ANEXO 4

POLÍTICA DE CIBERDEFENSA

LINEAS DE ACCION PRINCIPALES, EJES DE POLÍTICAS Y PLAN PARA LA PROTECCION DE LAS INFRAESTRUCTURAS CRITICAS DE INTERES PARA LA DEFENSA

A partir de conceptualizar al ciberespacio como un espacio soberano y la misión encomendada al Ministerio de Defensa de anticipar y prevenir ciberataques que pudieran comprometer la disponibilidad de los sistemas y redes de la Defensa, se han dispuesto acciones para fortalecer las capacidades de vigilancia y control en orden a cumplimentar los objetivos que se incorporan en PLANILLA ANEXA (IF-2019-82648870-APN-SSLYA#MD) al ARTÍCULO 2° del Decreto N° 684 del 3 de octubre de 2019.

Se establece así el siguiente ordenamiento:

OBJETIVOS DE LA MISIÓN DEL MINISTERIO EN EL CIBERESPACIO

- Anticipar y prevenir ataques en el ciberespacio.
- Disminuir vulnerabilidades y aumentar la resiliencia de los sistemas y redes TICs de las FFAA; EMCO y Mindef.
- Detectar amenazas y gestionar riesgos de ciberataques, y recuperación de los sistemas e infraestructura crítica de interés para la Defensa Nacional.
- Adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la Defensa.
- Contribuir a potenciar la base tecnológica e industrial nacional de ciberseguridad en trabajo conjunto con el Ministerio de Relaciones Exteriores y del Ministerio de Producción.
- Impulsar programas de capacitación, para superar brecha entre los recursos humanos disponibles y los demandados.

CUATRO LÍNEAS DE ACCIÓN PARA EL CUMPLIMIENTO DE LOS OBJETIVOS ENUMERADOS:

- **LA1** - Creación del Centro Nacional de Ciberdefensa
- **LA2** - Proteger la disponibilidad del ciberespacio como espacio soberano
- **LA3** - Reingeniería de las redes de las Fuerzas Armadas, del Estado Mayor Conjunto y del Ministerio de Defensa
- **LA4** - Convergencia de las capacidades de las FFAA

TRES POLÍTICAS A GESTIONAR PARA EL DESARROLLO DE LAS CUATRO LÍNEAS DE ACCIÓN:

- Política regulatorias (dictarlas, adaptarlas o interactuar)
- Política de desarrollo de capacidades para la interacción en el ciberespacio
- Política de concientización y capacitación

PLANES TRAZADOS HACIA EL CUMPLIMIENTO DE LOS OBJETIVOS:

- **Plan de Adecuación de las organizaciones militares.**
- **Plan Nacional de Infraestructuras críticas de la Defensa Nacional**

Tal como se indica, la ***primera*** línea de acción se relaciona con la ***creación del Centro Nacional de Ciberdefensa*** que funcionará en las instalaciones del CITEDEF, donde se concentrará el desarrollo de capacidades para interactuar en el ciberespacio y de tal forma asegurar la libertad de acción en este *QUINTO DOMINIO* evitando se vea afectada la confidencialidad, integridad y disponibilidad de la información que se transporta y/o procesa en las redes y sistemas TICs de las FFAA, el EMCO y el Ministerio de Defensa, y a su vez proteger las infraestructuras críticas de la Defensa Nacional, tanto las propias como las de interés para la Defensa.

Se prevé la localización de la Subsecretaria en el piso 5to de la Torre 1 y del Comando de Ciberdefensa en el piso 4to, para lo cual se adaptarán las estructuras edilicias actuales para posibilitar la pronta instalación y funcionamiento del CSIRT de la

Defensa, el CyberLab, las Salas de Situación y de Emergencia, la oficina del Consejo Asesor, otras oficinas administrativas y despachos de la Subsecretaria de Ciberdefensa, en el piso 5to y la mudanza de las oficinas operativas del Comando desde su actual lugar de asiento en Puerto Madero (CABA).

