AGETIC/IV/0022/2018
Expediente : 26904

AGETIC

09 de Marzo de 2018

INFORME DE VIAJE Y CONFORMIDAD

INFORME DE VIAJE

PARA: Nicolas Laguna Quiroga
Director General Ejecutivo

DE: Horacio Lopez Justiniano
Jefe de Unidad Centro de Gestión de Incidentes Informáticos

ASUNTO: Grupo de Trabajo de Medidas de Fomento de Confianza en el Ciberespacio.

N° de Memorándum: AGETIC/RA/0015/2018

ITINERARIO

Fecha de Salida	Fecha de Retorno	Hora de Salida	Hora de Retorno
27/02/2018	04/03/2018	9:20	7:00

Lugar/Ruta de viaje	Medio de Transporte
La Paz - Washington DC - La paz	Aéreo

DESARROLLO

Objetivo de Viaje

El objetivo del viaje era participar del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio, Organizado por CICTE en la OEA.

Como primer objetivo de esta mesa de trabajo era Elaborar un conjunto de medidas de fomento de cooperación y confianza en el ciberespacio, basados en los informes de UN-GGE. y mantener informado a CICTE

Actividades Realizadas

Se detallan a continuación las actividades realizadas por día:

Miércoles 28 de Febrero

Las reuniones del grupo de trabajo se llevaron a cabo en la sede de la OEA en el Salón Padilla Vidal del Edificio de la Secretaría General (GSB) de la OEA 1889 F St NW (esquina de 19th Street y F Street) Washington DC, 20006, EEUU.

Como primer objetivo de la mesa de trabajo, se procedió a elegir a los representantes o directorio de la mesa entre los representantes de los Estados Miembros, para esto la delegación de Canadá nomina a la delegación de Colombia pueda presidir la mesa, Estados Unidos apoya la nominación y se decide que Colombia es presidente de la mesa. La delegación de México nomina a la delegación de Chile como vicepresidente de la mesa, la delegación de Guatemala apoya la nominación de Chile y se decide que Chile es vicepresidente de la mesa. La delegación de Colombia nomina a la delegación de Argentina como relator, la delegación de Chile apoya la nominación y se elige a la delegación de Argentina como relator de la mesa de trabajo. Asimismo queda definido como secretaría técnica el Comité Interamericano contra el Terrorismo (CICTE).

Se realizo una extensa presentación por parte de Giovanny Snidle, representante de la misión permanente par OAS de Estados Unidos, haciendo un análisis de los antecedes de trabajo para esta mesa, mostrando un resumen de otros avances realizados en Medidas de Fomento de Confianza (MFC).

Se presentó un análisis de las Medidas de Fomento de la Confianza y la Seguridad establecidas en otros foros regionales, tales como la Organización para la Seguridad y la Cooperación en Europa (OSCE). Presentación que estuvo a cargo de Ben Hiller, quien detallo los puntos focales que hay que tomar en cuenta para trabajar estas medidas, ademas de la experiencia de compartir y generar confianza entre CSIRT de la región de Europa para establecer vínculos mas estrechos al momento de enfrentarse a problemas de ciberseguridad.

Se discutió con los Estados Miembros sobre el Desarrollo de Medidas de Fomento de Confianza cibernéticas en el contexto de la seguridad internacional, compartiendo la experiencia dentro de las Naciones Unidas, con la participación de un panel conformado por Sheila Flynn, del Gobierno de los Estados Unidos, Michael Walma del Gobierno de Canadá y Issac Morales del Gobierno de México.

Se planteará la posibilidad de debatir sobre una Mesa de trabajo para Infraestructuras Críticas dentro de los países.

Jueves 1 de Marzo

Se realizó las exposiciones de algunos Estados Miembros sobre las experiencias y desafíos regionales en materia de ciberseguridad.

