INSTITUTO DE CIBERDEFENSA DE LAS UERZAS ARMADAS
DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA
NOVIEMBRE DE 2023

TRABAJO FINAL INTEGRADOR

“Factores a tener en cuenta a nivel global para la protección de las infraestructuras en Argentina”

Claudio Alejandro TORRE
Mg. en Ingeniería de Software
Lic. En Análisis de Sistemas

……..

Gabriel Francisco URQUIDI ROLDAN
Licenciado en Seguridad

B. Resumen del Proyecto

El objetivo del presente trabajo final integrador consiste en diseñar las bases del plexo legislativo planificado para la protección integral de las infraestructuras críticas en Argentina, tanto en el plano del ciberespacio como en el de la seguridad física.

Dicho objetivo surge por análisis comparativo en virtud que la mayoría de los países democráticos de occidente, Australia y Japón, protegen sus infraestructuras críticas mediante proyectos de ley que se debaten y aprueban sinérgicamente en los Parlamentos.

C. Fundamentación

El Estado Nacional, ya desde el año 2011 estableció normativa necesaria pero no suficiente para la protección de las infraestructuras críticas. La publicación de decretos y resoluciones en esta temática se incrementó sensiblemente a partir de la pandemia Covid19.

C.1 A través de la Resolución n ° 580/2011, la Jefatura de Gabinete de Ministros (JGM) comenzó a elaborar un marco regulatorio específico denominado: "Programa de protección de Infraestructura Critica".

C.2 Por Decreto Presidencial 577/2017 se creó en la órbita del Ministerio de Modernización, el Comité de Ciberseguridad integrado por representantes del citado Ministerio, del Ministerio de Defensa y del Ministerio de Seguridad. Luego fue ampliado por Decreto n ° 480/2019 con representantes del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto y Justicia y Derechos Humanos y las Secretarías de Innovación Pública y Asuntos Estratégicos.

C.3 Por Resolución JGM, n ° 1523 de 2019, se definió el concepto de Infraestructura Critica, como *"aquellas estructuras que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía".*

C.4 Mediante Resolución n ° 829 de 2019 de la Secretaría de Modernización, se estableció la Estrategia Nacional de Ciberseguridad, la cual trata de manera más específica en uno de sus objetivos centrales, la temática de protección de Infraestructuras Críticas.

C.5 Con la Resolución n ° 44 de 2023 se aprobó la Segunda Estrategia Nacional de Seguridad, la cual entiende a la ciberseguridad como el "conjunto de políticas y acciones orientadas a elevar los niveles de seguridad de las infraestructuras de las TIC".

Justificación

Como se mencionó en el Resumen, la República Argentina carece hoy de un instrumento con fuerza de Ley Federal que regule la protección de las infraestructuras críticas. Nuestro propósito es detectar anomalías en la situación actual, debatirlas, arribar a conclusiones válidas y proponer un modo de acción en el ámbito legislativo.

Con el objeto de acercar al lector evidencias que aporten a su análisis inductivo, a continuación, se describen dos (2) hallazgos sobre incidentes recientes que plantean el problema de *"no contar Argentina con un plexo legislativo que le permita proteger de modo planificado a sus infraestructuras críticas, ya sea, en el plano cibernético como en el de la seguridad física".*

Hallazgos:

C.6 Afectación de Infraestructuras Críticas originadas por deficiencias en la seguridad del ciberespacio o ciberseguridad:

- 1 de agosto de 2023, ciberataque del tipo "ransomware" [ARG, 2023] al sitio web del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, más conocido como PAMI - Programa de Asistencia Médica Integral.
  Consecuencia: durante quince (15) días fue interrumpido el acceso a las historias clínicas de los pacientes, los turnos en consultorios, la logística de drogas oncológicas, el sistema de pagos a proveedores, entre otros servicios.

- 7 de junio de 2023: hackeo a la Comisión Nacional de Valores (CNV). La organización de ciberataques autodenominada *"Medusa",* especializada en ransomware [ARG, 2023], publicó en la "dark web" 500.000 documentos de bancos y empresas argentinas, alojados en los servidores de la CNV. Legalmente, el secuestro de datos personales afecta a los funcionarios públicos por incumplimiento de la ley 25.326, lo que los hace penalmente procesables.

C.7 Afectación de Infraestructuras Críticas causadas por anomalías en la seguridad física:

- 1 al 3 de marzo de 2023: masivo corte de energía originado por incendios de pastizales en proximidades de la Central Nuclear de Atucha. El ministro Massa denunció judicialmente el hecho para investigarlo como "posible sabotaje". Daños: se redujo la producción energética en 10.000 mega watts, es decir, un 35% del total de la generación nacional diaria en ese periodo. La ausencia de control en la seguridad física podría haber afectado el interior de Atucha, con el consecuente riesgo ecológico por propagación de radioactividad en una amplia área geográfica densamente poblada.

D. Planteamiento del Problema

A continuación, se detallan dos (2) documentos oficiales, generados, el primero en el Poder Ejecutivo Nacional y el segundo, en el Poder Legislativo, cuyos argumentos demuestran que Argentina trata erróneamente, mediante una perspectiva de compartimientos estancos, el problema de la protección de sus infraestructuras críticas.

D.1 El 28 de mayo de 2023, mediante la firma del Decreto del Poder Ejecutivo Nacional n° 284/2023, el presidente de la Nación designó a la JEFATURA DE GABINETE DE MINISTROS, como "Organismo Ejecutor" del "Programa de Ciberseguridad para Infraestructuras Críticas de la Información (ICI)". A través de un préstamo de 30 millones de dólares estadounidenses, financiado por el Banco

Interamericano de Desarrollo (BID) 5735/OC-AR, nuestro país comenzará a implementar la protección de sus Infraestructuras Críticas.

Los objetivos específicos del programa son: (i) aumentar la cobertura de gestión para la identificación y protección de las Infraestructuras Críticas de Información (ICI), (ii) mejorar la productividad en la gestión de incidentes cibernéticos y (iii) mejorar la eficacia en la gestión de la ciberseguridad de las ICI priorizadas.

D.2 El 17 de agosto de 2023 fue presentado en segunda oportunidad por la diputada Jimena H. Latorre (UCR-Mendoza), aún no tratado en el Congreso de la Nación, el proyecto de Ley sobre Protección de las Infraestructuras Críticas de la Energía (ICE). La Diputada señala: "Las Infraestructuras Críticas son indispensables para el funcionamiento de los servicios esenciales, con lo cual su destrucción o perturbación -total o parcial- afectaría significativamente al Estado y su población".

Anomalías

Tanto D.1, Decreto Presidencial como D.2, Proyecto de Ley de la diputada, exhiben un grave inconveniente: su alcance resulta restringido. En ambos casos se limitan en resolver la protección de las infraestructuras críticas exclusivamente en un campo de aplicación, sin extenderla a la contraparte.

- el Decreto Presidencial se centra en la protección cuando las amenazas provienen del ciberespacio (ICI), y;

- el Proyecto de Ley focaliza el problema sólo a las infraestructuras críticas de la Energía (ICE).

Las dos (2) documentos oficiales anteriores surgen como reacción para dar respuesta a la sociedad al producirse eventos puntuales no deseados: cortes de energía globales y ciberataques a sitios web públicos de uso masivo o crítico. Siguiendo con este esquema de razonamiento, es dable suponer que, en un futuro próximo, a medida que se produzcan este tipo de incidentes, surgirá anárquicamente tanta normativa de protección de infraestructuras críticas como áreas específicas existen: el agua, la salud, el transporte, la alimentación, la industria farmacéutica, etc.

Por otra parte, los hackeos al PAMI, a la CNV y el incidente en Atucha (descriptos en Hallazgos), a diferencia de lo que ocurre en el resto del mundo, ponen en evidencia la nula intervención del Sistema de Inteligencia Nacional (SIN), indispensable herramienta para prevenir este tipo de amenazas.

