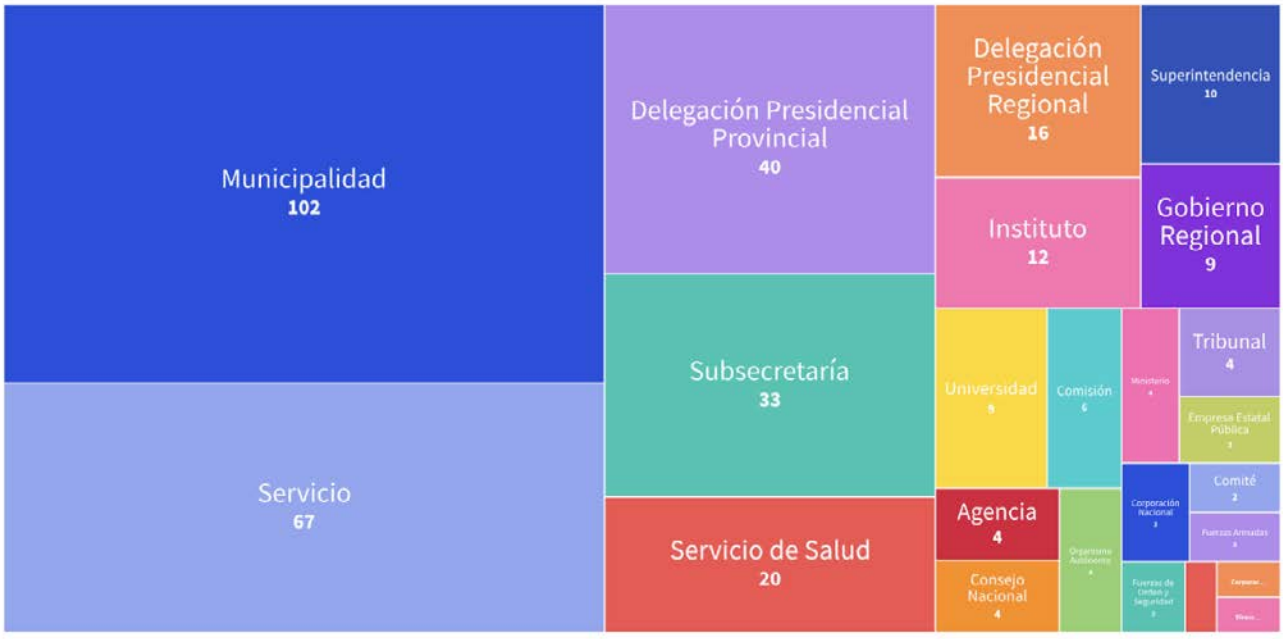
EXEMPLOS DE SISTEMAS DE IDENTIDADE NA REGIÃO

CLAVE ÚNICA NO CHILE

A Clave Única é a identidade digital que permite acessar aos serviços e aos benefícios do Estado do Chile por meio da Internet. Funciona como uma senha única que valida de forma segura a identidade de uma pessoa, facilitando o seu ingresso a todas as plataformas e processos virtuais do Estado para chilenos e residentes maiores de 14 anos.

“Esta ferramenta de autenticação digital se converteu na protagonista da transformação digital do Estado chileno. A pandemia acelerou todos os processos de digitalização e em 2024, 9 de cada 10 chilenos já tinham a sua Clave Única ativa”. (Esteban & Esteban, 2024).

Instituições que utilizam Clave Única
Serviços cidadãos que habilitaram a Clave Única nas suas plataformas digitais até junho de 2024.



Fonte: Análise e processamento de dados de Unholster com base na informação da Secretaria de Governo Digital, entre os anos 2018 a junho de 2024.

Figura 9. Ativações mensais de Clave Única no Chile (2018–2024).
Observação: Elaborado por Unholster com base na informação da Secretaria de Governo Digital (s. f.), em CNN Chile Data by Unholster. Consultado em 8 de setembro de 2025, em https://data.cnnchile.com/transformacion-digital/clave-unica/

Quais benefícios tem a Clave Única?

