LA REPÚBLICA ARGENTINA Y SUS ESFUERZOS EN CIBERDEFENSA

EL COMPROMISO CON LAS BUENAS PRÁCTICAS COMO PARTE DE SU IDEARIO

Por el GB **TOMÁS RAMÓN MOYANO**

ARTÍCULO CON REFERATO

Palabras Clave:
> Comando Conjunto
> Ciberdefensa
> Ciberseguridad
> Infraestructura

El presente artículo, elaborado por el Estado Mayor del Comando Conjunto de Ciberdefensa, es parte de una ponencia realizada por su anterior Comandante, el GB **Tomás Ramón Moyano,** ante el Inter-American Defense College, en el marco de la "1.a Conferencia sobre Ciberseguridad y Ciberdefensa, Mejores Prácticas y Lecciones Aprendidas", desarrollada en Washington DC el 6 y 7 de noviembre de 2019.

"El propio concepto de "Buena Práctica" otorga una validación que destaca e institucionaliza propiedades y cualidades que hacen a una práctica buena más allá de su contexto específico. El reconocimiento de una Buena Práctica lleva implícito el de su transferibilidad, dado que se la entiende susceptible de convertirse en referencia para la acción en otras situaciones similares. Es necesario considerar sin embargo que una práctica no sólo es buena porque es eficaz y eficiente sino porque lleva incorporados valores que se consideran positivos, en este sentido las prácticas nunca son neutras [...]".

Extraído de Reflexiones en torno al Intercambio de Buenas Prácticas El Ágora – Asociación Civil sin fines de lucro

INTRODUCCIÓN

1. Creación del Comando Conjunto de Ciberdefensa. Pilares organizacionales

En el marco de la transformación que ha experimentado el conflicto en el contexto internacional y los desafíos que este aspecto plantea en materia de Defensa, la República Argentina vio como necesario asumir el compromiso de preparar a sus Fuerzas Armadas para este nuevo escenario. Las acciones liminares a la creación del Comando Conjunto de Ciberdefensa las podemos representar en una sucesión cronológica, materializada en distintos documentos hasta mayo de 2014, momento de su creación. Posterior a ese año, otros documentos fueron complementando o adecuando la nueva organización.

La consideración del ciberespacio como una dimensión operacional utilizada por el hombre con distintos fines, que puede derivar en situaciones de tensión, crisis y conflicto, y la adecuación del Sistema de Defensa Nacional a las nuevas variables del conflicto, sumado a la característica de no ser propia de un ámbito específico, dio origen a la creación del Comando Conjunto de Ciberdefensa (en adelante CCCD) para garantizar la defensa de aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar y aquellos dirigidos a afectar los Objetivos de valor

El Comité de Ciberseguridad surge como una respuesta a la necesidad de reunir a los representantes de las principales áreas del gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada, desarrollar el plan de acción necesario para la implementación de dicha Estrategia.

CV

TOMÁS RAMÓN MOYANO

General de Brigada, Licenciado en Estrategia y Organización de la Escuela Superior de Guerra "Teniente General LUIS MARÍA CAMPOS" y Egresado del Centro de Estudios Hemisféricos de Defensa "WILLIAM J. PERRY". Se desempeñó en 2019 como Comandante Conjunto de Ciberdefensa, representando al Estado Mayor Conjunto como expositor en esta materia en Brasil, Colombia y Estados Unidos. Actualmente es el Comandante de la Fuerza de Despliegue Rápido del Ejército.

estratégico que se determinen para su protección.

Con los documentos rectores que establecen las bases fundacionales del CCCD, se dio inicio a la ardua tarea organizacional con un grupo destacado, pero a la vez reducido de personas. Sobre ellos recayó la responsabilidad de redactar los postulados que fijan la impronta de esta joven, dinámica y cada vez más experimentada estructura. Como es propio de aquellas organizaciones destinadas a evolucionar en el tiempo, se puso énfasis en aquellos aspectos trascendentes que NO van a cambiar y que van a acompañar al CCCD en su tránsito al futuro. En este marco se redactó la Visión, como leitmotiv de sus integrantes y los Valores que sustentan a la organización, los cuales una vez internalizados en cada uno de sus miembros, representan un intangible que trasciende a la organización de la que forma parte.

Comando Conjunto de Ciberdefensa

Visión
El Comando Conjunto de Ciberdefensa aspira a constituirse como la máxima instancia militar de coordinación del Estado Mayor Conjunto de las Fuerzas Armadas de la Nación, con el fin de alcanzar solidaria y armónicamente los objetivos que se determinasen, en un entorno caracterizado por la disciplina, la discreción y la vocación de servicio.

Valores
Ética – Lealtad – Discreción – Disciplina - Vocación de Servicio - Excelencia profesional – Alegría – Armonía -Trabajo en Equipo

Guiado por la visión y coherente con los valores expresados, el CCCD materializa sus acciones a partir de una Misión, clara y definida, otorgando de esta manera a sus integrantes fronteras dentro de las cuales poder desarrollarse.
–
Misión
Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

De acuerdo a la evolución que ha evidenciado la Ciberdefensa en la República Argentina desde el 2010 hasta la actualidad, se ha conformado una estructura que ha trascendido el ámbito del Sistema de Defensa Nacional, pero en el cual el CCCD participa activamente. Dentro de esa estructura y a través de distintas relaciones o vinculaciones, desarrolla las actividades que le son propias, manteniendo como premisa fundamental excluyente el ejercicio de las Buenas Prácticas.

2. El Sistema de Ciberseguridad de la República Argentina

El plexo legal de la República Argentina tiene diferenciados los ámbitos de Defensa y Seguridad a partir de la ley N° 23.554 - Defensa Nacional y la ley N° 24.059 – Seguridad Interior. Excepto en las circunstancias excepcionales que establecen las normas citadas, las Fuerzas Armadas no poseen atribución para involucrarse en aspectos que sucedan en el ámbito de la Seguridad Interior. Tal situación aplica a la protección cibernética. En este marco referencial, la Ciberdefensa en la República Argentina forma parte de un sistema mayor constituido por otros organismos del Estado, que adecuadamente integrados permiten a la Nación el ejercicio pleno de su soberanía.

El ápice del Sistema Nacional de Ciberseguridad está materializado por el Comité de Ciberseguridad, creado por Decreto del Presidente de la Nación Argentina N° 577/17. Posteriormente, esa norma jurídica fue actualizada y ampliada por el Decreto 480/2019.

