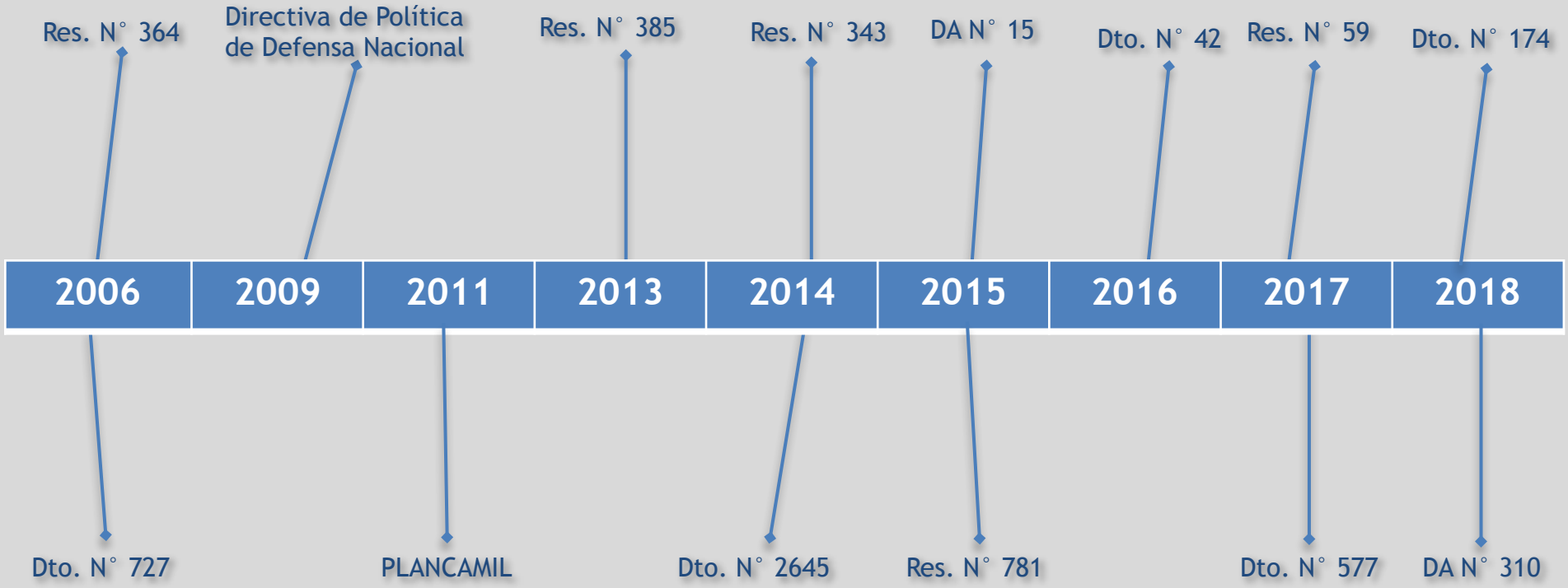
Ministerio de Defensa
Presidencia de la Nación

CIBERSEGURIDAD EN EL SECTOR PÚBLICO

Agenda

- Normativa Ministerio de Defensa
- Desafíos y Proyección
- Conclusiones


Res. N° 364
Directiva de Política de Defensa Nacional
Res. N° 385
Res. N° 343
DA N° 15
Dto. N° 42
Res. N° 59
Dto. N° 174
2006
2009
2011
2013
2014
2015
2016
2017
2018
Dto. N° 727
PLANCAMIL
Dto. N° 2645
Res. N° 781
Dto. N° 577
DA N° 310

2006

Comité de Seguridad de la Información

Por **Resolución N° 364**, del 12 de abril de 2006, se creó el Comité de Seguridad de la Información del Ministerio de Defensa. Ordena contribuir desde el Ministerio de Defensa en el proceso de protección de infraestructuras críticas (proceso coordinado desde la Jefatura de Gabinete de Ministros).

