GFCE Triple-I Day @LACIGF2023, 3 December 2023, Bogota, Colombia

Report by Roberto Zambrana, Lito Ibarra & Maarten Botterman

Summary

On Sunday 3 December, the LACIGF hosted the GFCE Triple-I Day for the second time in LAC region.
The Global Forum on Cyber Expertise (GFCE), as part of the activities on Day zero of the Latin American and Caribbean Internet Governance Forum, LACIGF 16, organized the GFCE Triple-I workshop “Creating a more trusted Internet experience, together”. This was a hybrid workshop that took place on Sunday, December 3, 2023, with the purpose of:

- Explain the most relevant aspects of open Internet standards, such as DNSSEC, DANE, RPKI, ROA, TLS, DMARC, DKIM, KINDS, MANRS, SPF and IPv6, to support more reliable communications.
- Share and report on good practices carried out by various organizations in the Internet ecosystem, which contribute to improving Internet reliability and collaborative security; segment that presented several examples of good practices in the LAC region and also in other regions;
- Promote exchange among participants to develop and commit to concrete actions that help improve the region's Internet ecosystem.

This workshop was supported by LACIGF (https://lacigf.org/), ICANN (http://www.icann.org), LACTLD (https://www.lactld.org/), LACNIC (https://www.lacnic.net/), nic.br/cgi.br (https://cgi.br/), Internet Society (http://www.Internetsociety.org), and EasyDMARC, and stakeholders from these and other organizations working in the development of the Internet in our LAC region participated in the workshop, both as speakers and participants, including the government, the private sector and the technical community. It was building upon the results of the previous workshop in La Paz, Bolivia, hosted by LACIGF in 2019 (report).

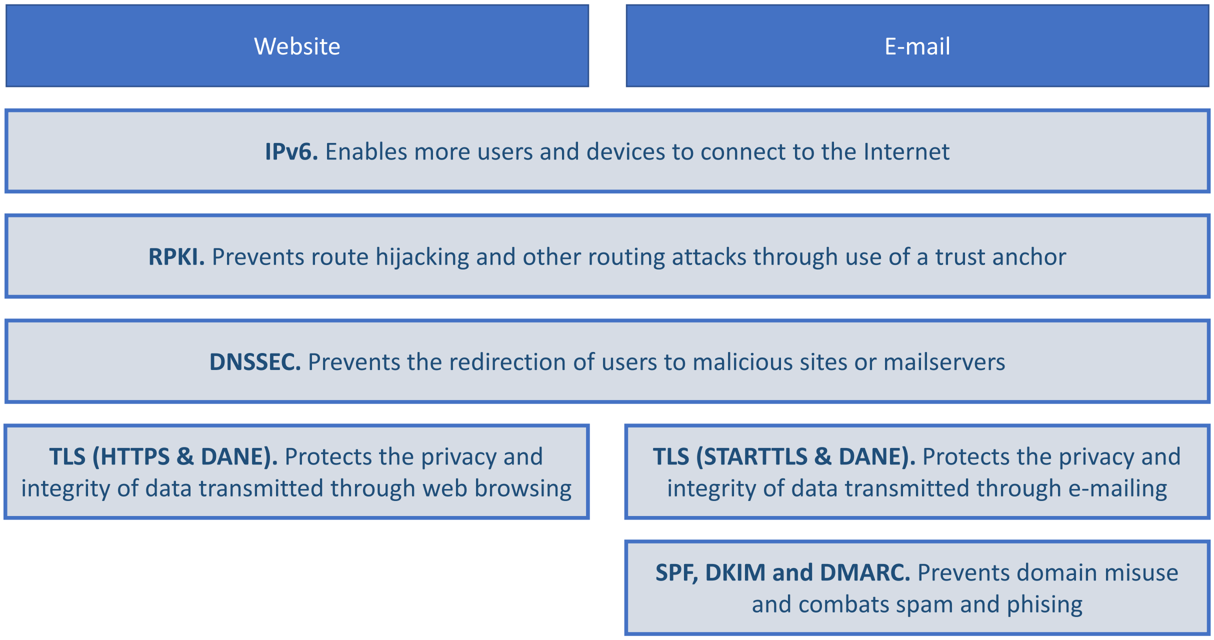
With thanks to all who helped make this happen, and with special thanks to Rafael Lito Ibarra and Roberto Zambrana. Also, we could not have done it without the invaluable support from the LACIGF Secretariat, the COLNODO organization, who helped reach out for all practical arrangements in Bogota.