El Comité de Ciberseguridad surge como una respuesta a la necesidad de reunir a los representantes de las principales áreas de gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada esta, desarrollar el plan de acción necesario para la implementación de dicha Estrategia. Es conveniente aclarar que a pesar de que los ámbitos de actuación en el ciberespacio están divididos en Ciberseguridad y Ciberdefensa, cuando hablamos de Ciberseguridad en términos de políticas o estrategias, nos referimos a un concepto sobre la situación en la cual una Infraestructura Crítica se considera protegida de amenazas o agresiones cibernéticas, proporcionando libertad de acción para el empleo de dicha infraestructura, de acuerdo a los lineamientos establecidos en la Estrategia Nacional de Ciberseguridad.

En el ámbito de la Ciberdefensa propiamente dicha, mediante Decreto del Presidente de la Nación N° 42/2016, se crea en la órbita del Ministerio de Defensa, la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares, con Control Funcional sobre el Comando Conjunto de Ciberdefensa.

Como se puede apreciar, la multiplicidad de actores involucrados en la problemática de la Ciberseguridad, la actualización de normas, la ampliación de atribuciones, entre otros aspectos, dan cuenta de la dinámica que presenta el ciberespacio como nuevo ámbito de operaciones. Para desenvolverse en él, el CCCD considera que adquieren particular relevancia en su accionar las "Buenas Prácticas", las cuales proporcionarán legitimidad a sus actos, convirtiéndose de esta manera, en una eficaz herramienta del Estado para hacer frente a este nuevo escenario del conflicto.

DESARROLLO

1. El Comando Conjunto de Ciberdefensa y la materialización de las Buenas Prácticas

A fin de poder enmarcar las acciones del CCCD en las Buenas Prácticas, hemos tomado como marco teórico las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad"[1], que ofrece la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad", para buscar trazar una relación de correspondencia entre lo descripto en ese documento y el accionar del CCCD, observando que algunas de las Esferas de Interés consideradas en las Buenas Prácticas han sido debidamente desarrolladas por este Comando. Si bien la Guía de referencia apela a un trabajo integral como es el desarrollo de una Estrategia Nacional de Ciberseguridad, también las Esferas de Interés pueden ser aplicadas a una escala menor (el CCCD), para alcanzar los propios objetivos y prioridades de acuerdo con la visión, valores y misión.

El siguiente esquema grafica las siete esferas de interés de las buenas prácticas.

Seguidamente, se describirán aquellas Esferas de Interés asociadas a las Buenas Prácticas en las que mayor injerencia tiene el CCCD.

a.Cooperación Internacional

Desde su creación, el CCCD ha buscado relacionarse internacionalmente con aquellos países de mayor trayectoria y experiencia en Ciberdefensa y con otros países con los cuales, por poseer experiencia similar a la nuestra y por formar parte del marco regional, interesa vincularse. En este sentido, este Comando sostiene tres tipos de relacionamien-

Fuente: elaboración propia del CCCD

1. La Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). 2018. *"Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad"*. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

tos, el primer tipo: Recibimiento de Autoridades, a través de visitas de militares o autoridades extranjeras al CCCD; el segundo tipo: Relaciones Bilaterales, a través de intercambios de personal, reuniones bilaterales, ejercicios y cursos. Tal es el caso de las experiencias realizadas con Brasil, Chile, Colombia, Italia, Japón, Perú, España, Alemania, Israel y Estados Unidos. El tercer tipo de relacionamiento es a través del Foro Iberoamericano de Ciberdefensa. La iniciativa del foro surge como una impronta del Reino de España en la que firma una Carta de Intenciones en mayo de 2016, inicialmente ocho países (Argentina, Brasil, Chile, Colombia, España, México, Perú, Portugal). Posteriormente solicitaron su incorporación al foro Uruguay y Paraguay, sumando a la fecha diez países. El objeto del foro fue promover la colaboración en Ciberdefensa entre las Fuerzas Armadas de los países miembros en las áreas de formación, ejercicios, intercambios de información, investigación, desarrollo e innovación, en el ámbito del ciberespacio como otro dominio inherente a la Defensa Nacional y por lo tanto motivo de análisis, estudio, formación y adiestramiento por parte de las Fuerzas Armadas. En atención al espíritu con que fue creado, en octubre de 2017 se desarrolló en Brasilia el I Ejercicio Iberoamericano de Ciberdefensa. En dicha oportunidad se propuso a la República Argentina como país sede del II Foro Iberoamericano de Ciberdefensa, a fin de continuar los esfuerzos de cooperación para alcanzar los objetivos comunes trazados, para fortalecer las relaciones existentes.

Entre el 20 y 22 de marzo de 2018 se desarrolló en Buenos Aires el II Foro Iberoamericano de Ciberdefensa (FIC) organizado íntegramente por el CCCD donde, además de los representantes de los Estados miembros, se invitó a representantes de los países de la región interesados en la problemática. Asimismo, participaron autoridades militares del Estado Mayor Conjunto de las Fuerzas Armadas, del Ejército, la Armada, y la Fuerza Aérea, autoridades del ámbito académico y de distintas áreas de Gobierno. Durante el desarrollo se dieron exposiciones por parte de las diferentes delegaciones asistentes al evento, donde se reflejaba la problemática de cada país y la manera como abordaban la solución. Como resultado de las intensas jornadas se firmó una Carta de Intenciones cuyos puntos salientes fueron:

1. Desarrollar durante el mes de marzo de cada año el FIC en aquellos países que sean designados sede y durante el mes de octubre de cada año se desarrollará el Ejercicio de Ciberdefensa.
2. Designar al país que se desempeñe como Sede del FIC como Secretaría Pro Tempore y responsable de la carga administrativa que devenga hasta el siguiente Foro.
3. Trabajar para el establecimiento de un protocolo de cooperación

El Comando Conjunto de Ciberdefensa asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de Ciberdefensa.

para la difusión de avisos, alertas y alarmas de ciberataques.
4. Trabajar en la creación y aplicación de una MISP *(Malware Information Sharing Platform),* para intercambio de información entre países iberoamericanos.
5. Brindar apoyo entre países amigos para grandes eventos.
6. Evolución de la Carta de Intenciones del FIC.
7. Evaluar posibilidades de colaboración en actividades de educación y entrenamiento (cursos).