Reglamentación de la Ley de Defensa Nacional 23.554

La **reglamentación de la ley realizada mediante Decreto N° 727/2006**, establece en su artículo primero los requisitos para el empleo de las Fuerzas Armadas, los cuales consisten en la existencia de agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s.

Define la agresión de origen externo como “el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas”.

2013

Unidad de Coordinación de Ciberdefensa

Creada por la **Resolución N° 385** en el ámbito de la Jefatura de Gabinete del Ministerio de Defensa.
Su función específica consistió en coordinar las políticas y el desempeño de los actores vinculados a la ciberdefensa en la jurisdicción.
Una tarea especialmente asignada a esta Unidad fue la de elaborar una propuesta de estructura orgánica que asuma las competencias relativas al desarrollo e implementación de las políticas de ciberdefensa en la jurisdicción del Ministerio de Defensa.

2014

Comando Conjunto de Ciberdefensa

La **Resolución N° 343**, del 14 de mayo de 2014, dispuso la creación de un Comando Conjunto de Ciberdefensa dependiente orgánica, funcional y operacionalmente del Estado Mayor Conjunto de las Fuerzas. La principal capacidad que debe desarrollar este nuevo comando es la de conjurar y repeler ciberataques contra infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar.

Actualización de la Directiva de Política de Defensa Nacional

La actualización de la **DPDN (Dto. N° 2645/2014)** contempló de manera expresa la importancia del ciberespacio para el desarrollo de las operaciones militares.

La Directiva plantea la necesidad de desarrollar capacidades operacionales en la dimensión ciberespacial tendientes a adquirir competencias en los ambientes terrestres, naval y aéreo; así como el de incrementar la ciberseguridad de redes pertenecientes al sistema de defensa nacional y de los objetivos de valor estratégico.

2015

Dirección General de Ciberdefensa.

La, **Decisión Administrativa N° 15,** crea dentro del Ministerio de Defensa la Dirección General de Ciberdefensa, dependiendo directamente de la Unidad Ministro.

Entre sus funciones destacan la coordinación con organismos y autoridades de los distintos poderes del Estado, la intervención en la orientación de las acciones de ciberdefensa ejecutadas por el Nivel Estratégico Militar, el control funcional sobre el Comando Conjunto de Ciberdefensa, la intervención en el diseño de políticas, normas y procedimientos de seguridad de la información y el fomento de políticas de formación de recursos humanos.

Política de Seguridad

Por medio de la **Res. N° 781** se aprobó la **Política de Seguridad** de implementación en la jurisdicción Ministerio de Defensa y organismos descentralizados en su órbita.

Tiene por objeto garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la jurisdicción.

2016

Subsecretaría de Ciberdefensa

El **Decreto N° 42** aprueba la nueva estructura del Ministerio de Defensa. Allí se jerarquizan las actividades vinculadas a la ciberdefensa y se crea la Subsecretaría de Ciberdefensa, atribuyéndole las siguientes responsabilidades :

- Planear, diseñar y elaborar la política de ciberdefensa.
- Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas y todas las responsabilidades que es esto se derivan.
- Coordinar con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la Jurisdicción Defensa a la política nacional de ciberseguridad y de protección de infraestructura crítica.

2017

Resolución N° 59, modificatoria de la Res. N° 781/15:

- Establece, dentro del artículo 5, de la Ley de Defensa Nacional, el alcance de la "Ciberdefensa", desde la seguridad de la información y la ciberseguridad, hasta la defensa "en" y "mediante" el ciberespacio del Sistema de Defensa Nacional, para ser aplicado al planeamiento, formulación, conducción y evaluación de políticas, planes, programas y acciones en el Ministerio de Defensa, sus organismos dependientes, Fuerzas Armadas y toda aquella infraestructura crítica que pueda afectar la soberanía del país, la integridad territorial, la capacidad de autodeterminación, o la vida y la libertad de sus habitantes, a los efectos de abordar este nuevo dominio de manera sistémica e integral."
- Define a la Ciberdefensa como el "Conjunto de acciones para prevenir, detectar, identificar, anular, disuadir, contrarrestar, contener y/o repeler una amenaza o agresión cibernética inmediata, latente o potencial a infraestructuras tecnológicas, los servicios que prestan y o la información que manejan".

