Generalidades de la Regulación en Ciberseguridad en los Estados Miembros de COMTELCA

III Foro Regional sobre Interconectividad, Ciberseguridad e IPv6.

Visión General

Fred L. Clark, M. Sc.

Superintendencia de Telecomunicaciones, Guatemala

Estados miembros de COMTELCA

- Los Estados miembros de la Comisión de Telecomunicaciones de Centroamérica, COMTELCA; son:
- Costa Rica;
- El Salvador;
- Guatemala;
- Honduras;
- Nicaragua;
- Panamá;
- República Dominicana.

De todos los Estados miembros

- Se cuenta con Centros de Respuesta a Incidentes de Seguridad Cibernética en:
- Guatemala
- Costa Rica
- Panamá.
- Y con legislación especializada en Cibercrimen en Costa Rica y en República Dominicana, en donde en sus Códigos Penales están tipificados varios delitos.
- Y con iniciativas de Ley de Cibercrimen en Costa Rica, Guatemala, Panamá y República Dominicana.

Antecedentes

- “La cadena se rompe por el eslabón más frágil”.
  - Este adagio se puede aplicar a la situación de la Ciberseguridad de los países de la Región Centroamericana.
  - La falta de cultura sobre seguridad informática, es uno de los principales obstáculos al momento de intentar implementar una política nacional de seguridad informática.
  - La mayoría de incidentes son escondidos, desvanecidos o ignorados, en diferentes estructuras: Industria y gobierno.
  - Hacer públicos estos hechos podría representar una pérdida de confianza y de clientes, en el caso privado y un despido o desprestigio en el caso del gobierno, por lo que priva el ocultamiento y la negación.

Antecedentes

- En la región centroamericana y el caribe, desde el año 2006 se han llevado a cabo distintos esfuerzos para promover un ecosistema menos vulnerable en nuestros países a través de:
  - Talleres de capacitación para formar Centros de Respuesta a Incidentes de Seguridad Cibernética;
  - Formación de personal identificado de instituciones clave;
  - Talleres de simulación de ataques y situaciones;
  - Cooperación técnica en la elaboración de proyectos de Ley que permitan la persecución de delitos informáticos;
  - Uso de estándares reconocidos;
  - Concientización de instituciones y empresas en aspectos de seguridad informática.

Antecedentes

- A pesar de toda esta cooperación por un largo período de tiempo, aún no se han producido los resultados óptimos.
- Hace falta formar esa masa crítica necesaria para impulsar acciones que puedan reconocerse a nivel nacional.
- Cada año que pasa se hace más necesario contar con legislación adecuada y especializada en el tema de Ciberseguridad.
- Pues cada año se producen más incidentes.

Definiciones:

- **Infraestructura Crítica:**
  - Son aquellas que proporcionan servicios esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
  - “Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas“.
  - *http://www.cnpic-es.es*

Definiciones:

- **Amenazas:**
- *“aquellos elementos que son peligrosos al hombre, instalaciones o patrimonio y que están causadas por fuerzas extrañas o conocidas».*
- **Riesgos:**
- *“la probabilidad de que una amenaza se convierta en un desastre, con graves consecuencias económicas, sociales y ambientales“.*
- **Vulnerabilidades:**
- *“conjunto de condiciones y procesos que se generan por efecto o defecto de factores físicos, tecnológicos, sociales, económicos y ambientales que aumentan la posibilidad de que personas, instalaciones o bienes puedan ser susceptibles de sufrir daños frente al impacto de los peligros o amenazas”.*

Origen:


PIRÁMIDE DE LAS AMENAZAS CIBERNÉTICAS — 2013
Estados
vs.
Estados
Ataques de
ciberespionaje corporativo
y "spyware de policía"
Ataques a usuarios communes y corrientes
por parte de criminales cibernéticos

Ciberespacio:

- *“Debe tenerse presente que, jurídicamente, territorio no es sinónimo de espacio geográfico, debido a que el territorio comprende todos los lugares a los que se extiende la soberanía del Estado, lo que debe incluir las redes, sistemas y ordenadores vinculados al Estado en el cual ocurre el incidente”.*

Ámbito de aplicación de una Ley de Cibercrimen

- Tomamos como base la Convención de Budapest sobre el Cibercrimen, de 2004.
- Dentro del territorio nacional;
- Desde el extranjero;
- Medios ubicados en el país;
- Cuando se caracterice complicidad desde el territorio en donde se origina el ataque.