A su vez se dejó plasmado en dicho documento el procedimiento para la incorporación de nuevos países que pretendan incorporarse al FIC. Portugal asumió la responsabilidad de redactar las normas que regirán tanto para la organización de los próximos foros como así también para las pautas que regulan el desarrollo de los ciberejercicios, las cuales fueron aprobadas durante el III FIC. También se propuso integrar al FIC a la República Oriental del Uruguay, para lo cual y conforme al procedimiento establecido y a las comunicaciones efectuadas por la Secretaria del Foro, se aprobó de manera unánime su inclusión.

El 30 de agosto de 2018, en el marco de las Ciberolimpíadas organizadas por Colombia, en su etapa *on line* el CCCD obtuvo el 3er puesto entre 13 países, lo que permitió que este Comando, en representación de las Fuerzas Armadas de la República Argentina, participara en la etapa presencial de ese importante evento. Para tal ocasión el personal seleccionado viajó a Bogotá – Colombia en noviembre de 2018, donde participó a lo largo de tres jornadas de las Ciberolimpíadas.

Entre el 22 y 25 de octubre de 2018 un equipo integrado por personal del CCCD, personal de la Dirección de Ciberdefensa del Ejército y personal de la Dirección de Ciberdefensa de la Fuerza Aérea, participaron del 2do Ejercicio del Foro Iberoamericano de Ciberdefensa, que tuvo lugar en España, en la Base de Retamares, sede del Mando Conjunto de Ciberdefensa español (MCCD). Los objetivos del ejercicio se elaboraron según las Normas para el Funcionamiento del Ejercicio a desarrollarse en el marco del Foro Iberoamericano de Ciberdefensa y fueron:
1. Fomentar la cooperación entre los países pertenecientes al Foro Iberoamericano de Ciberdefensa en este ámbito, sin espíritu de competición.
2. Mejorar la preparación para conducir un Ejercicio Internacional en el marco del Foro Iberoamericano de Ciberdefensa.
3. Entrenar las capacidades técnicas cibernéticas de los equipos involucrados en la actividad.
4. Identificar las posibilidades para realizar intercambio de información.
5. Fomentar el establecimiento del protocolo de cooperación para la difusión de avisos, alertas y alarmas de ataques cibernéticos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.
6. Fomentar la creación de una plataforma electrónica de intercambio de información de *malware* (MISP), para intercambio de información entre los países Iberoamericanos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.
7. Incrementar el conocimiento mutuo de las doctrinas de empleo en el espacio cibernético.

Conforme a las propuestas efectuadas, el FIC 2019 se desarrolló en Brasil y el Ciberejercicio en su tercera edición también tendrá a ese país como Sede.

De la Carta de Intenciones suscripta por los representantes de los países miembros, los puntos más salientes fueron:
1. Elaborar un "Marco de Referencia Doctrinario del Ciberespacio" que defina el rol de las Fuerzas Armadas y su marco de actuación general; y que incluya, además, un glosario de términos unificado en la materia.
2. Estudiar la posibilidad de compartir información, bilateralmente, acerca los siguientes asuntos:
   a. La forma en que están

El Comando Conjunto de Ciberdefensa se impuso como responsabilidad, "Especificar, coordinar la concientización, formación y el adiestramiento especializado en materia de Ciberdefensa para el Personal integrante de las FFAA".

desarrollando operaciones ofensivas, cuál es el proceso y si hay un marco jurídico que respalde estas acciones.

b. Difusión de doctrina conjunta, combinada y multilateral con aliados para el desarrollo de operaciones cibernéticas.

c. Plan de carrera para los cibercomandos y qué estrategias existen para retener el capital intelectual humano capacitado.

d. La forma en que están generando doctrina conjunta para Ciberdefensa.

3. El III Ejercicio Iberoamericano de Ciberdefensa definirá como objetivo integrar y fortalecer la cooperación entre países miembros para reaccionar ante un ataque cibernético con capacidad de respuesta. Se propuso incluir en el objetivo del III Ejercicio Iberoamericano de Ciberdefensa la integración del Planeamiento de Ciberoperaciones en apoyo a las Operaciones de mar, aire y tierra, a fin de continuar generando doctrina en este rubro.
4. Llevar a cabo los desarrollos y gestiones necesarios para implementar, en todos los países miembros integrantes del Foro Iberoamericano, bases integradas en la plataforma MISP (dicha intención ya se materializó).
5. Efectuar sesiones virtuales con los representantes de los países miembros cada 3 meses para dar a conocer buenas prácticas, lecciones aprendidas y casos emblemáticos en cada uno de los países, para compartir con los demás (dicha intención se viene cumplimentando de manera periódica a través de videoconferencias).

b. Legislación y Reglamentación

En esta esfera de Interés, la promulgación de la Legislación respectiva por parte de las distintas carteras ministeriales, como así también las necesidades que surgen para incorporar la Ciberdefensa al planeamiento y ejecución de las operaciones que realiza el Instrumento Militar, proporcionan el *input* para que el CCCD se aboque a la elaboración de la doctrina necesaria para el adecuado empleo de los medios de Ciberdefensa a disposición. La doctrina de Ciberdefensa elaborada en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas (denominada Doctrina Conjunta) sirve de base para la elaboración de la doctrina propia, por parte de cada una de las organizaciones de Ciberdefensa de las Fuerzas Armadas (denominada Doctrina Específica). De esta manera y desde el punto de vista de la Ciberdefensa, el circuito doctrinario queda debidamente articulado para todo el Instrumento Militar. A su vez, personal del CCCD con amplia formación y experiencia participa en equipos *Ad Hoc* para la actualización doctrinaria, asesorando sobre aquellos conceptos de Ciberdefensa que son necesarios incorporar en los diferentes reglamentos.