El incidente de seguridad en la Central Nuclear de Atucha [Atucha, 2023], nos permite inducir que sobre las Tecnologías de Operación (OT), no existe una adecuada gestión de crisis. En ese contexto, Defensa Civil, en los niveles municipal, provincial o nacional, brinda apoyo operativo, pero lo realiza de manera más reactiva, que planificada con las autoridades de la infraestructura críticas afectada.

E. Hipótesis: la protección de infraestructuras críticas en Argentina resulta insuficiente por carecer de un plexo legislativo que audite, coordine e integre de manera planificada, tanto la seguridad en el plano físico como en el plano de la información. Intentaremos esbozar a continuación el contenido de dicho plexo legislativo.

Los documentos oficiales presentados en D.1 y D.2, evidencian de manera explícita que en la República Argentina no se cumple el axioma CIS "*Carácter Integral de la Seguridad*". [BOE, 2022], el cual sostiene que: *"la seguridad física y digital son áreas que deben ser abordadas de forma interrelacionada y con una perspectiva holística. Esto redundará en una visión global, posibilitando el rediseño de una estrategia corporativa única, y optimizando el conocimiento, los recursos y los equipos".*

F. Objetivos a ser alcanzados para sustentar la Hipótesis

F.1 Impulsar el debate en el Congreso de la Nación Argentina de la *"Ley de Protección de Infraestructuras Críticas".*

F.2 Incorporar el axioma CIS *"Carácter Integral de la Seguridad"* en la reglamentación de la Ley, citado previamente en la hipótesis. [BOE, 2022]

F.3 Sumar nuevos miembros al Comité de Ciberseguridad: Si bien fue ampliado por Decreto n° 480/2019, la complejidad del problema aquí abordado requiere su ampliación. Deberían estar presentes en dicho comité, actores que representan otras áreas vitales como lo son el Ministerios de Salud, de Economía, de Transporte, el Sistema de Inteligencia Nacional (SIN), la Comisión Nacional de Energía Atómica, entre otros organismos.

F.4 Adoptar en Argentina el modelo español de protección de infraestructuras críticas (LPIC). Dicha elección está sustentada, analizando factores como la idiosincrasia, idioma común, métricas, diseño y prestigio técnico internacional. El modelo ibérico se basa en el axioma CIS "*Carácter Integral de la Seguridad",* presentado en la Sección E: Hipótesis. Fue implementado en veintiséis (26) meses, cumple con los requerimientos de la Comunidad Europea y de las organizaciones internacionales rectoras sobre protección de infraestructuras críticas (ONU, UIT, OSCE, NCSI, etc.). Ver detalles en sección G (Marco Teórico Preliminar).

A continuación, se exponen algunas métricas entre España y Argentina publicadas por el Índice de Ciberseguridad Nacional (NCSI) de Estonia. (https://ncsi.ega.ee/) El índice califica a los países de acuerdo a los niveles porcentuales de satisfacción de requerimientos en ciberseguridad: Como se aprecia en el siguiente párrafo, el déficit de Argentina respecto a España resulta notorio.

Puestos en el Ranking NSCI: España 10°, Argentina 51°.
Satisfacción de requerimientos entre ambos países:

- Área "Información y análisis de ciber amenazas": España 100 %, Argentina 40 %.
- Área "Protección de Servicios Digitales": España 100 %, Argentina 20%.
- Área "Protección de servicios esenciales", España 83 %, Argentina 16 %.
- Área "Identificación de usuarios y servicios de confianza": España 100%, Argentina 55 %.

F.5 Implementar, para la protección de infraestructuras críticas, el planeamiento iterativo piramidal de acuerdo a lo presentado en la Sección G (Marco Teórico Preliminar). Consta de cinco (5) niveles escalonados de planeamiento, aplica la metodología de análisis de riesgo [PHA, 2023) y el modelo de

Madurez de Capacidades [CMM, 2006] por mejora continua iterativa. La implementación total del plan demandará un periodo aproximado de tres (3) años.

El primer nivel de planeamiento, en la cúspide de la pirámide, será ejecutado por el Gobierno y el Congreso de la Nación (Planeamiento Estratégico). Se establecerán allí las metas, tiempos de cumplimientos y requerimientos para el resto de los niveles inferiores. (Planeamiento táctico y operativo).

F.6 Identificar las infraestructuras críticas y a los operadores que las financian. Dicha catalogación se documentará en los "*Planes Sectoriales*" y "*Planes de Seguridad de los Operadores"* (PSO). El encargado de realizarla será el *"Grupo de Trabajo de Protección de Infraestructuras Críticas (GTPIC)"*, establecido a tal efecto en el primer nivel de planeamiento.

F.7 Requerir a los puntos de contacto de cada infraestructura crítica identificada, que confeccionen sus "*Planes de Protección Específicos"* (PPE), tanto para cubrir amenazas originadas en la seguridad física / operación (OT) como en aquellas provenientes de las tecnologías de la información (IT), o mixtas. Cada infraestructura crítica determinará su CERT (Servicio de Respuesta a Emergencias), contratándolo en el ámbito privado (CERT de Referencia) o implementando un servicio propio. En caso de producirse un incidente, el CERT correspondiente brindará apoyo técnico inmediato.

Los PPE incluirán todas aquellas medidas de resiliencia que los CERT ejecutarán para neutralizar las amenazas. También aquí se deberán determinar las situaciones (anomalías / amenazas) en las que se requerirá soporte operativo externo.

Si por su envergadura, un incidente (ciberataque, sabotaje, ataque externo / interno, catástrofe natural, etc.) excediera las capacidades y tiempos de respuesta propia, la infraestructura crítica afectada solicitará apoyo estatal de acuerdo a su *"Plan de Apoyo Operativo"* (PAO), último nivel de planeamiento. El PAO lo ejecutará el Estado a través de los organismos establecidos a tal efecto (CCCD, CERT.ar, Defensa Civil, FF. SS, FF. AA), entre otros y en coordinación con el CERT de la infraestructura critica afectada.
Mediante análisis forense, se determinarán los gastos ocasionados por el apoyo operativo suministrado, los cuales deberán ser restituidos en tiempo y forma. (Ver Anexo J.1 Ejecución del Plan)

F.8 Crear la "*Unidad de Protección de Infraestructuras Críticas (UPIC)"*, dependiente directamente del Ministro de Defensa, en virtud de lo indicado en el Artículo 21 del Decreto 727 / 2006, que en materia de Defensa Nacional establece: *"Disponer la conformación de unidades operacionales específicas y/o conjuntas, de conformidad con la evaluación que el Ministerio de Defensa realice en el marco de los objetivos estratégicos y de la planificación estratégica militar".*

Visión (UPIC): *"La Unidad de Protección de Infraestructuras Críticas (UPIC) será la encargada del análisis, el tratamiento y la transmisión de información a los efectos de prevenir y mitigar los riesgos que afecten a los objetivos estratégicos".*
Misión: *"auditar el conjunto de infraestructuras críticas cuyo normal funcionamiento resulta esencial para el cumplimiento de las funciones vitales del país y coordinar la designación de los organismos del*

Estado, cuando la envergadura de un incidente requiera para su neutralización, apoyo operativo inmediato". Ver Anexo J.2 Organigrama UPIC.

Ámbito: involucra a los dominios terrestre, naval, aéreo, espacial y ciberespacial. Comprende tanto a las tecnologías de información (IT) como a las tecnologías de operación (OT). Su rol no es operativo, sino eminentemente de control, análisis y gestión.

Debe ser transversal a todas las infraestructuras críticas del Sector Público y Privado.

F.9 Definir los roles, restricciones y limitaciones de los organismos del Estado (CCCD, CERT.ar, Defensa Civil, FF. SS, FF. AA, etc.) a ser designados para ejecutar los Planes de Apoyo Operativo (PAO).

