Día “GFCE Triple-I” @LACIGF2019, 5 de Agosto 2019, La Paz, Bolivia

Informe por by Daniel Fink & Maarten Botterman
Traducción al español por Jannett Ibañez, Lia Solis y Hugo Salgado.

Resumen

El día lunes 5 de agosto, LACIGF hospedó el Día GFCE Triple-I por primera vez en la región LAC. Este taller fue apoyado por LACIGF (https://lacigf.org/), LACTLD (https://www.lactld.org/), LACNIC (https://www.lacnic.net/), LACAAWG, nic.br/cgi.br (https://cgi.br/), ICANN (http://www.icann.org), Internet Society (http://www.Internetsociety.org) y su Capítulo Boliviano, y el Ministerio Holandés de Asuntos Económicos y Clima.

La intención del taller es buscar formas de avanzar hacia la “Construcción de Capacidad”, para una experiencia de una Internet más confiable en la región. Los participantes de este taller incluyeron expertos globales y regionales, y grupos regionales de partes interesadas en Internet, incluyendo el gobierno, empresa y comunidad técnica, quienes contribuyeron en buscar soluciones para fortalecer una Internet abierta extremo-a-extremo. El taller fue realizado mayormente en Español, y parcialmente en Inglés.

Agradecimientos a todos los que ayudaron a su realización, especialmente a Rafael Lito Ibarra y Miguel “Nacho” Estrada por su apoyo desde un comienzo. Y no podría haber funcionado sin el apoyo invaluable de Roberto Zambrana, Presidente del Capítulo Boliviano de ISOC, quien ayudó con todos los temas prácticos e invitaciones en Bolivia.

Maarten Botterman, el facilitador de GFCE Triple-I, inauguró el taller presentando a Lito Ibarra como su co-facilitador en idioma Español para el taller, honrando el hecho que la mayoría de los participantes eran más fluídos en Español que en Inglés. Lito comenzó explicando que nos estábamos reuniendo para construir capacidades. LACIGF es un buen lugar para organizar el evento GFCE e intercambiar información relacionada con seguridad en Internet. Invitó a los participantes a enfocarse en ideas, planes y oportunidades como resultados del evento, que podrían ser anotados en un rotafolio puesto a disposición por los organizadores. Destacó la presencia de las organizaciones de apoyo y agradeció a Roberto Zambrano de ISOC Bolivia por la organización del evento.

Iván Zambrana, el Vice-Ministro de Telecomunicaciones de Bolivia, dió la bienvenida a todos los participantes a La Paz y agradeció su esfuerzo. Indicó que Bolivia tiene un territorio extenso con una población relativamente baja, desafiada con problemas básicos como salud, educación medios de producción y otros derivados. Cree que la Internet es una buena herramienta para

abordar estos desafíos y espera que del taller surjan ideas sobre cómo implementarlas. Desde el punto de vista del gobierno, hay una necesidad de implementar rápidamente soluciones para el pueblo Boliviano para tomar ventaja de Internet, y mejorar su seguridad es un factor muy importante. Dijo que está listo para trabajar en conjunto y está seguro que los resultados del taller echará una buena mano para mejorar la vida de la gente en Bolivia. Maarten Botterman agradeció el discurso del Vice Ministro indicando que todos estamos en buenas manos con el Vice Ministro Iván Zambrana.

Maarten Botterman continuó los comentarios de apertura explicando que la Internet no se construyó para ser segura, sino para ser usada. El rol de GFCE es contribuir a una mejor infraestructura, logrando una Internet más limpia por medio de la reducción de los impactos de los ataques.

BLOQUE I – Mejor uso de los actuales Estándares Abiertos de Internet

Duurante el primer bloque el foco estuvo en el uso y la utilidad de Estándares Abiertos de Internet como DNSSEC/TLS/DANE, RPKI/ROA, DMARC/DKIM/SPF e IPv6. Estos estándares son aceptados globalmente y representar ideas de vanguardia que, cuando se aplican, pueden ayudar a reducir los riesgos al usar Internet y el correo electrónico, en la actualidad.

