# MESAS DE TRABAJO SOBRE EL PLAN DE LA SOCIEDAD DE LA INFORMACIÓN Y EL CONOCIMIENTO

| ACTA DE REUNIÓN | Ministerio de Telecomunicaciones y de la Sociedad de la Información |
|---|---|

**PLAN DE LA SOCIEDAD DE LA INFORMACIÓN Y EL CONOCIMIENTO – EJE 1: INFRAESTRUCTURA DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y BUEN USO DE LAS TIC**

**TEMÁTICA: "SEGURIDAD DE LA INFORMACIÓN"**

**ACTA nro.: 01** **FECHA DE LA REUNIÓN: 2018-05-02**

## 0. ANTECEDENTES

En la ciudad de Guayaquil, el día jueves, 03 de mayo del 2018 a las 11:15 horas, en las instalaciones de la Facultad de Jurisprudencia de la Universidad Católica Santiago de Guayaquil, se instala la primera reunión de mesas de trabajo del Eje 1 del Plan de la Sociedad de la Información y el Conocimiento para tratar la temática "SEGURIDAD DE LA INFORMACIÓN"; con la presencia de las siguientes personas:

| Nro. | REPRESENTANTE | INSTITUCIÓN |
|---|---|---|
| 1 | José Luis Loaiza | AECI |
| 2 | Joffre Martínez | AGROCALIDAD |
| 3 | Jaime Benítez | ARCOTEL |
| 4 | Fabián Íñiguez | CFN B.P. |
| 5 | Christian Cascante | CNEL |
| 6 | Karina Astudillo | ELIXIRCORP |
| 7 | Robert Andrade | ESPOL |
| 8 | Cristian Piraquive | GAD MUNICIPAL ISIDRO AYORA |
| 9 | Mario Mendoza Torres | IBM |
| 10 | Cristopher Coello | INEC |
| 11 | Leny Bastidas Falconí | INEC |
| 12 | Blenda Sánchez | INEN |
| 13 | Luisa Heredia | MIES |
| 14 | Deyanira Kure | MJDHC - Z5 |
| 15 | Omara Salazar | MREMH |
| 16 | Erick Moreno Q. | MSP Zona 5 |
| 17 | Christian Mendoza | SECUINFOR S.A. |
| 18 | Fernanda Anchuncia | SENAE |
| 19 | Nicolás Pulgar | SENAE |
| 20 | Julio Silvestre | SGMS |
| 21 | Carlos Govea | SGR |
| 22 | Felipe Arévalo Cordovilla | UNEMI |

**ACTIVIDADES DE LA REUNIÓN**

a) Apertura e inicio de las mesas de trabajo sobre “Seguridad de la Información”.
b) Exposición sobre el Eje 1, Temática: Seguridad de la Información, Ciberseguridad y Sello de Calidad de la Seguridad de la Información
c) Conformación de mesas de trabajo
d) Exposición de observaciones y propuestas
e) Cierre

## 1. DESARROLLO DE LA REUNIÓN

### a) Apertura e inicio de las mesas de trabajo sobre “Seguridad de la Información”

En Ing. Oswaldo Rivera, y el Ing. Carlos Fernández del MINTEL realizaron la bienvenida y agradecimiento a la asistencia de la mesas de trabajo, donde se mencionó la importancia de la elaboración del Plan de la Sociedad de la Información y el Conocimiento.

Posterior a esto, se procedió la presentación de cada uno de los participantes a las mesas de trabajo, indicando su nombre y la institución a la que representan.

### b) Exposición sobre el Eje 1, Temática: Seguridad de la Información, Ciberseguridad y Sello de Calidad de la Seguridad de la Información

El Ing. Oswaldo Rivera, funcionario del MINTEL procedió a exponer la temática: Seguridad de la Información, donde se mostró una introducción y la situación actual en el Ecuador. Además se mostraron los objetivos que dicha temática quería tratar.

De acuerdo a estos objetivos, se expuso sobre las iniciativas que contiene esta temática como son: “Estrategia Nacional de Cibserseguridad” y “Reconocimiento por el Sello de Calidad de la Seguridad de la Información”.