Con vistas a implementar lo establecido, se fijan entre otras, las siguientes prioridades operacionales del Ministerio de Defensa en el Ciberespacio que habrán de atenderse coordinando con los diferentes actores del Sistema de la Defensa en el ámbito del ***CyberLab*** del **Centro Nacional de Ciberdefensa**:

- Detectar amenazas y gestionar riesgos de ciberataques, y en su caso la recuperación de los sistemas e infraestructuras críticas de servicios esenciales de interés para la Defensa Nacional (redes de energía, comunicaciones, centrales nucleares, sistema financiero y otros), y/o de productores de bienes de interés para la Defensa Nacional (ej. Producción de explosivos, etc) instalando sensores (Hw & Sw) en las redes TO de los objetivos estratégicos que se definan, para realizar las tareas de monitoreo en una primera etapa, previo a la instrumentación de sistemas de protección en una segunda etapa.
- Lograr un elevado grado de resiliencia a fin de permitir, luego de un ataque, una rápida recuperación de las capacidades del Sistema de Defensa y de los servicios esenciales del Estado Nacional, y de los procesos productivos de los bienes de interés de la Defensa Nacional, desarrollando el sistema de monitoreo y protección de las infraestructuras críticas a proteger adecuado a cada fin.
- Desarrollo de cursos de formación continua con progresivo ajuste de la currícula para nueva oferta académica.
- Selección, capacitación y gestión de incorporación progresiva de reservistas especializados en el espacio cibernético.
- Reformulación de los planes de formación de RRHH destinados al desarrollo de capacidades específicas en ciberdefensa y genéricas en los restantes espacios de operaciones militares.
- Desarrollar capacidad de disuasión y aptitudes ofensivas de respuesta ante amenazas de ataques que comprometan la libertad de acción en el ciberespacio.
- Promover la creación de un Consejo Asesor de Ciberdefensa, en el ámbito del Centro Nacional de Ciberdefensa con la participación del ecosistema de la especialidad, empresas, cámaras empresarias, institutos de capacitación, las universidades, entre otros y desarrollando programas de educación, incentivos a la inversión y acuerdos internacionales para el desarrollo de talento en materia

de inteligencia artificial, machine learning, IoT y su relación con la ciberseguridad.

- El Consejo funcionará en el Centro Nacional de Ciberdefensa, en el ámbito del CyberLab, en las instalaciones del CITEDEF, donde se desarrollarán planes de divulgación de información y de interacción con la industria y la academia a través de convocatorias a grupos de trabajos específicos, temporarios y/o permanentes, trabajos en redes abiertas y colaborativas, blogs informativos, etc.
- Propiciar la creación de un sistema de certificación específica para determinados productos de hardware y software, particularmente sensibles por la función que desempeñan en las redes y sistemas de información o respecto a las cadenas de suministro asociadas a la ciberseguridad o cuando no existan proveedores que cumplan las especificaciones mínimas aceptadas internacionalmente en materia de ciberseguridad en los ámbitos TI, OT e IoT (internet de las cosas).

