Internet Infrastructure Initiative

Triple I: a GFCE Capacity-building project

@LACIGF, Bogota, Colombia, 3 December 2023

Digital Dependencies and Cyber Vulnerabilities – Global Risk Report 2022

- *435% increase in ransomware in 2020*
- *3 million gap in cyber professionals needed worldwide*
- *US$800 billion estimated growth in value of digital commerce by 2024*
- *95% cybersecurity issues traced to human error*
- *"Cybersecurity failure" is one of the risks that worsened the most through COVID-19*

Digital Dependencies and Cyber Vulnerabilities – Global Risk Report 2022

- *435% increase in ransomware in 2020*
- *3 million gap in cyber professionals needed worldwide*
- *US$800 billion estimated growth in value of digital commerce by 2024*
- *95% cybersecurity issues traced to human error*
- *"Cybersecurity failure" is one of the risks that worsened the most through COVID-19*

Cybercrime and cyber-insecurity continues to be a key threat for decade to come – WEF 2023

WORLD ECONOMIC FORUM

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Standards matter

Website

E-mail

IPv6. Enables more users and devices to connect to the Internet

RPKI. Prevents route hijacking and other routing attacks through use of a trust anchor

DNSSEC. Prevents the redirection of users to malicious sites or mailservers

TLS (HTTPS & DANE). Protects the privacy and integrity of data transmitted through web browsing

TLS (STARTTLS & DANE). Protects the privacy and integrity of data transmitted through e-mailing

SPF, DKIM and DMARC. Prevents domain misuse and combats spam and phising

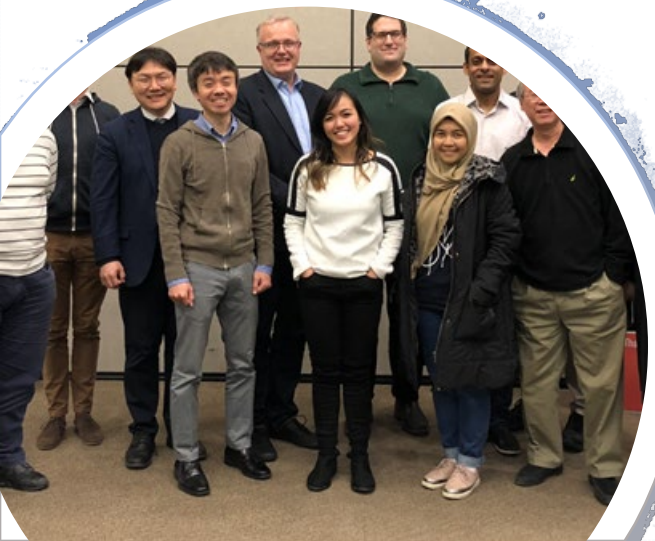
Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

Aim of the Capacity building events

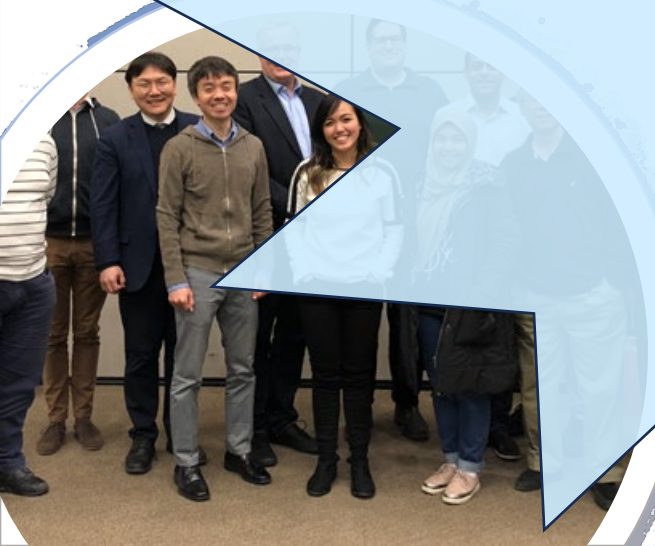
- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Tools
- Inspiration through Good Practice Examples (mix local/global)
- Impact through joint commitment for action


"What to do to improve justified trust in using the Internet and email in the region"
Purpose of the Day



9 events so far

1. Dakar, Senegal, hosted by the African Internet Summit, supported by AfricaCERT/AfriNIC/ISOC 2019, 7 May 2018
2. Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE NCC/ISOC/Kazachstan Telecom, 25 September 2018
3. Delhi, India, hosted by Ministry for Electronics and IT (MEITY) and INSIG, supported by ISOC/APNIC, 12 October 2018
4. Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019
5. Kampala, Uganda, hosted by the African Internet Summit, supported by AfricaCERT, AfriNIC, WACREN, ISOC, ICANN, 27 June 2019
6. La Paz, Bolivia, hosted by LACIGF, supported by LACTLD, LACNIC, ISOC, ICANN, CGI.br, 5 August 2019
7. Kolkata, India, hosted by INSIG, supported by APNIC, ICANN, ISOC, 25 November 2019
8. Guwahati, India, hosted by INSIG, supported by APNIC, ICANN, ISOC, 28 September 2023
9. Accra, Ghana, hosted by GC3B, supported by ICANN, ISOC, 28 November 2023



GFCE Triple-I workshop

10

Bogota, Bolivia, 3 December 2023

9 events so far

1. Dakar, Senegal, hosted by the African Internet Summit, supported by AfricaCERT/AfriNIC/ISOC 2019, 7 May 2018
2. Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE NCC/ISOC/Kazachstan Telecom, 25 September 2018
3. Delhi, India, hosted by Ministry for Electronics and IT (MEITY) and INSIG, supported by ISOC/APNIC, 12 October 2018
4. Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019
5. Kampala, Uganda, hosted by the African Internet Summit, supported by AfricaCERT, AfriNIC, WACREN, ISOC, ICANN, 27 June 2019
6. La Paz, Bolivia, hosted by LACIGF, supported by LACTLD, LACNIC, ISOC, ICANN, CGI.br, 5 August 2019
7. Kolkata, India, hosted by INSIG, supported by APNIC, ICANN, ISOC, 25 November 2019
8. Guwahati, India, hosted by INSIG, supported by APNIC, ICANN, ISOC, 28 September 2023
9. Accra, Ghana, hosted by GC3B, supported by ICANN, ISOC, 28 November 2023
10. Bogota, Colombia, hosted by LACIGF, supported by ICANN, LACNIC, ISOC, 3 December 2023

Follow-up from La Paz, Bolivia, LACIGF2019

Take-aways La Paz 2019

- set up more GFCE Triple-I type workshops in the region
- plan for better ways to inform users about the risks related to devices, and how to better deal with this
- analyze the real situation as to inform action where useful or necessary
- create the necessary awareness campaigns
- include security thinking from the outset in education curricula

GFCE Triple-I agenda, Bogota 2023

09:00 Opening

09:15 Block I: Better Use of Today's Open Internet Standards

10:30 Break

11:00 Block II Inspiration form Good Practice Actions

12:30 Buffet lunch

13:30 Block III: Action Planning for a More Trusted Internet

14:45 Conclusions and Closing Remarks

Triple I is a GFCE project

www.thegfce.com

For more information about this workshop contact:

Maarten Botterman: maarten@gnksconsult.com

Backup

Stimulating adoption of standards through measuring uptake

- **Dutch Internet Standards Platform** is the organization behind the test tool Internet.nl.
- Collaboration between parties from the Internet community and the Dutch government (public / private).
- The aim of the platform is to jointly increase the use of modern Internet standards to make the Internet more accessible, safer and more reliable for everyone. → stimulate adoption.

SIDN
RIPE NCC RIPE NETWORK COORDINATION CENTRE
Ministry of Economic Affairs and Climate Policy
nlnet FOUNDATION
Dutch Cloud Community
Internet Society
SURF NET
ECP
VVR VERENIGING VAN REGISTRARS
National Cyber Security Centre Ministry of Justice and Security
Dutch Standardisation Forum
NLNETLABS

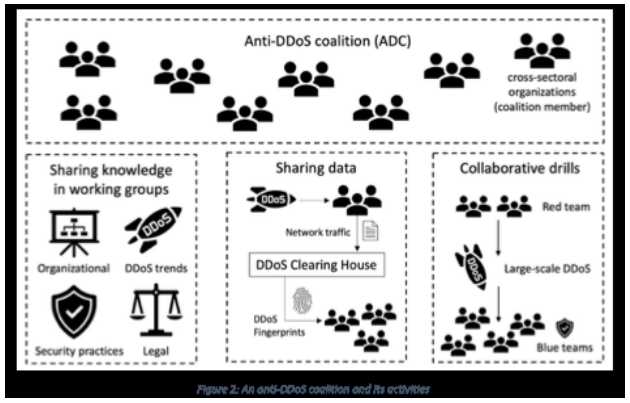
DDOS mitigation through multistakeholder collaboration

DDoS Clearinghouse Cookbook

https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf),

Anti-DDOS Coalition

Mission: investigate the phenomenon of DDoS from a social and economic point of view and to provide knowledge to reduce or stop the attacks.



IoT risk mitigation

IoT Global Good Practice

Zero-trust approach as global and context determined

Data protection is key

Embracing modern Internet standards

Certification and labeling to empower users

Governments lead through procurement

https://www.intgovforum.org/en/content/dynamic-coalition-on-the-internet-of-things-dc-iot

Societal challenges

Healthcare; Independent living; Secure society; Sustainable society

Economic challenges

Innovation; growth; profit

Environmental challenges

Scarce resources; waste reduction; environmental monitoring

Governance

Global standards, open standards, multistakeholder involvement, ethical IoT

Privacy and data collection

Big data issues, cloud issues (location, jurisdiction, accountability), digital literacy

Security

Access,Autonomous systems, cyber attacks on new end points

Source: GNKS 2014

Universal Acceptance and Internationalized Names

Vision:

All valid domain names and email addresses work in all software applications.

