

Relatoria LACIGF 12

Título da sessão: Sessão 9 – TEMA INTERSETORIAL – SETOR COMUNIDADE TÉCNICA: Segurança na Internet sob uma abordagem multi-participativa: diferentes realidades, desafios comuns e ferramentas convergentes

Resumo da sessão:

A sessão foi moderada por **Ernesto Majó (LACNIC, Uruguai)** e **Ernesto Bojórquez (LACTLD, México)**. **Ernesto Majó** começou com uma breve introdução conceitual sobre o tema da sessão, inicialmente mencionando que o conceito de segurança, hoje em dia, é muito mais amplo e chega a tomar distintas dimensões, entre elas a estabilidade e resiliência da Internet, as capacidades humanas e a infraestrutura. Ele crê que a dimensão humana é um fator imprescindível, do mesmo modo que a colaboração, que também considera como essencial para entender os desafios do campo. Ao mesmo tempo, mostrou um infográfico do ecossistema de Internet para dar visibilidade à complexidade e aos diversos atores que participam, cada um com várias responsabilidades. Também mencionou que, para alcançar uma Internet mais segura, nosso alcance é limitado devido a sua natureza, e que a Internet se encontra enquadrada no conceito central da cooperação, e devemos resolver o conjunto das problemáticas e trabalhar de forma conjunta para encontrar soluções.

Posteriormente à introdução, convidou-se o público a trabalhar em quatro grupos de trabalho, segundo os atores participantes:

- Comunidade Técnica;
- Sociedade Civil;
- Setor Empresarial;
- Setor Governamental.

Cada grupo deveria contribuir respondendo à dois questionamentos:

- Quais são as iniciativas ou protocolos para identificar os desafios da segurança?
- Levantar temas críticos e ferramentas ou protocolos que desenvolvemos.

Depois, cada grupo fez uma pequena apresentação sobre o debate realizado.

A apresentação do grupo da comunidade técnica foi realizada por **Sebastián Bellagamba (Internet Society, Uruguai)**, na qual ele comentou alguns dos temas que identificaram, dentre eles a conectividade, a confiança na Internet e a segurança.

Os desafios associados a esses temas, podem ser divididos em três partes:

1. Inicialmente associado ao PGP e à segurança da Internet, e como assegurar protocolos por padrão na transferência de pacotes para maior segurança;
2. Por outro lado, o tema da implementação de IoT e como lidar com o desconhecimento da segurança de redes dos fabricantes desses produtos;
3. Por último, o que se refere a fragmentação da Internet e seu impacto, que pode ter resultado tanto positivo como negativo.

Sobre o último ponto em particular, Bellagamba mencionou que a ISOC realizou um estudo sobre a consolidação nos segmentos de Internet, entre eles o mais discutido foi o da camada de serviços. Hoje em dia, a quantidade de serviços é incontável, visto que o custo de inovação é reduzido pelos provedores de nuvem em comparação a outras camadas.

Em coletivo foram listados os desafios que acreditam ser pertinentes:

- Vulnerabilidade de domínios DNS;
- Roteamento;
- Falta de coordenação entre a comunidade técnica;
- Assegurar a integridade da informação;
- Regulação;
- MANRS (Como levar nós de redes à instâncias nacionais e regionais?);
- Impossibilidade de rastreabilidade da implementação de IPv4;
- Necessidade de trabalhar na criação de capacidades.

Também apresentaram uma lista de ferramentas e projetos identificados pela comunidade técnica para contribuir com a segurança:

- OTA (*Over The Air*): a programação por ar se refere à vários métodos para distribuir software novo, ajustes de configuração e inclusive atualizar chaves de criptografia para dispositivos como telefones celulares, decodificadores ou equipamentos de comunicação de voz seguros;
- RPKI: emissão de material criptográfico que permita aos membros do LACNIC demonstrar digitalmente que possuem o direito de uso de endereços IPv4 e IPv6;
- CSIRTs: significa *Computer Security Incident Response Team*;
- BGP (*Border Gateway Protocol*): em telecomunicações, BGP é um protocolo mediante o qual se troca informação de encaminhamento ou roteamento entre sistemas autônomos.

Andrés Sastre (ASIET, Uruguai) fez a apresentação pelo setor privado. Em seu grupo de trabalho foram identificados os seguintes desafios:

- Falha de mecanismos de diálogo entre público e privado;
- Grandes exigências por parte do estado;
- Falta de inovação por parte das empresas;
- Falta de confiança e mau uso da navegação segura;
- Falta de disponibilidade de produtos na rede.

Algumas soluções propostas por esse grupo foram:

- Exigência de mínimos, por parte da indústria, em termos amplos;
- Educação digital para combater a desconfiança.

Julián Casasbuenas (Association for Progressive Communications - APC e Colnodo, Colômbia) apresentou a discussão feita no grupo de trabalho da sociedade civil. Inicialmente, identificaram alguns desafios de segurança na sociedade civil:

1. Apropriação Digital / Educação em temas de segurança digital e proteção de seus dados: identifica-se um grande desconhecimento da sociedade em geral em temas de segurança. Recomenda-se iniciar na educação primária para formar desde a primeira infância em segurança digital, convidando a escola a participar;

2. Incidir em políticas públicas através da sociedade civil, ser mais proativos do que reativos. Trabalhar com as múltiplas partes interessadas para a construção de regulações e políticas públicas que possam ser compartilhadas com toda a sociedade para receber também seus comentários;
3. Investimento em segurança e construção participativa;
4. Estabelecer proporcionalidade em temas de segurança e vigilância nos países da América Latina.

Algumas iniciativas propostas pelo grupo de trabalho:

1. Programas de proteção em segurança;
2. Alfabetização digital oferecidas pelos governos e todos os setores com maior atenção na educação básica;
3. Programas sustentáveis com continuidade;
4. Compartilhar experiências e materiais, usando as plataformas que integramos.

Alejandra Erramuspe (AGESIC, Uruguai) e Juan Cayoja Cortez (UMSA, Bolívia) foram os responsáveis por apresentar a discussão do setor governamental. O setor se dividiu em 2 grupos. Um grupo, por um lado, propôs gerar medidas e disposições legais, que permitam a formação de novos especialistas e produzam uma cultura de segurança. Por outro lado, o segundo grupo mencionou a necessidade de estabelecer marcos jurídicos, a partir do conhecimento das experiências de distintos países.

Ao finalizar as conclusões de cada grupo, o moderador principal Ernesto Bojórquez, fez a seguinte pergunta ao público: Como crêem que os diferentes setores poderiam colaborar para enfrentar os desafios propostos?

Vários participantes se aproximaram do microfone para realizar sua intervenção. Compartilhou-se experiências de países como Peru, Uruguai e Colômbia. Também se mencionou a importância e a responsabilidade dos governos por manter a continuidade nas políticas públicas, para além das mudanças de governo.

Outputs e outros links relevantes:

Sessão completa em: <https://www.youtube.com/watch?v=wlipzllXLxo>

Por: Raysa Alanes (Las De Sistemas, Argentina) e Juliana Novaes (Artigo 19, Brasil)

Traduzido por: Amanda Lemos (UnB, Brasil)

Revisado por: David Paredes Abanto (DIDEPTI SRL, Perú)

Coordenação e edição: Nathalia Sautchuk Patrício (NIC.br, Brasil) e Guilherme Alves (Youth Observatory, Brasil)