Daniel Fink (ICANN), Mauricio Oviedo (CEO SOCIUM) y Jannett Ibañez (ADSIB / NIC Bolivia) se enfocaron inicialmente en DNSSEC, como un estándar que ayuda a asegurar la integridad del origen en DNS. Daniel explicó cómo funciona actualmente el estándar, y qué era necesario para su uso. Otros tópicos relevantes en la implementación fueros discutidos por Mauricio Oviedo tales como los desafíos para firmar zonas de segundo nivel y cómo "adoptar un enfoque diferente" en su adopción. Mauricio indicó que es necesario disponer de más información en el idioma español para mejorar capacidades, y destacó que los administradores debieran tener más confianza y preparados para actuar en caso de fallas en las implementaciones. Hugo Salgado contribuyó indicando que existen buenas herramientas para automatizar la firma de zonas, pero que aún se necesita más tecnologías para monitorear los problemas con DNSSEC. Recomendó una herramienta escrita por NIC.br. Mauricio presentó la idea de crear laboratorios para aumentar la confianza de los administradores. Agregó que la alta rotación en las compañías puede también ser un desafío para la estabilidad de las implementaciones. Un representante de un ISP Boliviano informó que ellos tienen pocas zonas en operación, aún sin firmar. Por otro lado, ya implementaron DNSSEC en sus servidores recursivos. Su experiencia para superar la falta de confianza fue hacer pruebas en servidores experimentales antes de escalar a la operación real. Está de acuerdo que el miedo a enfrentar una falla de DNS es crítico. Jannett Ibañez presentó el bien estructurado plan de implementación DNSSEC para el ccTLD .BO. Desde el 2018 ADSIB / NIC Bolivia ha venido conduciendo sesiones de entrenamiento y talleres con expertos internacionales para preparar la implementación. Una buena práctica presentada por la Sra. Ibañez es el involucramiento de varias entidades de Bolivia en un estilo de múltiples partes

interesadas del plan desde un comienzo. Se presentó un cronograma sólido y se espera que la firma de .BO ocurra en Noviembre de 2019.

Lía Solis (LACNOG, ISOC Bolivia) habló acerca de DMARC, DKIM y SPF como estándares importantes para la integridad del correo electrónico (e-mail). Las recomendaciones de Lía buscan asegurar:

i. Adecuadas capacidades para lograr implementaciones exitosas;
ii. planificación y acciones con involucramiento de todos los interesados;
iii. confianza por diseño.

También presentó estadísticas de la adopción global de estos estándares que son publicadas en informes de Gmail. En la segunda parte de su presentación, Lía presentó IPv6 y los beneficios de su adopción tales como: Mejor conectividad, Soporte a la innovación, Reducción de costos (debido a la escasez de IPv4) y crecimiento económico. De acuerdo a su visión, los desafíos en la adopción de IPv6 en Bolivia pueden resumirse en recursos (humanos y financieros), la falsa percepción que no debería considerarse un problema, incompatibilidades en la infraestructura existente y una falsa percepción que NAT es una solución factible para la escasez de direcciones IPv4. La tasa de adopcion de IPv6 en Bolivia es ahora de 13.35. Durante su presentación, Lía recomendó que debieran crearse políticas que aceleren la adopción de IPv6, por ejemplo, agregar un requisito a los dueños de dominios de habilitar IPv6 cuando renueven sus cuentas. Las consolas de juego en línea, actualmente operando solo con servidores IPv4, también debieran considerar la adopción de IPv6 tan pronto como sea posible.

Gerardo Rada (LACNIC) presentó acerca de RPKI (Infraestructura de Llaves Públicas de Recursos), estándares que están enfocados para asegurar que el ruteo sea más seguro. Condujo un ejercicio interactivo para demostrar los posibles problemas en el ruteo BGP tales como el secuestro de un camino más corto o de una ruta más específica. Gerardo también discutió casos recientes de fallas de ruteo y presentó a ROA (Autorizaciones de Origen de Ruta) como una forma de promover la integridad del ruteo al tener rutas autorizadas por una instancia confiable. LACNIC desarrolló una herramienta para soportar estas implementaciones, que se encuentra ahora disponible.