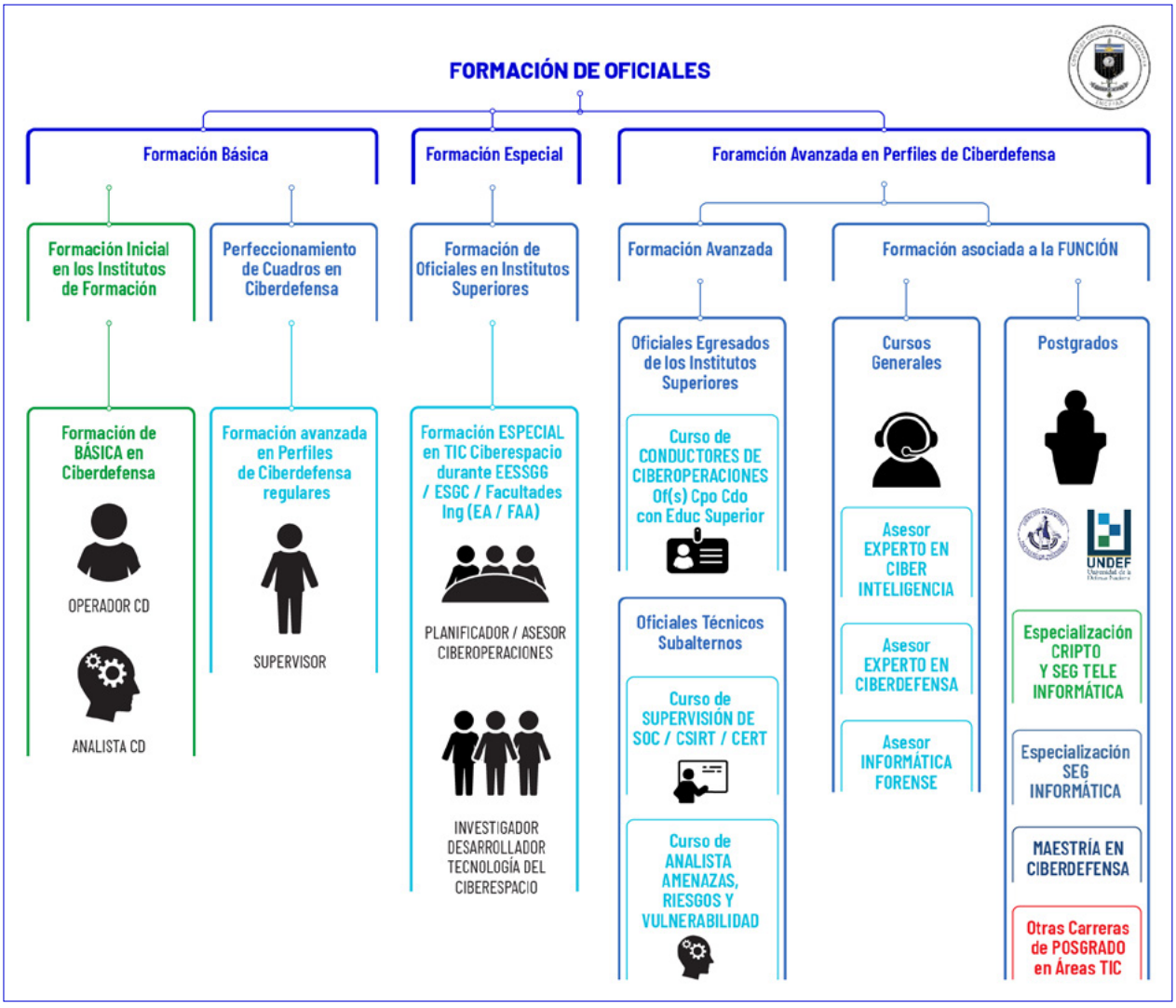
Vinculado con la Cooperación Internacional, a partir de acuerdos bilaterales que el Estado Mayor Conjunto de las Fuerzas Armadas suscribe con países amigos, se ha avanzado en la elaboración de Doctrina de Ciberdefensa Combinada en un paso más para lograr el adecuado entendimiento y avanzar en la aplicación de las Buenas Prácticas de la Ciberdefensa en la ejecución de Operaciones Combinadas.

c. Capacitación, Creación de Competencias y Sensibilización

1. Plan de Formación en Ciberdefensa

En esta esfera de Interés, el CCCD ha trabajado bajo la consideración de que la construcción de una Ciberdefensa eficaz y eficiente no sólo contribuye a mejorar en su conjunto la Seguridad de la Información del Instrumento Militar, sino que, como factor de disuasión, es un objetivo irrenunciable que depende en gran medida de la calidad de la formación de todos cuantos tienen alguna responsabilidad directa en la materia. La consecución de este objetivo debe basarse en la definición, implementación y continuo perfeccionamiento de una formación orientada hacia las funciones de cada uno de los puestos directamente relacionados con activi-