F.10 Requerir a los organismos citados precedentemente el diseño y ejecución de ejercicios / simulacros, planificados con el fin de adiestrar a la organización en lo relativo a amenazas procedentes del ciberespacio y de la seguridad física en función de los Planes de Protección Específicos (PPE) y Planes de Apoyo Operativo (PAO).

F.11 Asignar financiamiento: la UPIC deberá contar con autonomía y autarquía financiera (ídem Unidad de Información Financiera - UIF).

F.12 Designar a la UPIC, mediante concursos públicos, los RR. HH necesarios, de carácter profesional y técnico, en el campo de la seguridad informática y seguridad industrial. También deberá priorizarse la reasignación de personal capacitado y disponible de la Administración Pública con la debida recategorización. El cuadro de reservistas de las FF. AA. es una potencial fuente de dichos recursos, especialmente en tareas específicas por periodos de tiempo determinado (ejercicios y simulacros).

F.13 Participar al sector educativo nacional y privado en las tareas de I+D para la sistematización de la gestión de seguridad integral. Los colegios profesionales informáticos y de ingeniería industrial deberán dictar y hacer cumplir a los operadores de Infraestructuras Críticas, "prácticas de seguridad desde el diseño", como requisito previo a la habilitación de las mismas.

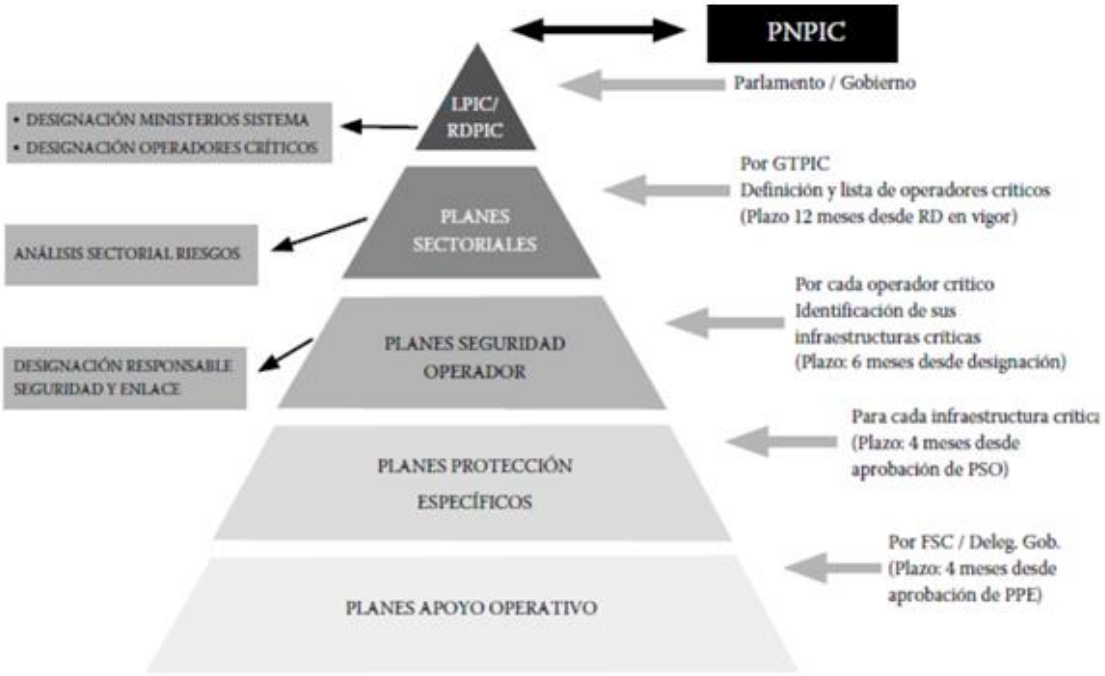
F.14 Gestionar con los puntos de contacto del BID, los mecanismos técnicos financieros que permitan ampliar los objetivos del crédito otorgado de treinta millones de dólares (30.000.000 U$D), extendiéndolos para cubrir no sólo las amenazas provenientes del ciberespacio sino también contemplar las amenazas que se originan en la seguridad física.

Un claro ejemplo de la necesidad de ampliar los objetivos del crédito, surge por la denuncia de "*posible sabotaje*" presentada en la Justicia por el ministro Massa, en virtud a los cortes de energía provocados por incendios en proximidades de la Central Nuclear de Atucha.

G. Marco teórico preliminar (Modelo implementado por el Reino de España)

Mediante la Ley de Infraestructuras Críticas [LPIC, 2008], el Reino de España diseñó e implementó su planeamiento iterativo piramidal de cinco (5) niveles.

Modelo Piramidal de cinco (5) niveles



G.1 Promulgación de la Ley LPIC española y su reglamentación. Responsable: Parlamento y Gobierno. Diseño Top Down, el cual planifica de lo general a lo particular. Se establecieron aquí los plazos para la implementación de planes en cada nivel.

G.2 Planes Sectoriales: mediante análisis de riesgos, se identificaron a los operadores de infraestructuras críticas, los cuales son los responsables de la inversión de cada instalación, red, sistema o equipo físico, catalogada como infraestructura crítica. Plazo: 12 meses desde aprobado el punto anterior.

G.3 Planes de Seguridad del Operador (PSO): Cada operador identificado en el Plan Sectorial, designó a sus puntos de contacto en las infraestructuras críticas a su cargo, los cuales fueron concientizados y capacitados. Plazo: 6 meses luego aprobado el punto anterior.

G.4 Planes de Protección Específicos (PPE): cada infraestructura crítica definió las buenas prácticas a aplicar en su ámbito, especificando las medidas de autoprotección y estableció las anomalías / amenazas por las cuales deberá recibir a través del Plan de Apoyo Operativo (PAO), soporte de fuerzas estatales. Plazo: 4 meses desde la aprobación del PSO.

G.5 Plan de Apoyo Operativo: Se les asignó a las FF. AA / FF. SS las responsabilidades de aplicar la protección definida en el PPE, interviniendo según el plan de seguridad (física y del ciberespacio) establecida en el paso anterior para cada infraestructura crítica. Su rol fundamental es brindar

apoyo operativo cuando se ve superada la infraestructura de seguridad de cada infraestructura crítica. Plazo: 4 meses desde la aprobación del PPE.

Dada la continua aparición de nuevas amenazas a las infraestructuras críticas, el modelo es cíclico por iteraciones sucesivas a los efectos de actualizar las técnicas, tácticas y normativas que den solución a los requerimientos no satisfechos de seguridad integral.

Es importante destacar el concepto que España estableció sobre *"responsabilidad compartida"*, el cual no solo involucra a la responsabilidades civiles y penales de los funcionarios del Sector Público, sino también a los responsables de las infraestructuras críticas del Sector Privado.

H. Metodologías y técnicas utilizadas para sustentar / contrastar la Hipótesis

H.1 Modelo de Madurez de Capacidades o CMM (Capability Maturity Model). Se recomienda aplicar esta metodología para la implementación del Modelo Piramidal de Cinco (5) Niveles de Planeamiento que propone este trabajo integrador. Consiste en un modelo evaluador de organizaciones. Fue desarrollado inicialmente para aportar una visión ingenieril a los procesos artesanales de diseño del software. El autor fue la Universidad Carnegie-Mellon a requerimiento del Software Engineering Institute (SEI).

Este modelo agrupa en cinco (5) *"niveles de madurez"* a las organizaciones. *De acuerdo al* porcentaje de procesos y buenas prácticas que una organización haya implementado, institucionalizado y documentado, se determina su nivel de madurez. Si llega al nivel *Optimizado*, se puede concluir que la organización arribó a su máximo nivel de madurez.