Mission UASG:

mobilize the software application developers to get their products UA ready by providing encouragement, documentation, case studies, tools and measures to deliver the right user experience to the end user

Work to do: map and address gaps in technology based on UA-readiness testing of programming languages, email tools, identity platforms, web hosting tools, websites, and more.

New short top-level ASCII domain names:
example.sky

New long top-level ASCII domain names:
example.engineering

Internationalized Domain Names (IDNs):
ļ ő.ŸŏŚ

Universal Acceptance

Click here for UASG and Workplan FY2024

EASYDMARC

DMARC

Prevent phishing before it reaches the inbox

Presented by

Gerasim Hovhannisyan

CEO & Co-Founder EasyDMARC

gerasim@easydmarc.com

Got questions?
Let's connect

EASYDMARC

Phishing Is The Most Common Form Of Cybercrime Worldwide

Two big changes in 2023 you can't ignore:

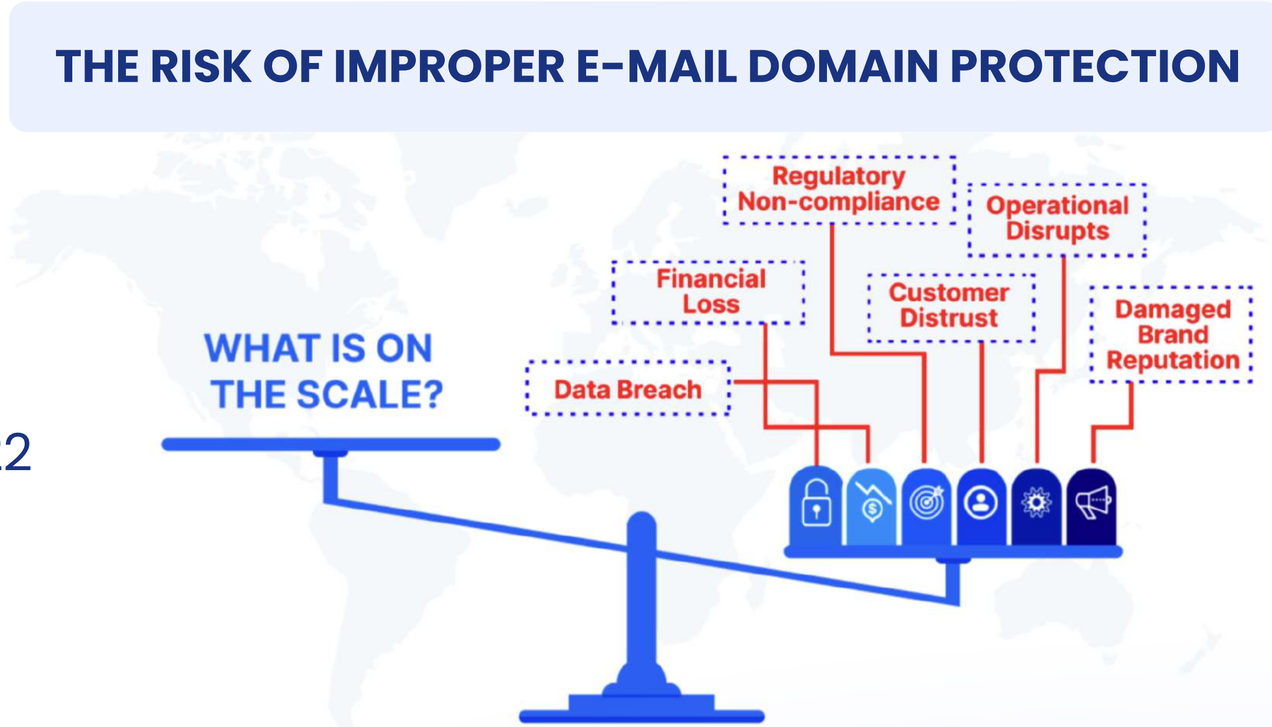
1. Detecting phishing emails has become much more challenging due to the use of AI
2. The volume and target areas of phishing attacks have dramatically increased

EASYDMARC

Security Breaches Are Very Expensive

$4.91 million average cost of a data breach caused by phishing attacks in 2022

93% successful attacks worldwide started from email security issues



EASYDMARC

Solution

Email Authentication

Establishes mechanisms to verify the authenticity of the sender and the integrity of the message.

SPF

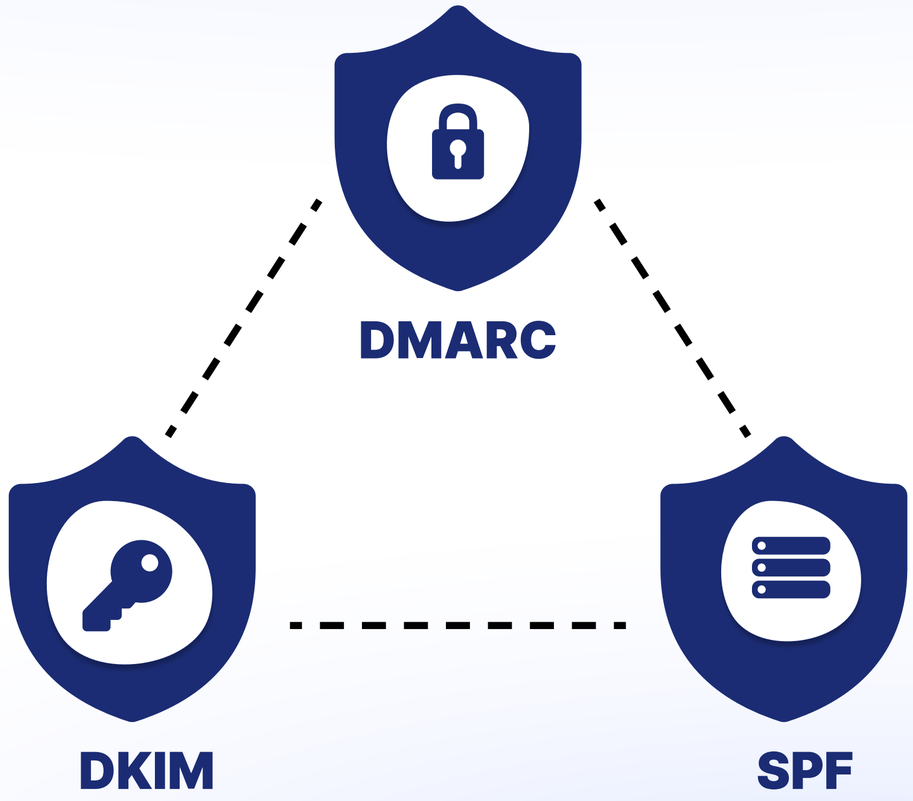
Allows domain owners to specify which mail servers are authorized to send emails on their behalf.

DKIM

Adds a digital signature to email messages to verify that the content has not been altered and that the message was indeed sent by the claimed sender.

DMARC

Builds on SPF and DKIM to provide additional protection and reporting capabilities. It enables domain owners to specify how their emails should be handled if they fail SPF or DKIM checks.

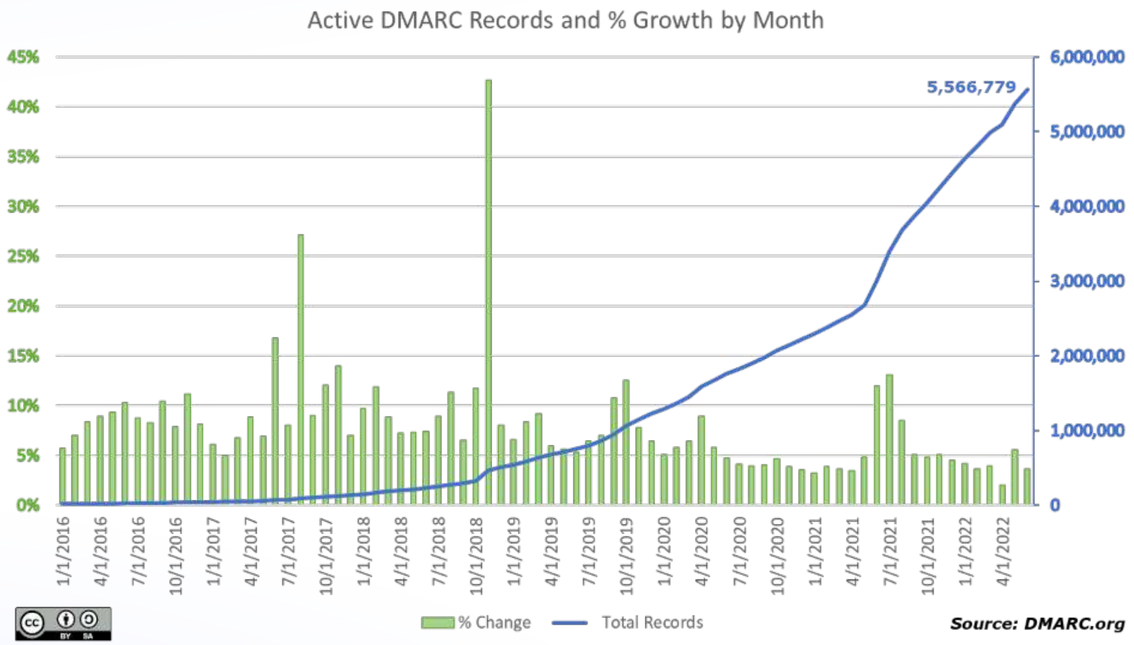


EASYDMARC

Adoption

Factors thanks to which the adoption rate is accelerating:

- Government regulations (USA, UK, Netherlands, Australia, New Zealand, Denmark, etc.)
- Requirements by industry giants (Google, Yahoo)
- International regulatory standards (PCI DSS, ISO)
- Incentives from regulators
- Education and awareness programs
- Easy implementation mechanisms



EASYDMARC

Implementation

Step 1 **Monitor:** Generate and add SPF, DKIM, and DMARC records for your domain. Track your legitimate senders and email volumes.

Step 2 **Quarantine:** Configure your sending sources. Start sending emails from suspicious sources into the spam box.