ESQUEMA DEL PLAN DE FORMACIÓN DE OFICIALES



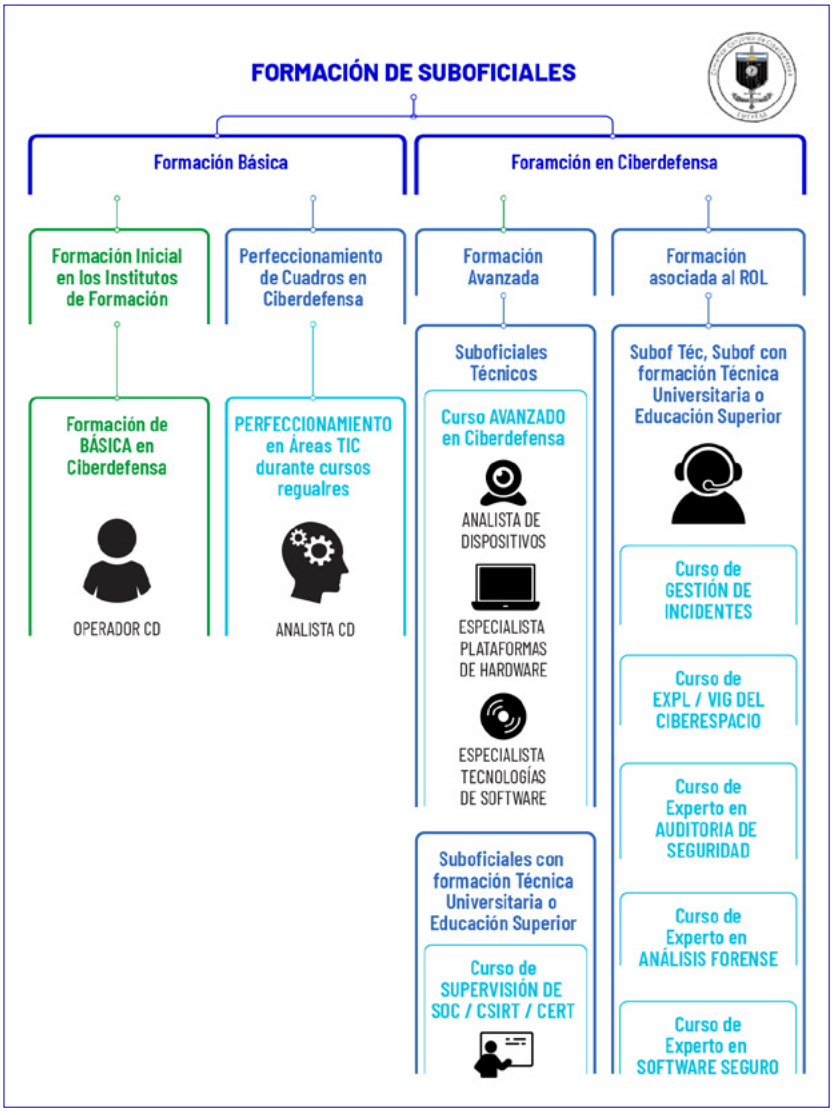
Fuente: elaboración propia del CCCD

dades de Ciberdefensa, tanto en la conducción de Operaciones del Ciberespacio como en los aspectos técnicos y eminentemente operativos. En ese sentido, es necesario alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita el Instrumento Militar para sustentar todos los objetivos de Ciberdefensa.

Conforme a lo expresado precedentemente, el Comando Conjunto de Ciberdefensa asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de Ciberdefensa. Del estudio de los cometidos relacionados con la Ciberdefensa y de las necesidades formativas que de todo ello se derivan, el Comando Conjunto de Ciberdefensa ha desarrollado un Plan de Formación en Ciberdefensa, que será el instrumento para la adquisición, mejora y actualización de competencias necesarias en aspectos relativos a la Ciberdefensa. Este plan facilita, además, la implementación de los trayectos formativos que permitirán alcanzar la capacitación necesaria a cada uno de los distintos grupos de formación identificados.

Un análisis de la situación ha permitido determinar que, en la actualidad, la formación en este ámbito es escasa, parcialmente satisfecha con perfiles técnicos del área TIC, sin conocimientos profundos de las Operaciones Militares ni de Operaciones del Ciberespacio, no está debidamente estructurada ni homologada, y no garantiza la capacitación del personal para el acceso a formación de mayor nivel tecnológico ni para satisfacer las necesidades reales de las FFAA en

ESQUEMA DEL PLAN DE FORMACIÓN DE SUBOFICIALES



Fuente: elaboración propia del CCCD

la Conducción de Ciberoperaciones. No obstante, se considera que la formación en Ciberdefensa se debe apoyar en gran medida en los activos de las FFAA y se acreditarán mediante títulos o certificados obtenidos de la forma que se determine para cada caso.

El Plan fue concebido con el objetivo fundamental de definir los requisitos de formación basados en perfiles, en materia de Ciberdefensa, que deberían alcanzar los integrantes de las FFAA que ocupen puestos de trabajo relacionados con la Ciberdefensa. Será también de aplicación tanto para el personal militar como para el personal civil que se incorpore a las organizaciones de Ciberdefensa. A su vez, este Plan persigue como finalidad la descripción de las responsabilidades generales en formación de Ciberdefensa en el ámbito de las FFAA. En este sentido, y a futuro, los programas de formación y los planes de estudio de los Institutos Militares en donde se desarrolle la formación en Ciberdefensa deberán tener en consideración el presente Plan. En su diseño se ha contemplado, en el mayor grado posible, el aprovechamiento de las estructuras de los Planes de Carreras vigentes en las FFAA. De igual manera, se definen también los mecanismos para la actualización continua en las competencias del personal.

El proceso de evaluación de este plan se llevará a cabo de acuerdo con las normas de evaluación del sistema de enseñanza militar, de manera progresiva, con el propósito de que se encuentre completamente implementado en el corto plazo. El análisis y estudio de los resultados de este plan servirán de base para los futuros reajustes.

Dentro del presente documento se establecen dos partes diferenciadas, una primera relacionada con la identificación de los grupos funcionales del personal relacionado de alguna forma con la Ciberdefensa y sus necesidades formativas, y una segunda relacionada con la mejora y adaptación de este Plan.

2. Plan de Concientización y Sensibilización

Por similitud a lo que sucede en otras áreas, se puede afirmar que en Ciberseguridad el eslabón más débil es el individuo como usuario del sistema. A su vez, si se considera que la innovación y avance tecnológico son continuos y aventajan, en algunos casos, la capacidad de adopción de medidas de seguridad resulta entonces necesario implicar activamente a todos los usuarios en la protección y defensa de las redes y de los sistemas de información vinculados a las FFAA. En este sentido se debe tener presente que la gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de Ciberseguridad. Ello requiere de los usuarios una comprensión particular respecto de los riesgos que existen al operar en este medio, así como del conocimiento de las herramientas para la protección de su información, sistemas y servicios.

La instalación en la conciencia del personal de las Fuerzas Armadas de una sólida cultura de Ciberseguridad proporcionará a todos los actores la responsabilidad y la confianza necesaria para su interacción en un medio tan complejo y sensible como es el del ciberespacio. El CCCD se impuso como responsabilidad la de "especificar, coordinar la concientización, formación y el adiestramiento especializado en materia de Ciberdefensa para el personal integrante de las FFAA", definiendo a la

