SEGUNDA RONDA DE TALLERES CAMINO A LA XIX CUMBRE JUDICIAL IBEROAMERICANA – ECUADOR 2018

GRUPO DE TRABAJO

E-JUSTICIA

DÍA 2: JUEVES 1o DE JUNIO DE 2017

Siendo las nueve horas, del día jueves uno de junio de dos mil diecisiete, constituidos en el salón Atrio 5, los integrantes del Grupo E Justicia, el señor Coordinador Luis Guillermo Rivas, Patricia Bonilla y Orlando Castrillo de Costa Rica, Martín Antonio García Díaz de Nicaragua, Luis Eduardo Yepes Gómez de Colombia, Paublino Escobar Garay de Paraguay y enlazados vía Skype con la república de Uruguay con el señor Marcelo Pesce y el magistrado Jhon Perez, así como también con don Gustavo Castillo de la república de Ecuador, se procedió de la forma siguiente: **PRIMERO**: Se dio lectura al acta suscrita el día de ayer a la que se le hacen las modificaciones y cambios correspondientes. **SEGUNDO**: Se procedió a trabajar en los dos subgrupos definidos el día de ayer, **Ciberseguridad**, integrado por los señores Orlando Castrillo, Luis Eduardo Yepes, Martín Antonio García Díaz y coordinado por el señor Luis Guillermo Díaz Loáciga, además por vía videoconferencia don Gustavo Castillo y **Ciberdelincuencia** integrado por los señores Patricia Bonilla y Paublino Escobar y enlazado por vía videoconferencia con el señor Jhon Pérez. **TERCERO:** Después de conocidas las propuestas, ambos subgrupos presentan el producto de su intercambio de opiniones, incorporando el primer grupo su documento de propuesta sobre el tema Ciberdelincuencia, el cual queda así:

ESTUDIO DE RECOMENDACIONES SOBRE CIBERDELINCUENCIA

La "*Evolución Tecnológica*", ha transformado el mundo y la forma en que las personas realizamos las diferentes actividades sean cotidianas, económicas, académicas, de servicios, comunicación, producción, entre otros.

Dicha evolución, también ha incidido en la forma en que se realizan las actividades delictivas, donde la tecnología es utilizada como "*medio*" para cometer delitos comunes y de crimen organizado, o bien, como "*objeto*" de la actividad delictiva.

El delito informático ha sido definido como aquella "*acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas -hardware- o de los programas – software*"[1]

Los delitos informáticos tiene como características que: a) son de rápida ejecución y alto alcance, b) de fácil encubrimiento, c) novedosos, d) no siempre son fáciles de tipificar, e) generan nuevos bienes jurídicos tutelados, f) son intangibles, g) difíciles de vigilar, h) transitorios por su naturaleza, i) pueden ser disociados en el tiempo, j) difícil identificación del autor, por lo tanto, son difíciles de investigar, perseguir y juzgar.

La ciberdelincuencia, es una amenaza que si bien es cierto actúa de forma silenciosa, el daño es de gran impacto, generando pérdidas a nivel mundial, siendo que, durante el año 2016, de acuerdo con estudios realizados, se estima que el total de costos financieros causados por la ciberdelincuencia durante dicho año, supera los US$125.900 millones de dólares.[2]

Las tendencias futuras en el incremento del cibercrimen, están orientadas a actividades como : el "*Crime-as-a-Service*", "*Ransomware*", "*Uso criminal de datos*", "*Fraude de pago*", "*Abuso sexual infantil en línea*", "*Abuso de la Darkenet*", "*Ingeniería Social*",

[1] Chinchilla Sandí, Carlos. (2004) Delitos Informáticos: Elementos básicos para identificarlos y su aplicación. San José, Costa Rica. Ediciones Farben
[2] Informe Norton Ciberseguridad 2016 recuperado el 30-May-2017 en https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

"*Monedas Virtuales*"[3], así como el ataque a infraestructuras críticas, lo cual pone en peligro vidas humanas y la economía de los países.

Estudios han señalado que los marcos jurídicos relacionados con la ciberseguridad y la ciberdelincuencia, de los diversos países de la región se encuentran aún en una etapa incipiente, en cuanto a la promulgación de leyes relacionadas con la materia.

A continuación, se presenta un cuadro referente a la situación de cada país, cuyos datos fueron extraídos del informe denominado *"Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016"*, realizado por el Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID).

