AGETIC/IV/0196/2023
Expediente : 210839
Código de verificación : 1-AM0RI8HN

16 de Agosto de 2023

Clasificación : Reservado

INFORME DE VIAJE Y CONFORMIDAD

INFORME DE VIAJE

PARA:	VLADIMIR TERAN GUTIERREZ DIRECTOR GENERAL EJECUTIVO
DE:	Franz Rojas Castillo RESPONSABLE CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS
ASUNTO:	Informe "I Ejercicio de Ciberseguridad para la Región Andina"

N° de Memorándum: AGETIC/M/0622/2023

ITINERARIO

Fecha de Salida	Fecha de Retorno	Hora de Salida	Hora de Retorno
09/08/2023	11/08/2023	06:45	06:05
Lugar/Ruta de viaje		Medio de Transporte	
La Paz - Lima - La Paz		Áereo	

DESARROLLO

Objetivo de Viaje

Participar en el "I EJERCICIO DE CIBERSEGURIDAD PARA LA REGIÓN ANDINA", tuvo el objetivo de comprender de mejor manera el panorama de las amenazas cibernéticas subregionales, explorar y practicar oportunidades de cooperación y coordinación regional en respuesta a un incidente con efecto transfronterizo.

Actividades Realizadas

Se detallan a continuación las actividades realizadas por día:

Miércoles 9 de agosto

El Centro de Competencia de Cibercapacidades de Latinoamerica y el Caribe "LAC4" planificó el viaje para la delegación Boliviana conformado por:

- 1 miembro de la Policía Boliviana (Tte. Pol. Enrique Reynaga)

- 1 miembro del Ejército de Bolivia (My. DIM. Guery Oscar de la Barra Cervantes)

- 2 miembros de AGETIC

Día oportuno para intercambiar las experiencias y el trabajo que realizan las tres instituciones en materia de ciberseguridad conforme a sus competencias y establecer acciones interinstitucionales futuras.

Jueves 10 de agosto (día del evento)

El evento inició a horas 10 a.m. con palabras de inauguración del Secretario General a.i. de la Comunidad Andina Sr. Diego Caicedo , seguido de las palabras de la Embajadora de la Unión Europea en Perú y del Director Regional LAC4 Sr. César Moliné Rodriguez, dando la bienvenida a las delegaciones de Bolivia, Colombia, Ecuador y Perú.

Posteriormente se inició el ejercicio describiendo el escenario (ficticio)sobre el cual se haría el trabajo en grupos por delegación, respecto al aumento en el número de delitos cibernéticos en la Región Andina, el surgimiento de un grupo terrorista y de crimen organizado que opera en muchos países de América Latina con células criminales en el extranjero que han empezado a utilizar capacidades cibernéticas extensas y profesionales para apuntar a bancos, instituciones financieras y proveedores de servicios críticos como las telecomunicaciones.

Bajo este escenario, se realizaron los siguientes ejercicios:

Fase 1: Preparación Nacional

Situación: Aumento de fraudes CEO en el sector financiero, empresas de las naciones que ha sido victimas de ransomware, ataques de denegación de servicio distribuidas con afectación parcial, filtración de datos personales, cortes de luz en entidades administrativas de diferentes países, algunos sitios web gubernamentales pierden disponibilidad y son desfiguradas durante un par de horas.

Bajo esta situación se evaluó la criticidad de los eventos, la definición de las acciones

prioritarias, elaboración de mensajes al público, propuestas de intercambio de información y actividades regional e internacional.

Fase 2: Respuesta a la cibercrisis nacional

Situación: Portales de medios y servicios estatales caen bajo ataques de denegación de servicio distribuido, de múltiples bancos sus servicios en línea dejan de estar disponibles por campañas de ransomware, cientos de empresas y proveedores de servicios han sufrido ataques de ransomware similares, afectando también a autoridades aduaneras en Bolivia y Perú, los atacantes piden un rescate de 200 BTC, conversaciones por correo electrónico entre miembros del gabinete de altos funcionarios son filtradas, sistemas de facturación y servicios en línea de empresas de telecomunicaciones dejaron de funcionar, los países afectados reciben atención negativa a nivel mundial porque no han tomado acciones cibernéticas suficientes.

