Dirección Cibernética Naval

MINISTERIO DE DEFENSA / ARMADA NACIONAL / JEFATURA DE INTELIGENCIA NAVAL

BOLETÍN No. 005

Bogotá, junio 2020

ARMADA DE COLOMBIA

COMO GESTIÓNAR UN INCIDENTE CIBERNÉTICO

A pesar que se dispongan de medidas de seguridad digital para la infraestructura crítica cibernética naval, siempre será probable que **el riesgo cibernético** se materializarse. Por este motivo, es imprescindible contar con un plan de acción que marque las pautas a seguir en el caso que se origine algún incidente cibernético.

Para la gestión de los reportes de eventos o incidentes cibernéticos es importante actuar de manera ágil y organizada en el menor tiempo posible, a fin de mitigar el impacto e identificar las acciones de la amenaza cibernética. Para ello, se debe tener en cuenta la severidad del incidente; aplicando las siguientes **fases para la gestión de un incidente cibernético,** así:

1. PREPARACIÓN

La institución debe tener el CSOC preparado con las personas, procedimientos y tecnología para poder estar listo ante cualquier suceso de carácter cibernético que pueda ocurrir.

2. DETECCIÓN

El evento o incidente cibernético es reportado al OSI de la guarnición, a fin de continuar el proceso de contención, detectando por medio de personas y herramientas propias, producto del constante monitoreo a la ICCN y correlación con inteligencia de amenazas cibernéticas.

3. CONTENCIÓN

Realización de acciones rápidas y ágiles para detener el evento o incidente cibernético, para que no escale o distribuya hacia otros sistemas, minimizando el posible y potencial daño de la ICCN.

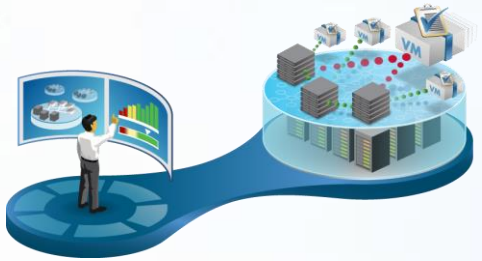
4. ERRADICACIÓN

Consiste en volver a el nivel de operación normal de la ICCN afectada, identificando, eliminando y recolectando evidencia de lo que originó el incidente cibernetico.

5. REPORTE POST-INCIDENTE

En esta ultima fase se retroalimenta el reporte cibernético en la mesa de ayuda, anexando y enviando los reportes de resultado de la ejecución de herramientas como antivirus, antimalware, recolección de indicadores de compromiso (IoC), muestras de malware con el fin de generar lecciones aprendidas.

NOTA: Los tickets que son creados en la mesa de servicios por la Dirección Cibernética Naval deben ser **únicamente** evaluados y cerrados por el **CSOC-DICIB**.



Fuente

- Gestión incidentes cibernéticos en la Infraestructura Crítica Cibernética Naval (PICCN).
- Guía Gestión de Reportes Cibernéticos.

Dirección Cibernética Naval
dicib.soc@armada.mil.co