Nivel Inicial: Las organizaciones en este nivel no disponen de un ambiente estable. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven afectados por falta de planificación. El éxito de los proyectos se basa en el esfuerzo personal, casi siempre implica retrasos y sobrecostos. El resultado de los proyectos es impredecible.

Repetible: En este nivel las organizaciones disponen ya de prácticas institucionalizadas de gestión de proyectos, existen métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente.

Definido: Además de buena gestión de proyectos, en este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detalladas y un nivel avanzado de métricas en los procesos. Se implementan técnicas de revisión entre pares de profesionales.

Gestionado: Se caracteriza por organizaciones que disponen de métricas de productividad, las cuales se usan de modo sistemático para la toma de decisiones con gestión de riesgos. Su resultante es de alta calidad.

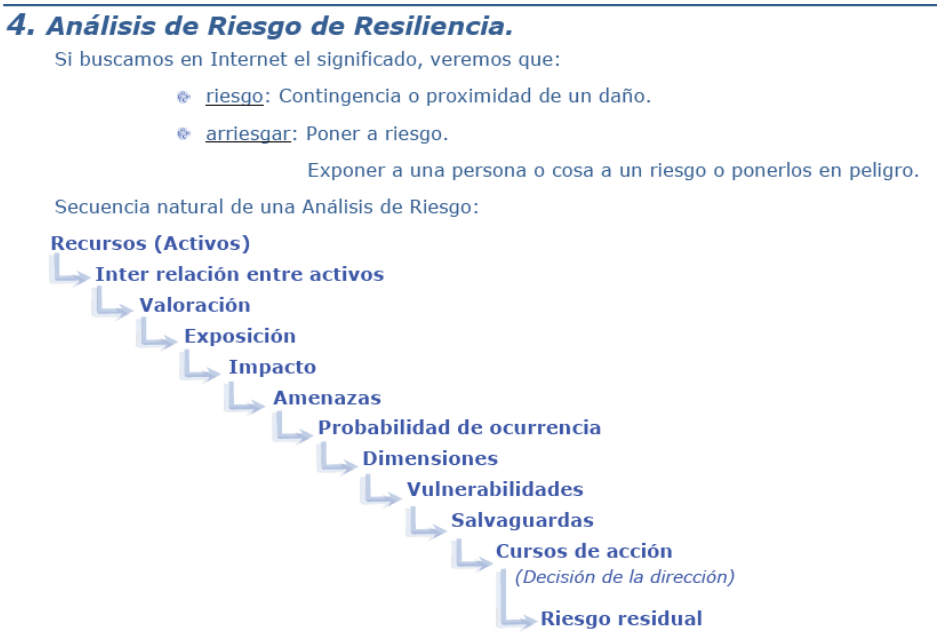
Optimizado: La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de métricas y se gestiona el proceso de innovación en forma iterativa.

H.2 La metodología de análisis de riesgo, también conocido como evaluación de riesgos o PHA por sus siglas en inglés. Process Hazards Analysis, es el estudio de las amenazas y probables eventos no deseados, que, de producirse, generarían daños sobre las organizaciones. Su objetivo es la mitigación de esos riesgos.

Este tipo de análisis utiliza métodos cualitativos y cuantitativos como herramienta de gestión en estudios financieros y, primordialmente en organizaciones de seguridad.

Se especifican los activos a proteger, las amenazas y riesgos asociados, valorando con probabilidades de ocurrencia a los eventos no deseados que generan vulnerabilidades a mitigar. Por último, se calcula el riesgo residual que se asume no cubrir por las limitaciones de la organización.

En la figura siguiente, extraída de la disertación que brindó a esta Diplomatura el Dr. Alejandro Corletti, se exponen los eventos en cadena a partir de evaluar el recurso (activos) y sus riesgos.



I. Referencias iniciales y bibliografía preliminar

BOE: Boletín Oficial del Estado Español.
CCCD: Comando de Ciberdefensa de las FF. AA.
CE: Comunidad Europea.
CIS: Carácter Integral de la Seguridad.
CMM: Modelo de Capacidad y Madurez.
LPIC: Ley de Infraestructuras Críticas

NCSI: Índice de Ciberseguridad Nacional – Estonia.
OSCE: Organización para la Seguridad y la Cooperación europea.
ONU: Organización de las Naciones Unidas.
SEI: Instituto de Ingeniería del Software.
UIT: Unión Internacional de Telecomunicaciones.
UPIC: Unidad de Protección de Infraestructuras Críticas.

I.1 ARG, Argentina.gob.ar (2023), "El ransomware, el software malicioso usado para atacar a las organizaciones" <disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-6>

I.2 BOE, Jorge Lozano Miralles, María José Carazo Liébana (2022) "Carácter Integral de la Seguridad". Agencia Estatal Boletín Oficial del Estado Español <disponible en: https://www.boe.es/biblioteca_juridica/codigos/abrir_pdf.php?fich=400_Ambitos_de_la_Seguridad_Nacional_Proteccion_de_Infraestructuras_Criticas.pdf>

I.3 CMM, Software Engineering Institute (2006) "Capability Maturity Model" < disponible en: https://cfpub.epa.gov/si/si_public_record_Report.cfm?Lab=ORD&dirEntryID=11663 >

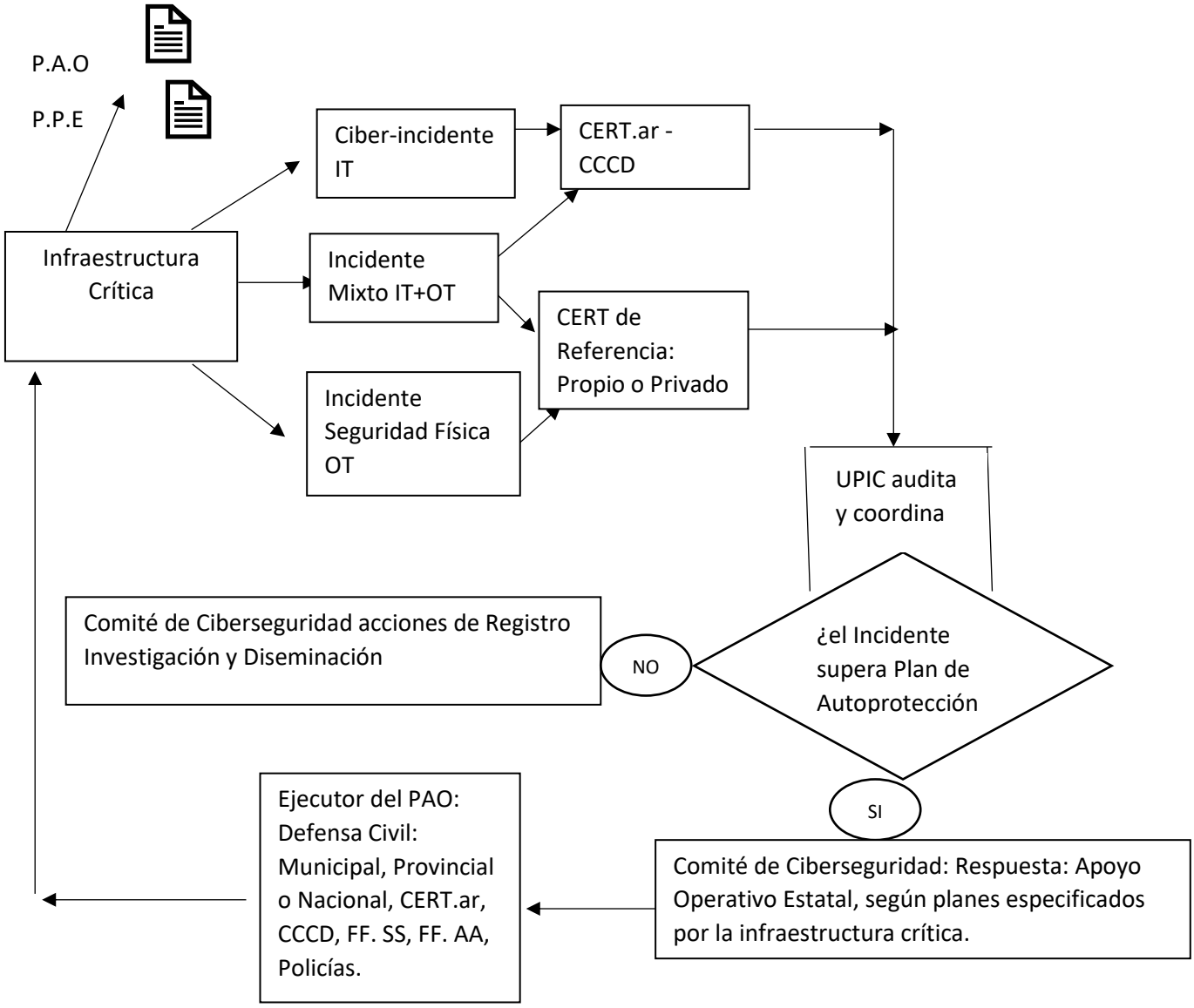
I.4 LPIC, Juan Carlos I Rey De España (2008), "Protección de las Infraestructuras Críticas " <disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf >

I.5 PHA, Health Administration (OSHA) Process Safety Management (1990) "Proceso de Análisis de Riesgos" <disponible en https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo>

J. Anexos:

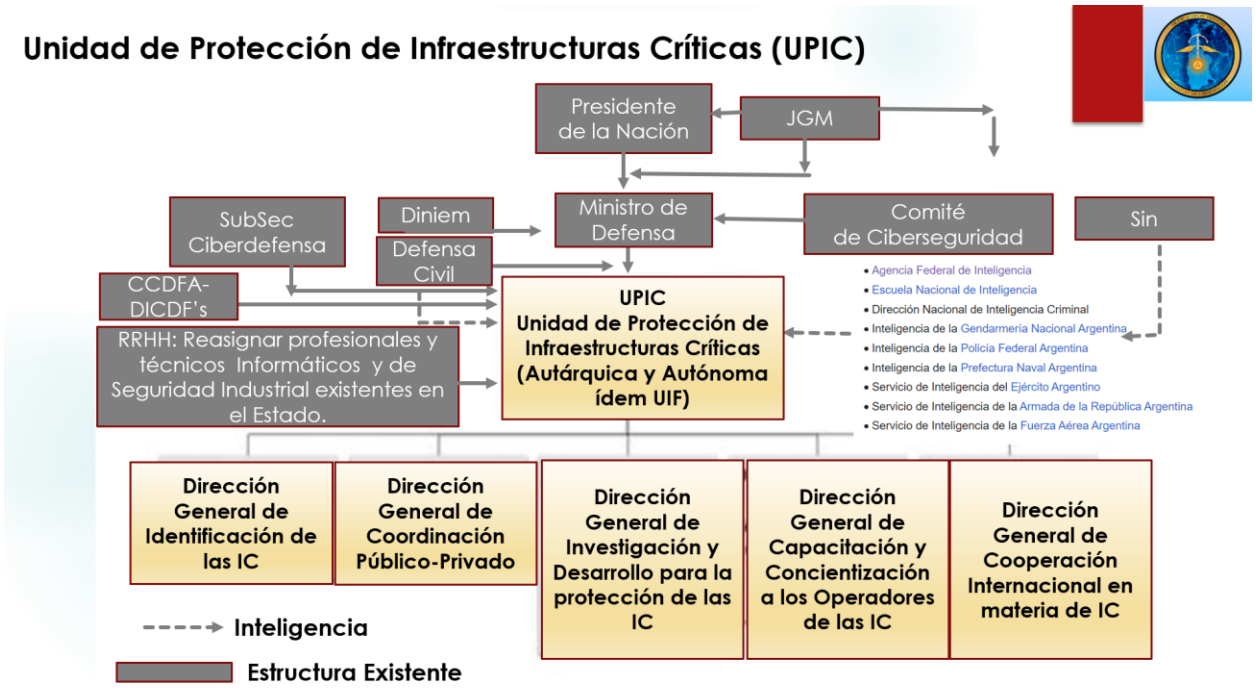
ANEXO J.1

Execution del Plan



ANEXO J.2

Organigrama UPIC



Dependiendo directamente del Ministro de Defensa y a través de la JGM se conecta con el comité de ciberseguridad. Recibe información estratégica militar de la DINIEM y del resto del Sistema Nacional de Inteligencia (SIN) para la identificación de amenazas y la detección de nuevas infraestructuras críticas. Se nutre de especialistas egresados del Instituto de Ciberdefensa de las FFAA. Los planes de apoyo operativo los ejecutará la Subsecretaría de Ciberdefensa, con personal del Comando de Ciberdefensa de las FFAA y las direcciones de ciberdefensa de cada Fuerza. La estructura de la UPIC queda materializada con las 5 Direcciones que se despliegan en la parte inferior de la orgánica.

K. CV de los ejecutores del Trabajo Final:

K.1 Nombre y Apellido: Claudio Alejandro TORRE.
Fecha de Nacimiento: 28/04/1961.
Capitán de Navío Retirado.
Título de Grado: Licenciado en Análisis de Sistemas (UCALP).
Títulos de Postgrado: Especialista y Magister en Ingeniería de Software Facultad de Informática, Universidad Nacional de La Plata (UNLP).

- ✓ Principales hitos de experiencia laboral:
  - Jefe del Servicio de Informática de la Armada (2015-2019).
  - Diseño e Implementación de la Red de Monitoreo a través del Sistema de Identificación Automática (AIS) de Buques de las Armadas de Argentina, Brasil, Uruguay y Paraguay (AMAS).
  - Representante de Argentina en Comité de Expertos Técnicos del Sistema de Identificación y Seguimiento de Largo Alcance de los Buques Mercantes (LRIT) de la Organización Marítima Internacional (OMI) en Londres, UK.
  - Evaluador del Sistema Satelital de Monitoreo de Buques Pesqueros (MONPESAT) Subsecretaría de Pesca de la Nación.
  - Diseño del Reglamento de Informática de la Armada.
- ✓ Publicaciones
  - 2008, Organización Marítima Internacional (OMI): Detección y soporte para resolver una falla en los mensajes de Búsqueda y Rescate de Buques (LRIT). OMI Londres (UK).
  - 2013 - Tesis de maestría: "Incorporación de la Psicología Social al Proceso de Elicitación de Requerimientos de Software". FACULTAD DE INFORMATICA; UNIVERSIDAD NACIONAL DE LA PLATA.
  - 2018 – Publicación del Reglamento de Informática de la Armada.
- ✓ Antecedentes Docentes
  - Profesor de la asignatura *"Sistemas Automatizados de Comando y Control",* S.A.C.C.O, Escuela de Oficiales de la Armada (ESOA), Base Naval de Puerto Belgrano, 1990.
  - Profesor titular de la asignatura, *"Sistema de Procesamiento de Datos I"*, Instituto de Estudios Superiores de Bahía Blanca, 1989.

K.2 Nombre y Apellido: Gabriel Francisco URQUIDI ROLDAN
Fecha de Nacimiento: 18/09/1974.
Título de Grado: Licenciado en Seguridad, Universidad Nacional de Lomas de Zamora, Facultad de Derecho, ingreso Julio de 2.019, egreso 12 de marzo de 2022.

Estudios de Postgrados:

- Diplomatura en Seguridad Bancaria y Tecnología Aplicada, Resolución A/Nro 0009/13, Universidad Nacional de Lomas de Zamora, Facultad de Derecho, ingreso Marzo de 2015, egreso Diciembre del 2015.

