Foro de Gobernanza 2018 El Salvador
Relatoría de la Canasta de Seguridad

Moderador: Nelson Chacón
Relatora: Sara Aguilar

Se hizo la presentación del moderador y relatora. La mesa estuvo compuesta por 12 personas a las cuales se les presentó los temas propuestos, así como se pidió su participación, en proponer temas de interés para el foro, o cambiar el orden propuesto por el moderador. Los temas propuestos fueron:

- Atención a incidentes de alcance nacional
- Protección de Datos Personales
- Protección de Infraestructura crítica nacional
- Seguridad y Redes Sociales
- Ciberdefensa
- Cifrado
- Correo no deseado
- Firmas digitales
- Seguridad infantil en línea

Propuestas de temas a discutir por parte de los participantes: 12 personas

- ✓ Seguridad de datos personales
- ✓ Protección en seguridad de las mujeres en línea
- ✓ Implementación de políticas en la educación para impulsar la seguridad de jóvenes y niños
- ✓ Ley de Delitos Informáticos en El Salvador y su aplicación
- ✓ Alfabetización digital
- ✓ Protección, Políticas de Ciber Seguridad
- ✓ Noticias falsas (Trolles)
- ✓ El papel más activo del centro de respuestas informáticos que ayudan a los gobiernos a resolver problemáticas de índole nacional regulados por la OEA
- ✓ Grupos que briden capacidad de conocimientos a todos los demás (searchs) se busca que sea una entidad u organismo público que brinde apoyo a nivel de país (caso Colombia),
- ✓ Vigencia efectiva de las leyes aprobadas (firma y delito)
- ✓ Protección de los Derechos de los Consumidores en el internet no es efectivo (casos de salud), Falta de conocimiento en la población
- ✓ Mecanismos de prevención de la violencia
- ✓ Seguridad en transacciones en línea (confianza del consumidor)
- ✓ Ciber investigaciones, pertinencia de investigaciones personales a delincuentes

- ✓ Ciber extorsión
- ✓ Criptomonedas manejo a nivel personal brokers.

Se observó como un común denominador el interés sobre el tema de leyes, y delitos informáticos, por lo que se realizó un pequeño giro a la agenda propuesta y se enfocó el primer tema en la ley de delitos informáticos.

Preguntas del moderador:

¿Sabían de la existencia de la Ley de los Ciber delitos?

Comentarios sobre su existencia:

Algunos participantes conocían de la existencia de la ley pero no la habían leído, es decir desconocían su contenido, los que habían tenido algún tipo de lectura de la misma, ya que algunos de los participantes en el mismo momento la estaban leyendo acotaron:

- ✓ Es muy técnica
- ✓ De carácter general
- ✓ Se debe incorporar delitos más delimitados (protección de las mujeres, niños y adolescentes)
- ✓ Debería de promoverse la creación de instituto de rehabilitación para víctimas de ciber ataques.

Por lo que el moderador hizo énfasis sobre la necesidad de leer esta ley, ya que según el Art. 8 del Código Civil- dice que nadie puede aludir desconocimiento de la ley, por lo que es importante conocer la ley para no caer en delitos.

Hay un avance significativo de nuestra ley en esta materia ya que se retomó de buena parte del Convenio de Budapest quien supone la máxima fuente de legislación en esta materia de ciber ataques aunque nuestra legislación interna aún tiene sus vacíos.

Algunos de esos vacíos es que la ley no puede obligar a los proveedores a dar información a los consumidores; tampoco la FGR puede obligar a los ISP a dar registros de conexión, por ejemplo los bancos tampoco están obligados a brindar información sobre sus registros, hay otros medios por los cuales se busca la colaboración en estos casos y esta es actuar por “buena fe”.

Otro de los vacíos de esta ley es que en el capítulo 4 sólo se habla de regulaciones para mujeres y niños por lo que se deja de fuera a hombres, se debe ser más inclusivo.

La escuela debe de ser un instrumento para controlar delitos y no un centro para cometerlos. Debido al acceso de herramientas tecnológicas que tienen los niños las

escuelas se convierten en centros de delito, debido a la falta de concientización de la correcta utilización de estas herramientas.