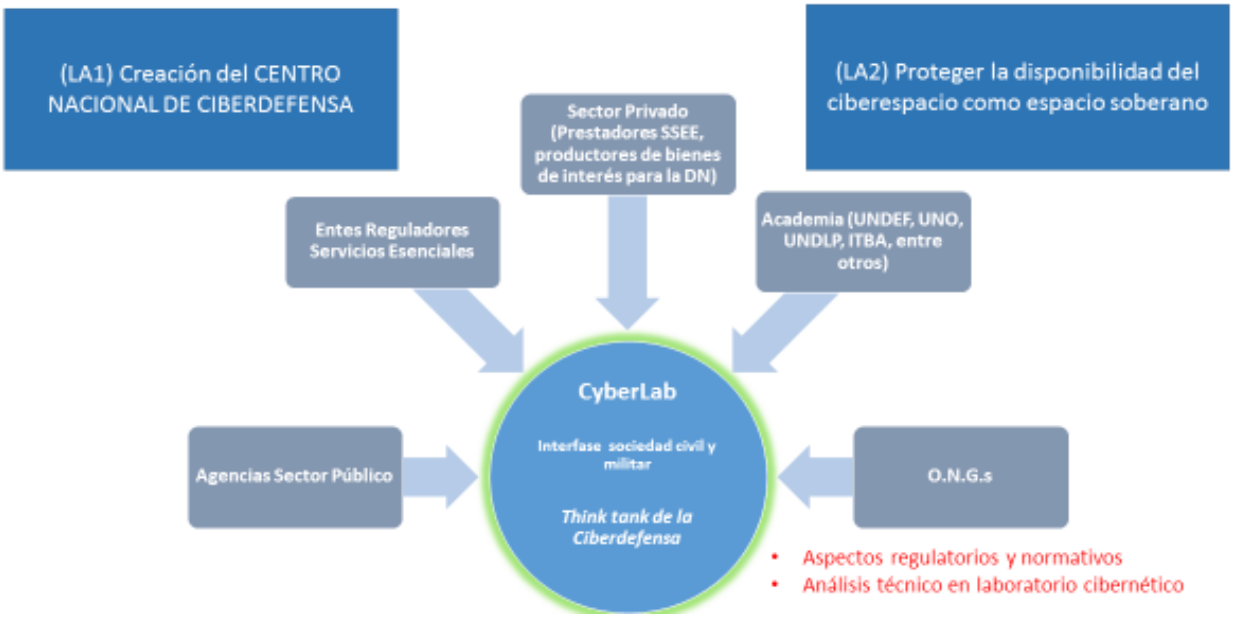
En la implementación de este Centro Nacional, se cuenta con la participación de personal calificado que actualmente desempeña tareas de investigación afectado a los diferentes proyectos científicos del CITEDEF, y que trabajarán en proyectos específicos de interés para el desarrollo de capacidades en ciberdefensa, procurando potenciar la base tecnológica e industrial nacional de ciberseguridad mediante programas específicos de investigación, desarrollo, innovación (I+D+i) y adquisiciones, así como fomentar acuerdos internacionales que faciliten a la industria nacional el acceso a tecnología y mercados.

Se prevé colaborar en la instrumentación del sistema de certificación específica de fabricantes de productos sensitivos por la función que desempeñan en las redes y sistemas de información o respecto a las cadenas de suministro asociadas a la ciberseguridad cuando las empresas no disponen de la tecnología necesaria para hacerlo o no existan proveedores que cumplan las especificaciones mínimas de ciberseguridad en los ámbitos TI, TO e IoT.

Se continuará la implementación de las siguientes etapas del ***Laboratorio de Análisis Cibernéticos (CyberLab)*** para la capacitación, concienciación y formación del personal y de los empleados en general, colaborando con la comunidad académica para superar la importante brecha entre los recursos humanos con formación técnica disponibles y los demandados en la materia, tanto en el sector privado como en el público.

Anualmente se propondrá al Ministerio de Defensa los proyectos y programas a desarrollar explicitando las fuentes de financiamiento, previendo la prestación de servicios a terceros a título oneroso, para lo cual se prepararán los actos administrativos respaldatorios de la modalidad.

El ***CyberLab*** se constituirá así en el punto de confluencia de los diferentes sectores con interés concurrente en la actividad, adoptando el formato de *Think Tank* de la Ciberdefensa, se habrá de trabajar desde allí sobre aspectos regulatorios y normativos complementando sus funciones de laboratorio cibernético para forensia, entre otras actividades, tal se muestra en el gráfico incorporado.



Tal lo indicado, la ***segunda*** línea de acción consiste en ***proteger la disponibilidad del ciberespacio*** como espacio soberano.

Mediante el uso de las herramientas de inteligencia artificial y machine learning, los ataques avanzados investigados en las redes y sistemas pueden ser registrados en el ***CSIRT de Defensa*** para elaborar estadísticas y también compartir esta información con otros CERTs internacionales relativo a grupos de grupos delictivos, hackers, amenazas cibernéticas e incidentes importantes

Este CSIRT del Ministerio de Defensa entre otras funciones, actúa como la puerta de enlace para la recepción de datos de incidentes o conductas cibernéticas anómalas desde otros CERT's nacionales y extranjeros y desde fuentes abiertas, tal de enriquecer la toma de decisión ante un ciberataque.

Asimismo, a través de la capacidad de captura de información sobre amenazas cibernéticas a objetivos estratégicos e infraestructuras críticas de la Defensa

Nacional es posible poner a disposición de los Entes Reguladores y organismos correspondientes y/o del Ministerio de Defensa, según se corresponda de acuerdo con el ordenamiento jurídico vigente, los datos necesarios para la construcción de la imagen situacional oportuna del ciberespacio.