La delegación de Colombia hablo sobre el crimen como servicio, hay crimen organizado que es muy fácil conseguir cualquier tipo de herramientas, solo son contratados a grandes coorporaciones de ciberdelincuentes. Identificaron tambien que el principal vector de ataque es el Malware que se propaga por la red y es causante de muchos otros daño para la seguridad de la información. También se hablo sobre el abuso sexual infantil mas alla de solo dejar el termino en pornografía infantil, y las medidas que deberíamos tocar como Estados para combatirla.

Colombia presento su Centro de Capacidades para la Ciberseguridad de Colombia (C4) y ofrece cooperación internacional a Interpol y Europol, que cuentan un un CSIRT de gran tamaño con mucho personal dedicado a atender incidentes de ciberseguridad en el país, y cuentan con programas académicos para mejorar la cultura de seguridad de la información.

La delegación de Brasil se presento como un país con gran potencial en seguridad de la información y la red de CSIRT con la que están conformados internamente. Los principales vectores de ataque identificados para Brasil son los ataques de denegación de servicios distribuidos (DDOS), que afectaron principalmente a los grandes eventos internacionales que organizó Brasil en los pasados años, como el Mundial de Futbol, Olimpiadas. Estos ataques de denegación de servicios se identifico que principalmente son ocasionados por los dispositivos sin control que se lanzan al mercado como parte de Internet de Las Cosas (IOT). Se propuso trabajar sobre alguna recomendación para enviar a los fabricantes de equipos tecnológicos para que se contemple la seguridad en sus dispositivos.

La delegación de Ecuador remarco la gran amenaza que existe por el uso de dispositivos móviles y redes de comunicación actuales, el acceso a las redes sociales por parte de los jóvenes y niños los convierte en el mayor grupo de uso de internet en Ecuador, y mostraron los desafíos que tienen con respecto a la ciberdefensa y operaciones de ciberexploración. Se menciono que al igual que Brasil tienen una red de CSIRT interna para la mejor respuesta a incidentes de acuerdo al sector involucrado.

Se realizo la presentación de un conjunto borrador de Medidas de Fomento de la Confianza Cibernéticas para el Sistema Interamericano, medidas prioritarias para su consideración inmediata y un plan de acción sugerido para establecer medidas regionales para promover la cooperación y la confianza. Se tuvo la participación de Liesyl Franz de Estados Unidos, Juanita Navarro de Colombia, Issac Morales de México y Daniel Alvarez de Chile. Se propuso las medidas prioritarias para consideración del grupo de trabajo.

Uno de los aspectos importantes es que los países voluntariamente compartirían documentos relacionados a la seguridad para lograr un común entendimiento entre los Estados Miembros.

Se abrió el debate y la discusión con respecto a este borrador propuesto. Había una marcada diferencia ideológica al referirse a la participación de empresas privadas en el proceso de elaboración de políticas de seguridad para los Estados Miembros.

La discusión sobre los puntos propuestos por las delegaciones de Chile, Colombia, México, Estados Unidos y Canadá, tuvo que realizarse en pequeños grupos fuera de la mesa de trabajo. Donde junto con las delegaciones de Perú, Ecuador, Brasil se sugieren varios cambios al documento presentado.

Una vez reinstalado el grupo de trabajo se procedió a leer todo el documento detalladamente incluyendo las observaciones realizadas por las delegaciones y aprobando párrafo a párrafo todo el contenido.

Las medidas de fomento acordadas por el grupo de trabajo son las siguientes:

- Proporcionar información sobre políticas nacionales de ciberseguridad, como son las estrategias nacionales, los libros blancos, marcos legales y otros documentos que cada Estado Miembro considere pertinente.
- Identificar un punto de contacto nacional a nivel político para discutir las implicaciones de las ciberamenazas hemisféricas. La labor de estos puntos de contacto podrá ser diferente, pero complementaria del trabajo en curso de las fuerzas de la ley y de otros expertos técnicos en la lucha contra el delito cibernético y la respuesta a incidentes cibernéticos preocupantes. La información sobre los puntos de contacto se actualizará anualmente, o tan frecuentemente como sea necesario, y se compartirá entre los puntos de contacto nacionales en un formato que sea transparente y de fácil acceso.