Delito Informático

- *"…se realiza por medio de un **sistema** que haga uso de las tecnologías de la información o un componente de éste, que lesione la **integridad**, **disponibilidad** o **confidencialidad** de la información."*
- Sistema: *"Todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos."*

Tipificación:

- **Delitos contra la integridad:**
  - Daño informático
    - Daño al equipo, virus, armas cibernéticas
  - Falsificación informática
    - *"Quien, a través de cualquier medio copie, altere o sustituya, deliberada e ilegítimamente,* ***datos informáticos*** *de un sistema que haga uso de tecnologías de la información o uno de sus componentes…"*
    - Falsificación de credenciales, suplantación de identidad
  - Fraude informático
    - Fraude, engaño

Tipificación:

- **Delitos contra la disponibilidad:**
  - Violación a la disponibilidad
    - Denegación de servicio (DOS)
  - Spam
    - Mensajes no solicitados, publicidad no solicitada, o sea violación de la privacidad, libertad de comercio

Tipificación:

- **Delitos contra la confidencialidad:**
  - Espionaje informático
  - Acceso ilícito
    - A su computador, cuenta de correo
  - Reproducción de dispositivos de acceso
    - En el teclado de su PC

Delitos Informáticos:

- **Medios de Investigación:**
  - Existentes;
  - Para la obtención y preservación de datos.
- **Medidas cautelares:**
  - Decretadas por Juez Competente;
  - Dispuestas por el Ministerio Público o Ente Investigador en casos urgentes.

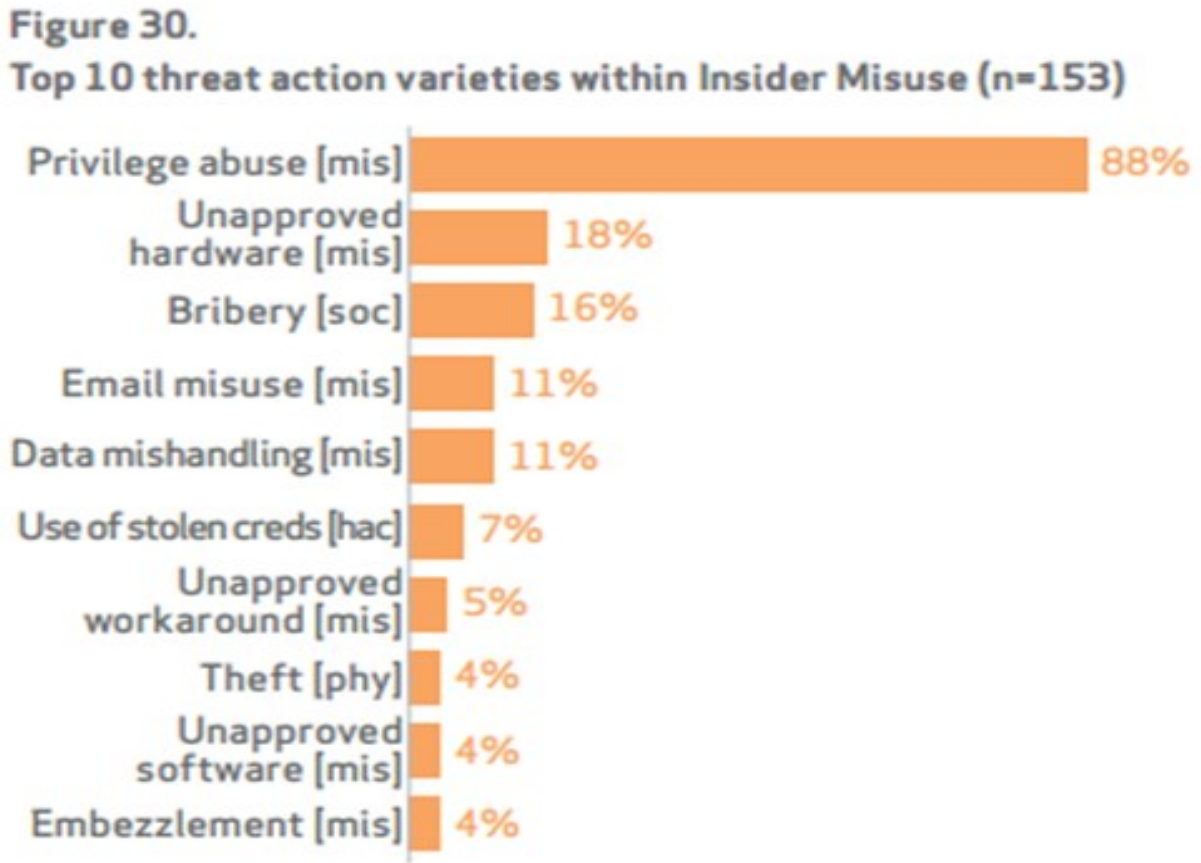
Entonces, la iniciativa de Ley deberá:

- **Solicitar Asistencia Jurídica Mutua,**
  - *El Estado podrá formalizar con otros Estados, de conformidad con la práctica internacional, la prestación de asistencia judicial recíproca en las investigaciones, procesos y actuaciones judiciales referentes a delitos tipificados en la presente ley, con apego al derecho interno y los instrumentos internacionales de los cuales es parte*.