Introduction

Maarten Botterman, the GFCE Triple-I facilitator, explained that the agenda included three blocks, in order to develop the described objectives, and reminded people of the results of the previous workshop in La Paz, Bolivia, 2019. Lito Ibarra, moderator for the day, thanked the audience for their participation on Sunday. After reviewing the agenda for the entire event and explaining the intervention methodology, the presentations began.

BLOCK I - Better Use of Today's Open Internet Standards

The first Block laid the foundation for understanding the current landscape of Open Internet Standards and Best Practices, their practical implications, and the collaborative efforts required to enhance their implementation in Latin America and the Caribbean. The interactive format allowed participants to contribute to the dialogue, fostering a shared understanding of the challenges and opportunities in this critical aspect of internet governance. Focus was on the use and usefulness of Open Internet Standards, Protocols and Best Practices, that matter for integrity and security of the DNS, routing and email (DNSSEC/TLS/DANE, RPKI/ROA, DMARC/DKIM/SPF), and IPv6. These standards are globally accepted and represent state-of-the-art insights that, when applied, can already help reduce the risks of using the Internet and email today. These are also reflected in the GFCE Triple I Handbook. Please find below a diagram indicating how these standards interrelate:



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

Fig.1 – Today's modern open Internet standards with in-build security considerations

DNSSEC, TLS and DANE

Nicolas Antoniello, from ICANN (OCTO for LAC region), introduced the matter of practical implementation and significance of DNSSEC, DANE, and TLS in securing the Domain Name System (DNS) and ensuring data integrity during transmission. He agreed that the stakes nowadays are high, and everything we can do to ensure "justified trust" should be done.

For its safest functioning of the DNS, it requires Registry operators and Registrants to sign their domain names. This should be facilitated by Registrars, DNS hosting providers, and DNS Operators, Internet Service Providers, mobile operators, hosting providers etc., which should activate DNSSEC validation for signed domains. DNS Security Extensions (DNSSEC): use public-key cryptography and digital signatures to protect the DNS data by providing (1) data origin authenticity (i.e. "Did this response truly come from the correct DNS server?") and (2) data integrity (i.e. "The data relating to the DNS server has not been modified after signing").

However, DNSSEC does not provide confidentiality for DNS data, unless combined with standards like HTTPS (DoH – RFC 8484) or TLS (DoT – RFC 7858) and achieve DNS encryption between the client and the resolver. Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet by ensuring authentication, confidentiality and integrity, allowing client/server applications to communicate over the Internet in a secure way (prevent eavesdropping, tampering, and message forgery), using digital certificates signed by a third party (Certificate Authority).

To go beyond the protection by DNSSEC (ideally in combination with SSL/TLS or HTTPS), DNS-based Authentication of Named Entities (DANE – RFC 6698) will allow administrators of a domain name to certify the keys used in that domain's TLS clients or servers by storing them in the DNS. This allows domain owners to specify which Certificate Authority (CA) is allowed to issue certificates for a particular resource – as there are many CA nowadays.

In combination with DNS-based Authentication of Named Entities (DANE: a protocol that helps authenticate the identity of Internet endpoints using the DNS infrastructure protected by DNSSEC) users will have the best assurances for integrity of data and end points.

A DNSSEC deployment checklist of adjustable action items that aims to simplify your journey into DNSSEC deployment can be found in the DNSSEC Deployment Guidebook.

ICANN supports DNS and DNSSEC capacity development and much more: reach out to TE or GSE teams, download the Guidebook, or check out the KINDNS program that is set up to promote best practices for DNS operators.

RPKI and ROA

Ignacio (Nacho) Estrada (LACNIC) focused on the role of Resource Public Key Infrastructure (RPKI) and Route Origin Authorizations (ROA), and discussed the challenges with routing (involving the IP addresses). He explained that, for Internet routing, it is important that the IP addresses before and after the specific address are registered. Basically routing runs on BGP, a trust model that originally wasn't build to be secure, but to work, and in which interruptions can cause disruptions. Over time, increasingly leakages of routes have caused outages – whether by purpose or by mistake.

In short, through global RPKI deployment:

1- Networks sign their prefixes i.e. "create ROA", and:
2- Networks validate other "networks signature".

This is to prevent "prefix hijacking" (i.e. someone pretending that they are originating an IP block that doesn't belong to them) and "route leaking" (i.e. announcing a route which they are not supposed to) by ensuring the integrity of the sources. Signing is one thing; however, checking whether the signature is correct closes the loop (i.e. validation). This is done by RPKI.