### c) Conformación de mesas de trabajo

Posterior a la exposición sobre la temática de Seguridad de la Información, se procedió a formar grupos de trabajo para los temas de los ejes que contempla la Estrategia Nacional de Ciberseguridad y el Sello de Calidad de la Seguridad de la Información. Cada eje contó con una persona que colaboró en el papel de líder de grupo que posteriormente realizó la exposición de las observaciones y propuestas de los temas tratados.

Los grupos de trabajo quedaron conformados de la siguiente manera de acuerdo a las actividades y experiencia de los presentes.

| REPRESENTANTE | INSTITUCIÓN | TEMA |
|---|---|---|
| Robert Andrade | ESPOL | Infraestructura de la Información |
| Jaime Benítez | ARCOTEL | |
| Mario Mendoza Torres | IBM | |
| José Luis Loaiza (*) | AECI | |
| Karina Astudillo | ELIXIRCORP | Prevención y Sanción |
| Deyanira Kure | MJDHC - Z5 | |
| Cristian Piraquive | GAD MUNICIPAL ISIDRO AYORA | |
| Christian Mendoza | SECUINFOR S.A. | |

| REPRESENTANTE | INSTITUCIÓN | TEMA |
|---|---|---|
| Omara Salazar | MREMH | Sensibilización, formación y difusión |
| Fernanda Anchuncia | SENAE | |
| Cristopher Coello | INEC | |
| Leny Bastidas Falconí | INEC | |
| Fabián Íñiguez | CFN B.P. | Cooperación y relaciones internacionales |
| Carlos Govea | SGR | |
| Erick Moreno Q. | MSP Zona 5 | |
| Joffre Martínez | AGROCALIDAD | |
| Christian Cascante | CNEL | Institucionalidad de la Ciberseguridad |
| Julio Silvestre | SGMS | |
| Nicolás Pulgar | SENAE | |
| Felipe Arévalo Cordovilla | UNEMI | |
| Luisa Heredia | MIES | Sello de Calidad de la seguridad de la Información |
| Blenda Sánchez | INEN | |

**d) Exposición de observaciones y propuestas**

**Mesa 1:** Institucionalidad de la ciberseguridad.

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Infraestructura de la información | • Definir la gestión del riesgo<br>• Identificación de estructuras críticas de la información<br>• Medidas para enfrentar un incidente<br>• Planes de contingencia en ciberseguridad | Gestión de la información. Una entidad que regule la creación del Gobierno de Seguridad de la información (políticas, roles, procesos) |
| | | Gestión del ciber-riesgo. Inventario de activos, metodología, estándares, tratamiento con auditorías internas de control |
| | | Protección de la información. Desarrollar normas de protección de información personal alineándose a las normas internacionales ya establecidas (GDPR). Derechos y obligaciones para el uso y tratamiento de datos |
| | | Infraestructuras críticas. Mapear e identificar los actores de las infraestructuras críticas de la sociedad (Energía, telecomunicaciones, salud, agua, transporte, servicios financieros, sistemas de Defensa Nacional) |
| | | Gestión de incidentes. Cada empresa debe disponer de un CSIRT interno o asociado que facilite la identificación de incidentes de Seguridad de la Información cubriendo a todos los actores |
| | | Resiliencia. Toda empresa debe incluir componentes, controles y tecnología que permita levantar los servicios de manera rápida frente a un incidente de seguridad |

**Mesa 2:** Prevención y sanción

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Prevención y sanción | • Definir las capacidades de levantamiento, estandarización e integración de datos e información, relacionados con el ciberdelito<br>• Aumentar la capacidad de investigación y generación de evidencia referente a ciberdelito<br>• Resguardo de derechos fundamentales en la prevención y sanción del ciberdelito | Todas las entidades o empresas guardar registros de eventos de las comunicaciones y acceso, activos informáticos e internet por un período de al menos 12 meses |
| | | Convenios bilaterales con empresas, redes sociales que brinden información eficaz para evidencia de un posible delito informático |
| | | Las penas deben ser acumulativas por lo tanto es importante la modificación al COIP |
| | | Crear una plantilla para el intercambio de la información entre las entidades de cooperación (privados, públicos, ISP, bancos, etc.) |
| | | Crear un formulario para denuncias de ciberdelitos o ciberataques |
| | | Crear boletines a los diferentes sectores de la sociedad |