Como parte del plan de acción los estados miembros acordaron colaborar regional y subregionalmente para abordar los desafíos comunes en el ciberespacio. El grupo de trabajo adelantará lo siguiente para el establecimiento de medidas adicionales de MFCs.

1. El grupo de trabajo incluirá en su agenda de la próxima reunión la identificación y discusión de las amenazas cibernéticas mas apremiantes para la región. incluyendo las amenazas cibernéticas a la infraestructura críticas compartidas. Los resultados se resumirán en un informe.

2. El grupo de trabajo con insumos del sector privado y de otras partes interesadas, elaborará una lista priorizada de desafíos cibernéticos clave y propondrá un plan de trabajo para abordar esos desafíos a nivel políticas. Los resultados se incluirán en un informe para el CICTE.

3. El grupo de trabajo elaborará un listado de mejores prácticas y lecciones aprendidas para guiar la respuesta de las partes responsables, a nivel de elaboración

de políticas en caso de ocurrir un incidentes cibernético que involucre estas amenazas.

4. El grupo de trabajo podrá revisar experiencias para gestionar incidentes cibernéticos y considerará la posibilidad de mayor cooperación a nivel técnico y de las políticas en esta área.

Se definió también que la siguiente reunión del grupo de trabajo se realizará del 20 al 22 de Agosto de 2018. y se confirmará después si esta reunión será presencial o virtual.

Viernes 2 de Marzo

Todas las actividades fueron suspendidas para este día debido al clima extremo que llego a Washington DC.

Se adjunta los correos oficiales que llegaron de la OEA para cancelar las actividades del día.

CONCLUSIONES

La reunión de este grupo de trabajo es de gran importancia para generar mejores relaciones con los países vecinos en materia de seguridad de la información y la generación de confianza para compartir información sobre los problemas que se presentan en el ciberespacio y como en la región se puede combatiros.

No es fácil trabajar en políticas de seguridad en los estados sin los datos técnicos necesarios para respaldar la toma de decisiones, en este sentido se concluyó que es importante que los Estados Miembros compartamos información de incidentes informáticos y existe un punto de contacto para dar solución o una respuesta en caso de que sea necesario.

Se buscará pedir a la OEA una recomendación para los que los proveedores de servicios de Internet (ISP) de los países puedan brindar información confiable cuando los CSIRT les requieran, ya que en la mayor parte de la región los ISP son empresas privadas, pero deben colaborar para hacer un ciberespacio mas seguro.

ANEXOS

- [X] Pases a Bordo originales o certificación de vuelo emitida por la línea aérea
- [ ] Boleto, Recibo o Factura originales por transporte terrestre
- [X] Otros (Detallados a continuación)

- Se adjunta los documentos que indican que las fechas del evento fueron cambiadas de las fechas originales y pospuesta para el 28 de febrero 1 y 2 de Marzo.

- Se adjunto el correo oficial de la OEA que indica que las actividades para el día 2 de marzo fueron suspendidas debido al clima extremo en Washington DC

CONFORMIDAD

PARA: Carmen Fedra Valverde Rossel
Jefe de Unidad Administrativa Financiera

DE: Nicolas Laguna Quiroga
Director General Ejecutivo

REF.: Grupo de Trabajo de Medidas de Fomento de Confianza en el Ciberespacio.

JEFE DE UNIDAD O AUTORIDAD COMPETENTE DEL COMISIONADO:

Habiendo revisado el Informe de viaje emitido por el comisionado, se establece que a través de las actividades realizadas, se ha dado cumplimiento al objeto del viaje. En este sentido se aprueba el informe del comisionado, dando mi plena conformidad con los resultados alcanzados, los mismos que aportan al cumplimiento de los objetivos y metas establecidas en la programación anual de la AGETIC.

FIRMA:

HLJ

Cc.:archivo