AGETIC/IV/0072/2023
Expediente : 196892
Código de verificación : 1-5CXKCXB3

AGETIC

25 de Abril de 2023

Clasificación : Reservado

# INFORME DE VIAJE Y CONFORMIDAD

# INFORME DE VIAJE

| | |
|---|---|
| PARA: | Franz Rojas Castillo<br>RESPONSABLE CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS |
| DE: | STEPHANIE KRISSIA FERREIRA PARAVICINI<br>PROF. GESTIÓN DE INCIDENTES Y VULNERABILIDADES INFORMÁTICOS |
| ASUNTO: | Asistencia III Jornada STIC - Capítulo República Dominicana |

N° de Memorándum: AGETIC/M/0255/2023 AGETIC/SPV/0082/2023 AGETIC/RA/0034/2023

## ITINERARIO

| Fecha de Salida | Fecha de Retorno | Hora de Salida | Hora de Retorno |
|---|---|---|---|
| 18/04/2023 | 23/04/2023 | 02:10 | 02:05 |

| Lugar/Ruta de viaje | Medio de Transporte |
|---|---|
| La Paz - Bogotá - Punta Cana - Bogotá - La Paz | Aéreo |

## DESARROLLO

### Objetivo de Viaje

Participar en los talleres prácticos presenciales y conferencias magistrales especializadas en ciberseguridad impartidos en las "III Jornadas STIC - Capítulo República Dominicana" además de ampliar la red de contactos a nivel internacional con organizmos de similiar función para la gestión de incidentes informáticos conforme a lo establecido en el DS. 2514.

### Actividades Realizadas

Se detallan a continuación las actividades realizadas por día:

III Jornada STIC - Capítulo República Dominicana

| Fecha | Actividades Realizadas |
|---|---|
| Martes, 18 de abril del 2023 | - Viaje de ida La Paz - Bogotá - Punta Cana<br>- Check in en hotel "Barceló Bávaro Palace" lugar dónde se llevaría a cabo el evento.<br>- Acreditación en el evento. |
| Miércoles, 19 de abril del 2023 | Asistencia en las siguientes conferencias:<br>- Inauguración.<br>- Un ciberescudo único para Iberoamérica. El intercambio es la clave.<br>- Lucha contra el Cibercrimen en Honduras.<br>- Respondiendo a Incidentes de Ciberseguridad usando Inteligencia de Amenazas.<br>- Gestión de Incidentes: por qué la remediación es clave.<br>- SOC contra el ransomware.<br><br>Asistencia en los siguientes talleres prácticos:<br>- Taller Ransomware: recuperación.<br>Expositor: CCN CERT<br>Descripción: En el taller se expuso cómo el ransomware entra en las redes institucionales, las facilidades que en ciertas ocasiones los usuarios les dan a los atacantes, tiempo de recuperación que suele tener una institución conforme al tamaño de la misma, medidas de prevención, medidas para defenderse del ransomware, dónde sugirieron el uso de Antivirus, EDR, IDS, IPS, firewall y la sementación de la red, sugirió la regla del 3,2,1 que implica tener 3 copias de datos, 2 formatos diferentes y 1 copia offline, considerando siempre probar las copias de respaldo. En la parte práctica nos proporcionaron logs del Firewall, de una herramienta de análisis denominada Thor, logs de la VPN, siendo que se enseñó cómo investigar la superficie de exposición y la correlación de los datos, para la recuperación indicó realizar:<br>- Análisis y búsqueda de IOC.<br>- Instalación EDR.<br>- Instalación microClaudia.<br>- Gestión de contraseña administrador local con LAPS.<br>- Análisis seguridad y vulnerabilidades.<br>- Establecer medidas de detección mediante monitoreo.<br>- Disponer de un plan de actuación para incidentes futuros.<br>- Taller práctico de Análisis de soluciones de intercambio ¿seguro? de información y ¿con cifrado extremo a extremo (E2EE)?<br>Expositor: Mónica Salas y Raúl Siles de la empresa DinoSec / GuardedBox<br>Descripción: En el taller se expuso la diferencia de un cifrado extremo a extremo para el envío de secretos entre varias partes interesadas y el cifrado únicamente realizado mediante SSL, siendo que la diferencia principal es que en un cifrado extremo a extremo correctamente elaborado únicamente las partes interesadas deben tener acceso a la información, siendo que ni siquiera el servidor, ni el cliente (en caso de una interceptación) debería registrar el secreto en ningun momento en forma plana, para ello la llave se utiliza después del # en la url siendo que el servidor nunca registrará lo que va después del #, y esta llave también va cifrada y es utilizada por el cliente para poder descifrar el mensaje, |