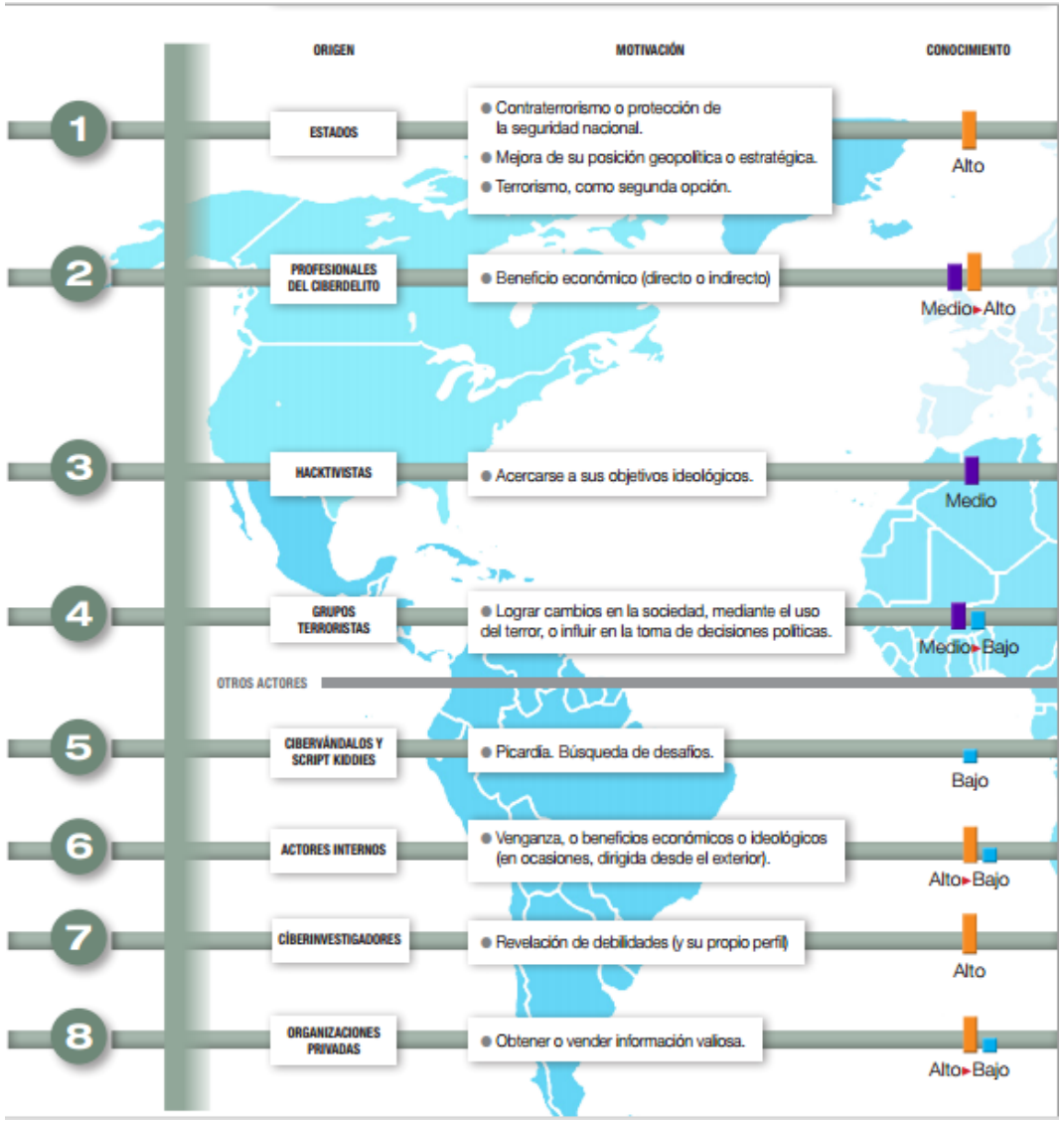
Estadísticas

- 79% de las víctimas fueron blancos de oportunidad;
- 96% de los ataques no representaron mayor dificultad;
- 85% de las brechas de seguridad tomó semanas o más para ser descubiertos;
- 92% de los incidentes fueron descubiertos por terceras personas;
- 97% de las violaciones a la seguridad pudieron prevenirse con controles simples o intermedios.

Por lo tanto el proyecto de Ley debe contemplar estos delitos:



Tendencias en Delitos 2014



Observaciones

- La protección de las infraestructuras críticas es una preocupación de los Estados desarrollados;

- El alto nivel de desarrollo de las sociedades occidentales radica mayoritariamente en una serie de servicios básicos y esenciales cuya prestación la presta el sector privado;

- Garantizar la seguridad de los suministros de estos servicios básicos ante nuevas amenazas es una responsabilidad no sólo de las administraciones públicas sino que es necesaria la concienciación y colaboración de los operadores privados.

Gracias por su atención.