EJEMPLO DE LÍNEAS DE CONCIENTIZACIÓN Y OBJETIVOS PERSEGUIDOS DEL PLAN DE CONCIENTIZACIÓN EN CIBERDEFENSA

Nro	Líneas de concientización	Objetivos generales de concientización	
1	General	1.1	Dar a conocer los riesgos del ciberespacio.
		1.2	Informar que las FFAA son objetivo de ciberataques, aumentando esta circunstancias el nivel de amenaza al que está sometido su personal.
2	Identificación y Credenciales de acceso	2.1	Concientizar de la importacia de una gestión adecuada de las contraseñas y de otras credenciales de acceso en la protección de la información.
3	Navegación de Internet	3.1	Promocionar el uso responsable de Internet.
		3.2	Difundir hábitos y buenas prácticas de navegación por Internet.
		3.3	Enseñar cómo identificar enlaces potencialmente peligrosos.
		3.4	Recomendaciones específicas para el uso de servicios electrónicos homebanking y pagos on-line
4	Correo electrónico	4.1	Advertir que el correo electrónico es uno de los medios más frecuentes de ciberataque, puesto que no es un método totalmente seguro para intercambiar información fuera del ámbito de las FFAA.
		4.2	Enseñar cómo identificar mensajes potencialmente peligrosos ("pishing" y fraudes on-line)
5	Servicios en la red	5.1	Difundir recomendaciones de uso seguro de servicios de internet, conciliando la productividad con la seguridad.
		5.2	Recomendaciones específicas para proteger la información personal en Internet.
6	Actividad en redes sociales	6.1	Explicar a los usuarios cómo pueden ser víctimas de ataques de "ingeniería social", especialmente en las redes sociales.
		6.2	Promover la prudencia en el uso de las redes sociales, especialemente a la hora de publicar información.
		6.3	Prevenir situaciones de riesgo para las FFAA o terceras personas que tienen relación con los usuarios.
7	USB y soportes de información	7.1	Avisar de los riesgos asociados al uso de soportes y dispositivos de almacenamiento USB (infección, pérdida de información y posible infracción de la normativa)
8	Protección del entorno personal	8.1	Explicar a los usuarios cómo pueden proteger su PC personal.
		8.2	Enseñar cómo es posible trasladar esta protección a los dispositivos y redes personales en el ámbito personal.
9	Fuera de la oficina: Movilidad	9.1	Informar a los usuarios de su especial vulnerabilidad en situación de movilidad fuera de su puesto de trabajo.
		9.2	Explicar a los usuarios cómo pueden proteger los dispositivos móviles y portátiles tanto en el ámbito profesional como el personal.
10	Prevención y reacción ante los incidentes	10.1	Poner de manifiesto la importancia de la participación de los usuarios en la detección temprana y respuesta a incidentes de ciberseguridad.
		10.2	Fomentar que el usuario acuda a informarse sobre los riesgos y alertas de seguridad a través de los portales falsos.
		10.3	Enseñar a identificar incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
		10.4	Difundir el procedimiento para comunicar incidencias de seguridad, sean reales o falsas alarmar a las unidades encargadas de gestionarlas.

Fuente: elaboración propia del CCCD

El Comando Conjunto de Ciberdefensa elaboró un Plan de Concientización de Ciberdefensa para el Personal de las Fuerzas Armadas, que tiene por finalidad definir un conjunto de acciones dirigidas a todos los usuarios de las Tecnologías de la información y la comunicación (TIC), integrantes de las FFAA para que sean conscientes de los riesgos y amenazas a los que diariamente se enfrentan en el ciberespacio.

concientización como las acciones necesarias para facilitar al personal la compresión de las amenazas generadas por los potenciales adversarios o elementos hostiles en el ciberespacio; así como la manera en la que, tanto a nivel individual como colectivo, se puede y debe contribuir a evitar o contrarrestar estas amenazas, reaccionando oportuna y adecuadamente. Al respecto se debe dejar establecido que la seguridad de la información es responsabilidad de todos los miembros de las Fuerzas Armadas, los cuales deberán estar adecuadamente formados y concientizados para el satisfactorio cumplimiento de sus responsabilidades.

A fin de contribuir a la toma de conciencia del personal, el CCCD elaboró un **Plan de Concientización de Ciberdefensa para el Personal de las Fuerzas Armadas,** el mismo tiene por finalidad definir un conjunto de acciones dirigidas a todos los usuarios de las Tecnologías de la información y la comunicación (TIC) e integrantes de las FFAA para que sean conscientes de los riesgos y amenazas a los que diariamente se enfrentan en el ciberespacio, así como la forma de prevenir, atenuar y mitigar sus efectos. Como aspecto secundario se persigue la extensión de estas acciones a su ambiente familiar, con independencia a que su puesto de trabajo implique o no el uso de las TIC, toda vez que este personal es susceptible de hacer uso de estas en otros ámbitos, con impacto posible en el entorno de las FFAA. A su vez, el plan describe las responsabilidades generales de la concientización en el marco de las FFAA y los recursos necesarios para su implementación.

d. Gestión de Riesgos para la Ciberdefensa / Preparación y Resiliencia

El CCCD ha confeccionado bajo un enfoque sistémico un manual de procedimientos estandarizados, los que pueden considerarse como actividades de procesos y subprocesos de Ciberdefensa Pasiva. Se enfocan principalmente en la descripción de los Procedimientos Operativos Normales destinados a ejecutar la Ciberdefensa de las Infraestructuras Críticas de la Información del Instrumento Militar (Sistemas de Comando y Control, Sistemas de Comunicaciones, Sistemas de Armas, Sistemas de Control, Sistemas Computarizados en apoyo a las Operaciones Militares) y otros Recursos Esenciales de Sistemas, Redes, Datos e Información de las FFAA, siendo de aplicación en tiempo de paz para adiestrar, entrenar y ejecutar las acciones del Sistema de Respuesta de Ciberdefensa por parte del Centro de Operaciones de Ciberdefensa del CCCD principalmente. El Manual de Procedimientos fue difundido a las FFAA para su implementación como así también para la incorporación de mejoras, conforme a las Lecciones Aprendidas de la Experiencia de cada organización, dado que las amenazas a la Ciberseguridad se presentan tan dinámicas como impredecibles, cualquier procedimiento que se instaure, requiere una actualización constante.

e. Servicios de Infraestructura Fundamental y Servicios Esenciales

Conforme a la misión impuesta, el CCCD debe estar en capacidad de repeler aquellos ciberataques contra las Infraestructuras Críticas de la Información y las Comunicaciones y los activos del Sistema de Defensa Nacional[2] y del Instrumento Militar. No obstante, a lo largo de los años y con especial énfasis desde la creación del CCCD, diversos documentos políticos han coincidido en señalar que:

1. Relacionado a Amenazas Cibernéticas: Resulta necesario encarar el abordaje de esta problemática desde la perspectiva de la Defensa Nacional a fin de adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional como así también aquellas que sean asignadas a dicho sistema para su protección.

