Dirección Cibernética Naval

MINISTERIO DE DEFENSA / ARMADA NACIONAL / JEFATURA DE INTELIGENCIA NAVAL

BOLETÍN No. 006

Bogotá, junio 2020

ARMADA DE COLOMBIA

PASOS BÁSICOS PARA GESTIONAR UN INCIDENTE CIBERNÉTICO

Para realizar una gestión adecuada, se establecen los siguientes pasos básicos a seguir que se podrán adoptar al momento de recibir un evento o incidente cibernético por parte del **CSOC-DICIB**, donde el OSI/Vigía deberá tomar acción en el menor tiempo posible, con el fin de mitigar el impacto cibernético y contaminación de otros sistemas de la Institución.

1. Realizar la instalación del agente de ciberseguridad.

2. Recolección de **Indicadores de Compromiso IoC.**

3. Activar políticas de seguridad en el Firewall del **S.O**.

4. Instalar el agente del antivirus y actualizarlo con la consola de la unidad y/o central.

5. Mantener activa la detección de amenazas automáticas y realizar escaneo.

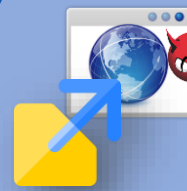
6. Verificar los procesos y recursos del S.O; memoria RAM, red de datos, memoria ROM y CPU.

7. Verificar los programas instalados sin permiso del departamento de telemática de la unidad.

8. Verificar los programas que inician automáticamente con el S.O.

9. Verificar componentes (Plugins y Addon`s) agregados en los navegadores web.

10. Comprobar que las cuentas de usuario local, estén sin privilegios de administración sobre el equipo institucional.



11. Verificar si existen accesos directos que dirigen a sitios web maliciosos.

12. Eliminar archivos temporales ingresando en modo seguro.

13. Mantener actualizados los S.O con los parches de seguridad disponibles.

14. Realizar endurecimiento a la seguridad del S.O.

Fuente

Guía Gestión de Reportes Cibernéticos.
Dirección Cibernética Naval
dicib.soc@armada.mil.co

Nota: No realice formateo del equipo comprometido sin antes realizar los **14 pasos básicos** anteriores.