Nacho explained this very vividly by doing a participatory and highly illustrative dynamic to explain RPKI and ROA. By placing participants on the floor, and making them connect as autonomous servers, as well as the role of the certification authority, he showed how RPKI and ROA are good practices and standards that seek to avoid IP addresses hijacking and prevent the wrong or illegitimate IP (Internet protocol) addresses announcements to be successful.

DMARC, DKIM, SPF

Gerasim Hovhannesyan from EasyDMARC delved into the importance of DMARC (Domain-based Message Authentication, Reporting, and Conformance), DKIM (DomainKeys Identified Mail), and SPF (Sender Policy Framework) in email authentication and protection against phishing attacks.

Today, the problem is that anyone who is on the Internet can send an email on other person's behalf. The two big changes in 2023 are:

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

Of all successful attacks globally, 93% would have been avoided when proper email security would have been applied. It is crucial to establish mechanisms to verify the authenticity of the sender, and the integrity of the message.

The standards mentioned above, together, handle these to a high extend. SPF allows domain owners to specify which mail servers are authorized to send emails on their behalf. DKIM adds a signature to verify that the content has not been altered and that the message was indeed sent by the claimed sender. And DMARC builds on SPF and DKIM to provide additional protection and reporting by enabling domain owners to specify how their emails should be handled if they fail SPF and/or DKIM checks.

DMARC makes email really safe, and once you start monitoring, implementation is relatively easy. Yet it is important to use DMARC well – today, a policy that just "rejects" emails that cannot be confirmed via SPF and/or DKIM will lead to many emails not reaching you at all. Quarantine is currently probably a better policy – the danger gets contained, yet can still be checked.

In the discussion, Nico underscored the importance of securing Internet and email, yet that it would be very important to do so by deploying standards and good practices rather than regulation. Nacho does not consider that any particular impact could occur that should concern us. For sure, Artificial Intelligence is a game changer, and will undoubtedly bring many changes to the security issue, as Gerasim reminded us. All agreed.

BLOCK II - Inspiration from Good Practice Actions

During the second block of the day, we had presentations and discussions of a number of global good practices and good experiences from the region that are deemed potentially relevant for capacity building and to inspire action in the region.

Internet Resilience measuring

Christian O'Flaherty (ISOC for LAC region) presented the Internet Resilience Index (IRI), an indicator derived from key pillars assessing a country's Internet resilience. These pillars include infrastructure (existence and availability of physical infrastructure that provides Internet connectivity), Performance (ability to provide fluid and reliable Internet services), Security (ability to resist intentional or unintentional interruptions) and Market Readiness (ability of the market to self-regulate and offer affordable prices). He highlighted the significance of data collection from over 30 different indicators, including routing hygiene. Country rankings can be accessed through the portal pulse.internetsociety.org. Next to resilience, Pulse also tracks Internet shutdowns; what state of deployment of technologies is critical for the evolution of the Internet; and Concentration of services (how much are services concentrated in the hands of a few).

The definition of Internet resilience used is: "A resilient Internet connection is one that maintains an acceptable level of service in the face of faults and challenges to normal operation." The focus is on the Internet, not on the applications and services on top of the Internet. It should be noted that the data is pulled from external public sources, and is not always up-to-date, so this is merely indicative. Without in-country measurements, it's difficult to validate the data, yet the methodology used is reproducible, and "robust" in that sense.

This measuring resource, available freely to all, can be used by policy and decision makers to better understand local and regional differences regarding various aspects, so that targeted improvement plans can be set up. Those advocating and lobbying for more investment and targeted improvements can get a better understanding of the real "pain points" – as well as in which countries these pain points are apparently successful addressed.

Mutually Agreed Norms for Routing Security (MANRS)

Nayreth González (MANRS Ambassador) presented measures that can be taken on a voluntary basis by network operators as described in the Mutually Agreed Norms for Routing Security (MANRS), which is a campaign originating from ISOC aimed at best practices adoption for prevention of routing incidents. As an Internet Exchange Point responsible she adopted MANRS as a way of working, and as MANRS Ambassador she steps up to help improve MANRS and help stimulate wider MANRS adoption.

Routing is a key element of making the Internet work. There are +70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks. Routers use Border Gateway Protocol (BGP) to exchange "reachability information" – about networks they know how to reach. Routers build a "routing table" and pick the best route when sending a packet, typically based on the shortest path.