- Diplomatura en Derecho Internacional Humanitario, Universidad de la Defensa Nacional, Facultad de la Fuerza Aérea Argentina, Instituto Nacional de Derecho Aeronáutico y Espacial, Ingreso Marzo del 2.018, egreso Diciembre del 2.018.
- Diplomatura en Derecho Aplicable a la Defensa, Universidad de la Defensa Nacional, Escuela Superior de Guerra Conjunta, iniciada en abril de 2.021, egreso Julio de 2.021.
- Diplomatura en Sistema de Video Observación Aplicable a la Seguridad, Instituto Universitario Policial Provincia de Buenos Aires Crio Gral Honiris Causa Juan Vucetich, Res 02/2023, egreso: 13 octubre de 2023.

Titulo Terciario Universitario: Técnico Superior en Seguridad, Universidad Nacional de Lomas de Zamora, Facultad de Derecho, ingreso: marzo de 2017, egreso: Junio de 2019

Carreras en curso:

- 2do año de la Maestría en Inteligencia Estratégica Nacional. Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional de la Plata, cohorte 2022.
- Diplomatura Universitaria en Gestión de la Ciberdefensa, Instituto de Ciberdefensa de las Fuerzas Armadas, cohorte 2023.
- Curso de Francés Nivel II, Escuela Superior de Gendarmería Nacional Argentina, cohorte 2023.
- Curso de Postgrado de Historia Naval y Marítima de la Escuela Superior de Guerra Naval, cohorte 2023.

Cursos Militares

- CURSO de Formación de Oficiales Profesionales de la Reservas del Ejército Argentino, Colegio Militar de la Nación, Universidad de la Defensa Nacional. 9 de octubre del 2.021.
- CURSO de Defensa Nacional, Disposición 17/05, Escuela de Defensa Nacional.
- CURSO de Negociación y Mediación en temas de defensa Nacional, Disposición 32/03, Escuela de Defensa Nacional.
- CURSO Armas de Destrucción Masiva y No-proliferación, Autoridad Regulatoria Nuclear, Escuela Superior Técnica, Ejercito Argentino.
- CURSO de Anticipación Estratégica y Prevención de Riesgo, Escuela Superior de Guerra Conjunta, Universidad de la Defensa Nacional.
- CURSO de Polemologia, Escuela Superior de Guerra Conjunta, Universidad de la Defensa nacional.
- CURSO de Introducción al Planeamiento Estratégico, Escuela Superior de Guerra Conjunta, Universidad de la Defensa Nacional.
- CURSO de Conflictos Contemporáneos Armados en África, Escuela Superior de Guerra Conjunta, Universidad de la Defensa Nacional.
- CURSO de Brigadista en Incendio Forestales, Secretaria de Coordinación Militar en Emergencias, Batallón de Ingenieros 601.
- CURSO de Investigación Médica y Factores Humanos en Accidentes Aéreos, Instituto Nacional de Medicina Aeronáutica y Aeroespacial, Facultad Fuerza Aérea Argentina, Universidad de la Defensa Nacional.

- CURSO de Evacuación Aeromedica, Instituto Nacional de Medicina Aeronáutica y Aeroespacial, Facultad Fuerza Aérea Argentina, Universidad de la Defensa Nacional.
- CURSO de Reanimación Cardio Pulmonar Modalidad Medicina en Altura, Instituto Nacional de Medicina Aeronáutica y Aeroespacial, Facultad de la Fuerza Aérea Argentina. Universidad de la Defensa Nacional.
- CURSO de GDE (CCOO-GEDO-EE), Escuela de Informática de Ejercito.
- CURSO, Liderazgo, su función en la sociedad, cohorte 2023, Centro de Oficiales de las Fuerzas Armadas.

Otros cursos

- CURSO de Capacitación para Agentes del Agrupamiento Comando, especialización en Seguridad Publica, Escuela de Suboficiales y Agentes “Agente Rosendo Matia” Ministerio de Seguridad.
- CURSO de Auxiliar Armero, Modulo 1, Escuela Penitenciaria Federal. Centro de formación Profesional Nro 401.
- CURSO de Auxiliar Armero, Modulo 2, Escuela Penitenciaria Federal. Centro de formación Profesional Nro 401.
- CURSO de Tiro Defensivo a Corta Distancia, Escuela de Suboficiales Coronel Rómulo Páez, Servicio Penitenciario Federal.
- CURSO de uso de Escopeta-Nivel Básico, Resolución 478/2010, División Grupo Especial de Intervención, Servicio Penitenciario Federal.
- CURSO de Operador Táctico de Escopeta, Centro Argentino de Seguridad, Resolución 384/2017.
- CURSO Tactical Shotgun Operator, Iron Tactical, IT Training and Education Section, Atlanta, GA USA. 15th day of Octubre, 2016.
- CURSO de Tiro con Armas de Avancarga y pólvora negra, Tiro federal de Lomas de Zamora, Asociación Argentina de Tiradores de Avancarga.
- CURSO de Historia y Evolución de la Armas, Museo de Armas de la Nación Tte Gral Richeri.
- CURSO de Resolución de Crisis con Explosivos, Sección Neutralización de Explosivos, Unidad Regional II – Rosario, Policía de la Provincia de Santa Fe.
- CURSO de Actualización en Explosivos para las Fuerzas Armadas, Fabrica Militar de Pólvoras y explosivos Azul, Fabricaciones Militares.
- CURSO de Explosivos, Fabrica Militar de Pólvoras y explosivos Azul, Fabricaciones Militares.
- CURSO de Técnico Electricista Instalador. Resolución 2265/01 D.G.C.y E. Centro de formación Profesional Nro 403. Lomas de Zamora. Provincia de Buenos Aires.
- CURSO de Electricista Instalador, Centro de formación Profesional Nro 403. Lomaz de Zamora de la provincia de Buenos Aires.
- CURSO de Combate y Defensa con Arma Blanca, Instituto Argentino de Perfeccionamiento Táctico y Combate.
- CURSO de Reducción y Control, Resolución 478/2010, División Grupo Especial de Intervención, Servicio Penitenciario Federal.
- CURSO de Operador de Radioaficionados, Resolución Comisión Nacional de Comunicaciones 50/98, LU7EO, Avellaneda Radio Club.

- CURSO de Conductor de Auto trasporte Público de Pasajeros, Escuela de Capacitación de Conductores, Nicolás Cirigiano, Resolución Secretaria de Trasporte 198/98.
- CURSO de Educación y Formación Profesional para Aspirantes a Conductores del Trasporte Automotor de pasajeros, Secretaria de Trasporte, Comisión nacional de Regulación de Trasporte, Universidad Tecnología Nacional, resolución 198/98.
- CURSO de Conducción Evasiva, Defensiva y Seguridad Urbana, SCFC Consulting Segurity & Risk Control.
- CURSO de Controladores de admisión y Permanencia, Centro de formación Profesional 420.
- CURSO de Dactiloscopia Forense, Escuela Penitenciaria Federal. Centro de formación Profesional Nro 401.
- CURSO de Negociación para la liberación de rehenes, Equipo de Negociación División Halcón, Centro de Cuadros de Reservas de las Fuerzas Armadas.
- CURSO de Negociación de Rehenes Penitenciario, Disposición 1755/11 DGCP, Escuela de Suboficiales Coronel Rómulo Páez, Servicio Penitenciario Federal.
- CURSO Protección VIP-Organización y Planeamiento, Unión de Oficiales de la Reserva de las Fuerzas Armadas.
- CURSO de Custodia Presidencial, Asociación de Infantería de Marina de la Armada Argentina.
- CURSO Básico de Custodia Vip, Entrenamientos Especiales, Sergio Susperregui, Instructor de Fuerzas Especiales División Halcón Nro 402/02, Omar Arce, ITA 1572.
- CURSO de Traslado de Alto Riesgo, Resolución 417/2011, División Grupo Especial de Intervención, Servicio Penitenciario Federal.
- CURSO de Pre Hospital Trauma Life Support, Hospital Militar de Campo de Mayo.
- CURSO de Incidente Medico Mayor, Comité de Emergencias, Hospital Panameño Piñeiro.
- CURSO de Buzo Deportivo 1ra estrella, Habilitación 282 Exp. PNA.
- CURSO de Buzo con Orientación al Empleo Táctico, Asociación de Infantería de Marina de la Armada Argentina.
- CURSO de Asalto en Altura, Asociación de Infantería de Maria de la Armada Argentina.
- CURSO Técnicas y Tácticas de Tareas con Cuerda, Sociedad de Bomberos Voluntarios de Dock Sud.
- 1er Curso de Rappel Táctico y Fast Rope, Delta Military Training Grup, Regimiento de Asalto Aéreo 601.
- CURSO Patrulla de Reconocimiento Nocturno, Asociación de Infantería de Marina de la Armada Argentina.
- CURSO de “Patrulla Táctica Móvil”, Grupo de Imobilizacoes e acoes tatitas, Centro Argentino de Seguridad, Resolución 384/2007.
- CURSO de “Operaciones Tácticas Contra Terror”, Grupo de Imobilizacoes e acoes tatitas, Centro Argentino de Seguridad, Resolución 384/2007