Step 3 **Reject:** Gradually move to p=reject policy. Block all illegitimate sources from sending emails on your behalf.

Start from monitoring and transition to the best security state for your domain

None	Quarantine	Reject
Messages failing authentication still deliver to the inbox	Messages failing authentication will be marked as Spam	Messages failing authentication will be rejected

EASYDMARC

Challenge

Getting started with the monitoring stage is easy.

BUT

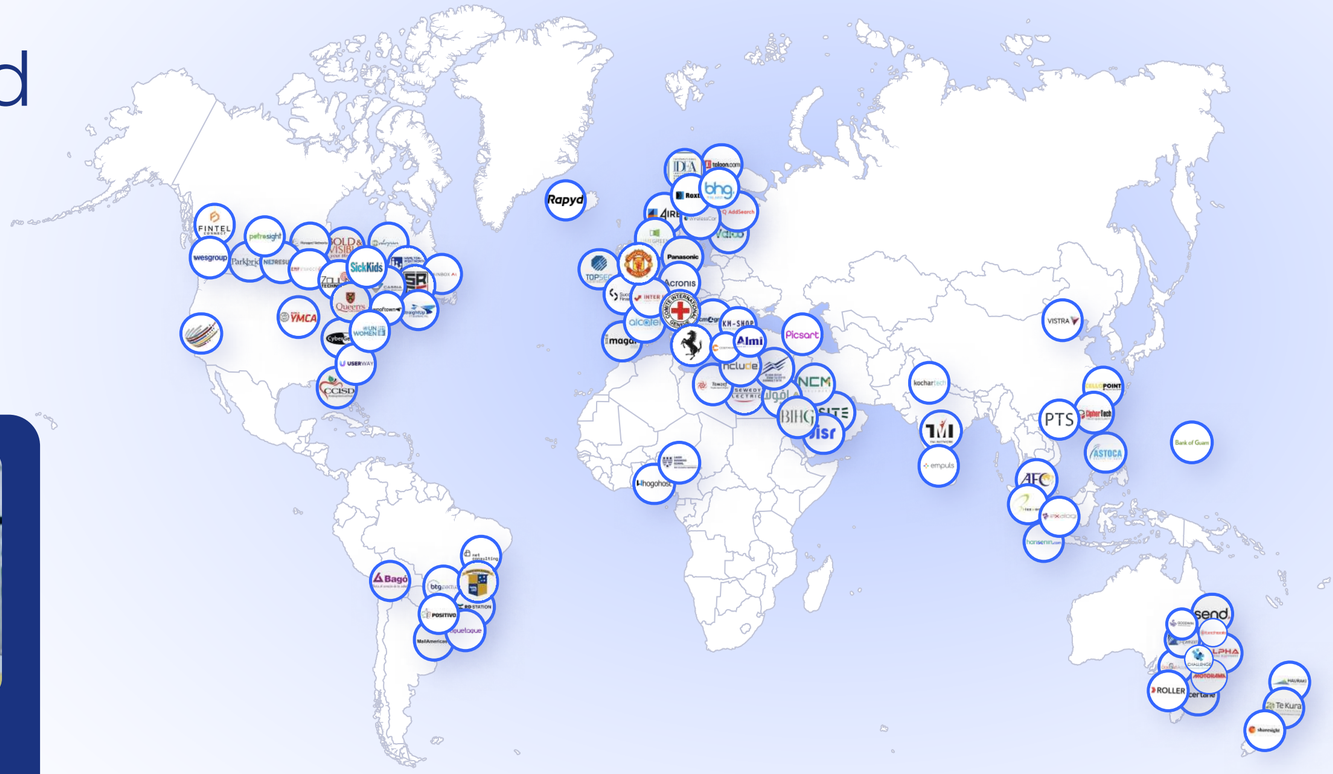
The journey from monitoring to the best security state with full DMARC enforcement is complicated and risky.

Dedicated software simplifies the process

- Centralized management to configure, monitor, and maintain settings
- Automation to reduce the risk of human error and streamline the implementation
- Reporting and analytics to make informed decisions quickly
- Alerts and notifications to stay on top of potential threats

Thank You

90,000+ domains protected
by EasyDMARC solutions



Presented by

Gerasim Hovhannisyan

CEO & Co-Founder EasyDMARC

gerasim@easydmarc.com

Got questions? Let’s connect

nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Program for a Safer Internet in Brazil

Gilberto Zorello / Flávio Kenji Yanai

GFCE Triple-I workshop at Day Zero of LACIGF in Bogota, Colombia

23/12/03

nic.br

Our Agenda

Program for a Safer Internet

About NIC.br

Program for a Safer Internet

The TOP Project

Security Notifications, MANRS and TOP Statistics

Implementation remarks

About NIC.br

The Brazilian Network Information Center, NIC.br, is a non-profit civil entity that since 2005 has been assigned with the administrative and operational functions related to the .br domain

In addition to providing and maintaining the domain names registration activity, NIC.br invests in actions and projects that bring a series of benefits to improve the Internet infrastructure in Brazil, with revenue collected exclusively through the provision of domain names registration

Some of our efforts are focused on many sectors of Brazilian society, disseminating knowledge about best practices to be adopted in networks and related areas. In some cases, we strengthen relationships with private, governmental, and nonprofit entities to encourage the adoption of best practices to be adopted in Internet services

Program for a Safer Internet
Objectives

Act in support of the Internet technical Community in Brazil

Reduction of Denial of Service attacks (CERT.br)

Improvement of the Network Routing Security (MANRS – Internet Society initiative)

Spread DNS security best practices (KINDNS & TOP)

Disseminate best security practices for configuring websites and e-mail services (TOP)

Encourage the implementation of IPv6 in final users and Internet services (TOP)

Program for a Safer Internet
TOP - Project

Developed by **NIC.br** to disseminate the best security practices in Brazil for user connection to Internet, web sites and e-mail services

https://top.nic.br

Uses the open-source code provided by the Dutch implementation of Internet.nl with a web interface in Portuguese to attend Brazilian users in local language

The project is part of the **Program for a Safer Internet** in Brazil, which works with ISPs and incumbent operators to disseminate the best security practices that they should implement on their respective networks.

The operation started in Dec/21 **Access: https://top.nic.br**

Program for a Safer Internet
Plan of Actions performed by NIC.br

Several internal teams of NIC.br participate in the Program (CERT.br, CEPTRO.br, Registro.br, IX.br, Systems)

Technical materials and good practices created

Awareness in the technical community by lectures, courses and training

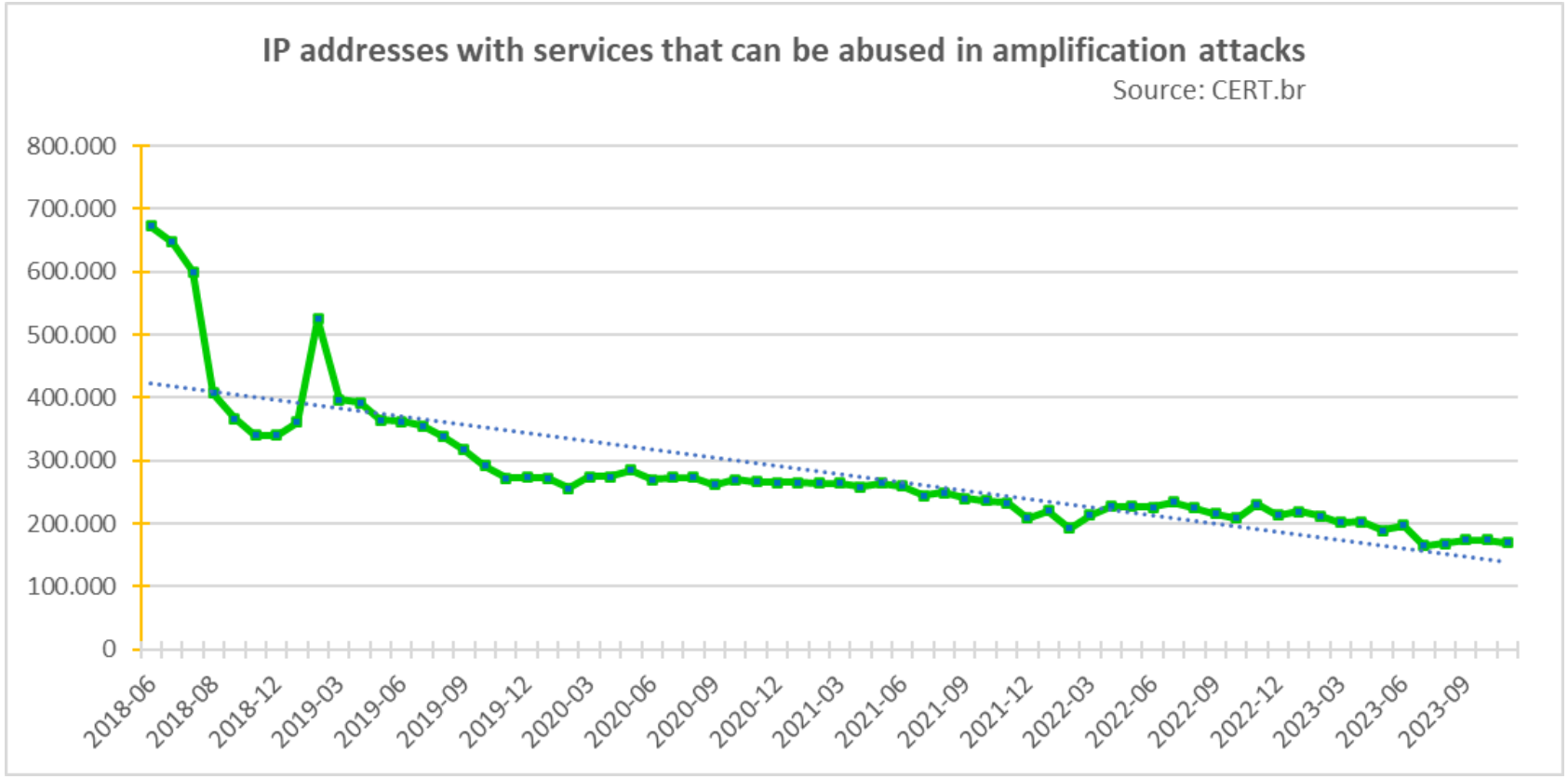
Direct interaction with network operators by bilateral meetings to explain how to implement the best practices recommended in each situation