BLOQUE II – Inspiración desde las acciones de buenas prácticas

En el segundo bloque del día, tuvimos presentaciones y debates sobre una serie de buenas prácticas globales y buenas prácticas de la región que se consideran potencialmente relevantes para el desarrollo de capacidades y para inspirar acciones en la región.

Trabajo Anti-abuse

El primer tema discutido fue el trabajo Anti-abuse. Lucimara Desiderá (Chair LAC AAWG; Miembro, M3AAWG) proporcionó antecedentes sobre el trabajo que se está realizando actualmente en la región y en todo el mundo, y explicó cómo otras partes interesadas pueden

beneficiarse de esto y contribuir a ello. El grupo de trabajo de mensajería, malware y grupo de trabajo contra el envío abusivo de mensajes móviles (M3AAWG) es una red internacional con el objetivo de reducir botnets, malware, spam, virus, ataques DoS y otros abusos en línea. M3AAWG pone a disposición documentos de mejores prácticas e información de abusos que podrían servir como un buen recurso para la acción local. Lucimara destacó que estos problemas de abuso son problemas globales que no pueden ser resueltos por actores individuales. Por lo tanto, recomendó un enfoque de grupo de trabajo de múltiples partes interesadas basado en la confianza y las colaboraciones, adoptado por M3AAWG como un buen procedimiento a seguir en la región, incluida la participación de más miembros regionales en M3AAWG. LAC AAWG es la iniciativa regional para enfocarse en esto.

Lucimara presentó el Programa Nacional de NIC.br "Por un Internet más seguro" en su calidad de Analista de Seguridad en CERT.br. En primera instancia, CERT.br se presentó como el organismo nacional para aumentar el nivel de seguridad y la capacidad de manejo de incidentes de las redes conectadas a Internet en Brasil. El incidente de Mirai comprometió el Equipo local del cliente (CPE) y Deutsche Telekom estuvo en la capacidad de remediar la actualización de firmware en solo 2 días. Desafortunadamente, la situación en la región de Latinoamérica y el Caribe es diferente, con más dispositivos CPEs heterogéneas y vulnerables implementadas por los ISP, lo que estaba creando un desafío sobre cómo recomendar mejores diseños a los fabricantes y/o compradores. Sebastian Bellagamba de ISOC señaló que los ISP suelen ser sensibles a los costos, donde unos pocos centavos podrían representar grandes ahorros en grandes compras de equipos. Lucimara estuvo de acuerdo, pero agregó que las consecuencias podrían ser mucho peores dado que algunos ataques tienen el potencial de simplemente destruir el firmware de los CPE y conlleva la necesidad de reemplazar todos los CPE en la red. La Iniciativa Nacional CERT.br para un programa de Internet más seguro abordó este desafío con los objetivos de:

- Reducir los ataques de denegación de servicio originados en redes brasileñas;
- Reducir el Prefix Hijacking, Route Leak, e IP Spoofing;
- Reducir las vulnerabilidades y fallas de configuración en los elementos de la red; y
- Crear una cultura de seguridad,
- Promover mejores prácticas tales como Hardening;
- Cerrar servicios abiertos,
- Implementar seguridad de enrutamiento y la suplantación de identidad (BCP 38).

La iniciativa fue promovida conjuntamente por NIC.br/CGI.br, ISOC e ISP, Hosting y Telco Asociación. Los resultados de esta iniciativa fueron alentadores con una reducción sustancial de los ataques nacionales. También recibieron reconocimiento internacional por el esfuerzo. M3AAWG y LACNOG publicaron los requisitos mínimos de seguridad para la adquisición de CPEs.