Seminarios

- Jornada de Actualización sobre Problemática Penales y Estrategias de Intervención, Escuela de Graduados y la Especialidad en Ciencias Penales, Universidad Argentina John F. Kennedy, 10 de Octubre de 2003.

- Seminario Arquitectura y Seguridad Publica, El empleo del diseño en la prevención del Delito, Universidad Argentina John F. Kennedy, 20 de octubre de 2003.
- VI* Encuentro Nacional de Estudios Estratégicos ”Los Nuevos Escenarios de la Seguridad Internacional”, Escuela de Defensa Nacional, 5 de noviembre de 2003.
- Segunda Jornada de Armamento y Seguridad de la República Argentina, Facultad Regional de Avellaneda, Universidad Tecnológica Nacional, 20 de noviembre de 2004.
- Simposio de Armas Militares Policiales, Efectos Balísticos en Chalecos Antibalas y Desarrollo de armas No Letales, Fabricaciones Militares, Centro de Cuadros de Reservas de las Fuerzas Armadas, SLUG, 18 de marzo de 2005.
- Simposio de Negociación en Situaciones de Crisis con Rehenes, Equipo de Negociación División Halcón, Centro de Cuadros de Reservas de las Fuerzas Armadas, 22 de abril de 2005.
- Clase de Operaciones Anfibias, Asociación de Infantería de Marina de la Armada Argentina, 30 abril de 2007.
- Jornada De Actualización En Tecnología, Escuela Superior Técnica, Ejercito Argentino, 22 junio de 2007.
- Clase de Combate Cercano, Asociación de Infantería de Marina de la Armada Argentina, 16 de Julio de 2007.
- Seminario “El uso pacífico y seguro de la energía nuclear-Roles en la actividad nuclear argentina”, Escuela Superior Técnica, Ejercito Argentino, 3 de octubre de 2007.
- Seminario “Jornada de Actualización en Tecnología”, Escuela Superior Técnica, Ejercito Argentino, 15 de Noviembre de 2007.
- Seminario de Seguridad Informático, CYBSEC, Escuela Superior Técnica, Ejercito Argentino, 18 DE Septiembre de 2008.
- Jornada de Capacitación Táctica, Desplazamientos, Intercepciones y Tiro, Entrenamientos Especiales, Sergio Susperregui, Instructor de Fuerzas Especiales División Halcón Nro 402/02, 17 de enero de 2010.
- Capacitación en Desplazamiento táctico y Tiro, Entrenamientos Especiales, Sergio Susperregui, Instructor de Fuerzas Especiales División Halcón Nro 402/02, 12 de febrero de 2010.
- Jornada de Técnicas de uso de Linterna, Tiro y Desplazamientos Tácticos Nocturno, Entrenamientos Especiales, Sergio Susperregui, Instructor de Fuerzas Especiales División Halcón Nro 402/02, 14 de marzo de 2010.
- Jornada de Capacitación Táctica en MOUTH (combate urbano) y CQB (combate a cuarto cerrado), Entrenamientos Especiales, Sergio Susperregui, Instructor de Fuerzas Especiales División Halcón Nro 402/02, 11 de abril 2010.
- Boot Camp Jungla, Situación límite, Kapap Argentina, CNcteMA sistema argentina, Hudson, Plátanos, Buenos Aires, 1 de Julio 2012.
- Segundo Simposio de Primeros auxilios Emocionales en Urgencias, Emergencias y Catástrofes, Cátedra de Medicina Legal y Deontología Medica, Facultad de Medicina, universidad de Buenos Aires. 04 y 05 de octubre de 2012.
- Seminario “Gestión De Alarmas: De La Normativa A La Practica” ISA, Escuela Superior Técnica, Ejercito Argentino, 5 de diciembre de 2012.
- 1er Congreso Argentino De Instructores De Tiro RENAR, Mutual de Suboficiales de la Policía Federal Argentina, 1 de mayo de 1013.

- Jornada Taller Sobre Fusiles y Óptica Para Instructores de Tiro, COMtac Internacional, 20 de Junio de 2013.
- Jornada Primer Respuesta a Incidentes con Materiales Peligrosos, NFPA 471 y 472, Defensa Civil de Ezeiza, La Hermandad de Bomberos, Hazmt Argentina, Ezeiza, 25 de agosto de 2013.
- Tercer Simposio de Primeros auxilios Emocionales en Urgencias, Emergencias y Catástrofes, 1 Cátedra de Medicina Legal y Deontología Medica, Facultad de Medicina, universidad de Buenos Aires, octubre de 2013.
- Taller Técnico de Mantenimiento de Armas Cortar y largas, COMtac Internacional, 17 de mayo de 2014.
- Jornada de debate e intercambio de la muerte y las religiones, 1 Cátedra de Medicina Legal y Deontología Médica, Facultad de Medicina, universidad de Buenos Aires, 12 de junio de 2014.
- Primeras Jornadas de Información en: Incidentes con Explosiones – Explosivos Unidades Caninas K9, Fundación CCDEX, Cascaraña, Santa Fe, 14 de abril de 2015.
- Clase Magistral La Aviación Civil y el Medio Ambiente, Instituto nacional de Derecho Aeronáutico y Aeroespacial, 22 de agosto 2016.
- Jornada Modalidades Delictivas en la cadena Logística, Instituto Universitario de la Policía Federal Argentina. 6 de septiembre de 2016.
- Jornada de “Métodos de Pasificación Social”, Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires. 15 de septiembre de 2016.
- Jornada de Uso Racional de la Fuerza, y Legítima Defensa, Instituto Universitario de la Policía Federal Argentina. 15 de septiembre de 2016.
- Jornada sobre Espacio Aéreo Nacional su Vigilancia y Control, Centro aeronáutico de estudios estratégicos, instituto Nacional de Derecho Aeronáutico y Espacial, Fuerza Aérea Argentina, 20 de septiembre de 2016.
- Clase Magistral de Ciber Defensa, el derecho y la operaciones militares en el ciberespacio, Instituto nacional de Derecho Aeronáutico y Aeroespacial, 27 de septiembre 2016.
- Jornada de V.A.N.T. evolución partir de la resolución 527/2015, Colegio de abogados de Lomas de Zamora, Instituto nacional de Derecho Aeronáutico y Aeroespacial y Comisión de Estudios de Derecho Marítimos, 29 de septiembre 2016.
- Taller Histórico Soldados de la Independencia, Regimientos de Granaderos a Caballo Gral. San Martin, Editorial Universitaria del Ejército, 29 de septiembre de 2016..
- Jornada de Historia y Evolución Técnica de los Fusiles de Francotirador, Museo de Armas de la nación, Tte. Gral. Pablo Riccheri, 12 de octubre de 2016.
- Jornada La Defensa en la Agenda Pública, Estado Mayor del Ejército, 27 de Octubre de 2016.
- III Jornada de Enfermería, Colegio Militar de la Nación Ejército Argentino, 18 de Noviembre de 2016.
- I Jornada Capacitación Prevención y Abordaje al Abuso Sexual, Instituto Universitario de la Policía Federal Argentina, 18 de noviembre de 2016.
- Seminario de Seguridad Bancaria, Resolución 1021/17, Facultad de Derecho, Universidad Nacional de Lomas de Zamora, septiembre de 2017.
- Taller Desafíos para la Prevención de Genocidio y otros Crímenes Atroces, Universidad de la Defensa Nacional, 28 de agosto de 2018.

