Establecer equipos especializados en monitoreo y respuesta para Infraestructuras de Información Crítica (IIC).

Capítulo 5, Infraestructura Críticas.

Acciones (agregar en el Objetivo, al final del párrafo)

Las capacidades de los equipos definidos SOC-IIC y/o CSIRT-IIC, deberán ser especialistas en su ámbito de aplicación. Si bien podrán ser reforzados por equipos de respuesta y monitoreo que actualmente ya existen, SOC y/o CSIRT, estas acciones deberán ser lideradas por equipos especializados de IIC.

De no contar con las capacidades y recursos requeridos para ejecutar dichas acciones, se recomienda generar lazos con organizaciones internacionales y locales expertas en IIC necesaria.

Las organizaciones internacionales podrán favorecer en los eventos e incidentes que pueden ocurrir en el ciberespacio local, considerando el ciberespacio de infraestructuras críticas, el activo primario del país.

Estos lazos serán de carácter fundamental para mantener relaciones de ciber diplomacia y cooperación internacional, ya que se podrán ver afectados países y organizaciones internacionales.

Esto último es de carácter prioritario para mantener la cooperación entre grupos de trabajo y medidas de fomento de la confianza en el ciberespacio[1] promovido por los países que conforman la OEA.

[1] https://www.oascybercbms.org/es

Línea 5.2 Proteger las IIC

Acciones (agregar)

Establecer un SOC-IIC que abarque el ámbito operativo en cada organismo que gestione infraestructura de información crítica (UTE, OSE, ANCAP, Aeropuerto Internacional, BCU, etc). Este centro debe contar con un equipo altamente capacitado en ciberseguridad de infraestructuras y sistemas críticos (en algunos lugares denominados *ambientes operativos*).