Bajo esta situación se evaluó los impactos de los ciberincidentes y su importancia en la seguridad nacional, la definición de acciones y actividades prioritarias, mensajes orientados a la ciudadanía y propuestas para reuniones de gabinete para mejorar la coordinación nacional en la gestión de crisis.

Fase 3: Respondiendo a la crisis cibernética regional/internacional

Situación: Problemas serios en las redes eléctricas de los diferentes países regionales, apagones por tiempos cortos, problemas de fondo que no tienen una solución; los problemas también se ven en operadores de telecomunicaciones móviles en todos los países ya que sufren cortes de servicio de datos y telefonía, el frente patriótico de ciberliberación se atribuyen los ataques y mencionan que tienen el control de servicios críticos, expertos confirman que las redes parecen estar controladas desde fuera del país ya que se descubren servidores de comando y control. La gente está molesta y ocurren protestas amenazantes contra el gobierno y los jefes de estado se reúnen pidiendo planes de corto y largo plazo para resolver el problema.

Bajo esta situación como grupo de trabajo se definieron acciones prioritarias para emprender como región andina.

Para cada fase las delegaciones expusieron sus acciones conforme a lo solicitado por los moderadores en plenarias de discusión y retroalimentación, de las cuales se destacan las siguientes:

- No se debe burocratizar la respuesta a las crisis cibernéticas, las comunicación debe ser la

más rápida posible.

- Al interior de cada país deben estar claramente identificados los canales de comunicación, roles y coordinación público/privado en la respuesta a las crisis cibernéticas.

- Informar al Presidente del Estado sobre el estado de la ciberseguridad con regularidad y sobre todo cuándo hay crisis que afectan servicios críticos y esenciales.

- Los países de la región deben contar con procedimientos comunes de respuesta a las crisis cibernéticas, para ello los estados necesitan contar con normas similares, por ejemplo delitos cibernéticos, estrategias de ciberseguridad.

- El intercambio de información entre autoridades competentes en ciberseguridad de los países de la región andina.

- Ecuador cuenta con un embajador digital que se encarga de informar de manera diplomática asuntos de ciberseguridad a nivel local e internacional.

- Establecer puntos de contacto para intercambiar experiencias e información relevante sobre amenazas potenciales para la región andina.

CONCLUSIONES

Se participó en el "I Ejercicio de Ciberseguridad para la Región Andina", en la que participaron delegaciones de Colombia, Ecuador, Perú y Bolivia, evento auspiciado organizado por la Secretaría General de la Comunidad Andina de Naciones en el marco de la Agenda Digital Andina, y auspiciado por el Centro de Competencia de Cibercapacidades de Latinoamerica y el Caribe "LAC4".

En el ejercicio se puso a prueba las capacidades organizativas, normativas y operativas en respuesta a las crisis cibernéticas al interior de cada país y también como región, mediante escenarios dónde se producen ataques a proveedores de servicios esenciales.

ANEXOS

[X] Pases a Bordo o certificación de vuelo emitida por la línea aérea (firmado digitalmente)

[ ] Factura, boleto o recibo por transporte terrestre (firmado digitalmente) (solicitar reembolso por caja chica)

[X] Otros (como ser fotos, planillas de asistencia, certificaciones, invitaciones etc.) (firmado digitalmente)

Documentos adjuntos:
Tarjeta de Embarque _Retorno_ LATAM Airlines-firmado.pdf
Tarjeta de Embarque _ LATAM Airlines-firmado.pdf
actividades_lac4-firmado.pdf
fotografias-firmado.pdf
Certificado-firmado.pdf

CONFORMIDAD

PARA:	Claudia Soraya Cuevas Simons JEFE ADMINISTRATIVA FINANCIERA
DE:	VLADIMIR TERAN GUTIERREZ DIRECTOR GENERAL EJECUTIVO
REF.:	Informe "I Ejercicio de Ciberseguridad para la Región Andina"

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.

Firmado por el Jefe de Unidad o Autoridad competente del comisionado.

FRC
Cc.:archivo