KPIs to monitor the effectiveness of actions

Program for a Safer Internet
Statistics of Notifications of IP Addresses

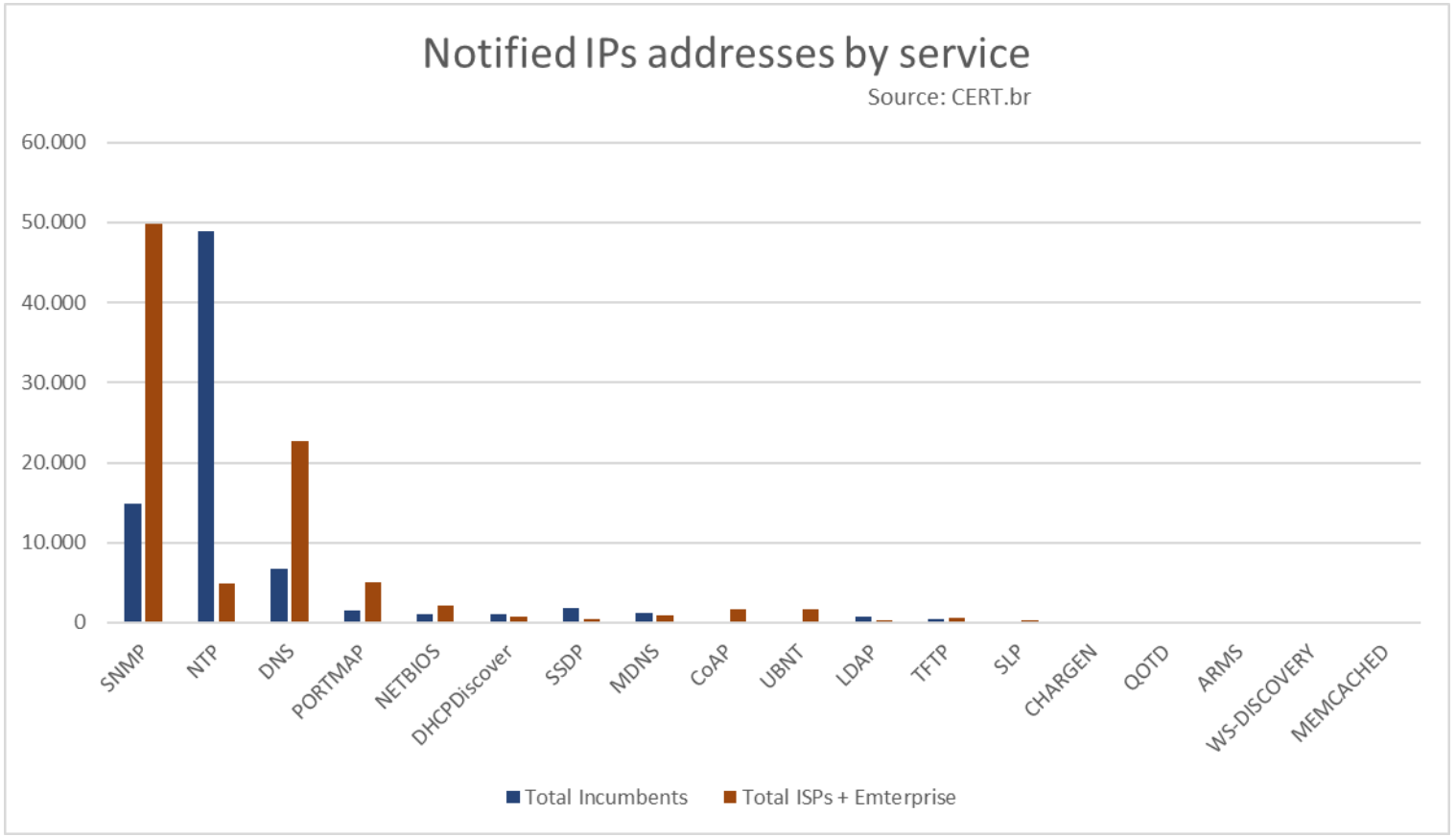
PROGRAMA INTERNET +SEGURA

Quantity of IP addresses notified with misconfigured services



76% reduction in misconfigured IP addresses since the begining of the Program

Program for a Safer Internet
IP Addresses notified monthly by service



Nov/23

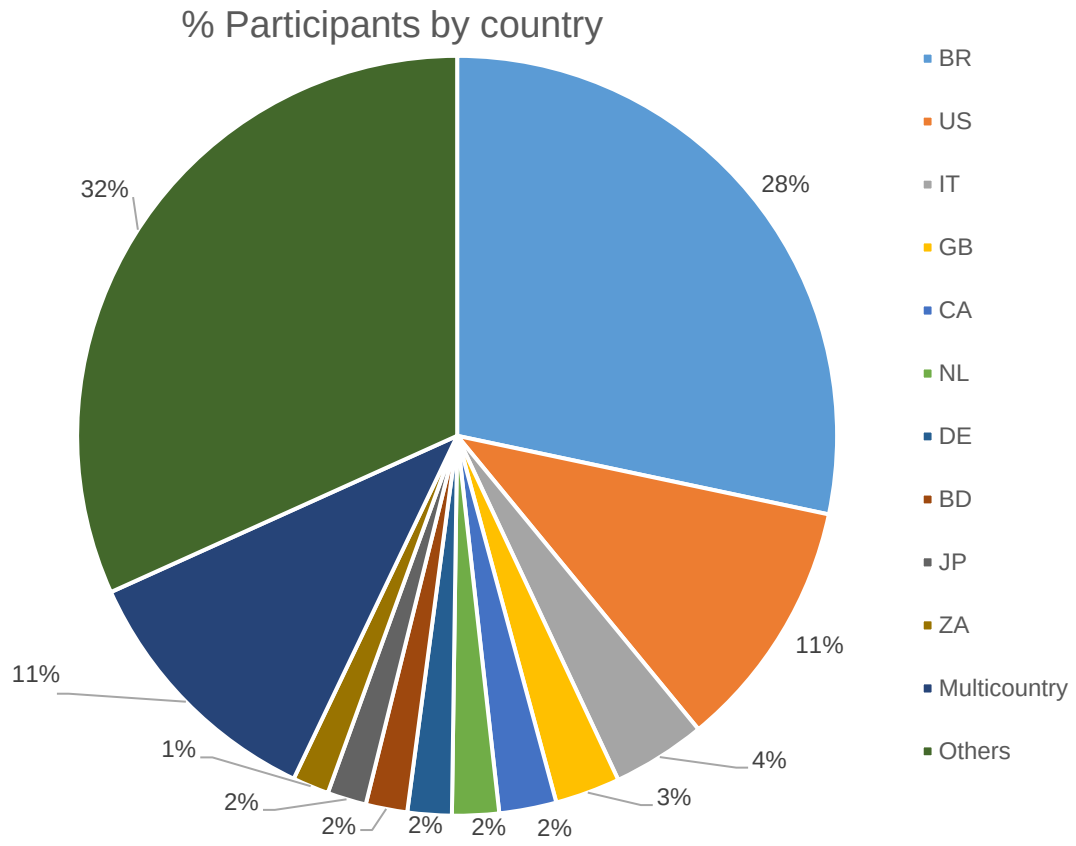
Top offenders: ISPs + enterprise → SNMP enabled e DNS recursive open

Incumbents → NTP misconfigured

Program for a Safer Internet

Statistics of MANRS Participants by Country

Distribution by country of providers participating of the MANRS initiative



Total of MANRS participants: 904

Participants in Brazil: 256 (Nov/23)

206 (2022)

174 (2021)

140 (2020)

Source: https://www.manrs.org/netops/participants/ Acess nov/23

Program for a Safer Internet

TOP Test - IPv6 DNSSEC - Recursive and User Network

KINDNS

Action 1 – Shared Private Resolver

Total Measurements Completed - IPv6 DNSSEC	Recursive DNS Server tested with Validated DNSSEC	% Recursive DNS Server tested with Validated DNSSEC
160.688	104.316	65%

