

Exposición sobre Dimensión 3 del Foro: Factor D 3.4 Investigación e Innovación en Ciberseguridad (según Oxford CMM2)

La presentación del Factor D 3.4, a cargo de su moderador, el profesor Julio Fenner, se centró en la investigación e innovación para enfrentar desafíos tecnológicos, sociales y empresariales. Se examinó la cultura de investigación en el país y los inputs necesarios para crear programas, incentivos y políticas nacionales que impulsen estos desarrollos.

Niveles de Madurez en I+D en Ciberseguridad

El modelo CMM2 de Oxford clasifica la madurez en investigación y desarrollo (I+D) en ciberseguridad en cinco niveles: Startup, Formativo, Establecido, Estratégico y Dinámico. Cada nivel representa un avance en la capacidad de I+D del país, desde actividades limitadas en el nivel Startup hasta una plena integración y contribución en el nivel Dinámico.

Evaluación de Chile en 2024

Según la evaluación de 2024, Chile se encuentra en el nivel de Startup. Esto revela un retraso en el desarrollo estratégico nacional hacia la madurez en ciberseguridad, pero también sugiere amplias oportunidades para mejorar y establecer nuevas políticas públicas.

Plan de Acción "Construyendo la Ciberseguridad en Chile"

El informe detalla programas específicos destinados a alcanzar el nivel de Establecido en cuatro años, incluyendo la creación de un Centro Nacional de Investigación en Ciberseguridad, un centro de escalamiento y nuevos negocios, un laboratorio nacional distribuido, y un Centro Iberoamericano de Investigación.

Colaboraciones y Reuniones Clave

Se han realizado reuniones regulares para fomentar el intercambio de ideas y colaboración entre investigadores, manteniéndolos alineados con las tendencias globales. Destaca una reunión con Cristian Bravo Lillo, director del CSIRT, para explorar estrategias avanzadas en ciberseguridad y mejorar las competencias del equipo.

Oportunidades y Futuras Iniciativas

El informe subraya la importancia de desarrollar tecnología avanzada, fomentar colaboraciones estratégicas entre academia e industria, ampliar la capacitación en ciberseguridad y participar en la creación de políticas equilibradas. Además, se identifican problemáticas futuras como el manejo de big data y la investigación en vulnerabilidades humanas.

Recomendaciones del Foro

Se recomienda implementar efectivamente la Ley Marco de Ciberseguridad, aumentar la inversión en I+D, invertir en la formación continua de profesionales, desarrollar un marco legal para la inteligencia artificial, y promover la colaboración internacional para enfrentar las amenazas cibernéticas.

Propuesta para Octubre 2024

El foro propone colaborar en la formulación de un documento sobre directrices para configurar un espacio nacional de Investigación e Innovación Avanzada en Ciberseguridad. Este documento será presentado en la reunión de octubre, con el objetivo de sentar las bases para una mayor madurez en IAC.

Chile enfrenta desafíos significativos en ciberseguridad, pero también tiene numerosas oportunidades para mejorar su protección digital y fomentar la innovación tecnológica. Siguiendo las recomendaciones del informe, el país puede fortalecer su infraestructura de ciberseguridad y avanzar hacia una mayor competitividad global.