Border Gateway Protocol (BGP) is based entirely on trust between networks. It was created before security was a concern, and assumes all networks are trustworthy. There is no built-in validation that updates are legitimate. This chain of trust spans continents, and there is a clear lack of reliable resource data.

In 2019 alone, over 10,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more. About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet were affected. Incidents are global in scale, with one operator's routing problems cascading to impact others. With that, insecure routing is one of the most common paths for malicious threats. Attacks can take anywhere from hours to months to recognize, and inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage. Being vigilant and having procedures in place is therefore of key importance. MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. MANRS recommends four simple but concrete actions that network operators must implement to improve Internet security and reliability.

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure. Network's safety depends on a routing infrastructure that eradicates damaging actors and accidental misconfigurations that wreak havoc on the Internet. The more network operators work together, the fewer incidents there will be, and the less damage they can do.

Next to Network Operators, MANRS also addresses possible actions for Internet Exchange Points and calls upon them to adopt MANRS as working practice. Since 2020, MANRS also includes a CDN and Cloud Provider Programme that helps by requiring egress routing controls so networks can prevent incidents from happening. Leveraging CDNs' and cloud providers' peering power can have significant positive spillover effect on the routing hygiene of networks they peer with – and they serve many end users.

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet. Adopting MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. MANRS sets a new norm for routing security: joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure. The commitment to adopt MANRS is truly growing throughout the industry. And the MANRS observatory truly helps to understand the preparedness from a region towards cyber hygiene and resilience; hence the call to the industry to adopt MANRS, and to government and end users to ask for MANRS from their service providers.

Knowledge Sharing and Instantiation Norms for DNS and Naming Security (KINDNS)
Nicolas Antoniello, from ICANN (OCTO LAC region), presented the ICANN initiative KINDNS (Knowledge Sharing and Instantiating Norms for DNS and Naming Security), emphasizing the importance of configuration in providing internet services and how this program would help to do so in the best possible way. Like the MANRS initiative, it deals with good practices that can be implemented in the context and use of the Domain Name System. He called for increased collaboration among operators to enhance internet resilience, as well as security of the infrastructure. KINDNS is a simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations. Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices:

- self-assessment is anonymous
- reports can be downloaded directly from the web site

Participants in the KINDNS initiative become a community of operators voluntarily committing to implement/adhere to agreed practices. They also become goodwill ambassadors and promote best practices – as the wider spread the best practices, the healthier the Internet.

ICANN is in the process of promoting this in multiple languages, and continues to improve the tools, based on interaction experience with those that participate and contribute. Workshops and webinars are organized to further raise awareness on KINDNS practices as part of ICANN's overall DNS ecosystem security awareness program. All operators are encouraged to sign up, follow the practices and contribute to the continuous improvement of the platform.

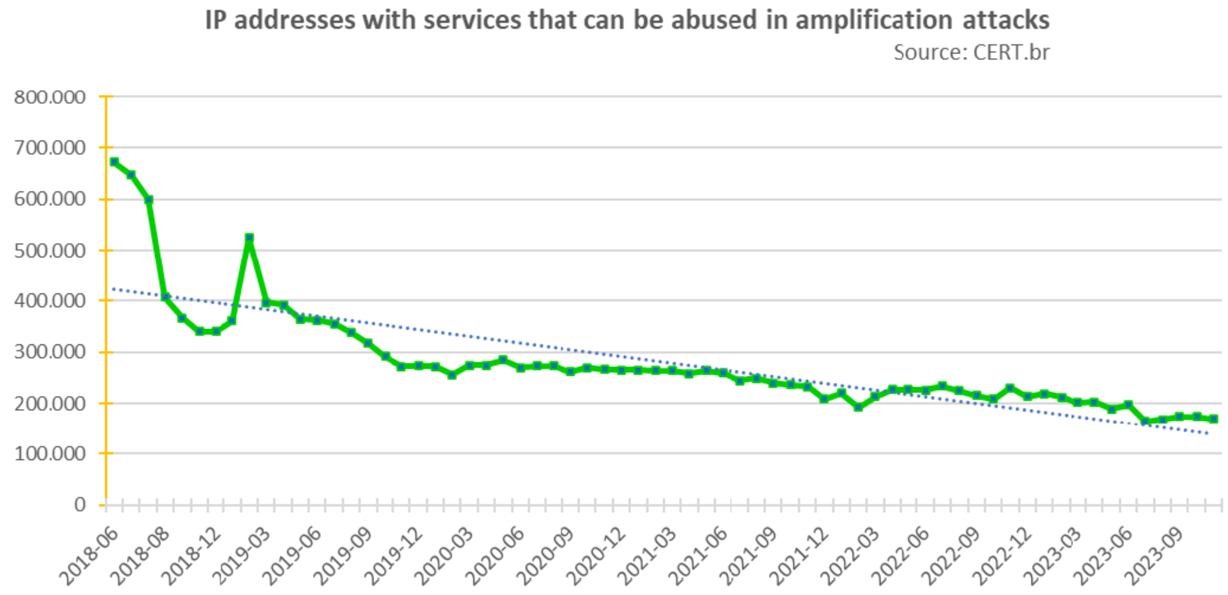
Brazil Safer Internet Program
Gilberto Zorello (NIC.br) presented the Brazil Safer Internet Program, which is an initiative developed by the Brazilian Internet Steering Committee (CGI). This program is a comprehensive approach towards introducing a number of measures that can be deployed in Brazil, targeting the Internet Technical Community in Brazil. Its main aims are:

