Foro de Gobernanza 2019 El Salvador
Relatoría de la Canasta de Seguridad
Ciberseguridad en empresas, instituciones y organizaciones salvadoreñas

Moderador: Francisco Moreno
Relatora: Thelma Lizbeth Rivas

I. Internet para los salvadoreños
- Es una ventana facilitadora de información
- Es una maravilla
- Internet es como la muralla china, al buscar información solo retiramos un ladrillo y podemos ver lo que hay tras de ella.

II. Riesgos para el internauta salvadoreño
- Como ciudadanos salvadoreños, no estamos disfrutando de los beneficios de Internet como lo hacen otros países, ya que no hay en El Salvador verdadera digitalización.
- Internet también demanda responsabilidades, por eso requiere una etapa de aprendizaje; muchos de nosotros somos analfabetas en Internet, por eso estamos expuestos a riesgos.
- Las condiciones de uso de seguridad de las aplicaciones y servicios en Internet no dejan de dar miedo, debido a las experiencias negativas que se han tenido al usar algunos servicios electrónicos.
- Muchas veces los usuarios ceden a brindar sus datos personales porque hasta cierto punto se les obliga, como en el caso de los préstamos bancarios.
- Troles: Ante un hostigamiento por parte de un trol, no se debe responder, no en el mismo nivel, pero sí debe hacerle ver que no es correcto lo que está haciendo, a nivel informático se puede rastrear el dispositivo utilizado por el trol.

III. La identidad digital, firma electrónica y protección de datos
- El problema de la implementación de la firma electrónica es el costo del certificado digital que valida la firma y aún haciendo uso de ella, si la persona lo permite es posible suplantar su identidad cuando ella brinda su código.
- En El Salvador hubo un interno de crear un CSIRT (Computer Security Incident Response Team) a nivel nacional, pero no se consolidó.
- Quien debería atender los temas en relación a la violación de datos personales, legalmente debería ser una comisión especial amparada bajo la Ley de Delitos Informáticos.

IV. Ciberdelitos y abuso en manejo de información
- Tipos de ciberdelitos: Robo de identidad, ciberfraude, ciberbullying, DDOS, suplantación de identidad, ransomware.

- Uno de los ransomware más conocidos es Wannacry el cual hizo destrozos en Colombia, a pesar que ellos cuentan con un CERT (Computer Emergency Response Team), fue especialmente desastroso en aquellas entidades que no contaban con respaldo en papel ni en medios magnéticos. Este ransomware también afectó a muchas entidades en el país.
- ICANN contrarrestó una amenaza de Anonymus, haciendo más robusta la estructura repartiendo copias del servidor raíz a nivel mundial.
- ICANN también capacita a las agencias de justicia de diferentes países para que conozcan los temas de Ciberdelitos.
- Casos de robo de información: Wikileaks, Ashley Madison, Facebook-Cambridge Analytica.
- ¿Qué pueden hacer con nuestra información en Internet? Venderla, suplantar información, vaciar cuentas bancarias, obtener más víctimas.
- Medidas que debería tomar un Gobierno para notificar robo de certificados masivos:
  - No cerrar el sistema, mantener un respaldo para ser evaluado.
  - La información sigue siendo de cada persona, no es del Gobierno.
  - La responsabilidad es amplia y pueden haber personas afectadas de diferentes partes del mundo.
- Hay pocos jueces especializados en delitos informáticos, pocos investigadores en la policía y la fiscalía para que un incidente de seguridad informática sea contrarrestada.
- La universalidad de Internet permite que hayan más delincuentes y más “peces que capturar”.

V. <u>Regulaciones y educación en ciberseguridad</u>

- Utilizamos muchas plataformas cuyos términos y condiciones se regulan por legislaciones internacionales.
- La Ley de Delitos Informáticos de El Salvador debido a su redacción se presta a diversas interpretaciones sobre lo que conlleva un delito.
- Deberían existir legislaciones para las cookies que autorizamos.
- Se necesitan leyes claras que obliguen a las personas que manejan datos de los ciudadanos a que no puedan hacer uso de los datos fuera del país.
- Se debe saber que nuestra información está en muchas partes, por ejemplo, cuando se va a votar, en el ISSS, en AFP, por eso se debe tener como base la legislación para saber a qué tengo derecho.
- Debe dotarse de vida a las leyes existentes, para lo cual debe existir un ente regulador y alguien que haga ejercer la ley, integrado con abogados y auditores para ejecutar la política para saber cuáles serán las sanciones. El regulador debe estar empapado del ecosistema y a partir de ahí la regulación puede ser mejor.
- A nivel de las instituciones deben existir procedimientos, políticas, controles de mantenimiento, auditorías, rotación de personal, sensibilización con el personal y en los contratos debe estar regida la fuga de información, pero esto debe monitorearse.

- Es importante la labor multisectorial, el sector tecnológico y legal no deben estar separados.
- La ignorancia que se tiene, sobre lo que viene y lo que está en el ámbito legal de la tecnología es porque ha faltado difusión y enseñanza, por esto es importante que se brinde un seguimiento a la formación en estas temáticas para la población salvadoreña.
- En cada entidad existen políticas técnicas para seguridad.
- ¿Cuál debe ser el criterio para abrir el contenido de un correo electrónico? La confianza se basa en la desconfianza, por eso es mejor preguntar a la persona de la cual recibo un correo si de verdad me envió el archivo.
- Se pueden prevenir los riesgos de seguridad aplicando nuestras propias medidas de seguridad, muchas de las cuales podemos encontrar en las plataformas que utilizamos: envío de mensajes de texto, notificación emergente de cambio de sesión, recordatorio de cambio de contraseña, entre otras.
- Que el gobierno salvadoreño a través de las escuelas pueda crear capacitaciones sobre buenas prácticas del uso de Internet.
- Es necesario conocer la seguridad informática desde la educación básica hasta la educación superior, porque es algo que vivimos a diario.
- Es necesario que se eduque a la población sobre la información que se comparte. Es difícil negar información pero se puede evitar compartir cierta información.
- Se debe educar en el uso de las tecnologías y enseñar el manejo y protección de nuestra información.