A Chave Única permite acessar a uma variedade de serviços públicos on-line, tais como:

- **Solicitar certificados do Registro Civil,** tais como nascimento, casamento, óbitos, antecedentes, etc.
- **Postular a benefícios sociais,** tais como o Ingresso Familiar de Emergência, o Bônus Covid, o Subsídio ao Emprego, etc.
- **Realizar procedimentos tributários,** tais como declarar renda, solicitar restituição de impostos, emitir notas fiscais, etc.
- **Consultar o seu prontuário,** os seus atestados médicos, as suas contribuições previdenciárias, os seus bônus de saúde, etc.
- **Acessar à sua informação acadêmica,** tais como as suas notas, as suas bolsas de estudo, os seus créditos, os seus cursos, etc.
- **Participar em processos eleitorais,** tais como mudar o seu domicílio, votar em plebiscitos, etc.

Um projeto para dar uma olhada:

Convidamos você para consultar o trabalho da Organização da Sociedade Civil Derechos Digitales. Trabalham “pela defesa dos direitos humanos no entorno digital, combinando pesquisa, análise de políticas públicas e tecnologia, assim como a divulgação e a capacitação em direitos e segurança digital”.

PERGUNTA: Quais são as vantagens e desvantagens que você poderia identificar neste sistema de identidade?

ID DIGITAL NO BRASIL

A plataforma GOV.BR reúne em um único lugar os serviços de identificação que demonstra em meios digitais que “você é você”. Nela, os cidadãos podem identificar-se de forma segura para acessar aos serviços digitais. É gratuita e está disponível para todos os cidadãos brasileiros.

Por outro lado, existe a Carteira de Identidade Nacional (CIN), é o novo documento de identificação que utiliza o CPF[7] como número único e tem um padrão nacional. A CIN aumenta a segurança da identificação dos brasileiros, melhora os registros administrativos e contribuem para reduzir a fraude no Brasil. A CIN também tem uma versão digital.

O objetivo da Carteira de Identidade Nacional (CIN) é fortalecer e modernizar o sistema de identificação do país para que a prestação de serviços públicos e privados melhore continuamente. Também visa reduzir as fraudes milionárias, mitigar os problemas sociais e os delitos como a falsa identidade, a falsificação de documentos e a estafa. O seu objetivo é estabelecer a confiança e garantir a integridade dos dados de identificação.

7. Cadastro de Pessoa Física ou Registro de Contribuinte. É o número que identifica a pessoa diante da Receita Federal (ou Ministério de Fazenda).

A CIN integra os dados de identificação dos cidadãos de forma segura e estabelece um fluxo nacional em tempo real para todas as entidades de identificação.

Entretanto, a identificação civil apresenta múltiplos desafios devido à fragmentação e insegurança dos sistemas de identificação, as diversas normas legais e a falta de um padrão nacional para a verificação da identidade das pessoas. Neste sentido, a CIN visa transformar a identificação dos cidadãos, com a integração segura de dados e um fluxo em tempo real, o que permitirá que diferentes áreas do governo ajam de maneira integrada para satisfazer as necessidades dos cidadãos.

A proposta da Carteira de Identidade Nacional (CIN) também deve ser analisada criticamente. Embora visa integrar dados e oferecer um fluxo em tempo real que facilite a coordenação estatal, a sua implementação deve garantir:

- **Não discriminação:** que nenhum grupo (povos indígenas, comunidades rurais, pessoas sem acesso à tecnologia) fique excluído do sistema.
- **Proteção da privacidade:** que a centralização de dados não derive em vigilância massiva ou uso indevido da informação pessoal.
- **Transparência e participação:** que a cidadania conheça como são usados os seus dados e possa exigir prestação de contas.
- **Segurança digital:** que existam salvaguardas efetivas contra filtragens, abusos ou manipulações.