Dicho estudio realiza una evaluación, donde identificaron cinco niveles de madurez de la capacidad de seguridad cibernética en Latinoamérica, a saber: "*Inicial*", "*Formativo*", "*Establecido*", "*Estratégico*" y "*Dinámico*". Para efectos del cuadro, se representarán con los valores: 1, 2, 3, 4 y 5, respetivamente.

Si bien es cierto, el estudio realizado por la OEA, no hace relación al sistema jurisdiccional propiamente dicho, el mismo sirve de base, para tener una visión global de la situación actual de algunos de los países miembros, puesto que, no se abarca a los países ibéricos.

Ahora bien, en relación con el "***Derecho Penal Sustantivo***", cada uno de los niveles se valora de la siguiente manera:

[3] http://www.ituser.es/seguridad/2016/10/europol-presenta-su-informe-sobre-el-cibercrimen-en-europa

1: "*El derecho penal sustantivo específico para la delincuencia cibernética no existe, o existe el derecho penal general y se aplica ad hoc a la delincuencia cibernética*".

2: *"Existe una legislación parcial en el derecho penal sustantivo que aplica losmarcos legales y regulatorios a algunos aspectos de los delitos cibernéticos;*

está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley".

3: *"La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal".*

4: *"El país se adhiere a las mejores prácticas y normativas regionales e internacionales pertinentes sobre derecho de delito cibernético y asigna los recursos de acuerdo a las prioridades nacionales".*

5: *"El país continuamente busca incluir el desarrollo de las mejores prácticas internacionales sobre delito cibernético en la legislación nacional y es un colaborador activo en el discurso global sobre la mejora de los instrumentos de la lucha contra delitos cibernéticos internacionales; existen medidas para superar en el país las líneas de base mínimas de seguridad internacional".*

En cuanto al "***Derecho procesal de delincuencia cibernética***", los niveles valoran lo siguiente:

1: *"No existe el derecho penal procesal adecuado para la delincuencia cibernética*

y el uso de la prueba electrónica en otros crímenes, o existe el derecho penal procesal general y se aplica ad hoc a la delincuencia cibernética y al uso de la prueba electrónica en otros crímenes".

2: *"Se está discutiendo y desarrollando el derecho procesal penal en relación con la prueba electrónica; el derecho procesal penal se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos".*

3: *"Se ha implementado el derecho procesal penal integral y los requisitos probatorios relacionados; las mejores prácticas se emplean por aplicación de la ley en el ejercicio de poderes procesales".*

4: *"En el caso de la investigación transfronteriza, el derecho procesal estipula las acciones que es necesario realizar bajo las características de casos particulares, con el fin de obtener con éxito la prueba electrónica".*

5: *"El país se adhiere a las mejores prácticas internacionales sobre procedimiento penal de delito cibernético y la obtención de pruebas electrónicas, y constantemente busca implementar estas medidas en la legislación nacional y sirve como un colaborador activo en el discurso global sobre la mejora de la lucha contra los delitos cibernéticos internacionales; existen medidas para superar las líneas de base mínimas de seguridad internacional, que contribuyen al desarrollo de mejores prácticas internacionales".*

Y en lo que se refiere al "***Cumplimiento de la ley***", el estudio señala que:

1: *"No existe la capacidad de las autoridades policiales para prevenir y combatir los delitos relacionados con la cibernética".*

2: *"Existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima".*

3: *"Se ha establecido una capacidad institucional integral para investigar y manejar casos de delincuencia cibernética y delitos relacionados con pruebas electrónicas, incluyendo los recursos humanos, procesales y tecnológicos, medidas exhaustivas de investigación, cadena de custodia digital y gestión de integridad de las pruebas y mecanismos formales e informales de colaboración con interesados internacionales y nacionales (actores de los sectores privado y público)".*

4: *"Los oficiales de las fuerzas de la ley reciben una formación continua basada en las responsabilidades relativas y en entornos de amenazas nuevas y cambiantes y pueden utilizar herramientas forenses digitales sofisticadas para investigar delitos informáticos complejos y delitos relacionados con pruebas electrónicas; los organismos locales de aplicación de la ley colaboran con contrapartes regionales e internacionales en investigaciones".*