Unique AS tested	User tested with IPv6	% User tested with IPv6
5.948	101.034	63%

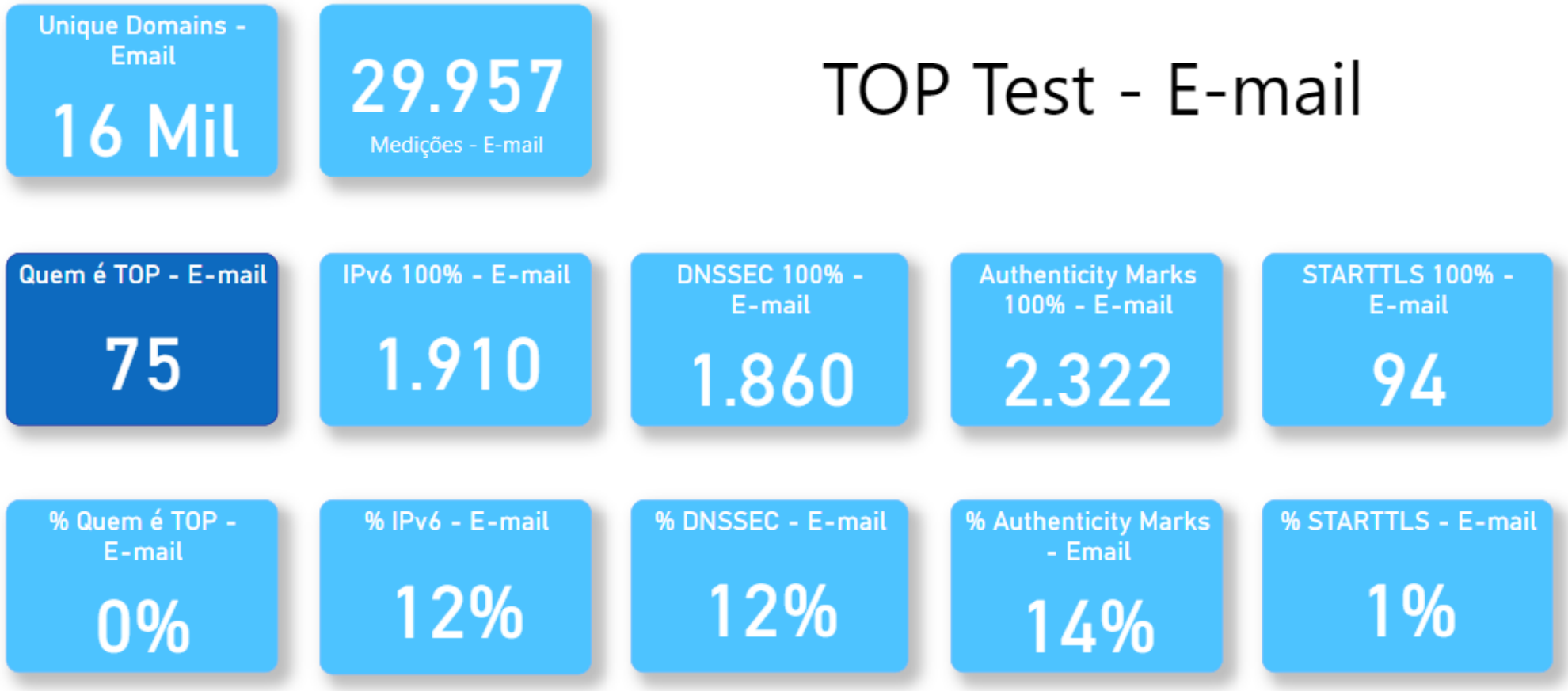
TESTE OS PADRÕES

Program for a Safer Internet

TOP
TESTE OS PADRÕES

26/11/23

Program for a Safer Internet



TOP
TESTE OS PADRÕES

26/11/23

TOP – Associations of Brazilian ISPs and Academia

TOP
TESTE OS PADRÕES

conexis
brasil.digital
A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraHosting
ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET

REDETELESUL

abrint

TelComp
Competição para o Futuro Digital

abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

APRONET
Associação Catarinense dos Provedores de Internet

RNP
REDE NACIONAL DE ENSINO E PESQUISA

InternetSul

TOP – Teste os Padrões

Implementation remarks

Delivered in Dec/21, currently runs 1.4 v. of Internet.nl

The 1.7.1 v. of Internet.nl is implemented and in validation

https://top.nic.br

The 1.8.1 version will be implemented in 1stH 2024

The best practices recommended by the tool are recommendations from NIC.br to the technical community in Brazil

The tool is being disseminated together with the **Program for a Safer Internet** at technical events and for specific sectors such as government, academia and Internet operators

TOP – Teste os Padrões
Implementation remarks

The accounting area of Brazil's legislature carried out tests of the websites and e-mail services used by the government

https://top.nic.br

The TOP tool provides important indication of the implementation status of recommended best practices and provides a baseline for operators to implement them in their networks

Brazil has continental dimensions and it is a challenge to keep up with the evolution of the use of standards

Thank you

https://top.nic.br

gzorello@nic.br

yanai@nic.br

2023 December, 03

nic.br cgi.br

www.nic.br | www.cgi.br

Octubre de 2023

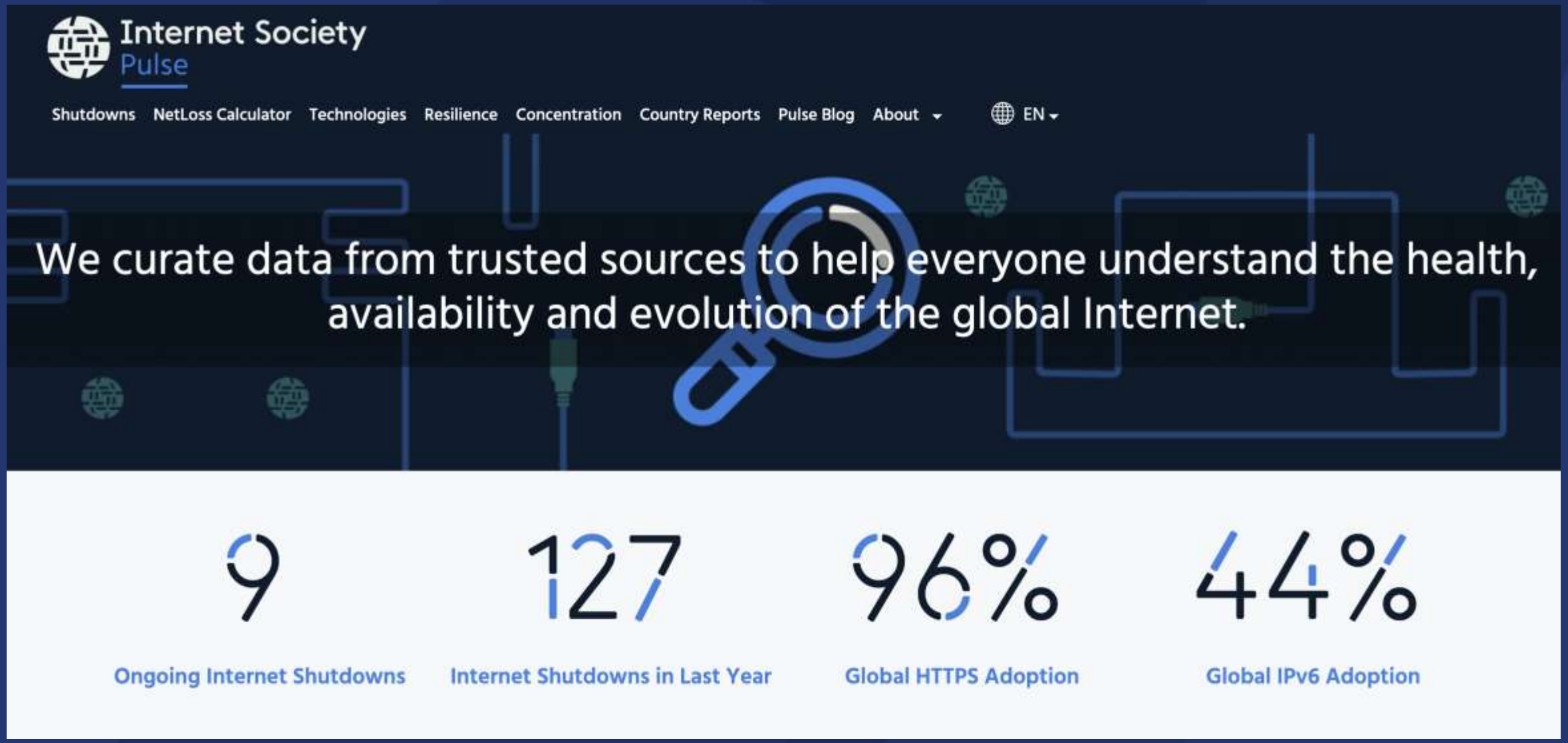
Internet Resilience Index

PULSE

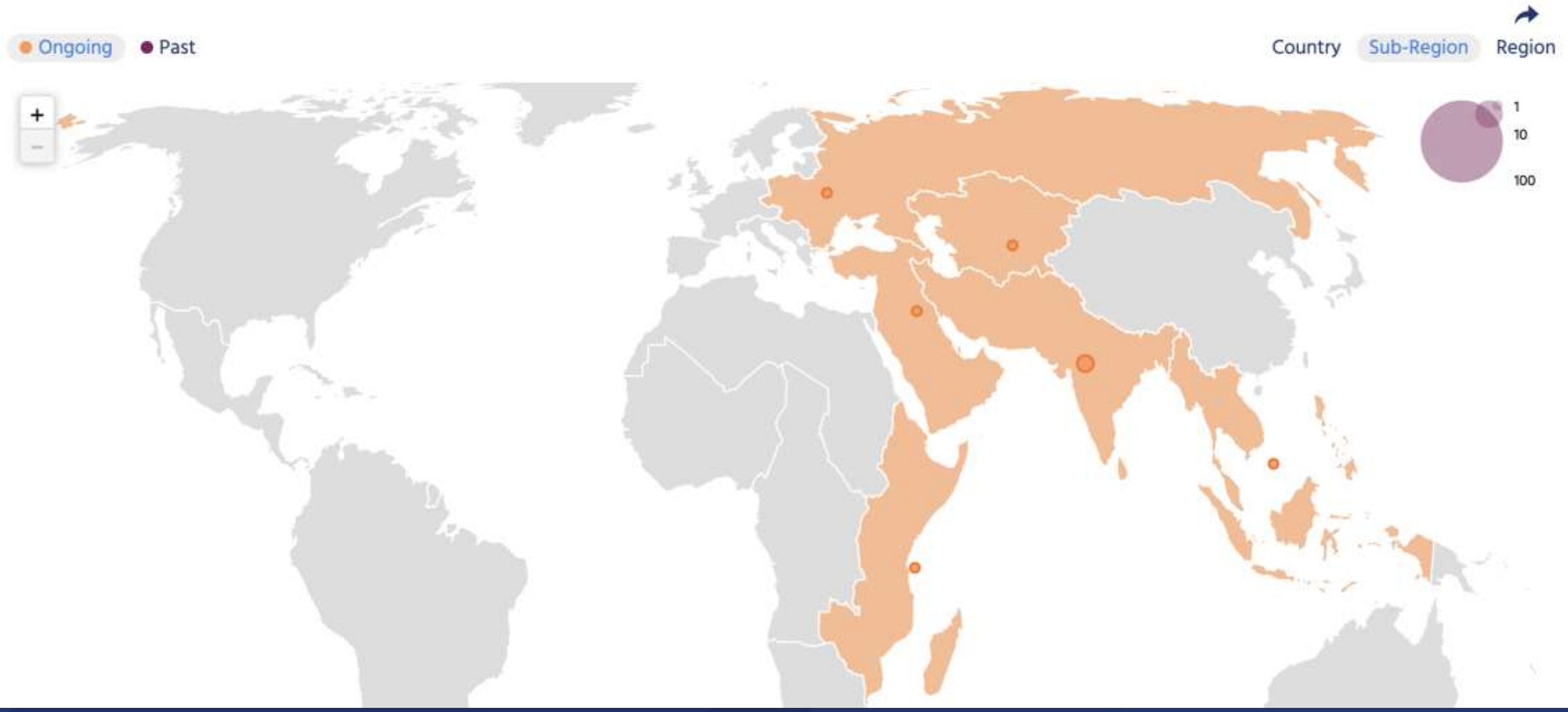
Christian O’Flaherty

Vicepresidente Regional, América Latina y el Caribe

oflaherty@isoc.org


Internet Society
Pulse
Shutdowns
NetLoss Calculator
Technologies
Resilience
Concentration
Country Reports
Pulse Blog
About
EN
We curate data from trusted sources to help everyone understand the health, availability and evolution of the global Internet.
9
Ongoing Internet Shutdowns
127
Internet Shutdowns in Last Year
96%
Global HTTPS Adoption
44%
Global IPv6 Adoption