Figura 10. Publicidade da identificação digital no Brasil
Observação. Extraído de “Identificação do Cidadão e Carteira de Identidade Nacional”, por Governo Digital de Brasil (s. f.). Consultado em 8 de setembro de 2025, em https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional

Figura 11. Diferentes formatos e tipos de identificação no Brasil
Observação. Extraído de "Identificação do Cidadão e Carteira de Identidade Nacional", por Governo Digital de Brasil (s. f.). Consultado em 8 de setembro de 2025, em https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional

Um projeto para dar uma olhada:

data_labe é um "laboratório de dados e narrativas na favela Maré, do Rio de Janeiro. A equipe está formada por jovens resid

RENAPER NA ARGENTINA

É uma versão virtual do DNI que é usado através da aplicação Mi Argentina. Tem as mesmas funções que o DNI cartão, exceto para votar e para viajar para fora do país.

Figura 12. Tela de Início do portal Mi Argentina
Observação. Extraído de Mi Argentina [Captura de tela], por Argentina. Presidencia de la Nación (s. f.). Consultado em 8 de setembro de 2025, em https://www.argentina.gob.ar/miargentina/

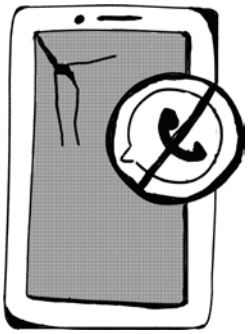
Um projeto para dar uma olhada:

Reconoceme é uma campanha na Argentina que visa gerar consciência sobre os sistemas de reconhecimento facial (SRF), os seus riscos e as suas implicações para os direitos civis e a privacidade. A iniciativa defende o direito das pessoas a não ser identificadas sem garantias nem controles adequados, promovendo um debate público sobre o seu impacto na democracia e sobre as liberdades individuais.

DESAFIOS E RISCOS PRINCIPAIS DOS SISTEMAS DE IDENTIFICAÇÃO NA REGIÃO:

A identificação digital pode trazer benefícios, mas também apresenta riscos que devem ser analisados com cuidado: exclusão, vigilância, brechas de acesso e segurança.

Um ponto crítico é a proteção de dados pessoais, que em projetos governamentais costuma ser limitada. Existem dois problemas centrais:



1. **Falta de limites claros:** nem sempre é definida com precisão como, para que e até onde podem as entidades públicas coletar e usar a informação pessoal.

1. **Escassos mecanismos de defesa:** as pessoas não contam com processos acessíveis e eficazes para apelar ou reclamar se sentem que a sua informação foi mal utilizada.

IDENTIDADE DIGITAL E GOVERNANÇA DA INTERNET

Desde uma perspectiva de direitos e desenvolvimento inclusivo, a identidade digital é muito mais que uma credencial tecnológica: é uma porta de acesso às oportunidades, aos serviços e à participação cidadã. A sua relação com a governança da Internet se reflete em três âmbitos essenciais:

Segurança e confiança

A identidade digital deve garantir que cada indivíduo possa autenticar-se on-line de forma segura, protegendo a sua informação e evitando a fraude ou a falsificação de identidade.

Na governança da Internet, isto significa estabelecer marcos claros de proteção de dados, auditorias transparentes e mecanismos de prestação de contas que fortaleçam a confiança da cidadania.

Inclusão digital – consultas prévias

A identidade digital tem que ser acessível para todas as pessoas, sem importar a sua localização geográfica, nível socioeconômico ou condição física.

A governança da Internet responsável inclui promover conectividade acessível, alfabetização digital e desenho inclusivo de plataformas.

Além disso, as consultas prévias com povos indígenas e com comunidades locais são fundamentais para que as soluções respeitem a diversidade cultural, as línguas e as visões próprias sobre privacidade e uso de dados.

DIREITOS HUMANOS

A identidade digital deve proteger e promover direitos, não os restringir. Isto implica:

- Defender o direito à privacidade diante de usos abusivos ou vigilância massiva.
- Garantir a não discriminação no acesso e uso de serviços digitais.
- Garantir o direito à participação, permitindo que mais pessoas possam exercer cidadania plena através de canais digitais seguros e transparentes.

ESPAÇOS DE PARTICIPAÇÃO REGIONAL: LACIGF AND YOUTH LACIGF

Conhecer espaços de governança da Internet, os temas que tratam e a sua importância –já vistos no módulo anterior– permite analisar possíveis oportunidades de incidência e de participação em vista da digitalização dos serviços do Estado. Este não é um processo puramente técnico: envolve decisões políticas sobre como são desenvolvidos, regulamentados e garantidos os direitos em entornos digitais.