5: *"Existen recursos dedicados a unidades de delitos informáticos plenamente operativas, incluyendo capacidades avanzadas de investigación y de gestión de integridad de los datos; es posible recoger y analizar las estadísticas y tendencias que mejorarían la investigación sobre los delincuentes con el fin de facilitar una comprensión exhaustiva del ambiente delictivo en línea y contribuir a la toma de decisiones estratégicas; las agencias de aplicación de la ley nacionales están participando plenamente en la investigación y redes transfronterizas".*

País	Derecho sustantivo de delincuencia cibernética	Derecho procesal de delincuencia cibernética	Cumplimiento de la ley
Argentina	3	3	3
Bolivia	2	2	2
Brasil	3	4	4
Chile	3	4	3
Colombia	3	3	3
Costa Rica	3	3	3
Ecuador	3	2	2
El Salvador	2	2	2
Guatemala	2	1	2
Honduras	2	1	1
México	3	2	4
Nicaragua	1	3	1
Panamá	3	2	2
Paraguay	3	2	2
Perú	3	2	2
República Dominicana	5	5	5
Uruguay	1	2	2
Venezuela	3	1	2

Para conocer cuál es la situación real de cada país, en relación con su legislación referente a los delitos informáticos, se considera oportuno realizar un estudio a través de una matriz, donde se especificarán los tipos penales, leyes especiales o procesales de sus legislaciones, así como la estructura organizativa, jurisprudencia y convenios suscritos por sus respectivos estados.

A partir de este estudio de campo, se podrá precisar el estado en que se encuentra cada país, en relación a este tipo de hechos punibles, y a partir de allí dictar recomendaciones, o bien, este podrá ser de utilidad para cada uno a efecto de que tomen las precauciones y realicen las iniciativas que consideren oportunas, para armonizar sus legislaciones conforme a los nuevos estándares internacionales.

Un aspecto importante a considerar, es que en la medida que los países tengan armonizada la normativa jurídica, con el resto de la región, la misma, facilitará mayor cooperación internacional, con el fin de perseguir y castigar a los partícipes de este tipo de hechos, y consecuentemente facilitar la extradición tanto activa, como pasiva, de este tipo de conductas al margen de la ley.

Es por lo anterior que se recomienda a los países miembros de la Cumbre Judicial Iberoamericana, promover los mecanismos jurídicos, procesales y de cooperación internacional, que faciliten la lucha contra este tipo de criminalidad, razón por la cual, se presenta el siguiente informe, el cual muestra un catálogo de tipos penales, utilizados en los diferentes países para sancionar conductas delictivas relacionadas con el ciber-crimen.

ESTUDIO NORMATIVO RELACIONADO CON EL CIBERCRIMEN

Se solicita a cada uno de los países de Cumbre Judicial, llenar el siguiente formulario, el cual nos permitirá obtener los insumos necesarios, para precisar las normas que regulan los delitos determinantes o que se refieran al ciber-crimen, así como, jurisprudencia relacionada y la estructura organizacional de las instituciones involucradas en este tipo de actividades ilícitas.

El documento se ha dividido en cuatro puntos:

I. Legislación de los países miembros de la Cumbre Judicial Iberoamericana, relacionada con los delitos informáticos

II. Convenios Internacionales ratificados y/o en trámites de ratificación en los países miembros.

III. Jurisprudencia relacionada con ciberdelincuencia en los países miembros.

IV. Estructura organizativa en el marco de los delitos informáticos, donde se incluya la Policía Judicial, Ministerio Público y la Judicatura

El presente formulario tiene como objetivo elaborar un mapeo sobre el estado de las legislaciones de los países en relación con la Ciberdelincuencia.

I. LEGISLACIÓN DE LOS PAÍSES MIEMBROS DE LA CUMBRE JUDICIAL IBEROAMERICANA, RELACIONADA CON LOS DELITOS INFORMÁTICOS

Este apartado se ha divido en dos áreas: normas sustantivas y normas procesales. Para complementar los datos, la tabla se divide en cinco columnas, a saber:

a) **Tipo penal de referencia:** En esta columna se presentan algunos tipos penales que se encuentran incorporados en el derecho positivo. El dato allí señalado, debe considerarse sólo como referencia, por cuanto, el "*nom iuris*" en cada país podría variar.

b) **Artículo:** Se debe anotar el número del artículo

c) **Cuerpo normativo:** Nombre del cuerpo normativo donde se encuentra tipificada la norma

d) **Nombre de la norma:** "*Nom iuris*" conforme a la legislación del país estudiado

e) **Descripción del tipo penal:** Descripción literal del tipo penal

Además, es importante destacar que los tipos penales de referencia aquí anotados, son una guía, no obstante, cada país puede incorporar aquellos que tengan en su legislación y que no se encuentren aquí señalados.