Global Internet Shutdowns



Shutdown Events

End Date

21 Nov 2023

Search

Search For Shutdowns

November 2023

Iran (Islamic Republic of)

2 November, 2023 12:00 - 14:30 (2 hours)

Regional

> Read More

India

1 November - 2 November, 2023 (2 days)

Regional

> Read More

India

1 November - 2 November, 2023 (2 days)

Regional

> Read More

NetLoss Calculator

¿Quieres saber cuánto costó a la economía un reciente corte de Internet en tu país? ¿O desea conocer las repercusiones de un cierre anticipado de Internet? Utilice la calculadora de pérdidas netas de Internet Society Pulse para obtener más información.

Seleccione el país en la lista desplegable, luego seleccione las fechas que le interesan (deje la fecha actual para el final de un Cierre en curso) y, por último, seleccione el tipo de Cierre de Internet.

La calculadora NetLoss no distingue entre cierres nacionales y regionales, por lo que debe utilizarse con precaución a la hora de estimar el impacto económico de los cierres en países que interrumpen con frecuencia el acceso a Internet a nivel regional.

País: Chile

Fecha de inicio: 21 Nov 2023

Fecha final: 21 Nov 2023

Tipo

- ◯ Internet Shutdown
- ◯ Service Blocking

Tecnologías de apoyo

Las nuevas tecnologías son esenciales para que Internet siga creciendo, evolucionando y satisfaciendo las cambiantes expectativas de los usuarios. Las tecnologías facilitadoras contribuyen a mejorar la escalabilidad, la seguridad, la confianza y la disponibilidad de Internet.

Internet Society Pulse recopila información sobre los niveles de adopción de IPv6 en países y redes de todo el mundo, los avances hacia una web cifrada, los indicadores de adopción de DNSSEC por parte de los registros de nombres de dominio con código de país y los datos sobre la adopción mundial de TLS1.3 y HTTP/3.

Pulse Artículos Relacionados

- ¿Utilizan IPv6 la mitad de los sitios web más populares?
- De Afganistán a Zimbabue, los informes nacionales Pulse ilustran la salud de Internet en cada país
- ¿Por qué ha caído en picado la capacidad de IPv6 en algunas redes?

HTTPS

96%

Porcentaje actual de los 1000 sitios web más importantes del mundo que admiten HTTPS.

IPv6

44%

Porcentaje actual de los 1000 sitios web más importantes del mundo que soportan IPv6.

TLS 1.3

81%

Porcentaje actual de los 1000 sitios web más importantes del mundo que admiten TLS 1.3.

Nuestra medida global de la resistencia de Internet se basa en los siguientes pilares:

Infraestructura

La existencia y disponibilidad de la infraestructura física que proporciona la conectividad a Internet.

Rendimiento

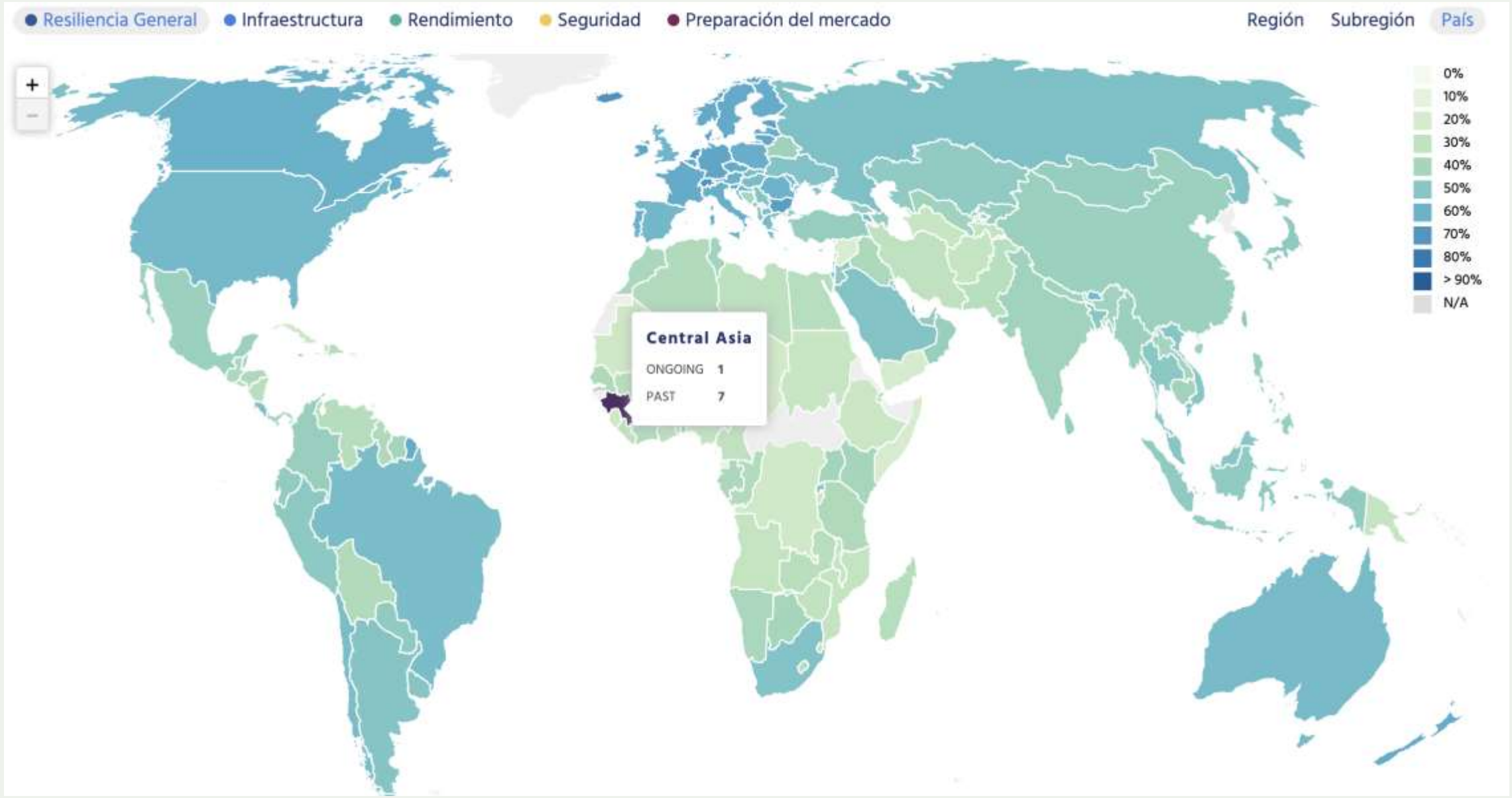
La capacidad de la red para proporcionar a los usuarios finales un acceso fluido y fiable a los servicios de Internet.

Seguridad

La capacidad de la red para resistir interrupciones intencionadas o no intencionadas mediante la adopción de tecnologías de seguridad y mejores prácticas.

Preparación para el mercado

La capacidad del mercado para autorregularse y ofrecer precios asequibles a los usuarios finales manteniendo un mercado diverso y competitivo.


Resiliencia General
Infraestructura
Rendimiento
Seguridad
Preparación del mercado
Región
Subregión
País
0%
10%
20%
30%
40%
50%
60%
70%
80%
> 90%
N/A
Central Asia
ONGOING 1
PAST 7

MANRS

Concentración del mercado

Internet se basa en una arquitectura descentralizada en la que el control de los servicios básicos de Internet se distribuye por la"red de redes". Esto garantiza una red más resistente y evita los puntos únicos de fallo o control.

En esta área de interés, presentamos datos sobre la distribución de las cuotas de mercado de las principales tecnologías e infraestructuras de la web para ver cómo los servicios se concentran en unos pocos actores y países o se distribuyen entre muchos, y para seguir cómo cambia esto a lo largo del tiempo.

Presentamos dos visiones diferentes de la concentración del mercado:

- **Concentración del mercado:** La concentración de proveedores en un mercado determinado
- **Cuotas de mercado de los países:** La competencia de los proveedores en un mercado determinado.

Para inferir el grado de concentración o distribución del poder y su evolución en el tiempo, calculamos dos métricas basadas en los datos subyacentes de las cuotas de mercado:

MANRS

Informes nacionales

Los informes nacionales de Internet Society Pulse consolidan y contextualizan los datos que recopilamos y conservamos a través de las cuatro vías de investigación de Pulse (cierres, tecnologías facilitadoras, concentración y resiliencia) para cada país. Pulse Country Reports puede ayudarle:

- Los responsables políticos y de la toma de decisiones deben comprender las diferencias locales y regionales en relación con diversos aspectos de Internet. Esto puede ayudar a orientar los planes de mejora y a trabajar en favor de políticas que apoyen el desarrollo.
- Grupos de la sociedad civil y periodistas para defender y presionar en favor de más inversiones y mejoras específicas de las infraestructuras.