Precisamente, neste ponto, a cidadania tem um papel fundamental, pois pode indicar as brechas e riscos que as políticas públicas costumam ignorar: desde a falta de conectividade em zonas rurais e a exclusão de populações com menor alfabetização digital, até os riscos de vigilância, a ausência de políticas de acessibilidade ou o uso de tecnologias que não respondem às necessidades locais. Os espaços de governança da Internet como o LACIGF e o Youth LACIGF oferecem mecanismos concretos de participação, onde essas preocupações podem ser convertidas em contribuições que influenciam na agenda regional.

Neste ponto nos centraremos em dois eventos de governança da Internet abordados superficialmente no módulo anterior. Tanto o LACIGF como o Youth LACIGF têm lugar na nossa região e se consolidaram como espaços valiosos para tornar visíveis problemáticas locais. Veremos os temas mais comuns nestes espaços e um guia breve para aplicar ao LACIGF. Você pode propor um espaço para dialogar sobre os problemas da digitalização de serviços fundamentais na nossa região!

Figura 13. Logotipo do LACIGF.

O Fórum de Governança da Internet da América Latina e do Caribe (LACIGF) se converteu ao longo das suas edições em um espaço de encontro regional para o diálogo político multisetorial no qual atores de governos, setor privado, comunidade técnica, setor acadêmico e organizações da sociedade civil apresentam e discutem as sus perspectivas.

Nos últimos anos a região avançou na compreensão dos desafios atuais da governança da Internet formando um espaço próprio para o debate e a identificação das prioridades regionais, ao mesmo tempo que foi ampliada significativamente a participação e a contribuição da região nos debates do Forum de Governança da Internet.

Figura 14. Logotipo do Youth LACIGF

Do LACIGF nasce o Fórum de Governança da Internet para as juventudes da América Latina e do Caribe (Youth LACIGF), onde jovens da região se articulam para discutir temas relacionados com a governança da Internet.

Este encontro multisetorial foi criado no ano 2016 na cidade de San José, Costa Rica; desde então foi sediado em diferentes cidades da LAC. Foi chave para a participação das juventudes interessadas na governança da Internet em relação com a diversidade, a troca de experiências, a perspectiva de baixo para cima, a criação de redes regionais e a garantia de espaços seguros e livres de violências.

O Youth LACIGF tem abordado temas como o acesso à conectividade e infraestrutura digital, privacidade, cibersegurança, economia digital, direitos humanos e vigilância. Todos estes temas incidem diretamente em como são desenvolvidos, implementados e percebidos os serviços digitais do Estado.

Também, tem respondido a iniciativas globais como o Pacto Digital Global e desafios que deixou a pandemia em torno do uso da tecnologia: marcos regulatórios que respeitem a privacidade e a autonomia das pessoas usuárias, brechas de acesso e conectividade, exposição de dados pessoais, entre outros, que afetam a governança e a inclusão digital.

FORMAS DE CONTRIBUIÇÃO CIDADÃ

1. **Intervenções em plenárias e oficinas.**
A cidadania pode tomar a palavra para indicar problemas locais (ex. preocupações diante da digitalização de serviços do Estado, falta de conectividade em comunidades rurais, riscos de vigilância, necessidade de políticas de acessibilidade).

2. **Propostas escritas ou consultas prévias.**
O LACIGF e o Youth LACIGF costumam abrir períodos de consulta on-line onde qualquer pessoa ou organização pode enviar contribuições que logo se integram à agenda de discussão.

3. **Participação em grupos de trabalho.**
Os fóruns geram mesas temáticas (como dados pessoais, serviços públicos digitais, inclusão de gênero, IA) onde a cidadania pode contribuir com insumos ou somar-se como voluntária.

4. **Depoimentos e experiências.**
Pessoas ou organizações compartilham casos de uso.