FORMULARIO
ESTADO ACTUAL DE LA CIBERDELINCUENCIA EN LOS PAÍSES DE CUMBRE JUDICIAL IBEROAMERICANA

País: _____

Nombre contacto del país: _____

Correo electrónico: _____

- **Normas jurídicas sustantivas relacionadas con ciberdelincuencia**

Tipo Penal de referencia	Artículo	Norma	Nombre de la norma (conforme a su legislación)	Texto de la norma
DELITO INFORMÁTICO COMO MEDIO DE LA ACCIÓN DELICTIVA				
Delitos Sexuales				
Corrupción				
Seducción o encuentros con menores por medios electrónicos (Grooming)				
Turismo sexual				
Fabricación, producción o reproducción de pornografía				
Pornografía virtual y pseudo pornografía				
Tenencia de material pornográfico				
Difusión de pornografía				
Delitos contra el ámbito de intimidad				
Violación de correspondencia o comunicaciones				
Violación de datos personales.				
Delitos contra la propiedad				

Extorsión informática (Ransomware)				
Estafa informática				
Daño agravado				
Narcotráfico y crimen organizado				
Espionaje				
DELITO INFORMÁTICO COMO OBJETO DE LA ACCIÓN DELICTIVA				
Delitos informáticos y conexos				
Sabotaje informático				
Daño informático				
Suplantación de identidad				
Espionaje informático				
Instalación o propagación de programas informáticos maliciosos				
Suplantación de páginas electrónicas				
Facilitación del delito informático				
Difusión de información falsa				

- **Normas jurídicas procesales relacionadas con ciberdelincuencia**

Norma procesal de referencia	Artículo	Cuerpo normativo	Nombre de la norma (conforme a su legislación)	Descripción de la norma procesal penal

II. CONVENIOS INTERNACIONALES RATIFICADOS Y/O EN TRÁMITES DE RATIFICACIÓN

Indicar aquellos convenios internacionales ratificados, o en proceso de ratificación, en su país.

a) **Nombre convenio:** Señalar el nombre del convenio
b) **Estado:** Se refiere si el mismo está ratificado, o bien, se encuentra en pendiente o en proceso de ratificación
c) **Fecha de promulgación:** En caso de estar ratificado, indicar la fecha de promulgación
d) **Fecha de ratificación:** Señalar la fecha de ratificación en su país

Nombre Convenio	Estado	Fecha de promulgación	Fecha de ratificación

III. JURISPRUDENCIA RELACIONADA CON CIBERDELINCUENCIA

Con el fin de obtener información de criterios jurisprudenciales de los diversos países, se considera oportuno, obtener las resoluciones emitidas por los altos tribunales (Tribunales o Sala de Casación), relacionados con los delitos informáticos

a) **Tribunales de Apelación o Sala de Casación:** Indicar el nombre órgano que dicta la resolución
b) **No. Voto o Sentencia:** Anotar el número de voto o sentencia, que la identifique
c) **Fecha:** Fecha de emisión del voto o sentencia
d) **Tipo Penal:** Indicar el tipo penal que fue objeto de discusión en el recurso
e) **Nombre documento adjunto:** Indicar el nombre del documento que se adjunta a este formulario con el contenido del voto o sentencia señalado.

Tribunal de Apelación o Sala de Casación	No. Voto	Fecha	Tipo penal	Nombre documento adjunto

IV. ESTRUCTURA ORGANIZATIVA EN EL MARCO DE LOS DELITOS INFORMÁTICOS

Con el fin de conocer la estructura organizativa de cada Institución, relacionada con los delitos informáticos, se considera oportuno conocer, si en los países miembros, se cuenta con unidades de especialización creadas para investigar, combatir y judicializar, los hechos punibles cometidos a través del uso de la tecnología informática, desde la investigación, recolección, manejo de evidencia y prueba digital, entre otros. Por ejemplo, si existen Fiscalías, Unidades de la Policía o Jurisdicciones especializadas en Delitos Informáticos.

