

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 Encuentro Regional de Políticas Públicas de Seguridad Informática

N° de Memorandum: AGETIC/RA/0120/2022

ITINERARIO

Fecha de Salida	Fecha de Retorno	Hora de Salida	Hora de Retorno
21/09/2022	24/09/2022	07:25	21:25
Lugar/Ruta de viaje		Medio de Transporte	
Buenos Aires/La Paz-Santa Cruz		Aéreo	

DESARROLLO

Objetivo de Viaje

Compartir las políticas públicas en seguridad informática implementadas por el Estado Plurinacional de Bolivia desde la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, en el encuentro Regional organizado por la Fundación Vía Libre, el Observatorio de Derecho Informático Argentino y Democracia en Red apoyado por la Iniciativa por los Derechos Digitales en Latinoamérica y la Friedrich-Ebert-Stiftung Argentina.

Actividades Realizadas

Se detallan a continuación las actividades realizadas por día:

Jueves 22 de septiembre 2022

Se conformo una mesa de trabajo que inicia a horas 15 aproximadamente, de la que participaron representantes de Democracia en Red, Funación vía Libre y el Observatorio de Derecho Informático Argentino, Subsecretaria del Interior de Chile, Dirección General de Ciberseguridad y Protección de la Información de Paraguay.

En la mesa se trataron los incidentes que vienen ocurriendo en Argentina, los organizadores describieron la iniciativa "datosenfuga" que es un proyecto que busca concientizar a la población y al gobierno Argentino sobre la importancia de proteger los datos personales.

Los organizadores expusieron casos en que personas de la sociedad civil reportaron problemas de seguridad y que producto de la acción fueron procesados judicialmente, casos de Joaquin Sorianello y Ariel Ortmann que están publicados en <https://datosenfuga.org/#/casos>.

Respecto a Paraguay, la representante Gabriela Ratti expuso el marco normativo en temas de delitos informáticos, que no tuvieron casos en que reportantes fueran procesado, siendo que el CSIRT de su País es el que recibe y comunica las vulnerabilidades.

Respecto a Chile, el representante Daniel Alvarez indicó que vienen trabajando en la modificación del mecanismo de reporte, que busca eximir de responsabilidad a las personas que reportan fallas de seguridad, que un escaneo es considerado delito informático.

Respecto a las experiencias en Bolivia sobre el reporte de vulnerabilidades, se compartió la experiencia del muro de la fama, el cual es un medio para recibir reportes de personas nacionales e internacionales sobre fallas de seguridad en sistemas de información de las entidades públicas, además de exponer el avance en la implementación del uso de software libre.

Viernes 23 de septiembre de 2022

El evento público inició a horas 10 aproximadamente, la primera parte en la que el panel conformado por representantes de las 3 organizaciones hicieron el análisis de la situación actual en ciberseguridad respecto a incidentes informáticos, reporte de vulnerabilidades, los proyectos que están en curso para actualizar la ley de protección de datos personales, haciendo referencia a las conclusiones del día anterior. Concluyen que es importante establecer procedimientos seguros de reporte de fallas de seguridad para evitar casos como

Sorianello y Ortmann.

En la segunda parte del evento, conformado por representantes de Chile, Paraguay, Argentina y Bolivia que tienen competencia sobre las políticas en seguridad informática. Se puso en debate la importancia de asignar recursos para implementar acciones y políticas de ciberseguridad y que la misma sea resiliente en el tiempo sin importar cambios de autoridad, se mencionó que la ciberseguridad es inminentemente política porque de ella depende la viabilidad de aprobar leyes, generar un entedimiento en palabras no técnicas con las autoridades políticas, judiciales, que involucrar a la sociedad representada por sus organizaciones es vital para generar consenso y concientización, que en algunos casos es también aprovechar las oportunidades, porque la ciberseguridad no siempre es prioridad.

Se compartió con el público la experiencia que Bolivia tienen en la reducción significativa de incidentes informáticos, desde la creación de la AGETIC y operación del CGII, que con enfoque de colaboración apoyada en las comunidades de hacking se pudo avanzar en reducción de brechas de seguridad a través de reportes que el CGII canaliza por mandato normativo y que es de cumplimiento de las entidades afectadas.

CONCLUSIONES

Se participó del evento Encuentro Regional de Políticas Públicas de Seguridad Informática, que se realizó en el Salón Vélez Sarsfield de la Facultad de Derecho, Universidad de Buenos Aires el 22 y 23 de septiembre.

Como aporte al encuentro se brindó la experiencia en la gestión de vulnerabilidades informáticas y también la oportunidad fue útil para conocer los avances y desafíos de Argentina, Chile y Paraguay en Ciberseguridad, y ver en que punto nos encontramos respecto al resto de países de la región. Como conclusión es importante proponer normativa en ciberseguridad con alcance a todo el estado con la finalidad de proteger la información de las instituciones y personas.

Los gatos de pasajes y estadía fueron cubiertos por la organización.

ANEXOS

- 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)
- Otros (como ser fotos, planillas de asistencia, certificaciones, invitaciones etc.) (firmado

AGETIC/IV/0329/2022
Expediente : 172234
Código de verificación : 1-EPVTDBJW



13 de Octubre de 2022

digitalmente)
Documentos adjuntos:
BoardingPass-firmado.pdf
PasesaBordo-firmado.pdf
fotos-firmado.pdf

CONFORMIDAD

PARA: JORGE RAMIRO MENDIETA FRANCO
Responsable de Planificación
VÍA: VLADIMIR TERAN GUTIERREZ
DIRECTOR GENERAL EJECUTIVO
DE: Franz Rojas Castillo
RESPONSABLE CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS
REF.: Informe Encuentro Regional de Políticas Públicas de Seguridad Informática

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