Israel Rosas (ISOC) hizo una presentación sobre las normas mutuamente acordadas para la seguridad del enrutamiento (MANRS), que es una campaña dirigida a la adopción de mejores prácticas para la prevención de incidentes de enrutamiento. MANRS mejora la seguridad y

confiabilidad del sistema global de enrutamiento de Internet, basado en la colaboración entre los participantes y la responsabilidad compartida de la infraestructura de Internet. Israel discutió los principales factores de motivación que llevaron a este llamado a la acción, como estadísticas de incidentes, titulares y ataques comunes. MANRS recomienda cuatro acciones simples pero concretas que los operadores de red deben implementar para mejorar la seguridad y confiabilidad de Internet:
1. Filtrado: previene la propagación de información de enrutamiento incorrecta
2. Anti-spoofing: previene el tráfico con direcciones IP de origen falsificadas
3. Coordinación: Facilita la comunicación operativa global y la coordinación entre operadores de red.
4. Validación global: facilitar la validación de la información de enrutamiento a escala global

Una buena discusión tuvo lugar durante este segmento con contribuciones de muchos participantes. MANRS podría usarse como un diferenciador competitivo y reducir la cantidad y el impacto de los incidentes de enrutamiento. Un representante de un ISP boliviano informó que ya están implementando las buenas prácticas. ISOC también ha estado promoviendo seminarios web para difundir información. Lía Solis e Israel Rosas ofrecieron colaboración a cualquier persona interesada en unirse a la iniciativa.

Después de eso, Daniel Fink informó sobre el proyecto de Informe de Actividad de Abuso de Dominio (DAAR) de ICANN. DAAR es una base de datos que informa sobre el registro de nombres de dominio y el comportamiento de amenazas de seguridad (abuso de dominio) en los registros y registradores de dominio de nivel superior (TLD). El sistema no está construido de ninguna manera para exigir el cumplimiento, sino para proporcionar transparencia sobre las debilidades en el DNS. La herramienta de informes está dirigida a la comunidad de ICANN, que luego puede usar los datos para facilitar decisiones informadas sobre políticas. DAAR proporciona a la comunidad de ICANN un conjunto de datos confiable, persistente y reproducible a partir del cual se puede realizar análisis de amenazas a la seguridad (abuso), y puede servir como una plataforma para estudiar o informar actividades de registro o abuso en forma diaria o histórica. Recopila datos de zona de TLDs, un gran conjunto de datos de registro, y complementa estos conjuntos de datos con un gran conjunto de fuentes de datos de reputación de alta confianza (amenaza de seguridad). Se publica un informe mensual en el sitio web de ICANN disponible gratuitamente para que las personas lo consulten. Como tal, incluye datos de dominios genéricos de nivel superior (gTLD) contratados por ICANN, pero también está abierto a trabajar con ccTLD voluntarios que estarán interesados en proporcionar datos para medir el comportamiento del TLD en el marco de DAAR. Los ccTLD interesados pueden comunicarse con ICANN para obtener más información sobre cómo proceder para unirse.

Collaboración CERT

Lucimara Desidera (miembro de CERT.br y FIRST), describió cuáles son hoy las preocupaciones y actividades claves del CERT, cómo pueden beneficiarse las partes interesadas y qué hacen

las partes interesadas para ayudar. Expuso que un equipo de respuesta a incidentes de seguridad informática (CSIRT) es una organización de servicio que es responsable de recibir, revisar y responder a los informes y actividades de incidentes de seguridad informática y sus servicios generalmente se realizan para una circunscripción definida que podría ser una entidad matriz, como una organización corporativa, gubernamental o educativa; una región o país; una red de investigación; o un cliente pagado. Un incidente es cualquier evento adverso real o sospechoso en relación con la seguridad de los sistemas informáticos o las redes informáticas. Internet ha crecido exponencialmente desde 1969, así como la ocurrencia de incidentes desde entonces. Se hizo imperativo que los CSIRTS trabajen en conjunto bajo los principios de objetivos comunes y confianza, algo que se construye y que no es obligatorio. Como recomendación a los gobiernos, Lucimara explicó que los CSIRTS no deberían crearse desde un enfoque de arriba hacia abajo y no deberían implementarse dentro de las agencias de inteligencia. Maarten agregó que hay ejemplos en los que los gobiernos jugaron un enfoque facilitador importante, por ejemplo creando un CERT gubernamental ejemplar, y le permitieron desempeñar un papel facilitador en la comunidad CSIRT (como la organización de reuniones y el intercambio de buenas prácticas), apoyando así el desarrollo de CSIRT de forma ascendente.