En caso de no existir unidades especializadas, indicar cuál es la estructura utilizada.

a) **Institución:** Nombre de la oficina
b) **Funciones:** Indicar las funciones que realiza dicha unidad

Institución	Funciones
Policía Judicial	
Ministerio Público	
Judicatura	

Así mismo, el segundo grupo presentó su documento de propuesta sobre el tema Ciberseguridad, el cual queda así:

ESTUDIO DE RECOMENDACIONES SOBRE CIBERSEGURIDAD

Introducción

La seguridad informática busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos.

Se parte de la premisa de que no existe la seguridad informática al 100%. Bajo esta óptica, podemos dividir los esfuerzos en esta materia en dos tipos: los que van orientados a mantener la continuidad de los servicios y los que van orientados a recuperarse en el caso en que, a pesar de todos los esfuerzos realizados, se haya presentado una interrupción en los servicios.

El gasto en seguridad informática tiene un comportamiento asintótico con respecto a la mejora que se obtiene al incrementar la inversión en tecnología. Al principio se pueden realizar mejoras muy importantes con poca inversión, pero conforme se avanza las mejoras que se obtienen son cada vez menores y para obtenerlas se requiere un mayor gasto.

Por más esfuerzo que se haga, aún la organización con mayor capital y mayores recursos tendrá aspectos susceptibles de mejora. El límite del gasto que se realiza en esta materia se define con base en una valoración costo – beneficio y en una adecuada administración de riesgos.

Se propone la creación de una red de cooperación en materia de ciberseguridad entre los países miembros de la Cumbre Judicial Iberoamericana. La finalidad de esta red es crear un medio para que los especialistas en la materia de los diferentes países puedan compartir las

mejores prácticas generando así una sinergia que evite, en la medida de lo posible, el desgaste de esfuerzos y que facilite la cooperación entre los miembros, y la socialización de experiencias con el fin de uniformar la fortaleza ante las amenazas cibernéticas.

Existen diferentes factores que forman parte de los esfuerzos que las organizaciones deben realizar para garantizar la continuidad de los servicios. En el Anexo #1 se listarán estos servicios con la finalidad de que sean considerados sin embargo no serán tratados en la red de cooperación propuesta.

Se presentará a continuación una breve descripción de los aspectos que serán tema de discusión de la red de cooperación. Este listado será socializado con los países miembros para incorporar sus aportes.

La siguiente etapa del proceso será la realización de un diagnóstico, mediante un instrumento idóneo, que permita a cada país determinar los aspectos susceptibles de mejora y los países que podrían colaborar en el proceso.

RECURSOS ESPECÍFICOS PARA REPELER ATAQUES CIBERNÉTICOS

Los siguientes aspectos serán de interés y discusión en la red de cooperación.

Cultura organizacional

El primer elemento de un esquema de seguridad informática es la cultura de los usuarios. Ningún esquema de seguridad, por más fuerte que sea puede compensar los descuidos y faltas que puedan tener los usuarios. Si los usuarios insisten en abrir correos maliciosos, ingresar a sitios dudosos o utilizar software ilegal, no hay forma de cerrar todos los portillos

existentes por lo que mediante estas acciones pondrán en riesgo la seguridad informática de la organización.

Se requiere por tanto que se defina en primera instancia un marco de control, compuesto por políticas, procedimientos, reglamentos y sanciones apoyados y aprobados por la administración superior de la organización.

Pero además se requiere instruir al usuario en temas de seguridad informática de tal forma que tenga los elementos para valorar los riesgos a que se enfrenta y las posibles consecuencias de sus actos. Esto puede realizarse mediante diferentes formas tales como campañas de información sobre diferentes temas y cursos específicos.

Sin temor a equivocarse los esfuerzos que se realicen en estos temas cubren más del 50% del trabajo que implica la seguridad informática de la organización y la inversión requerida para su implementación es relativamente baja.

Elementos del esquema de seguridad informática

Además de la seguridad que se puede implementar propiamente con los componentes de la plataforma tecnológica de la institución existen una serie de recursos que se adicionan específicamente para solventar debilidades en materia de seguridad informática. Algunos de estos recursos resultan onerosos para muchas organizaciones sin embargo debe valorarse su uso, aún y cuando se limite a áreas muy críticas de la plataforma. También deben considerarse opciones de software libre. Entre estos recursos se puede mencionar:

- Firewall: Estos dispositivos, también conocidos como paredes de fuego, trabajan por denegación por omisión, es decir, lo que no está expresamente autorizado está denegado. Se utilizan para controlar el flujo de información entre dos redes o

segmentos de estas. Existen firewalls que trabajan en capas 3 y 4 y otros que trabajan a nivel de aplicación en la capa 7 del modelo OSI. La gama de opciones para un dispositivo de este tipo va desde uno hecho con una PC con dos o más tarjetas de red y una distribución de Linux hasta los más sofisticados que reconocen mediante inteligencia artificial posibles ataques y los repelen. Algunos tienen, previo contrato de servicio, conexión con el fabricante para que este alimente y actualice las firmas (patrones de ataques que reconoce el dispositivo) y las diferentes listas de sitios potencialmente peligrosos para que el administrador defina si se bloquea o se permite el acceso a esos sitios. El fin último de un firewall es permitir el tráfico estrictamente necesario y su efectividad estará en relación directa con la habilidad de su administrador.

- Antimalware: Los delincuentes informáticos generan software que, una vez que ha ingresado en la organización, puede ejecutar diferentes acciones, desde borrar información hasta dar acceso al hacker para que tome control del equipo en que se instaló. Para evitar este riesgo existen productos que se encargan de revisar en cada equipo de la plataforma el software que ingresa. Para que este esquema sea efectivo el software debe estarse actualizando constantemente para incorporar las nuevas amenazas que van surgiendo y para incorporar mejoras a su funcionamiento y efectividad. Estos productos consumen un porcentaje importante de la capacidad de cómputo de los equipos y también tienen un consumo significativo de ancho de banda en la red por lo que su correcta administración resulta crucial para que se constituyan en una solución y no en un problema.

- Antispam: Mención aparte merece el recurso que se encarga de evitar que ingrese correo basura a la organización. Este correo es molesto, consume recursos de red, de almacenamiento y de procesamiento y podrían presentar patrones virales que lo faculten a reproducirse con lo cual se agravan los problemas indicados y además se compromete la credibilidad de la organización al convertirla en fuente de correos

indeseados. Sirven además como transporte de otras formas de malware lo que los hace doblemente peligrosos.

- Análisis de vulnerabilidades: Los diferentes productos de software que se instalan en los equipos que componen la plataforma de la organización no son perfectos. Con el paso del tiempo se detectan fallos que los delincuentes informáticos pueden utilizar para sobrepasar los mecanismos de seguridad que se hayan establecido. Estos fallos se conocen como vulnerabilidades. Encontrar y reparar estas vulnerabilidades es una labor titánica por lo que se han desarrollado productos que buscan, con base en la información que publican los distintos fabricantes, estas vulnerabilidades y las informan a tiempo junto con una recomendación para su reparación de tal forma que se hace posible mantener el nivel de vulnerabilidad de los equipos en un rango aceptable. Estos productos deben complementarse con servicios de instalación automatizada de los parches que solventan las deficiencias encontradas.

- Prevención de intrusos: Dado que no se puede asumir que los esquemas de seguridad, en ningún caso, son impenetrables, siempre existe la posibilidad de que un delincuente informático vulnere esas defensas y logre llegar hasta los dispositivos críticos de la organización. Los sistemas de prevención de intrusos contemplan esta posibilidad e incorporan mecanismos para detectar y repeler el acceso de intrusos a los dispositivos clave.

- Administrador de contenidos: A pesar de las advertencias y capacitaciones los usuarios podrían por alguna razón terminar tratando de ingresar a un sitio en internet inadecuado, ya sea por su contenido o porque representa un riesgo potencial para la seguridad informática de la organización. Mediante la administración de contenidos los sitios que se pueden accesar se pueden limitar conforme a las políticas organizaciones evitando riesgos y pérdida de tiempo laboral.

- Correlación de eventos: La mayoría de los dispositivos de la plataforma tecnológica de la organización generan eventos que en forma aislada podrían no dar mayor información pero que si se correlacionan con los que generan otros dispositivos podrían indicar la materialización de algún riesgo. Este tipo de productos buscan recolectar los eventos que generan los distintos dispositivos y realizar una correlación para determinar comportamientos que de otra forma pasarían inadvertidos.

- Auditorías internas y externas en materia de seguridad informática: El esfuerzo por detectar y corregir debilidades debe ser constante. Bajo esta premisa es importante contar con personal especializado a lo interno que realice diferentes estudios e intentos controlados de intrusión con el fin de eliminar los portillos que pudieran utilizar los delincuentes informáticos antes de que estos los encuentren. También se debe contratar, al menos una vez al año, este tipo de revisión por parte de un tercero experto con un enfoque diferente.