1. Reduction of Denial of Service attacks (CERT.br)
2. Improvement of the Network Routing Security (MANRS)
3. Spread DNS security best practices (KINDNS & TOP)
4. Disseminate best security practices for configuring websites and e-mail services (TOP)
5. Encourage the implementation of IPv6 in final users and Internet services (TOP)

With this, we see a truly comprehensive program addressing the priorities also indicated in the GFCE Triple-I Handbook, and it is exemplary as such, for other countries and regions to see how leadership and stepping up to the plate can help improving justified trust in the use of the Internet and email.

The TOP project referred to above stands for Teste Os Padrões – a test website to see how well modern Internet standards have been deployed. It 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.

Several internal teams of NIC.br participate in the Program (CERT.br, CEPTRO.br, Registro.br, IX.br, Systems), and in interaction with the community they develop Technical materials and good practices, and raise awareness in the technical community by organizing and participating in lectures, courses and training. There is also direct interaction with network operators by bilateral meetings to explain how to implement the best practices recommended in each situation, when necessary. In order to measure the impact, NIC.br regularly tests websites for their mis-configuration (see picture below).


IP addresses with services that can be abused in amplification attacks

Source: CERT.br

Fig. X – Quantity of IP addresses notified with misconfigured services (source: CERT.br)

The trend is clear: measuring helps. There is a 76% reduction in misconfigured IP addresses since the beginning of the Program. Gilberto offered his help for further set up and development of such activities throughout Latin America.

IoT Security
Later it was Ignacio (Nacho) Estrada's turn to comment on security in the Internet of Things (IoT), followed by comments and contributions from Maarten and Lito.

He started stating that the security problems with IoT have to do with the configuration and design of the devices. These devices are built in large scale and the reuse other components that may perform several functions, not only what the designer of the IoT appliance needs to accomplish, but the component is cheaper. This fact is a risk for the security.

On the other hand, most of these devices used to come with preset passwords that are easily obtained, and most users do not change them when they install the device, thus making it easier to hack the device.

Nacho sees three types of problems around IoT security: 1) Privacy: If someone has easy access to a camera, for instance, he may see the intimacy of my home or office, or have unauthorized access to our data. 2) Data manipulation: Hackers may alter the information in a device and cause problems. 3) Hijacking Iot devices to perform Service Denial attacks and/or other types of mass intrusion.
Maarten commented on the security standards, labels and protocols for IoT that are being revised or developed by international organizations, such a IEEE. Governments can be of great help by including in their procurement processes the demand for these security standards for the suppliers. Labeling and certification of security and privacy features will be an important enabler for end users to make smart and conscious decisions.

Finally, Lito mentioned that the topics proposed for the Internet Governance Forum this year, and surely for the future, have started to include emergent technologies, such a Artificial Intelligence and Internet of Things, showing a growing concern for their impact for humanity.

Universal Acceptance
Lia Solis (Ambassador for the Universal Acceptance Study Group UASG) explained the importance of improving Universal Acceptance to new Domain Names and internationalized scripts for Domain names and email. She presented the Call to Action for the upcoming year, as expressed by the UASG. The Action Plan calls:

For Businesses:

- Organize internally and assess if your business' systems are compliant with UA standards.

* Update your own IT systems to be UA-ready. See UASG026 UA-Readiness Framework, UASG004 test cases, free code samples, and EAI Self-Certification Guide.

For Governments:

* Evaluate the possibility of including UA requirements in government procurements.
* Coordinate with your national ccTLD managers and ICANN Governmental Advisory Committee (GAC) delegates to participate in and strengthen UA-related actions.