Despliegue seguro de IoT: ideas globales en el camino a seguir

Existe una gran necesidad de garantizar y mejorar la seguridad de los dispositivos IoT, ya que IoT se está convirtiendo en parte de la estructura de la sociedad, y nos volvemos cada vez más dependientes del funcionamiento de los ecosistemas de IoT. Hasta hace poco, las medidas de seguridad eran excepcionales, y a menudo insuficientes, pero ahora se están sensibilizando tanto los fabricantes como los usuarios (incluidos los gobiernos) de que se necesita mejorar, incluso a pesar de que signifique que el costo inicial para el despliegue de dispositivos se incremente. Otras partes interesadas en la cadena de valor también tienen un papel que desempeñar, como los proveedores de acceso que deben desarrollar y adoptar metodologías para detectar de manera temprana los intentos de abuso del acceso de dispositivos IoT a Internet. La discusión estuvo a cargo de Sebastián Bellagamba (Internet Society); Maarten Botterman (IGF DC IoT).

Sebastián presentó el Marco de confianza de IoT para privacidad y seguridad, diciendo que se espera que los dispositivos de IoT sean 5 veces la población mundial para 2022. Eso significa que nuevos jugadores se unirán a la red junto con riesgos de seguridad y preocupaciones de privacidad. Se identificó una lista de desafíos relacionados con fabricantes, servicios y consumidores. El marco de confianza requerirá una responsabilidad colectiva y es un trabajo en progreso que considera 40 principios estratégicos necesarios para abordar los problemas de seguridad, privacidad y ciclo de vida de IoT. Sebastian concluyó con actualizaciones sobre el trabajo actual, como iniciar procesos de múltiples partes interesadas en los países para la adopción del marco, señalando la reciente conclusión del proceso en Canadá disponible en https://iotsecurity2018.ca.

Maarten Botterman recordó el caso de Mozilla e ISOC que escribieron a Amazon pidiendo vender dispositivos IoT con niveles mínimos de seguridad. Señaló el trabajo de DC IoT en Building Global Trust en Internet of Things, explicando que Internet of Things Good Practice tiene como objetivo

desarrollar sistemas, productos y servicios de IoT teniendo en cuenta consideraciones éticas desde el principio, tanto en el desarrollo, implementación y uso fases del ciclo de vida, para encontrar un camino ético y sostenible con IoT para ayudar a crear un entorno libre, seguro y propicio basado en los derechos: un futuro que queremos.

Contribuciones flash: otras prácticas ejemplares

Hugo Salgado Hernández (NIC Chile / LACTLD) presentó Anycast Cloud de LACTLD, una actualización de la cooperación previa entre las operaciones regionales de ccTLD que ofrece características de mayor capacidad de recuperación y escalabilidad. Anycast puede ayudar a reducir el impacto de los ataques DDoS (cuando un servidor está sobrecargado con solicitudes y bloqueos) a través de un mejor equilibrio de carga haciendo uso de otras rutas y servidores. Con anycast, las solicitudes se responden en otras ubicaciones durante la mitigación y la recuperación. La nube Anycast está disponible para todos los ccTLDs de la región LAC para hospedar sus zonas, y para todos los ISPs/IXPs que quieran hospedar un nodo en sus instalaciones y así utilizarla nube para sus propios servicios y ahorrar costos con una administración compartida. Las operaciones comenzaron en 2015 al servicio de 8 ccTLD en la región de LAC y 7 instancias de trabajo en todo el continente. El proyecto está creciendo para agregar nuevos ccTLD y expandir instancias de difusión ilimitada en otras regiones, como Europa y EE. UU. Hugo concluyó mencionando que este es un buen ejemplo del mejor uso de la tecnología para ahorrar costos, integrar la región y brindar un mejor servicio a los usuarios.