Los informes Pulse Country consolidan e ilustran los datos que Pulse recopila de nuestros socios de datos. Para más detalles, consulte el documento metodológico.

Nuestra medida global de la resistencia de Internet se basa en los siguientes pilares:

Infraestructura

La existencia y disponibilidad de la infraestructura física que proporciona la conectividad a Internet.

Rendimiento

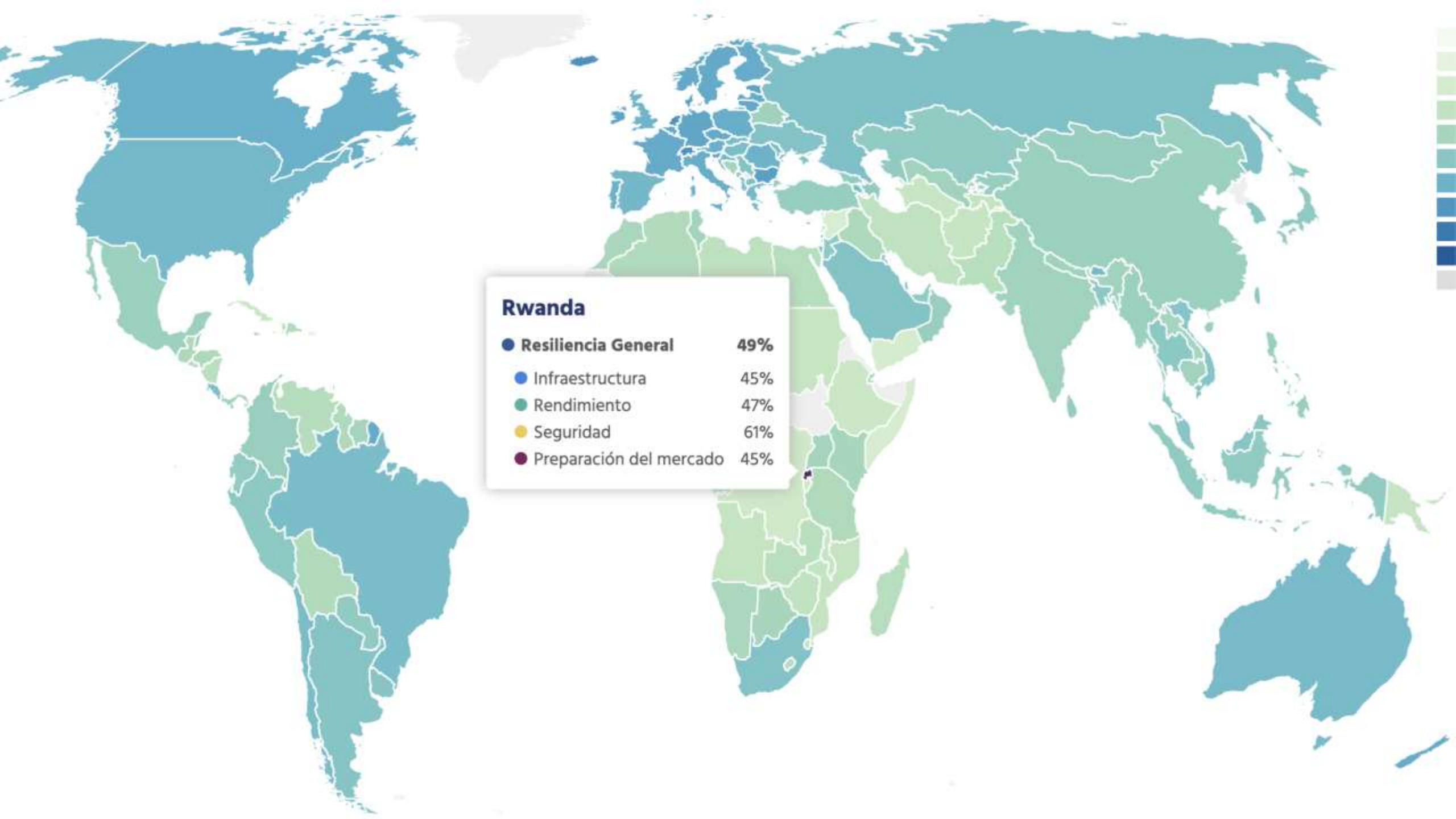
La capacidad de la red para proporcionar a los usuarios finales un acceso fluido y fiable a los servicios de Internet.

Seguridad

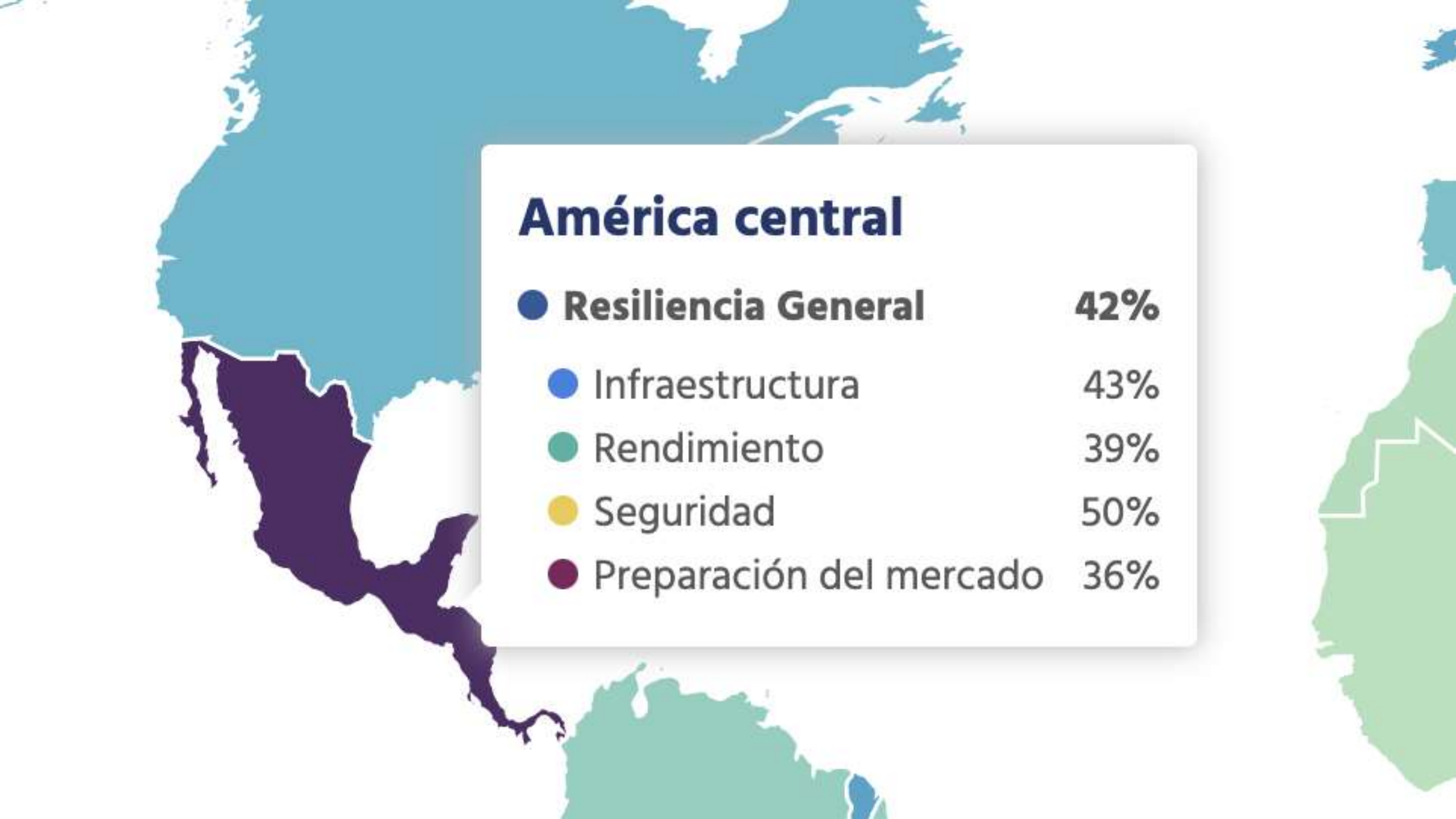
La capacidad de la red para resistir interrupciones intencionadas o no intencionadas mediante la adopción de tecnologías de seguridad y mejores prácticas.

Preparación para el mercado

La capacidad del mercado para autorregularse y ofrecer precios asequibles a los usuarios finales manteniendo un mercado diverso y competitivo.