- Recursos en línea: Existen numerosos recursos en línea que pueden utilizarse para mejorar la seguridad informática. Tal es el caso del servicio de revisión de páginas web que provee la fundación OWASP (www.owasp.org) o el escaneo de metadatos que ofrece el sitio www.elevenpaths.com mediante su aplicación FOCA. Si bien es cierto no se puede hacer uso de cualquier página, existen servicios como los mencionados que brindan un aporte significativo.

- CSIRT: Dado que no existe garantía de que no se presenten incidentes, la organización debe estar preparada para actuar en estos casos. Un CSIRT es un equipo de respuesta a incidentes, el cual sabe de antemano como se debe actuar en estas situaciones. Este equipo monitorea además las alertas a nivel mundial con la finalidad de prevenir la ocurrencia de incidentes conocidos y mantiene además

comunicación con otros equipos similares a nivel mundial con fines de mutua cooperación.

Socialización de los temas de interés

La lista de los temas de interés se va a socializar con todos los países miembros para que sus especialistas puedan hacer aportes. Con la incorporación de los aportes se generará una lista definitiva que se hará de conocimiento de los países miembros.

Se propone el uso de un blog en el que se publicará la lista base que se propone en este documento y se dará un tiempo prudencial para la discusión y definición.

Costa Rica propone hacerse cargo de la implementación de este blog.

Características del instrumento que se definirá

Con base en la lista de los temas que se incluyan como de interés de la red de cooperación se realizará un diagnóstico que permita determinar el nivel de seguridad, de cada país, en cada uno de los aspectos incluidos.

Se propone para este fin la utilización de una encuesta en línea que, en la medida de lo posible, deberá respetar los siguientes parámetros:

- Deberá ser fácil de llenar y tomar el menor tiempo posible
- Deberá respetar la independencia y confidencialidad de los países miembros
- Deberá utilizar una escala que permita la comparación entre los diferentes países

Costa Rica propone hacerse cargo de la implementación de la encuesta en línea.

Análisis de Brecha

El diagnóstico servirá de base para iniciar un proceso de colaboración entre los países miembros en el que, con base en las diferencias encontradas, se definirá la forma en que se minimizará la brecha existente.

Se propone que se definan y prioricen los temas de mayor interés y se busquen mecanismos para compensar las deficiencias. Estos mecanismos van desde la asesoría del país que mayor desarrollo tiene en un tema a los demás hasta la contratación por parte de alguno de los países de un especialista y la posterior replicación del conocimiento y la experiencia a los demás.

Colaboración

Conforme las experiencias positivas y el flujo de información lo permitan, los participantes podrán tener discusiones respecto a las mejoras que se requieren para enfrentar los diferentes retos que presentará el futuro. Se compartirá información respecto al comportamiento de amenazas a nivel mundial y los mecanismos más efectivos para enfrentarlas.

Se espera además que los especialistas puedan realizar investigaciones conjuntas, acordar temas de interés y preparar capacitaciones de unos a otros y que se apoyen cuando alguno tenga un incidente de seguridad que atender.

Mecanismos de integración de la red de cooperación en ciberseguridad

Uno de los principales temas que debe definirse en el proceso de implementación de la red de cooperación es el mecanismo que utilizarán los especialistas para comunicarse en forma efectiva.

Debe ser un medio que permita compartir distintos tipos de información (texto, audio, video) y de preferencia debe tener a los miembros en línea permanentemente.

Se deberá definir también un protocolo para el uso de este medio de comunicación que permita su mejor aprovechamiento.

CUARTO: Se dio por concluida esta sesión, finalizando la misma a las dieciséis horas del uno de junio de dos mil diecisiete, firmando esta acta los presentes, con su previa lectura y ratificación de su contenido.

Coordinador de mesa:

.....

Dr. Luis Guillermo Rivas Loáiciga
Magistrado (Costa Rica)

Integrantes de mesa:

.....

Orlando Castrillo Vargas
Subdirector TI (Costa Rica)

.....

Patricia Bonilla Rodríguez

Asesora Presidencia Corte Suprema de Justicia (Costa Rica)

.....

Paublino Escobar Garay

Juez Penal (Paraguay)

.....

Luis Eduardo Yepes Gómez

Unidad Informática de la Rama Judicial (Colombia)

.....

Martín Antonio García Díaz

Director General de Tecnologías de la Información y Tecnologías