En los servidores del sistema de monitoreo y protección de infraestructuras críticas del mencionado CSIRT se procesará además, la información recibida desde los sensores y demás hardware específico de las redes TO que se instalen en los puntos acordados con los Entes Reguladores de los servicios esenciales y objetivos estratégicos de las IICC de interés para la Defensa Nacional.

El creciente nivel de vulnerabilidad en estas redes TO, sobreviene de un entorno en el que es común la supervisión remota de los equipamientos y maquinaria gestionada por sus proveedores tecnológicos (mantenimiento on-line por defecto), la variedad y cantidad de dispositivos inalámbricos IIoT (IoT para uso industrial), sistemas operativos obsoletos, entre otras vulnerabilidades.

Para los Servicios esenciales de interés para la Defensa, ej: plantas de generación eléctrica convencionales, de energía nuclear, entre otros, se instrumentarán convenios entre el Mindef y el Ente Regulador que corresponda para la determinación de los sitios de red OT que por ser de interés para la Defensa ameriten ser objeto de monitoreo, sin que ello pueda interpretarse como interferencia con las funciones de regulación y control establecidas por la normativa vigente para el Ente en su relación con el prestador del servicio esencial en cuestión.

La digitalización de prácticamente la totalidad de los sectores industriales y la utilización creciente de metodologías de compartición de la información para el desarrollo de la actividad empresarial, así como los procesos industriales propiamente dichos, deviene inevitable la convergencia en las políticas de seguridad entre los sistemas de información del ámbito TO y los sistemas corporativos TI de esas empresas de prestación de servicios esenciales y/o de producción de bienes considerados de valor estratégico para la Defensa Nacional.

Tal como se mencionara, las redes TO poseen un escenario de exigencias específicas en cuanto a la disponibilidad, integridad y confidencialidad de la información, sensiblemente diferenciadas de los requerimientos de seguridad de los sistemas TI empresariales o corporativos.

A esto se añade el constantemente creciente flujo de amenazas de distinta naturaleza canalizadas a través del ciberespacio y muchas oportunidades orientadas a alterar el funcionamiento de las infraestructuras críticas de los servicios esenciales o de la producción de bienes de interés estratégico para la

Defensa Nacional, ya sea por razones geopolíticas o económicas (ciberespionaje, etc) o bien como parte de una ofensiva terrorista o de individuos aislados.

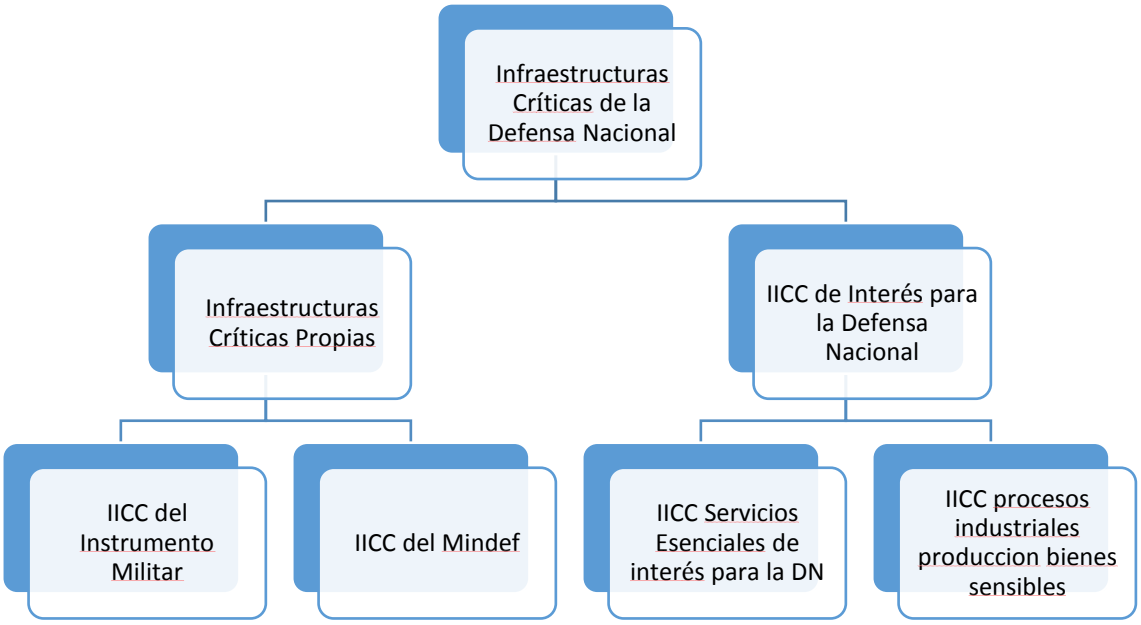
Descripción del Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas de la Defensa Nacional:

Objetivo Fortalecer la seguridad y la capacidad de recuperación de la infraestructura crítica de la Defensa, mediante la gestión de riesgos físicos y cibernéticos a través de los esfuerzos colaborativos e integrados de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras de soporte, conforme corresponda según se trate de IICC Propias o IICC de Interés para la Defensa Nacional.

En el siguiente esquema se representa la relación entre los diferentes grupos de infraestructuras críticas, según definiciones de tomadas del ANEXO II: Glosario de Términos de Ciberseguridad de la RESOL-2019-1523-APN-SGM#JGM.

Complementariamente, se definen:

a) Infraestructuras críticas de la Defensa: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto en la capacidad operacional del Instrumento Militar en el ciberespacio y/o en la prestación de los servicios esenciales así como la producción de bienes de interés para la Defensa.
b) Infraestructura Cibernética: son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y/o Tecnologías de Operación (TO).
c) Análisis de riesgos: el estudio de las amenazas posibles para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles consecuencias a la Defensa Nacional que la perturbación o destrucción de las infraestructuras que le dan apoyo puede ocasionar.
d) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios de la Defensa.
e) Protección de infraestructuras: implantación de las medidas de seguridad oportunas, tanto en su vertiente física como lógica y cibernética, redes TI y TO, con el objeto de prevenir y neutralizar el posible daño que puede causar un ataque contra las IICC de la Defensa y a garantizar la integración de estas actuaciones con los sujetos responsables dentro del ámbito de su respectiva competencia.



Actores intervinientes en la protección de infraestructuras críticas cibernéticas

- Comité de Ciberseguridad

  Creado por el Decreto 577/2017 y modificado recientemente por el Decreto 480/2019 que amplió su integración inicial, por lo que ahora resulta

  > *"ARTÍCULO 1°.- Créase el COMITÉ DE CIBERSEGURIDAD en la órbita de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, el que estará integrado por representantes de la citada Secretaría de Gobierno, de la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la JEFATURA DE GABINETE DE MINISTROS, del MINISTERIO DE DEFENSA, del MINISTERIO DE SEGURIDAD, del MINISTERIO DE RELACIONES EXTERIORES Y CULTO y del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad."*

  Adicionalmente también allí se establece que deberá fijar los lineamientos y criterios para la definición e identificación de las Infraestructuras Críticas de la Información nacionales.

- Secretaría de Gobierno de Modernización

Mediante el Decreto N°802 de fecha 5 de septiembre de 2018 se creó en el ámbito de la JEFATURA DE GABINETE DE MINISTROS, la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, la que tiene entre sus objetivos intervenir en la definición de estrategias y estándares sobre TIC y sistemas electrónicos de tratamiento de información además de entender en procesos, tecnologías, infraestructura informática y sistemas y tecnologías de gestión de la Administración Pública Nacional.

En ejercicio de sus facultades el 24 de mayo de 2019 dictó la Resolución N° 829 por la que se aprueba la Estrategia Nacional de Ciberseguridad que incluye entre sus objetivos la Protección de las Infraestructuras Críticas de Información del país.

- Entes Reguladores

Son los organismos estatales responsables del control de las condiciones de prestación de los servicios públicos a cargo de empresas privadas, concesionarios, licenciatarios, etc, o del sector público y serán los responsables de elaborar el catálogo de infraestructuras críticas del sector estratégico que les corresponda. Además de ser los responsables de ejercer el poder de policía de los servicios que regulan, tienen también a su cargo establecer las normas que arbitren sobre la topología de las redes TI y TO para garantizar los niveles de seguridad cibernéticas que se establezcan para esos servicios esenciales.

