How the .CO ccTLD handles Cybersecurity

Cooperate Action on Colombian and Global Cybersecurity and Cyberdefense issues

1. Introduction

As the Registry, and based on its delegation from the Colombian government (through the Ministry of Information Technology and Communications), **.CO INTERNET**[1] (a **NEUSTAR**[2] subsidiary in Colombia) is committed to protecting the Integrity, Stability and Reliability of infrastructure and services of the .CO ccTLD.

Misuse, abusive, malicious, and commitment situations threatening the technological infrastructure which handles the Domain Name System (DNS), challenged global security and the smooth functioning of the Internet; attacks against DNS affect users, individuals, businesses, civil society and governments. As a core of our cybersecurity policies, we deploy, along with our Registrar's channel, a *Rapid Domain Compliance Process (**RDCP**)*[3], which includes (a) an exhaustive validation and verification of contractual obligations (Terms and Conditions) compliance of all our .CO Registrants, and (b) a *Registry Threat Mitigation Service (**RTMS**)*, the operational workflow for RDCP's infringements and violations.

To deal with the facts and circumstances described above, ICANN and its members and governance organizations, among which are the Registries and the global community, must seek to maintain ***cooperate action*** efforts around conservation of a healthy and stable ***ecosystem***, looking always to improve the security and resilience of its components, and to strengthen its capacity to meet the new needs and technological and human challenges as well.

.CO INTERNET understands that his duty and responsibility as an organization which handles Internet services and as part of the ***ecosystem***, is to provide and manage quality services, as well as participate and contribute to initiatives, efforts, activities and processes which contribute to maintaining the" Security, Stability and Resiliency (SSR) " of the Internet.

2. Collaboration Activities

.CO INTERNET has been conducting a series of initiatives and efforts which understand as necessary, in terms of its management responsibility with the *Ministry of Information Technologies and Communications of Colombia (MINTIC)*, its Registrars[4] and Registrants of .CO domains worldwide, the Internet users community, and ICANN; is therefore also **.CO INTERNET** assumes cyber safety issues associated with the ".CO" ccTLD as part of their fundamental axes within its corporate strategy, all this through the management of standards, good practices, policies, processes and procedures, as well as an ***added value*** for those who register a .CO domain name anywhere.

.CO INTERNET as a Registry supports collaboration and active cooperation with cybersecurity related communities; that's why it has established official agreements and memberships with several enterprises, programs, organizations and communities, such as **APWG**[5], **NCMEC**[6], **CICILE**[7], **DNS-OARC**[8], **WEF-PCR**[9], **OPS-TRUST**[10], **THE-SECURE-DOMAIN-FOUNDATION (TSDF)**[11], as well as well-known security enterprises worldwide.

At the national level, through cooperation agreements with major Colombian organizations and entities equally committed with safety issues, including the *Colombian Chamber of Information and Telecommunications (C.C.I.T.)*, national node traffic exchange

---

[1] .CO Internet = http://www.go.co.
[2] NEUSTAR = http://www.neustar.biz.
[3] Details: http://www.go.co/company/global-responsibility/rapid-domain-compliance-process.
[4] More information = http://www.go.co/partners/get-involved/become-reseller-or-accredited-registrar.
[5] APWG = Anti-Phishing Working Group (http://www.apwg.org).
[6] NCMEC = National (USA) Center for the Child Protection (http://cybertipline.com).
[7] CICILE = European Union (EU) initiative to facilitate the exchange and dissemination of information on prevention and combating cybercrime; members are Law Enforcement Agencies (LEA's), public and private sector, as well as NGO's (http://europa.eu/sinapse/directaccess/CICILE).
[8] DNS-OARC = Center Operations, Analysis and Research DNS (http://www.dns-oarc.net).
[9] "WEF Commitment to Cyber-Resilience": http://www.weforum.org/issues/partnering-cyber-resilience-pcr.
[10] OPS -TRUST = global community of security experts (https://ops-trust.net)
[11] Details = http://www.thesecuredomain.org/

(NAP/IXP) manager, achieved in 2.011 the membership of its incident response center, **CSIRT-C.C.I.T.**[12]**,** to **FIRST**[13], one of the most renowned security communities worldwide.

After that first effort accomplished, Colombian cybersecurity community has continued to promote this environment management and international affiliation recognition of their incident response centers, and thus already achieved the "DIGIWARE CSIRT (DIGICSIRT)[14]", was also a member of FIRST. In turn, these CSIRT's, and as members of FIRST, together supported the membership of the "National Police CSIRT **(CSIRT-PONAL)[15]".**

Following the CSIRT's certification for two (2) major national ISP's: **E.T.B.**[16] and **CLARO-Colombia**[17] (late 2.012), and **COLCERT**[18] (our National CERT®) and **SOC-CCOC**[19] (November 2.013), both from the National Defense Ministry (MDN), Colombia now has *seven* (7) incident response entities certified by the **FIRST** global community.

Additionally, **.CO INTERNET** maintains an agreement with **CSIRT-PONAL** since 2.011 to manage cybersecurity issues. Thanks to this agreement, jointly managed security incidents relating to domains under "GOV.CO", "MIL.CO", "ORG.CO" and "EDU.CO" (Defacement and Phishing Web sites, in particular), as well as reports of malicious activity (C2, malware, phishing, among others) generated by reporting services like ShadowServer[20], also along with the **CSIRT-CCIT** support.

.CO INTERNET also signed last year a joint cooperation agreement to exchange information on cybersecurity incidents with the *Colombian Ministry of Defense (MDN)*, which leads the National Cyber Emergency Response Group (**COLCERT**),[21] coordinator of cybersecurity and cyberdefense matters, according to a national public policy[22].

Finally, it is important to emphasize that **.CO INTERNET**, as Administrator of the Colombian ccTLD, has actively participated in the action plans and activities, both technical and communication and interaction, training and knowledge transfer, which have been leading government entities such as (a) the Ministry of National Defense-MDN (via "COLCERT" and "Cyber Joint Command-CCOC"), (b) the National Police (via the "Police Cyber Center" and "Cyber Joint Command"), (c) the MinTIC (via the "Sub-area of Security and Privacy" in the "Direction of Standards and IT Architecture"), (d) the Office of the President (via their CSIRT), with the support from local CSIRT's, C.C.I.T. and ISP's, and Security Operation Centers (SOC's) of public and private banks, among others, to deal with incidents, attacks or threats to "Stability, Security and Resiliency (SSR)" of IT critical infrastructure of the country. Joint action exercises like (a) the generation of an information circular to government and military entities to update contact details of domain names under "GOV.CO" and ". MIL.CO" within the WHOIS.CO query system, (b) engineering meetings held on national holidays, (c) active participation in relevant presentations during the monthly workshops organized by Incident Management COLCERT, (d) attendance to monthly critical infrastructure meetings hold by SOC-CCOC (MDN), are proofs of that effort.

[12] Details = http://www.csirt-ccit.org.co
[13] Details = http://www.first.org
[14] Details = http://www.first.org/members/teams/digicsirt
[15] Details = http://www .first.org / members / teams / csirtponal
[16] Details = http://www.first.org/members/teams/csirt-etb
[17] Details = http://www.first.org/members/teams/soc_team_claro_colombia
[18] Details = http://www.first.org/members/teams/colcert
[19] Details = http://www.first.org/members/teams/soc-ccoc
[20] Details = http: / / www.shadowserver.org
[21] Details = http://www.colcert.gov.co
[22] Details = https://www.dnp.gov.co/LinkClick.aspx?fileticket=-lf5n8mSOuM% 3D & tabid = 1260