Después de la presentación de Hugo, Maarten Botterman presentó la herramienta de prueba de cumplimiento en Internet.nl (desarrollada por NLnet Labs y los estándares holandeses de Internet de la plataforma). Internet.nl es una forma fácil y amigable para el usuario para probar la adopción de estándares con la prueba de cumplimiento, exclusivamente estándares de seguridad, y proporcionar sugerencias para posibles mejoras. Fue creado para ser una herramienta a demanda dirigida por el usuario que cualquiera puede usar para probar sus conexiones. Las pruebas cubren mediciones en conexión, web y correo electrónico. Maarten mostró algunas características de la herramienta con ejemplos de capturas de pantalla. Las pruebas por lotes están disponibles para evaluaciones grandes, que, por ejemplo, permitirían enviar una lista de direcciones web de todos los servicios gubernamentales en un país. La herramienta está actualmente disponible en holandés e inglés en www.internet.nl, y el código está disponible como código abierto para que pueda aplicarse, regionalmente, en contexto regional e idiomas adicionales. Sin embargo, esto requeriría una acción local para implementar el código fuente en una configuración local. Una herramienta fantástica de hecho.

Bloque III: Planificación para una Internet más confiable: Marketplace para la acción

Durante este bloque, se delinearon conclusiones y posibles acciones destinadas a aumentar la confianza en el uso de Internet y el correo electrónico en la región. La discusión fue facilitada por Maarten Botterman y Lito Ibarra. Lito comenzó estableciendo que existe la posibilidad de que las soluciones para los problemas que enfrentamos ya existen. Invitó a miembros de organizaciones a expresar sus ideas. Ernesto Bojorquez, presidente de LACTLD, agradeció el taller y agradeció el formato del evento donde pudimos construir relaciones de confianza para futuras colaboraciones. Predijo que esta iniciativa podría tener grandes impactos y destacó la importancia de todos los estándares que se discutieron. Sebastian Bellagamba, Director Regional para América Latina y el Caribe de ISOC, explicó que Internet es una red de redes con un valor inmenso para la sociedad. Este valor debe ser protegido y esta labor es para las fuerzas conjuntas. Eventos como este taller GFCE Triple-I, que reúne a múltiples partes interesadas para discutir diferentes aspectos de las actividades relacionadas con Internet que se relacionan entre sí y que requieren acción, son increíblemente importantes. Nacho Estrada (LACTLD) dijo que los silos deben romperse y estos eventos ayudan, y deben repetirse en otras comunidades. Mauricio Oviedo expresó su preocupación por los malos actores que están trabajando activamente, en la actualidad, para explorar vulnerabilidades. Él cree en compartir experiencias y la creación de una cadena de confianza, y también llamo a la acción.

ACCIÓN PROPUESTA: establecer más talleres del tipo GFCE Triple-I en la región

Los usuarios deberían preferir comprar equipos de mejor calidad y los gobiernos deberían tener formas de homologar los dispositivos WiFi e IoT. Ayudar a los usuarios a comprender lo que obtienen, en términos de soporte de seguridad, y cómo garantizar que sea como se indica, requiere etiquetado y certificación. Lucimara agregó que es difícil homologar el software en esos equipos y que las certificaciones podrían crear una falsa percepción de seguridad. Su recomendación es pensar en procesos para garantizar la seguridad en esos equipos y estar preparado para incidentes de forma permanente. Sebastián agregó que los procesos de certificación en la actualidad son diferentes de los utilizados en el pasado. Hay muchos más fabricantes y más productos disponibles en estos días.

ACCIÓN PROPUESTA: planificar mejores formas de informar a los usuarios sobre los riesgos relacionados con los dispositivos y cómo lidiar con esto. La colaboración en el marco de acción de ISOC puede ser un buen comienzo

Un miembro de ISOC Bolivia solicitó una herramienta para medir la calidad de la velocidad de Internet y comparar la banda ancha en Bolivia con otros países, para informar la formulación de políticas. Las conexiones a Internet en Bolivia se perciben como lentas, principalmente debido a configuraciones incorrectas y acceso no autorizado de otros usuarios a las conexiones. Además, en las edificaciones densamente poblados se enfrentan a la falta de canales de 2.4 GHz.