La Subsecretaría de Ciberdefensa podrá dictar recomendaciones específicas destinadas a asistir a los Entes Reguladores de cada servicio esencial con el propósito de preservar la disponibilidad y disminuir vulnerabilidades de las redes OT, y en su caso determinar los puntos de monitoreo en tales redes pertenecientes a aquellos servicios esenciales que sean de interés para la Defensa Nacional.

- Operadores críticos

Los operadores críticos son los proveedores de los servicios esenciales y los productores de bienes de interés para la Defensa Nacional, que deben realizar las prestaciones y/o proceso productivo a su cargo en un todo de acuerdo a las nuevas medidas de seguridad que se establezcan e intercambiar información sobre eventos e incidentes cibernéticos con el CSIRT DEFENSA y otros centros de respuesta que corresponda conforme lo determine el Ente Regulador con competencia en la actividad.

- Ministerio de Defensa

La Subsecretaría de Ciberdefensa es el órgano del Ministerio de Defensa responsable de la Protección de las infraestructuras críticas de la Defensa Nacional por lo que desde el CSIRT DEFENSA se realizará el monitoreo de las redes OT de las IICC de los servicios esenciales de interés para la Defensa Nacional, según se acuerde con el Ente Regulador especifico de la actividad. En lo relativo a la protección de las IICC, entre sus funciones se destacan las siguientes:

- ✓ Entender en la planificación, desarrollo y establecimiento de los procedimientos operativos relativos al funcionamiento del equipo de respuesta ante emergencias informáticas en el Ministerio de Defensa (CSIRT DEFENSA) para la atención de los incidentes relacionados con el monitoreo de las redes OT de interés para la Defensa.
- ✓ Asistir a los Entes Reguladores de los servicios esenciales de interés para la Defensa Nacional, en el dictado de normas para redes OT que contribuyan a reducir el riesgo de vulnerabilidades que limiten su disponibilidad y/o el acceso al Ciberespacio y en su caso determinar los punto de monitoreo en dichas redes y los protocolos de intercambio de información sobre incidentes cibernéticos que pudieran eventualmente producirse.

Instrumentos de política

a) Instrumentos regulatorios

Los entes reguladores de cada sector estratégico que tienen a su cargo el dictado de normas mandatorias para los prestadores de los servicios que ellos regulan, en materia de ciberseguridad contarán con las recomendaciones que la Subsecretaría de Ciberdefensa elaborará con participación del Consejo Asesor de la Ciberdefensa en el seno del ***CYBERLAB*** cuando así corresponda, siguiendo y adaptando las normativas internacionales y nacionales para las redes TI y TO que utilicen los operadores críticos y/o los productores de bienes de interés para la Defensa Nacional.

Las redes TI incluyen las tecnologías que procesan, almacenan, sintetizan, recuperan y presentan información de la forma más variada. En cambio, las TO se refieren a los sistemas que realizan funciones de control en sectores industriales e infraestructuras críticas. Es decir, con ánimo de simplificar, puede asumirse que las TO controlan el mundo físico y los sistemas de TI administran los datos e información.

Conforme lo analizado, dado la diferencia de criterios que rigen ambos entornos tecnológicos, las recomendaciones que efectúe la Subsecretaría de Ciberdefensa a los entes y organismos reguladores estarán ajustados a las normas de la Unión

Internacional de Telecomunicaciones (UIT) para la seguridad de las telecomunicaciones y las tecnologías de la información y del Instituto Nacional de Estándares y Tecnología (NIST) para la seguridad de los sistemas de supervisión, control y adquisición de datos (SCADA), sistemas de control distribuido (DCS) y otras configuraciones de sistemas de control como controladores lógicos programables, entre otros.

b) Instrumentos para la interacción en el ciberespacio

Se dispone de una solución tecnológica escalable y flexible para permitir añadir otros componentes en el futuro. Se adoptó tecnología de *inteligencia artificial* y *machine learning* para mejorar la eficacia y eficiencia de los procesos de investigación de incidentes en el ciberespacio, destinada a la prevención, detección, respuesta y recuperación ante ciberamenazas que tuviesen por destino las redes y sistemas de la Defensa.