Falta la divulgación sobre la existencia y aplicación de la misma de la ley. Otra de las debilidades en esta materia es que existe poca confianza en el sistema judicial para aplicar la ley y es debido a eso que las personas o instituciones prefieren no iniciar procesos judiciales (Estadísticas del año 2017, 147 casos son presentados como denuncias, 20 pasan a la etapa de instrucción, ninguna resolución fue condenatoria).

Hay un profundo desconocimiento de la ley en primer lugar, la normativa y reglamento de esta ley no la poseemos y por lo mismo podemos quebrantarla sin saberlo (por ejemplo en casos de replicación de la información) pero se debe recordar que no se puede argumentar desconocimiento de la ley.

Instituciones a las que se puede abocar para la denuncia de estos delitos son: Unidad de Delitos Especializados de la PNC y la FGR.

Conclusiones:

1. Es necesario que se eduque a la ciudadanía en general sobre el tema de delitos informáticos
2. Que se cree un programa de educación escolar, ya que los menores pueden ser los más vulnerables a cometer o ser víctimas de delitos informáticos.
3. Como profesionales de TI debemos conocer los riesgos que nuestra profesión conlleva y uno de ellos es el delito informático por una mala manipulación de la información o la gestión de incidentes.

¿Qué tipo de control debemos tener con nuestros datos personales?

La venta de base de datos puede ser tomado como algo positivo pero también posee sus desventajas, por un lado las ofertas que podemos recibir de nuestro interés pero también por otro lado es peligroso que tengan los datos de mis préstamos, ingresos etc.

Que posean nuestros datos personales nos afecta ya que vulnera nuestro derecho a la intimidad y privacidad.

En tema de redes sociales, se debe ser cauteloso con las actividades que publicamos ya que estamos siendo tipificados por gustos, edades etc.

Cuando ofrecen tarjetas de crédito de otros niveles es porque nuestra información está siendo divulgada.

La videovigilancia ¿es positiva o negativa? Hay una delgada línea entre vigilancia y la privacidad.

La confidencialidad es un tema complejo.

¿Los programas nos controlan? Existen otros medios que pueden sustituir a estos medios sociales que divulgan nuestra información pero no los usamos ya que nosotros los usuarios estamos consintiendo esta usurpación de privacidad y estamos acomodados.

La alfabetización tecnológica debe ser implementada desde edades tempranas.

Debemos agilizar los mecanismos para reducir la brecha digital, y ser más precavidos con lo que firmamos y aceptamos ya que no leemos las cláusulas y sólo aceptamos.

Las bases de información están presentes en tarjetas de crédito, aplicaciones, foros etc.

Se debe tener una culturización y sensibilización sobre lo que nos conviene y no nos conviene, pero que sin embargo la sociedad nos empuja a utilizar para ser aceptados, eso es un reflejo de vacíos personales.

En el año 2003 a través de ASPROC se presentó un amparo a la Sala de lo Constitucional sobre una empresa que tenía una base de datos ilegal, pero la Sala desestimó esta denuncia ya que esta organización no tenía la facultad para defender los derechos de estas personas. Las personas deberíamos hacer uso de los mecanismos que proporciona la ley y conocer que nuestros derechos están siendo vulnerados. Pareciera que lo material pesa más que lo inmaterial (derechos.) La demanda no procedió debido a que ASPROC no está apta para poder abogar por los derechos generales de los ciudadanos.

El instituto de acceso a la información pública está tratando de proteger la información médica de las personas, esto representa un avance en el acceso de la información pública, pero sólo atañe a las entidades públicas, a las empresas privadas nadie las supervisa.

Las mismas compañías nos globalizan para seguir consumiendo y siendo usuario de ciertas redes sociales como condición para usar otras. Por ejemplo al querer utilizar ciertas aplicaciones se debe tener cuenta en otras redes sociales obligatoriamente para acceder a ellas.

La seguridad debe ser parte de la educación que se debe tener – se cita un libro “el control de tu vida personal y tu vida digital”

Conclusiones finales:

- ✓ Es necesario que como sociedad civil exijamos una Ley de Protección a los datos personales.
- ✓ Por desconocimiento los DTI podemos incurrir a un delito.
- ✓ La Unión Europea está trabajando en Mecanismo de Protección de Datos Personales. Esto tiene como consecuencia que si en las empresas tienen empleados o tenemos ciudadanos pertenecientes a la Unión Europea estamos obligados a darle cumplimiento a esa ley. Representa uno de los máximos avances en la protección de personas sobre esta materia.