ACCIÓN PROPUESTA: *analizar la situación real con respecto a la velocidad de Internet, para informar la acción cuando sea útil o necesario.*

Un miembro del sector privado informó que está trabajando en un clúster de innovación y cree que las tecnologías discutidas durante el taller deberían compartirse con las nuevas empresas de tecnología bolivianas. Lito Ibarra agregó que los usuarios tienen poca conciencia sobre estos temas y que las personas no se ven a sí mismas como posibles objetivos de ataques en línea. A la pregunta de qué se puede hacer para crear más conciencia en los ciudadanos. Un participante de Ecuador informó que durante la reciente entrega de Julian Assange de la Embajada de Ecuador a las autoridades, se publicaron varias amenazas (y se comentaron en la prensa) contra Ecuador, lo que generó preocupaciones de la población en general. Según él, la información de los medios no estaba lo suficientemente bien fundados, como para proporcionar una orientación adecuada a las personas. Lía Solis destacó la importancia de la participación en foros de Gobernanza de Internet y el tema de la seguridad es transversal a todas las discusiones. Los usuarios deben tener cuidado de su poder y ser más conscientes.

Un participante dijo que le gustaría socializar estos temas con la ayuda del viceministro boliviano, Iván Zambrana, quien asistió a la mayor parte del taller, con gran interés. Sería muy importante compartir los requisitos mínimos con las empresas locales. Otro participante de Bolivia preguntó si sería más importante educar a la población o al sector privado. El creía que, por seguridad, el sector privado debería ser una prioridad en los programas educativos. Y como parte de la responsabilidad social, las empresas deben educar a sus clientes sobre la ciberseguridad. Educar a la población podría ser una de las formas de responsabilidad social que las empresas podrían adoptar. Los periodistas y los medios de comunicación deben participar en estas actividades.

ACCION PROPUESTA: organizarse para crear las campañas de sensibilización necesarias e incluir el pensamiento de seguridad desde el principio en la curricula educativa

Oportunidades de rotafolio

Además, surgieron durante el día varias ideas para llevar adelante. Si bien no hubo un compromiso explícito de acción, el interés de participar en uno o más de estos temas se expresó explícitamente:

- DNSSEC:
  - Creación de plataformas para probar y monitorear implementaciones de DNSSEC;
  - Fomentar la validación de DNSSEC en los ISP
- Automatizar los procesos de firma de zona
- ISP y empresas / organizaciones para crear ROA para RPKI
- Hacer conocer y promover las mejores prácticas operativas actuales (BCOPs) en equipos de instalaciones del cliente (CPE) para seguridad (en inglés y español);

- MANRS:
    - Participar en las reuniones de LAC AAWG;
    - Implementar MANRS si administra un ASN
- Alojar un nodo Anycast de LACTLD
- Probar los dominios sobre la actualización de los protocolos utilizados en www.Internet.nl
- Discutir y enumerar las normas que deben adoptar los gobiernos y otras organizaciones.
- Implementar una iniciativa de marca de confianza para garantizar la implementación segura de IoT, considerar la certificación de dispositivos IoT antes de que se permitan en las plataformas de ventas (considerando la seguridad y el firmware);
- Desarrollar normas de calidad y mediciones para conexiones a Internet;
- Mantener y aumentar la colaboración entre países, organizaciones y personas, y en todos los sectores, y desarrollar una comprensión clara de los roles para hacer de Internet un lugar más confiable para los usuarios;.

Al final del taller, el anfitrión chileno de LACIGF2020 invitó al taller GFCE Triple-I a formar parte de LACIGF2020.

For more information about GFCE Triple-I, including results of earlier events, please go to the. If you are interested in improving the trusted Internet experience in your region. Para obtener más información sobre GFCE Triple-I, incluidos los resultados de eventos anteriores, vaya a las GFCE Triple-I pages. Si está interesado en mejorar la experiencia confiable de Internet en su región.

-=(O)=-