| | |
|---|---|
| | mostraron ejemplos de plataformas que prometen enviar de forma cifrada los secretos sin embargo no realizan correctamente esta función, ellos elaboraron una herramienta que realizar el cifrado extremo a extremos y nos demostraron mediante proxy todo lo indicando. |
| Jueves, 20 de abril del 2023 | Asistencia en las siguientes conferencias:<br>- Presentación Guía Práctica para CSIRTs.<br>- Introduction to the Canadian Centre for cyber Security.<br>- Experiencias de un CSIRT en el Intercambio de información.<br>- La importancia del Gobierno de la Ciberseguridad: Aproximación y desafíos.<br>- Seguridad en Telefónica_Capacidades propias.<br>- Arquitectura segura de aplicaciones de pagos y de comercio electrónico.<br>- Laguun - Virtual Ciso Evolving Platform.<br>- Incidente controlado. ¿y ahora qué hago?.<br>- Gobernanza de la ciberseguridad.<br>- Gestión de Cibercrisis: modelos organizativos y operacionales.<br><br>Asistencia al siguiente taller práctico:<br>- Estudios forenses y amenazas en dispositivos móviles.<br>Expositor: Buenaventura Salcedo de la empresa S2 Grupo<br>Descripción: En el taller estaba enfocado a amenazas y análisis forense de dispositivos iOS, en el taller se realizó una copia de todo un dispositivo iOS en busca de información de las diferentes aplicaciones instaladas, para ello utilizó iLEAPP y libimobiledevice, la primera copia generada sus carpetas y ficheros estaban cifrados, para descifrar el backup utilizó mvt-ios y se verificó que los metadatos no fueron alterados, también mostró el uso de la herramienta idevicecrashreport para obtener los logs del dispositivo y otorgó una lista de ficheros a revisar después de ejecutar exitosamente la herramienta como por ejemplo para mostrar información de las particiones, los procesos que están corriendo, el listado de hilos de los procesos, servicios remotos, telemetría WiFi entre otros, también explicó la diferencia entre realizar un análisis dinámico sin obtener el Jailbreak, explicando sus limitantes, dónde resalta que los datos obtenidos del triage son más limitados y requiere una instalación previa en el dispositivo móvil iOS. |
| Viernes, 21 de abril del 2023 | Asistencia en las siguientes conferencias:<br>- DNS: Seguridad e Investigaciones.<br>- Rep. Dom. Archipiélago para la defensa del ciberespacio<br>- Tendencias del cibercrimen en República Dominicana (Ciberdelicuencia)<br>- ITLA: Educación, Ciberseguridad y Nuevos Retos. Caso de Éxito Instituto Tecnológico de las Américas<br>- CSIRT Sectorial para sistemas financieros: experiencia de la República Dominicana.<br>- Ciberterrorismo: Otro Ángulo del Cibercrimen.<br>- Ciberescudo Dominicano: Aplicación práctica de inteligencia cibernética.<br>- ACTO DE CLAUSURA |
| Sábado, 22 de abril del 2023 | Vuelo de retorno por etinerario Punta Cana - Bogotá - La Paz |
| Domingo, 23 de abril del 2023 | Llegada a La Paz horas 02:05 AM. |

## CONCLUSIONES

Se participó en las “III Jornadas STIC - Capítulo República Dominicana” cuyos talleres prácticos y conferencias magistrales estaban enfocados en la prevención de incidentes informáticos, cibercrimen, amenazas y cómo fue abordado en diferentes países, se presentaron también diferentes herramientas, técnicas y estadísticas de ciberseguridad; información útil para el Centro de Gestión de Incidentes Informáticos para el conocimiento y toma de decisiones con respecto al desarrollo de políticas y estrategias en ciberseguridad y gestión de incidentes informáticos.

Se estuvo en contacto con diferentes CSIRT Internacionales y empresas especializadas en ciberseguridad para intercambio de información y gestión de incidentes informáticos.

## 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:
pases-a-bordo-y-fotos-KRISSIA-FERREIRA-firmado.pdf

# CONFORMIDAD

| | |
|---|---|
| PARA: | Claudia Soraya Cuevas Simons<br>RESPONSABLE ADM-FINANCIERO |
| DE: | Franz Rojas Castillo<br>RESPONSABLE CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS |
| REF.: | Asistencia III Jornada STIC - Capítulo República Dominicana |

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.

SKFP
Cc.:archivo