La arquitectura de la plataforma instalada consta de un SIEM centralizado, al que reportan entre otros un ***CyberLab*** para forensia de archivos y redes, una plataforma WebInt para tareas de inteligencia cibernética. Toda la información originada en estos subsistemas es colectada en el sistema inteligente que la correlaciona para la toma decisiones en los niveles de analista que corresponde según la configuración adoptada. Tal correlación se realiza en función de reglas predeterminadas que se "ajustan" automáticamente conforme el "aprendizaje" de los sistemas.

Por su parte, las interacciones entre el iSOC, el CSIRT y las plataformas de intercambio de información **TIP** (*Threat Intelligence Platform*) tipo **MISP** (*Malware Information Sharing Platform*) y **TAXII** [1], entre otras, permite recibir datos y la posibilidad de mantenerse actualizados contra las nuevas amenazas y las conocidas. En cuanto a las amenazas de *zero-day*, el sistema inteligente dispone de herramientas tecnológicas a su disposición para procesar la información generada desde los sensores para detectarlas e investigarlas.

Completa el escenario de acción de la plataforma incorporada, el procesamiento conjunto de los datos recibidos desde sitios remotos donde se capturan por medio de los sensores y hardware específico para entornos industriales instalados en puntos acordados con cada regulador del servicio, en las redes TO de los prestadores de Servicios Esenciales de interés para la Defensa, (plantas de

[1]MISP (Malware Information Sharing Platform) es una plataforma de inteligencia para el intercambio de información sobre amenazas de código abierto. TAXII (Trusted Automated eXchange of Indicator Information), por otra parte, es un conjunto de servicios y formatos estandarizados para intercambiar información sobre ciberamenazas de uso extendido en Estados Unidos.

generación eléctrica, convencionales o nucleares, redes de transporte de la energía, etc).

Ello permitirá extender las funciones de monitoreo y de protección cuando así corresponda, tanto a los activos estratégicos expuestos a vulnerabilidades en el ciberespacio, como a otras infraestructuras soporte de servicios esenciales o productivas de interés estratégico para la Defensa.

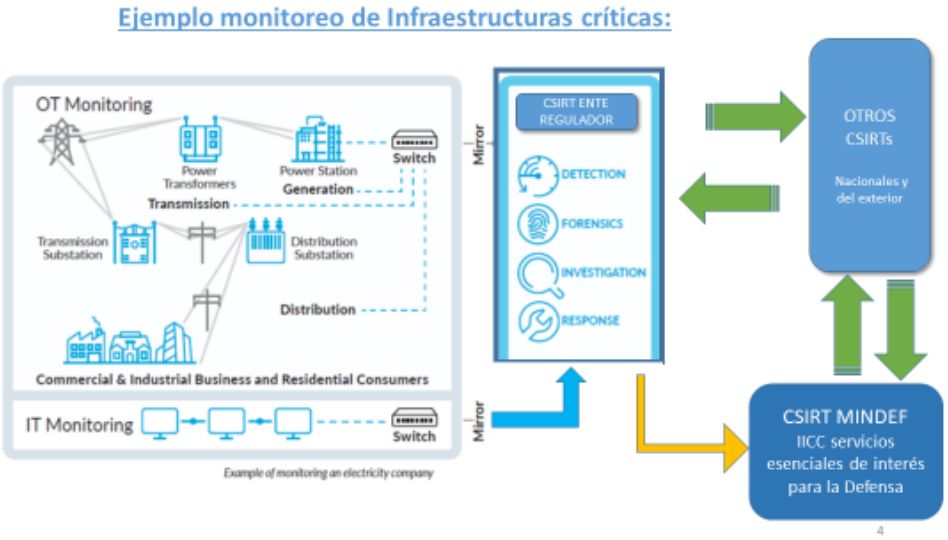
Es de gran valor para el cumplimiento de los objetivos de prevención, detección y recuperación de las infraestructuras críticas referidas, la posibilidad de relevar los activos instalados, los protocolos utilizados, en la operación, control, o envío de información, etc, a través del monitoreo las redes TO y producir las alarmas necesarias ante la detección de comportamiento anómalo en la operación, así como los intentos de intrusión a los controladores de procesos de los sistemas de producción protegidos.

