# Dirección Cibernética Naval

MINISTERIO DE DEFENSA / ARMADA NACIONAL / JEFATURA DE INTELIGENCIA NAVAL

**BOLETÍN CIBERNÉTICO No. 007**

**Bogotá, julio 2020**

ARMADA DE COLOMBIA

## TIPS PARA UNA CORRECTA HIGIENE CIBERNÉTICA NAVAL

### ¿Que es la Higiene Cibernética Naval?

Son todas aquellas buenas practicas en ciberseguridad aplicadas diariamente al operar activos críticos cibernéticos de la Infraestructura Critica Cibernética Naval (ICCN) que ayudan a minimizar el riesgo cibernético y preservar la integridad de estos cibersistemas críticos. **Ayude a reducir el riesgo cibernético y mantenga la DISCIPLINA CIBERNÉTICA, aplicando los siguientes Tips.**

### RECOMENDACIONES GENERALES

- Proteger la Información que contienen los cibersistemas (TI y TO) de las ICCN.
- Reforzar reglas de navegación (equipos seguridad perimetral) hacia el ciberespacio.
- Realizar y mantener copias de seguridad de los sistemas e información crítica (Donde aplique).
- Aplicar protección en capas contra Amenazas Persistentes Avanzadas (APT), virus y otros tipos de malware.
- Realizar configuración segura (Endurecer) de los sistemas cibernéticos (TI/TO) de las ICCN.
- Verificar, analizar y escanear todos los correos electrónicos entrantes a la institución.
- Minimizar cuentas administrativas en los sistemas y activos cibernéticos de las ICCN.
- Implementar y garantizar controles de seguridad digital adecuados en cualquier acuerdo de servicio (Proveedores) implementado en los sistemas de las ICCN.
- Implementar los controles del Centro de Seguridad de Internet (CIS) para una defensa efectiva. (https://www.cisecurity.org).


### 1 Acceso Controlado

Controlar y monitorear los permisos otorgados para el acceso a los sistemas y plataformas de las ICCN.

### 2 Actualización de los sistemas

Realizar actualización y mejora en la seguridad a los sistemas operativos de los activos cibernéticos institucionales.

### 3 Protección de la red naval

Verificar el estado de los sistemas de seguridad perimetral y antivirus, que se mantengan actualizados y funcionando de manera correcta.

### 4 Copias de seguridad

Realizar copia segura de la información, puede realizarse diaria o semanalmente.

### 5 Protección de equipos cibernéticos TI y TO

Mantener actualizados los equipos de TI y TO de las ICCN a nivel de software, hardware y firmware de seguridad, teniendo en cuenta el riesgo cibernético.

### 6 Gestionar reportes cibernéticos

Gestionar oportunamente las recomendaciones suministradas por los reportes cibernéticos generados desde el Centro de Operaciones de Ciberseguridad Naval (CSOC).