2017

Comité Nacional de Ciberseguridad

El **Decreto N°577**crea el Comité Nacional de Ciberseguridad.
Este Comité está integrado por los Ministerios de Modernización, Seguridad y Defensa.
En ese marco, se encuentra desarrollando la Estrategia Nacional de Ciberseguridad, la cual es un documento transversal con alcance para todo el sector público y privado, que servirá de fundamento para establecer las previsiones a nivel nacional en materia de protección de las actividades que se desarrollen en el ciberespacio.

2018

Decreto 174/2018

- ✓ Este decreto aprueba los organigramas de varios ministerios nacionales, entre ellos el del Ministerio de Defensa. Allí se establece que la Subsecretaría de Ciberdefensa queda en la órbita de la Secretaría de Investigación, Política Industrial y Producción para la Defensa.
- ✓ Asimismo, este decreto establece para la Subsecretaría de Ciberdefensa los mismos diez objetivos que le fueron otorgados por el Decreto 42/2016.

Decisión Administrativa 310/2018

- ✓ Esta normativa aprueba las estructuras organizacionales inferiores de los ministerios nacionales. En la órbita de la Subsecretaría de Ciberdefensa se crearon: **la Dirección de Asuntos Regulatorios de la Ciberdefensa, la Dirección de Diseño de Políticas para la Ciberdefensa y la Coordinación de Operaciones para la Ciberdefensa.**


CIBERESPACIO
ESPACIO
AIRE
AGUA
TIERRA

El ciberespacio como quinto dominio de naturaleza militar

Operación militar:

Planificación y movilización de las fuerzas militares asignando recursos para conseguir metas u objetivos específicos.

Implicancias:

Redefinición de los conflictos internacionales y de las políticas de ciberdefensa.

- Guerra o conflicto tradicional: entre fuerzas militares de los Estados.
- Nuevos conflictos: frontera difusa paz/guerra.
- Conflictos asimétricos: no existe un frente determinado ni acciones militares convencionales.
- Conflictos híbridos: combinan el empleo de medios irregulares y convencionales, puede darse entre actores estatales y no estatales. Incluyen ataques en tiempos de paz por medio ciberataques.

Comité de Ciberseguridad

Comité de Ciberseguridad Ampliado

Ejes de trabajo del Comité de Ciberseguridad

Estrategia de Ciberseguridad

- Creación del Comité
- Definición e implementación de la Estrategia Nacional

Infraestructuras Críticas

- Definición e identificación
- Normativa para definir Medidas de protección
- Metodología de auditoría

Marco Normativo

- Andamiaje legal de la Estrategia Nacional
- Normativa para la protección de la información del Sector Público

Formación de RRHH

- Construcción de conocimiento y habilidades en ciberseguridad en el Estado
- Desarrollo de carreras técnicas y de grado
- Concientización sobre uso seguro del ciberespacio

Procesos / Protocolos de Interacción

- Definición e implementación de procesos, procedimientos, roles e intercambio de información sobre incidentes de ciberseguridad.

Coordinación Operativa

- Solución con herramientas compatibles
- Eficiencia en las inversiones
- Eficacia en la operación y gestión de incidentes y ciberataques

Conclusiones

- Coordinarnos en las tareas a partir de la **competencia**.
- Estandarizar procesos y **protocolos**.
- Trabajar desde el punto de vista del **CIUDADANO**.

Muchas Gracias

Ministerio de
Defensa
Presidencia de la Nación