For Academia:

* Upgrade email systems to support EAI.
* Update IT curricula to include teaching and learning of UA and software internationalization-related concepts.

The Action Plan also includes a global UA Day, to be held on the 28th of March, as was done in 2023 for the first time. Aim is to have one global event, and a series of regional and national events in the same period.

Block III: Planning for a More Trusted Internet: Marketplace for Action

Lito gave the introduction and Maarten presented the summary of the topics discussed in the morning, including:

- "Justified trust in the use of the Internet and email" an important subject to discuss and progress on an ongoing basis;
- there are Resources and testing tools available online let's use them and contribute to continuous improvements of their usefulness;

The comments are as follows:

- Esteban Lazcano commented that it is important to know the processes, and on the part of the users, it is important as much as on the actors who in many cases are gathered at different organizations in the regions, such as LAC ISP (Latin American and Caribbean Internet Service Providers organization), and others. In particular, the interest is to replicate initiatives like these in the countries through existing Internet Service Providers (ISP) chambers, or similar organizations;
- Maarten responded that documents such as the manual on the web portal can be shared. In particular, he mentioned and offered the Triple-i resources (available online) as well as his own experience;
- Rodrigo de la Parra commented that it is good to organize these events, and that indeed each actor in the technical community has been important, and

ICANN believes that it is good to work collaboratively, knowing what we are doing, but it is also important to measure, to know what more should we do, what is missing, or how can we work to improve what is missing. He mentioned the importance of the ISOC index and the Brazilian initiative.

- Maarten responded that there are many things that can be done, and Brazil is an example of what is possible. And in fact it is so simple that anyone can do it, placing portals on a website, to evaluate it. The other important thing is to listen to the ideas of the participants in similar events in the region.
- Dominique Paz, from Argentina, mentioned her contribution from the legal aspect. And about this she commented on the existing threats in the area of security, and a critical issue has to do with training, which is why the experiences presented are crucial for the people involved. Something that has to do with criminal law is that companies do not report security incidents, which is why users who are affected by these incidents do not know about them. One of the technical issues that she commented was on Network Address Translation (NAT) technology , that does not allow the origins to be identified, and that this should probably be resolved through regulations that force the transition to IPv6;
- Gerardo commented on how the Brazilian initiative was progressing, first promoted by the CGI, then adding MANRS and now it is adding KINDNS. It looks to constantly improve its impact, measure its impact, and the team stands ready to help others in the LAC region to start up similar initiatives;
- Then, one participant from Honduras took the floor, mentioning that there are other entities that work on these issues, and that we should not invent the wheel, but rather use existing resources. This was acknowledged. Maarten explicitly expressed that the aim is to facilitate, bring together, and when gaps are found in what is needed and what is available in a region, it is important to seek solutions, together, with other supportive organizations.
- Then there was an exchange about the idea of regulating protocols, Honduras says that it is not practically possible to do so. However, Dominique believes that this is how it should be. Nacho commented that LACNIC does not consider that forcing the IPv6 transition by national laws is an appropriate path;
- Then Raúl Echeverría commented on the ISOC resilience index initiative, and commented that it is an important work, which is in a maturation process. He also commented on the importance of these events. He discussed about the lack of security data, which prevents us from seeing the reality of security incidents. In addition, he mentioned that we must work with Small and Medium Enterprises (SME).
- Nicolás Antoniello commented that everything that is the Internet is not a personal construction, and in the last 20 years, he has realized that it is important to work as a team. Do not look for partial or fragmented solutions. And it is important to be careful with regulations that may affect the ecosystem, but develop them together.

- Lía Solis commented that it is not good to work under the obligation approach. But it is also important to listen to and address other emerging demands.
- Dina Santana Santos, from Brazil and Colombia ISOC Chapters, commented on the importance of the academic environment and its inclusion.
- Valeria Betancourt, from APC, asked about the initiatives that exist to design protocols with a human rights focus.

After these interesting contributions, Maarten closed the event by thanking the organization and the participants for their support. He reiterated about the availability of existing documentation and support. He also commented on how it is possible to work in regions, and in different dimensions. Part of what GFCE does is to look for what organizations and people can work with in each region and country.

This report will be used as a basis for further action development. Feel free to reach out with suggestions and ideas for taking further forward. For more information about GFCE Triple-I, including results of earlier events, please go to the GFCE Triple-I pages, if you are interested in improving the trusted Internet experience in your region.