Rwanda
Resiliencia General 49%
Infraestructura 45%
Rendimiento 47%
Seguridad 61%
Preparación del mercado 45%


América del Sur
Resiliencia General 47%
Infraestructura 46%
Rendimiento 38%
Seguridad 56%
Preparación del mercado 47%


América central
Resiliencia General 42%
Infraestructura 43%
Rendimiento 39%
Seguridad 50%
Preparación del mercado 36%


El Caribe
Resiliencia General 44%
Infraestructura 49%
Rendimiento 48%
Seguridad 43%
Preparación del mercado 36%

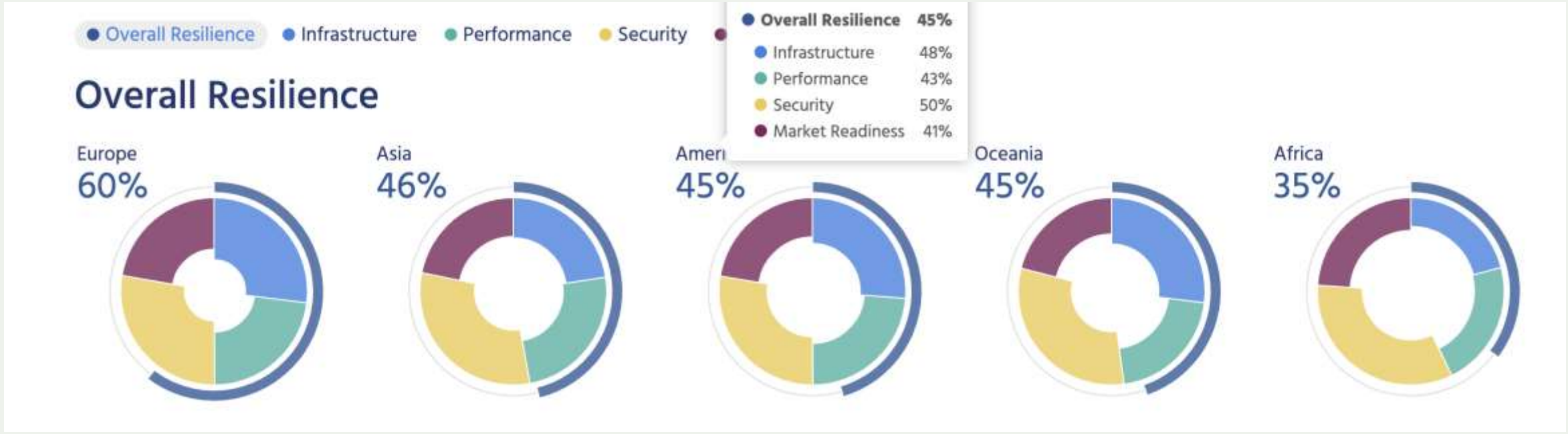
Internet Society
Pulse

Internet Resilience Index Methodology

2023

July 2023 v1.0

Table of Contents


Overall Resilience
Infrastructure
Performance
Security
Overall Resilience 45%
Infrastructure 48%
Performance 43%
Security 50%
Market Readiness 41%
Overall Resilience
Europe
60%
Asia
46%
45%
Oceania
45%
Africa
35%

y Apoya Nuestra Misión

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

6 Battery Road #38-04
Singapore 049909

Gracias

Internet Society

Universal Acceptance

lacnog

Aceptación Universal

Lia M. Solis M

Aceptación Universal - UA

Es el principio de aceptar, validar, almacenar, procesar y mostrar nombres de dominio y direcciones de correo electrónico de forma correcta y uniforme en todos los dispositivos, sistemas y aplicaciones.

- **Aceptación**, proceso por la que un dominio o dirección de correo es recibido
- **Validación**, comprobar la sintaxis correcta de una dirección de correo electrónico o nombre de dominio.
- **Almacenamiento**, almacenar de forma temporal o a largo plazo nombres de dominio y direcciones de correo electrónico en formatos bien definidos.
- **Procesamiento**, siempre que una aplicación o un servicio utiliza una dirección de correo electrónico o un nombre de dominio para realizar una actividad
- **Visualización**, interfaz del usuario representa visualmente

https://uasg.tech/

Problema

- Rapidos: Nuevos dominios, cambios de dominio con más de tres caracteres de longitud o en formato no ASCII (internacionalizado Nombres de dominio o IDN).

- Muchos sistemas no reconocen o procesan adecuadamente nuevos nombres de dominio

Objetivo

Universal Acceptance

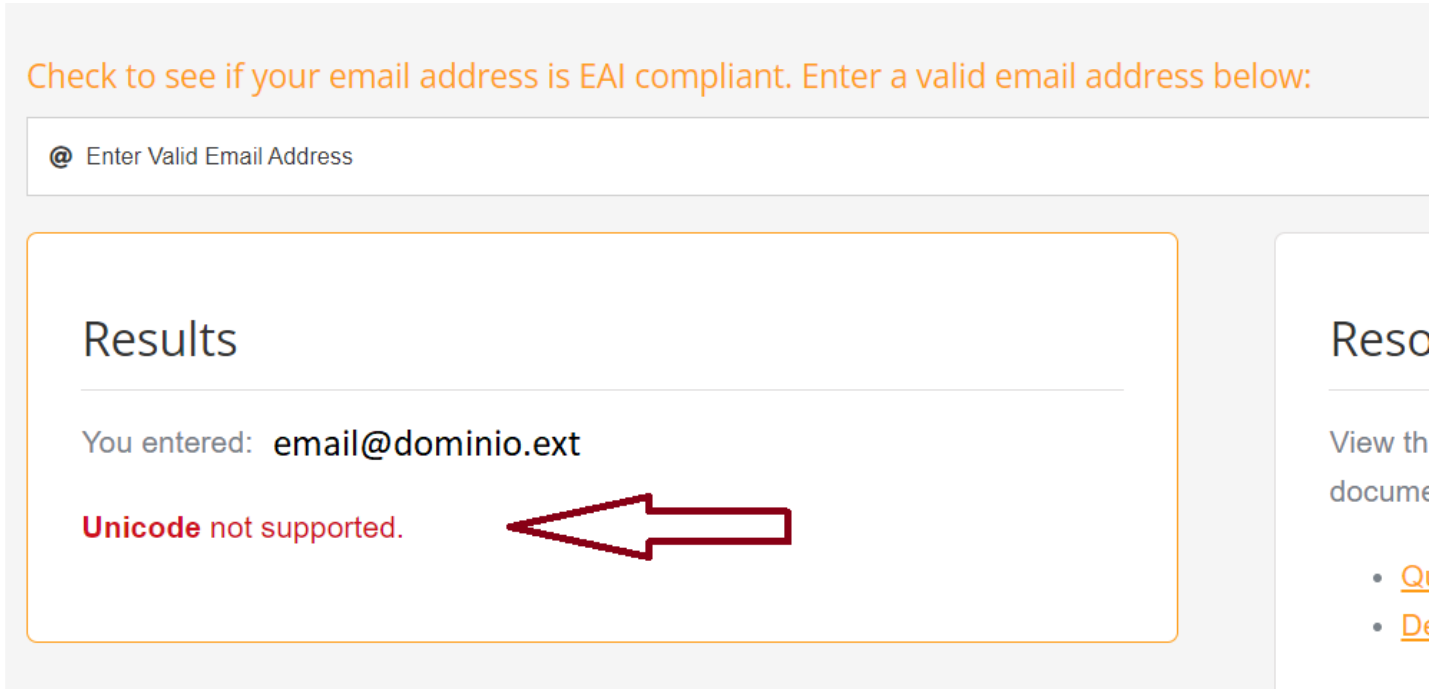
Crear una comunidad preocupada por mejorar la forma en que los nombres de dominio y direcciones de correo electrónico asimilan o conectan cuando incluyen caracteres multilingües.

A través de …

- Compartir experiencias de aprendizaje y mejores prácticas sobre aceptación universal en la comunidad.
- Organizar y apoyar eventos de capacitación sobre aceptación universal.
- Generar un repositorio de documentación sobre aceptación universal.

Primer paso

- Test del dominio: https://uasg.tech/eai-check/

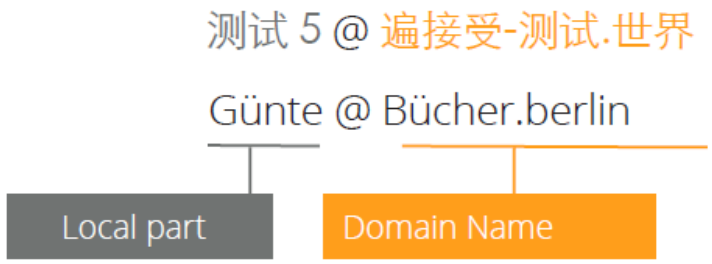


Universal Acceptance

Internacionalización de direcciones de correo electrónico EAI

Proveedores de software y servicios de correo electrónico a considerar al planificar sus ofertas

- EAI es el protocolo que permite direcciones de correo electrónico con IDNs en la parte de dominio y/o Unicode (no ASCII) en la parte local del nombre del buzón.
- Es necesario realizar cambios específicos para admitir EAI, ya que el correo EAI es conceptualmente un flujo de correo separado del correo ASCII heredado.



Consideraciones para implementación EAI

- MUA
  - Almacenar y mostrar la parte local y el nombre de dominio en Unicode
  - Verifique que el MTA (Agente de transporte de correo) maneje EAI, es decir, anuncie el SMTPUTF8 función, al enviar correo EAI
  - Seguir guías de buenas prácticas de Linkificación dentro del cuerpo del correo electrónico (SG 010 – Quick Guide to Linkification)
  - Seguir guías de buenas prácticas para la validación de nombre de dominio. (See UASG 007 –Introduction to Universal Acceptance.)
- MTA
  - Al recibir correo, anuncie la función SMTPUTF8.
  - Al enviar correo, verifique la función SMTPUTF8 en el servidor de correo remoto, use la opción SMTPUTF8 al enviar correo.
  - No envíe correo EAI a servidores remotos que no lo admitan; proporcionar informes de errores legibles cuando los usuarios intenten hacerlo.
  - Acepte versiones con etiqueta U y etiqueta A de nombres de dominio en direcciones de correo electrónico.
  - Permitir una coincidencia "difusa" de partes locales en direcciones entrantes, de forma análoga a permitir mayúsculas o minúsculas al hacer coincidir nombres ASCII.

En el proceso

Universal Acceptance

Provocar acciones inesperados:

- Rechazo o No entrega de mensajes
- Los IDN pueden mostrarse en su formato ASCII (A-Label). No deseable
- Mensajes recibidos por algunos destinatarios en un mensaje de varios destinatarios pero no recibido por otros.
- Inconsistencia o falla en la creación y entrega de mensajes de error. (RFC 3463)

Cómo garantizar la entrega a sistemas de correo que no están preparados para EAI

- Proporcionar direcciones ASCII alternativas para los usuarios
- Proporcionar una manera de utilizar direcciones ASCII en el correo a sistemas de correo que no sean EAI

Universal Acceptance

UA Day aplicaciones hasta el 15 de diciembre

Únase a nosotros

www.lacnog.net