**Mesa 3:** Sensibilización, formación y difusión

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Sensibilización, formación y difusión | • Promover la cultura de ciberseguridad en ciudadanía, estudiantes y funcionarios públicos<br>• Fomento de la investigación y desarrollo para la seguridad del ciberespacio; generar capacidad tecnológica propia, de acuerdo a las necesidades nacionales,<br>• Promover programas de capacitación, educación y formación a nivel pre y posgrado en ciberseguridad | Desconocimiento de los riesgos. Difundir información de manera directa e indirecta |
| | | Generar cultura informática para salvaguardar la integridad de las personas |
| | | Promover charlas sobre ciberseguridad orientada hacia diferentes tipos de público enfocados a los rangos de edades |
| | | El desconocimiento de las leyes no exime de responsabilidades de dar un mal uso a la información |
| | | Dar a conocer las sanciones por mal uso de la información pública y privada. |
| | | Falta de un ente regulador |
| | | Convenio entre el Ministerios e instituciones privadas (operadoras) para difundir y mejorar la cultura de ciberseguridad |

**Mesa 4:** Cooperación y relaciones internacionales

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Cooperación y relaciones internacionales | • Participación en foros internacionales referentes a ciberseguridad<br>• Impulso de medidas de cooperación en investigación y asistencia técnica en otros países | Buscar asesoramiento o acompañamiento de países con un nivel de madurez alto en temas de ciberseguridad (Se sugiere revisar la CCN de España) |
| | | Reforzar e impulsar competencias de EcuCERT para que ingrese a cooperar con demás CERT en Latinoamérica |
| | | Ser nosotros los que propongamos e impulsemos los foros internacionales con mira a la creación de alianzas y convenios |
| | | Sugerir la creación de comité de Seguridad de la Información internacional con países hermanos |

**Mesa 5:** Institucionalidad de la ciberseguridad

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Cooperación y relaciones internacionales | • Participación en foros internacionales referentes a ciberseguridad<br>• Impulso de medidas de cooperación en investigación y asistencia técnica en otros países | No se tiene definido a nivel de país que sectores comprenden la infraestructura crítica para poder establecer competencias de acuerdo su criticidad |
| | | Definir a nivel gobierno, cuales se consideran infraestructuras críticas y establecer una ley para proteger dichas infraestructuras de amenazas que puedan materializarse |
| | | El Estado establezca y se empodere de alianzas con privados para brindar a las entidades público – privadas de dichas alianzas |
| | | Establecer un Comité interdisciplinario con integrantes del sector público y privado |
| | | Implementar en cada empresa, colectores de logs que contribuyan a garantizar la disponibilidad de los registros para futuros análisis y/o revisiones |

**Mesa 6:** Reconocimiento del sello de calidad QSI-IKAY

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| Reconocimiento del sello de calidad QSI-IKAY | El sello de calidad de la seguridad de la información (QSI-IKAY) será un reconocimiento que el Ministerio de Telecomunicaciones otorgará a las instituciones | Definir los requisitos para la obtención del sello |
| | | Estructura de sistema de gestión mínima basada en ISO 27001 |
| | | Verificar su cumplimiento mediante auditoría, con auditores certificados en su competencia |
| | | Establecer la vigencia del sello de calidad |

| Áreas Claves | Descripción | Observaciones/Aportes |
|---|---|---|
| | público, privadas y academia, con el fin de incentivar el buen uso de las normas técnicas ecuatorianas basadas en la Seguridad de la Información | Establecer sanciones cuando no se cumpla (Ej: retiro del sello) |
| | | Definir competencias de auditores para el sello de calidad: conocimiento, habilidades, experiencia |
| | | Definir alianzas público-privadas con empresas certificadoras (Ej: SGR, BuQi, SAE, MINTEL) |
| | | Definir un plan de capacitación MINTEL en sistemas de Seguridad de la información a entidades público – privadas |

**e) Cierre**

Como parte final, los ingenieros Oswaldo Rivera y Carlos Fernández agradecen a todos los participantes sobre la importancia de crear estos espacios y generar ideas a través de ellos para la construcción del Plan de la Sociedad de la Información y el Conocimiento.

Además se indicó que los aportes se recopilaran en un acta de reunión y enviada vía correo electrónico a los participantes, a fin de que nos ayuden con la validación de la información recogida en las mesas de trabajo.

Siendo las 13:30 horas se levanta la sesión.