2. El Sistema de Defensa Nacional se encuentra definido en el Art 9 de la Ley 23.554 - Defensa Nacional

CIBERDEFENSA

PROCESOS Y SUBPROCESOS

Análisis en Tiempo Real
> Centro de llamadas
> Monitoreo de eventos y priorización de incidentes en tiempo real

Inteligencia y Análisis de Tendencias
> Recopilacion y análisis de noticias del ciberespacio
> Distribución de noticias del ciberespacio
> Creación de noticias del ciberespacio
> Fusión de noticias del ciberespacio
> Observatorio de Tecnologías y Tendencias
> Advertencias, alertas y alarmas de amenazas, vulnerabilidades, incidentes y ciberagresiones
> Evaluación de amenazas

Análisi de Incidentes y Respuesta
> Análisis de incidentes
> Análisis de actividad sospechosa o maliciosa
> Servicios de detección de Intrusiones
> Coordinación de respuesta a incidentes
> Implementación de costramedidas
> Respuesta "en sitio" a incidentes
> Respuesta remota (on-line / off-line) a incidentes
> Respuesta a vulnerabilidades
> Coordinación de Respuesta a vulnerabilidades
> Respuesta a componentes o dispositivos afectados
> Coordinación de Respuesta a componentes o dispositivos afectados
> Continuidad de las operaciones y planeamiento de recuperación antes desastres

Auditoría y Amenza Interna
> Recopilación, retención y almacenamiento de datos para auditorias
> Creación de contenido y administración de datos para auditorias
> Apoyo en caso de amenaza interna
> Investigación en caso de amenaza interna

Exploración y Evaluación
> Mapeo y estadística de redes
> Búsqueda de vulnerabilidades
> Evaluación de vulnerabilidades
> Prueba de intrusión

Aptitudes de Máxima Capacidad
> Análisis de riesgos
> Protección de IICC / Recursos Esenciales
> Consultoría en seguridad (Tecnológica y Legal)
> Sensibilización y concientización
> Formación y Capacitación
> Evaluación de producto
> Certificación de producto

PROCESOS Y SUBPROCESOS

Análisis de Dispositivos y Componentes
> Manejo de componentes, dispositivos o imágenes forenses
> Análisis de implantes y malware
> Análisis de componentes, dispositivos o imágenes forenses

Apoyo al Ciclo de Vida de Herramientas del Sistema de Respuesta
> Obtención y mantenimiento de Dispositivos de Protección de Borde
> Obtención y mantenimiento de Infraestructura del Sistema de Respuesta
> Ajuste y mantenimiento de sensores
> Servicios de soporte en lúnea para descarga de software y firmware
> Distribución de actualizaciones de software, firmware y hardware
> Creación de "firmas" personalizadas
> Ingeniería y despliegue de herramientas de ciberseguridads
> I+D de herramientas de ciberseguridad y ciberdefensa
> Scripts y automatización

Aptitudes de Máxima Capacidad
> Planeamiento de Operaciones del Ciberespacio
> Conciencia de la situación
> Coordinación, comando y Control de Operaciones
> Gestión de la Interoperabilidad de sistemas y redes
> Integración de metadatos y Correlación de eventos
> Servicios de mesa de ayuda para PPOONN
> Construcción de Conocimiento y Entrenamiento
> Virtualización y simulación
> Servicios de Ciberequipo Colorado
> Actualización de normas legales, técnicas o doctrinas
> Difusión de Tácticas, Técnicas y Procedimientos (TTPs)
> Relación con los Medios de Comunicación
> Acciones de Respuesta Inmediata (Canalizar, Bloquear o Detener, Neutralizar o Mitigar, Degradar, Anular)

FUNCIONES
> Reactivas
> Proactivas
> Gestión de Calidad de Seg Información
> Preventivas
> Otras

2. Relacionado a Riesgos (ataques a objetivos estratégicos): El Sistema de Defensa Nacional debe planificar y proteger los objetivos estratégicos que puedan ser objeto de una agresión. La atención de este riesgo debe focalizarse particularmente en aquellas infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes.

Considerando los dos conceptos referidos, será responsabilidad del CCCD, planificar la protección cibernética de aquella Infraestructura Crítica y Objetivos Estratégicos, alguno de los cuales prestarán un servicio esencial a la Nación. En esa planificación adquirirá un valor especial las vinculaciones con todos aquellos estamentos del Estado, necesarios para lograr las coordinaciones a fin de evitar superposiciones en el esfuerzo que demande la protección. Asimismo, debe contemplarse un estrecho relacionamiento con el ámbito privado, ya que muchos de los servicios esenciales del país están en manos de ese sector. En tal sentido, el ejercicio de las Buenas Prácticas y fundamentalmente los antecedentes que se tengan de su correcta implementación en otras esferas de Interés, serán de particular importancia ya que operarán como un catalizador para generar los lazos de confianza necesarios para la eficiente y eficaz Ciberdefensa del objetivo que se trate.

La República Argentina, en la búsqueda de la Ciberseguridad y Ciberdefensa de sus Infraestructuras críticas, viene realizando esfuerzos que se materializan en el ámbito político, legislativo, judicial, académico y científico tecnológico.

CONCLUSIONES

Los distintos Estados han buscado enfrentar las amenazas y riegos que implica el ciberespacio y que afectan a los conceptos de seguridad y defensa de diferentes maneras, pero que básicamente responde, entre otros aspectos, a la conformación de estructuras organizativas que permitan proteger sus activos digitales; a la adecuación del marco legal que le permita desenvolverse en ese ambiente para marcar los límites que tiene su accionar y penalizar a quienes los infringen; a la incorporación de contenidos en sus programas educativos, buscando desde la temprana edad crear conciencia de los riesgos que acechan en el ciberespacio y facilitar la formación de especialistas; a la suscripción de acuerdos internacionales que favorezcan la cooperación de esfuerzos y a la creación de estrategias y políticas que permitan alcanzar los objetivos deseados.

Las organizaciones internacionales también se han esforzado en dotar con modelos o estrategias para afrontar las amenazas de Ciberdefensa y Ciberseguridad de los Estados. Han publicado varios documentos o estándares, como la *Guía de la ciberseguridad para los países en desarrollo* (ITU 2007) o el *National Cybersecurity Strategy Guide* (ITU 2018). Ambos son modelos de referencia basados en la valoración de activos, capacidades, necesidades, amenazas y riesgos en sectores públicos y privados del Estado para construir y ejecutar una estrategia de ciberseguridad nacional. No podemos dejar de hablar de entidades de estandarización como la Organización Internacional de Normalización (ISO), que con sus *Sistemas de Gestión de Seguridad de la Información (SGSI)* contenidas en la ISO/IEC 27000, *Tecnologías para la seguridad de la Información y Técnicas de Seguridad* pretende dar una propuesta más orientada a los aspectos específicos de seguridad en una entidad u organización.