5. **Construção coletiva de recomendações**
Ao final de muitos fóruns, são elaboradas sínteses ou declarações que recolhem as vozes cidadãs e são enviadas para instâncias globais (como o IGF da ONU).

Passos para elaborar uma contribuição cidadã:

As contribuições cidadãs ajudam a incluir perspectivas locais e diversas nas discussões regionais.

Primeiro passo: revisa os temas propostos na convocatória anual (p. ex.: conectividade, direitos digitais, cibersegurança, governança de dados ou inclusão digital).

1. Escolha um que seja relevante para a sua comunidade ou experiência.
2. Inclua dados, casos e evidências que mostrem por qual razão a sua contribuição é importante.

Você pode usar:

- Estatísticas oficiais e estudos (CEPAL, ONU, relatórios de ONGs).
- Experiências e depoimentos locais.
- Normas ou marcos legais relevantes.

Pergunte-se:

- Qual problema ou necessidade quero tornar visível?
- Qual proposta ou solução sugiro?
- Como se relaciona com a governança da Internet e com os direitos humanos (privacidade, acesso, não discriminação, liberdade de expressão)?

Formato.

Título: breve e descritivo.

Contexto: explicar a situação atual e por qual razão que é relevante.

Problema ou desafio: detalhar as barreiras, riscos ou vulnerações a direitos humanos, civis ou políticos.

Proposta ou recomendação: ações concretas que o LACIGF e outros atores poderiam considerar.

Impacto esperado: como a sua proposta melhoraria a situação.

Dados ou exemplos: evidências que apoiam a sua contribuição.

Se for possível, compartilhe-a com redes comunitárias, coletivos juvenis ou pessoas especialistas no tema para receber retroalimentação.

Segundo passo: verifica que cumpra com o formato e com o prazo do LACIGF ou do Youth LACIGF.

- Revise na convocação:
  - Limite de palavras ou páginas.
  - Idiomas aceitos.
  - Formato de envio (correio, formulário web).
- Envie a sua contribuição antes da data limite.

FECHAMENTO DO MÓDULO: GOVERNANÇA E PARTICIPAÇÃO

Compreender a digitalização não se trata apenas de aprender a usar tecnologias, mas de entender como estas impactam as nossas vidas, os nossos direitos e as nossas comunidades.

ATIVIDADE

1. **Reflexão, perguntas e ferramentas para construir um olhar crítico diante da digitalização desde a soberania cidadã.**
   - Quais barreiras enfrenta a minha comunidade para participar nestes processos?
   - Qual papel eu gostaria de assumir diante desta transformação digital?
   - Como me afeta (ou não) a digitalização de serviços cidadãos na minha vida diária?

2. **Redija o seu próprio manifesto**
   - Quais princípios deveriam guiar a digitalização do Estado?
   - Quais demandas você considera urgentes desde o seu papel como cidadão digital?

RECURSOS ADICIONAIS

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 e Thorsten Thiel

Digitalización de Trámites y Servicios | Ministério TIC Colômbia

Política de Gobierno Digital | Ministério TIC Colômbia

Decreto 088 de 2022 | Função Pública

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

REFERÊNCIAS

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. Consultado em 8 de setembro de 2025, em https://biblioguias.cepal.org/gobierno-digital/defniciones

Portal Gov.br. (s. f.). Checklist [Guia de edição de serviços]. Governo do Brasil. Consultado em 8 de setembro de 2025, em 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/transformacion-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). Consultado em 8 de setembro de 2025, em https://www.redgealc.org/site/assets/files/17944/brasil_-_taller_rg.pdf