Finalmente, el CSIRT del Ministerio de Defensa intercambiará datos de inteligencia con otros CERTs nacionales e internacionales, poniendo la información la actividad de grupos delictivos, hackers, amenazas cibernéticas e incidentes importantes, a disposición de los organismos que correspondan, tal lo prescripto por la legislación vigente

Se establecerán protocolos para el intercambio multilateral de información relativa a la protección de las redes y sistemas TIC e IICC de la Defensa incluyendo las de interés para la Defensa, trabajando en forma conjunta con otros organismos nacionales que corresponda para establecer acuerdos con los países líderes en materia de ciberdefensa.

Conforme la *Estrategia Nacional de Ciberseguridad* aprobada por **RES2019-829-APN-SGM#JGM** podrán asignarse infraestructuras críticas específicas para el monitoreo y en su caso protección de las misma por parte del Ministerio de Defensa, en cuyo caso se ajustará el plexo normativo que resulte aplicable para el cumplimiento de la misión que se encomiende respecto a dicha infraestructura crítica.

Se expone a continuación un gráfico que representa los flujos de datos de monitoreo hacia la Plataforma de Inteligencia Artificial y Machine Learning interactuando con sensores y órganos de red tal como se describe más arriba.



c) Instrumentos educativos y de concientización

Estos instrumentos se pueden dividir en dos grupos: (i) concientización y (ii) capacitación.

(i) La concientización consiste en iniciativas de sensibilización en temas vinculados con la ciberseguridad. Mediante la realización de este tipo de eventos, se genera confianza dentro de la población objetivo y se crea conciencia del propósito y la función del equipo de respuesta a emergencias, lo que le permite operar con mayor eficacia. Uno de los aspectos más importantes de estas actividades es identificar las carencias y las necesidades de información de la comunidad objetivo.

(ii) La capacitación de recursos humanos es otro tema fundamental a abordar y se instrumentará conjuntamente entre los distintos actores del Sistema de Ciberdefensa, convocados en el Consejo Asesor de Ciberdefensa, con la participación especial de la Universidad de la Defensa Nacional., entre otros organismos académicos de la especialidad.

Contempla la oferta de Maestría y Especialización en Ciberdefensa dirigidos a profesionales con experiencia y conocimiento en diferentes aspectos específicos vinculados a la ciberdefensa y la ciberseguridad (TIC's, sistemas, derecho informático, políticas públicas, etc.), siguiendo modelos de currícula de los centros de formación de RRHH de renombre internacional.

Asimismo, también se prevé el dictado de diferentes cursos de formación continua. Los cursos técnicos estarán destinados a formar a especialistas

en seguridad informática y de redes; los cursos operacionales a entender al ciberespacio como un ámbito militar desde una perspectiva operativa, jurídica y técnica; y los cursos de nivel político – estratégico estarán destinados a desarrolladores de políticas de ciberdefensa y a adquirir conocimiento sobre el derecho internacional aplicable a las operaciones cibernéticas.

INFRAESTRUCTURAS CRÍTICAS DE LA DEFENSA NACIONAL

IICC DE INTERÉS PARA LA DEFENSA NACIONAL	***Infraestructuras TO soporte de los Servicios Esenciales***	- Energética - Nuclear	CSIRT - MINDEF
	Infraestructuras TO soporte de procesos industriales de fabricación de bienes sensibles	- Explosivos - Moderadores de fisión en reactores nucleares - Con capacidad de producir daños masivos al medioambiente	CSIRT - MINDEF
IICC DEL SISTEMA DE DEFENSA	***Infraestructuras TO y TI del Instrumento Militar y Mindef***	No disponible	No disponible

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2019-96172220-APN-SSC#MD

CIUDAD DE BUENOS AIRES
Jueves 24 de Octubre de 2019

Referencia: ANEXO 4 - LA, Ejes Pol y Plan ICC de interés para la Defensa Nacional

---

El documento fue importado por el sistema GEDO con un total de 14 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.10.24 22:18:34 -03:00

Alfredo Raul Parodi
Subsecretario
Subsecretaria de Ciberdefensa
Ministerio de Defensa

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.10.24 22:18:35 -03:00