- IV Jornada de Narcotráfico, Impacto en la República Argentina, Resolución 1648/17 Facultad de Derecho, Universidad Nacional de Lomas de Zamora, septiembre de 2018.
- Jornada sobre Normativa de Armas de Fuego, Resolución 1480/18, Facultad de Derecho, Universidad Nacional de Lomas de Zamora, octubre de 2018.
- Jornada I- Modalidad Delictivas en la cadena logística, Visión estratégica, 2da Jornada Modalidades Delictivas en la cadena logística, Instituto universitario de Policía Federal, 18 de octubre de 2018.
- Jornada III- Investigación y Resolución de Casos en el Ámbito Privado Corporativo, 2da Jornada Modalidades Delictivas en la cadena logística, Instituto universitario de Policía Federal, 31 de octubre de 2018.
- Segundo Seminario de Seguridad Bancaria, Resolución 1900/18, Facultad de Derecho, Universidad Nacional de Lomas de Zamora, noviembre de 2018.
- Taller de Medicina Táctica para profesionales de la Seguridad, Asociación de Tiro de precisión de larga distancia de la República Argentina, Museo de Armas de la nación, 8 de abril de 2019.
- Practica de vuelo con VANT, Work Shop introducción al uso profesional de Drones, marzo de 2019.
- IV Jornada en Emergencias y Desastres: La Comunidad de las Actividades en el Sector Gubernamental y Privado, Instituto universitario de Policía Federal, 15 de mayo de 2019.
- Primer Seminario de Ciberdefensa de la República Argentina, Escuela Superior de guerra Conjunta, Comando Conjunto de Ciberdefensa, 6 y 7 de junio de 2019.
- Conferencia Geoestratégia y tendencias Geopolíticas en el Siglo XXI, Escuela Superior de Guerra Aérea, 13 de junio de 2019.
- Jornada de Historias Aeronáutica, Escuela Superior de Guerra Aérea, 16 de julio de 2019.
- Jornada de capacitación en atención pre hospitalaria en alta montaña y deportes de riesgo, ministerios de salud de la nación, 31 de marzo de 2020.
- Simposio de unificación de criterios en situaciones de emergencia III, Colegio militar de la nación, Universidad de la Defensa, 28 de octubre de 2020.
- Disertación: La administración de riesgo como sustento de la seguridad, Instituto Universitario de Policía Federal Argentina. 24 de mayo de 2.022.
- Curso “Claves para una comunicación efectiva en la organización intra hospitalaria de las emergencias”, Comité de Emergencia Panameño Piñeiro, junio de 2.022.
- IV Jornada de Actualización Aeronáutica, Instituto Nacional de Derecho Aeronáutico y Aeroespacial, Fuerza Aérea Argentina, julio de 2.022.
- Seminario de régimen Legal de los intereses Marítimos Argentino, Escuela Superior de Guerra Naval, mayo del 2.022.
- Seminario de Gestión Pesquera, Escuela Superior de Guerra Naval, Noviembre de 2.022.
- Seminario de Geopolítica en el Atlántico Sudoccidental, Escuela Superior de Guerra Naval, agosto de 2.022.
- Seminario La Defensa de los Interés Marítimos y Fluviales, Escuela Superior de Guerra Naval, noviembre de 2.022.
- Taller de Accidentes por animales ponzoñosos, manejo inicial, Dirección de Vigilancia Epidemiológica y Control de Brotes de PBA y el Centro Provincial de Referencia de Toxicología, Dirección Provincial de Defensa Civil, 13 de diciembre de 2022.

- V Jornada de Actualidad Aeronáutica, Instituto Nacional de derechos Aeronáutico y Aeroespacial de la Fuerza Aérea Argentina, 23 de agosto de 2023.
- 5to Taller de Capacitación de medicina Forense, Consejo de la Magistratura de la Ciudad de Buenos Aires. 25 de agosto de 2023.
- Seminario Prevención de Riesgo Laborales, Tema: Practica profesional y equipamiento de monitoreo adecuado, para obtener resultados confiables. Unión de Aseguradoras de Riesgo de Trabajo; 28 de septiembre de 2023.
- V Jornada de Actualidad Espacial, Instituto Nacional de derechos Aeronáutico y Aeroespacial de la Fuerza Aérea Argentina, 12 de octubre de 2023.
- Jornada de Relaciones Publicas, Ceremonial, Protocolo y Comunicación Institucional, Secretaria General, prefectura Naval Argentina. 15 de noviembre de 2023.

Antecedentes docentes

- Instructor Ac-Honoren del “Curso De Medicina Táctica.” Hospital Militar de Campo de mayo-Año 2011.
- Instructor Ac-Honoren del “Curso Pre Hospital Trauma Life Support.” Hospital Militar de Campo de Mayo Año 2011.
- Instructor Ac-Honoren De Especialización en “El Uso De Escopeta. Programa Anual de Capacitación, Técnicas de Combate Cercano (combate urbano), técnicas especiales policiales adaptadas al ámbito penitenciario”, Escuela de Suboficiales Coronel Rómulo Páez, Servicio Penitenciario Federal, Año 2012.
- Docente de Operaciones Policiales, Mantenimiento Y Conducción De Móviles Policiales. Escuela de Policía “Juan Vucetich”- Sede Lomas de Zamora, 2do Curso, Resolución 3506/10 Año 2014.
- Docente del “Curso Conducción Segura De Vehículos De Emergencia Policiales.” 2.014. Dirigido al Personal de Conductores del Centro de Protección Ciudadana. Departamento de Capacitación de la Secretaria de Justicia y Seguridad del Municipio de Lomas de Zamora. Asesoramiento didáctico, coordinación, gestión y diseño, del Programa Integral de Protección Ciudadana.
- Docente de la “Jornada de inmovilizaciones Policiales”, Secretaria de Extensión Universitaria, Universidad Nacional de Lomas de Zamora, 11 de junio de 2014.
- Docente de la “Jornada de Operaciones policiales, Traslado de Alta Complejidad”, Secretaria de Extensión Universitaria, Universidad Nacional de Lomas de Zamora, 19 de junio de 2014.
- Disertante del “Curso de Incidente Medico Mayor”, Comité de Emergencias, Hospital General de Agudos Panameño Piñeiro. 2023.

Antecedentes profesionales

- Suboficial, del escalafón Seguridad, retirado, Policía de la Provincia de Buenos Aires.
- Oficial, ostentando la jerarquía de Subteniente, en situación de revista de reserva, del Ejército Argentino.

Premios y distinciones recibidos

- Herido en Acto de servicio, en 2 oportunidades diferentes, reconocido por Resolución del Ministro de Seguridad de la Provincia de Buenos Aires.
- Premio en el acto del día de la policía de la provincia de buenos Aires, el 13 de Diciembre de 2006, mediante la adquisición de una medalla cuya leyenda se encuentra tipificada “por su destacada labor” Baldomero Alvares de Olivera, Intendente Municipal, Gestión 2003-2007”..”22-11-2006”.