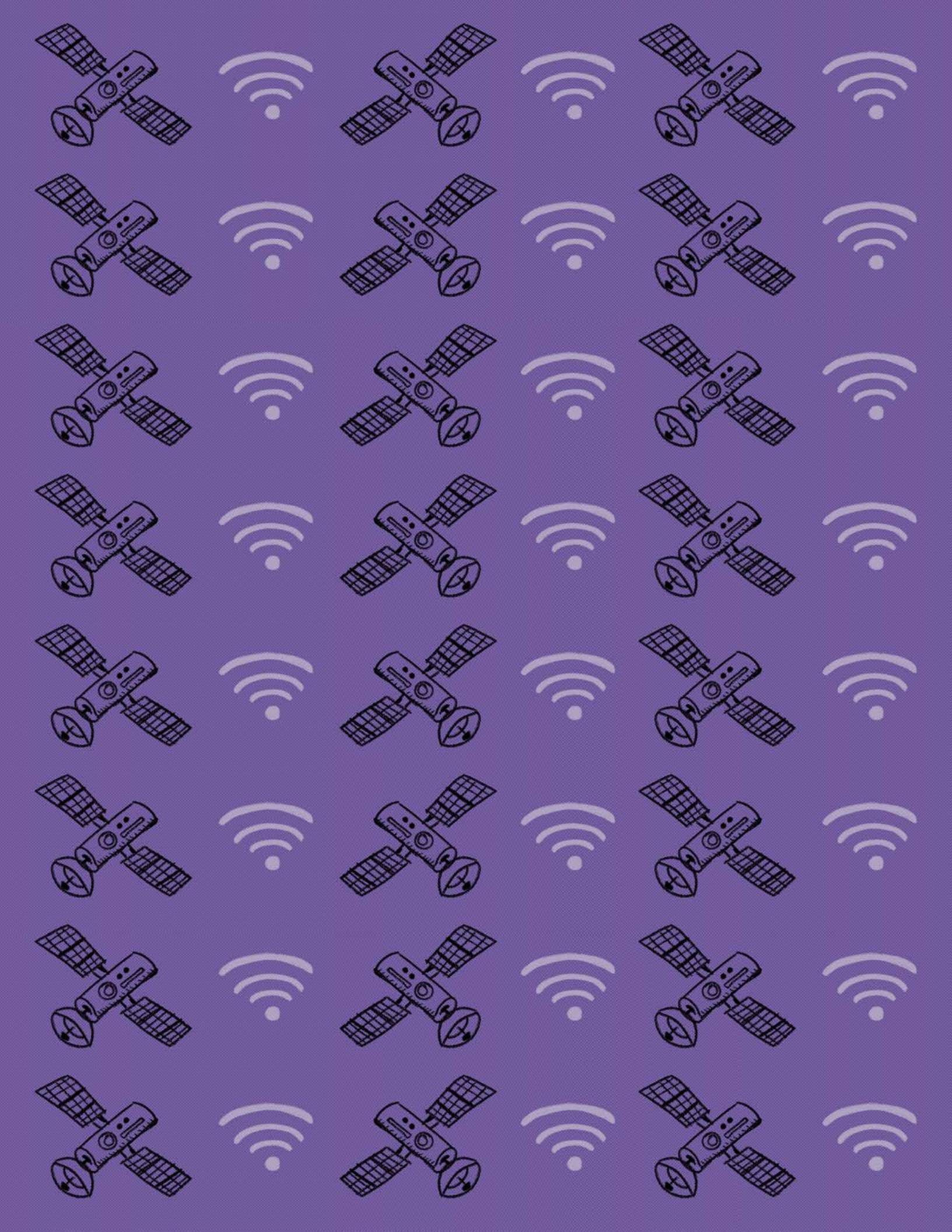
Comisión de Regulación de Comunicaciones (CRC). (2024, 13 de dezembro). La CRC presenta el análisis sobre infraestructura y cobertura móvil en Colombia. CRC. Consultado em 8 de setembro de 2025, na página CRC. https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-analisis-sobre-infraestructura-y-cobertura-movil-en

Fundación Karisma. (2021, 7 de dezembro). Conceptos básicos de los sistemas de identidad [Entrada de blog]. Proyecto ID Colombia. Consultado em 8 de setembro de 2025, em https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id

Argentina. Presidencia de la Nación. (s. f.). Mi Argentina [Sitio web]. Consultado em 8 de setembro de 2025, em 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]. Consultado em 8 de setembro de 2025, em https://youthlacigf.lat/

Internet Governance Forum. (s. f.). Internet Governance Forum [Sitio web]. Consultado em 8 de setembro de 2025, em https://intgovforum.org/es/



Fundación
Karisma

karisma.org.co