La República Argentina, en la búsqueda de la Ciberseguridad y Ciberdefensa de sus Infraestructuras críticas, viene realizando esfuerzos que se materializan en el ámbito político, legislativo, judicial, académico y científico tecnológico. La creación del Comando Conjunto de Ciberdefensa es parte de la respuesta, desde el punto de vista de la Defensa, a la problemática que plantea el ciberespacio. A pesar de que, como se expresara en el párrafo precedente, existen modelos integrales para encarar la Ciberseguridad y la Ciberdefensa, el país no ha logrado adaptarse completamente a alguno de estos modelos.

No obstante, desde su origen, el CCCD ha buscado erigirse como un referente en materia de Ciberdefensa, donde el ejercicio de las Buenas Prácticas en todo su accionar responde a los conceptos rectores de su creación. Asimismo, y a partir de las relaciones orgánicas y funcionales otorgadas para su vinculación con las Direcciones de Ciberdefensa de las Fuerzas Armadas, permite trasladar su impronta a ellas. Su relacionamiento internacional, fundamentalmente a través del Foro Iberoamericano de Ciberdefensa como así también la participación en otros espacios de debate, es un intento de intercambiar experiencias y conocimientos que resulten beneficiosos para la organización. En el ámbito de la formación y concientización, se considera que la excelencia en la capacitación de los recursos humanos es fundamental. A partir de esa premisa y a través de la elaboración de sendos planes, el CCCD pretende dar un aporte a los decisores que tienen en sus manos la posibilidad de su implementación y articulación. La gestión de riesgos a partir de la elaboración de un Manual de Procedimientos, que se suma a la elaboración de Doctrina Conjunta y Combinada, ha tenido su correlato de éxito en la ciberseguridad y Ciberdefensa de grandes eventos, tal como fue la colaboración prestada con miembros del CCCD en el Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT por su sigla en inglés: *Computer Security Response Team*) del Gobierno de la Ciudad Autónoma de Buenos Aires, durante la realización de los Juegos Olímpicos de la Juventud en el 2018, como así también durante la Ciberdefensa de la Cumbre del G-20, realizada en Buenos Aires

en diciembre de 2018. El enfoque que adoptan distintos documentos políticos, en los aspectos referidos a riesgos y amenazas cibernéticas, le confieren al CCCD la posibilidad de la planificación de la Ciberdefensa de aquellas Infraestructuras Críticas y Objetivos Estratégicos que el nivel político le asigne para su protección, en un ambiente tan difuso y sin límites físicos como es el ciberespacio, a lo que se suma la dificultad de la atribución y donde el CCCD deberá articular su accionar con el ámbito público y privado, resulta casi condición *sine qua* non la transparencia y las buenas prácticas.

En el desarrollo del presente trabajo se ha intentado establecer, por analogía, pero a un nivel sensiblemente inferior, utilizando como marco conceptual las esferas de interés establecidas en las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad" que ofrece la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad", aquellos aspectos que ha podido desarrollar el CCCD, en su reducido radio de acción como es la Ciberdefensa. Muchos de los aspectos referidos fueron realizados por iniciativa propia. Es de prever que, a partir de la recientemente promulgada Estrategia de Ciberseguridad Nacional, la expansión del Comité Nacional de Ciberseguridad con la participación de otras carteras ministeriales, la definición de términos a partir de un glosario común, sumado a la manera de definir las infraestructuras críticas, impulsarán acciones sobre los distintos actores responsables de la Ciberseguridad/Ciberdefensa, que en el caso particular del CCCD potenciarán el crecimiento de los aspectos ya referidos en un intento de alcanzar las Capacidades de Ciberdefensa planificadas para el corto, mediano y largo plazo, a fin de proporcionar a la República Argentina de una organización valiosa para la Ciberdefensa de sus activos digitales y al Instrumento Militar de un elemento multiplicador de fuerzas. En ese escenario incierto que representa el futuro, el CCCD no abandona un instante el esfuerzo que la tarea le demanda.

BIBLIOGRAFÍA Y SITIOS WEB CONSULTADOS

Marco Legal

Ley N° 23.554 – Defensa Nacional. *Boletín Oficial de la República Argentina*, 13 de abril de 1988.

-

Ley N° 24.059 – Seguridad Interior. *Boletín Oficial de la República Argentina*, 6 de enero de 1992.

-

Decreto Presidencial N° 42/2016 – Administración Pública Nacional (Modificación). *Boletín Oficial de la República Argentina*, 08 de enero del 2016.

-

Decreto Presidencial N° 577/2017 – Comité de Ciberseguridad (Creación). *Boletín Oficial de la República Argentina*, 31 de julio del 2017.

-

Decreto Presidencial 480/2019 – Comité de Ciberseguridad (Modificación). *Boletín Oficial de la República Argentina*, 12 de julio del 2019.

-

Resolución Ministerial N° 343, Ministerio de Defensa, del 14 de mayo de 2014.

Doctrina Militar

Estado Mayor Conjunto de las Fuerzas Armadas. Reglamento Orgánico del Comando Conjunto de Ciberdefensa – Proyecto (OC 30-19), Buenos Aires, 2019.

-

Comando Conjunto de Ciberdefensa, Plan de Formación en Ciberdefensa, Buenos Aires, 2018.

-

Comando Conjunto de Ciberdefensa, Plan de Concientización en Ciberdefensa, Buenos Aires, 2018.

Acuerdos Internacionales

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Madrid, España, 27 de mayo de 2016.

-

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Buenos Aires, Argentina, 22 de marzo de 2018.

-

Foro Iberoamericano de Ciberdefensa, Carta de Intenciones. Brasília, Brasil, 17 de abril de 2019.

Material Académico

Unión Internacional de Telecomunicaciones, Banco Mundial, Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. 2018. "Guía para la elaboración de una estrategia nacional de ciberseguridad

-

Participación estratégica en la ciberseguridad". Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). Consultado en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf, el 25de octubre de 19.

-

Unión Internacional de Telecomunicaciones. "Guía de ciberseguridad para los países en desarrollo", 2017. Consultado en http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf, el 25 Oct 19.

-

Unión Internacional de Telecomunicaciones. "Guide to developing a national cybersecurity strategy", 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf, el 26 Oct 19.

-

Organización Internacional de Normalización, norma ISO/IEC 27001. "Tecnologías para la seguridad de la Información y Técnicas de Seguridad", 2017. Consultado en https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/, el 26 de octubre de 19.

-

El Ágora Asociación Civil sin fines de lucro. "Reflexiones en torno al Intercambio de Buenas Prácticas". Consultado en https://www.elagora.org.ar/site/documentos/Intercambio-BP.pdf, el 20 de octubre de 19.