CEIICOM CHILE
Centro de Estudios Investigación de Inteligencia Competitiva

Occidental Studies Institute

PROGRAMA:

# Máster Ciberseguridad en Infraestructuras Críticas (MACIC)

**Año: 2020**

# FORMULARIO PROGRAMA DE ESTUDIOS

## A. IDENTIFICACIÓN

**NOMBRE DEL PROGRAMA:**

**Máster en Ciberseguridad en Infraestructuras**

**Críticas Menciones:**

- Diplomado en Ciberseguridad (Mención en Gestión CSIRT)
- Diplomado Ciberseguridad (Mención Ciberseguridad em Infraestructura critica)
- Diplomado Hacking Ético (Mención Hacking informático)

**MODALIDAD**
Clases online.

**CARÁCTER:**
Programa de carácter profesionalizante.

### A.2 PÚBLICO OBJETIVO:

El programa "Master de Ciberseguridad en Infraestructuras críticas (MACIC)", es dirigido a profesionales y técnicos de Instituciones, Fuerzas y Cuerpos de Seguridad del país que gestionan sistemas de información, plataformas tecnológicas e implementación de políticas de trabajo de seguridad de los sistemas informáticos de infraestructuras críticas, que deban velar por la confidencialidad, integridad y disponibilidad de las plataformas tecnológicas de información y Operaciones en Redes.

### A.3 PERFIL DE EGRESO:

Al término del "Master de Ciber Seguridad en Infraestructuras Críticas de información (MACIC)", los participantes habrán incorporado competencias en gestión de equipos de respuesta a incidentes de seguridad informática denominados CERT, CIRT, CSIRT y/o SOC, planificar, implementar y asegurar la continuidad de los sistemas de Ciber Seguridad de infraestructuras críticas y evidenciar amenazas de terceros detectando vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas y asumir las medidas pasivas y activas para asegurar la continuidad del negocio y evitar el robo de la información.

**A.4 OBJETIVOS DEL PROGRAMA:**

**Objetivo General**

Formar profesionales y técnicos especializados en la gestión de CERT, CIRT, CSIRT y/o SOC y de hacking ético en las aplicaciones de técnicas, tecnologías y procedimientos de Ciberseguridad, con la finalidad de resguardar las operaciones en redes y sistemas de información de las infraestructuras críticas de las instituciones, ministerios y empresas privadas.

**Objetivos Específicos**

- Identificar contexto histórico, tendencias conceptuales, políticas jurídicas, experiencias cibernéticas en infraestructuras críticas y gestión de respuesta ante incidentes informáticos (CERT, CIRT, CSIRT y/o SOC).

- Aplicar técnicas, tecnologías y procedimientos activos y pasivos de Ciberseguridad en infraestructuras críticas.

- Materializar técnicas y tecnologías de Hacking ético, para evidenciar y neutralizar amenazas tecnológicas de terceros y mitigar los riesgos cibernéticos provenientes del ciberespacio.

- Aplicar Juego Cibernético teórico práctico de gestión CERT, CIRT, CSIRT Y/O SOC, ciberseguridad y gestión de respuesta para proteger las infraestructuras críticas de los sistemas de información en redes informáticas.

**B.1. CUPOS:** 20 estudiantes

**B.2. COSTE MASTER**: El cote de master por alumno es de 10.000 dólares.

**B.2a.- Inscripciones:** El alumno para inscribirse debe mandar un mail a:
info@osifoundation.com

**B.3. GRADUACIÓN**

**B.3.a REQUISITOS DE GRADUACIÓN:**

El estudiante deberá aprobar la totalidad de los módulos de la malla curricular del Máster con nota mínima 4.0 y al menos con un 75% de asistencia.

Para obtener el grado de Máster el estudiante deberá desarrollar un" Proyecto de Ciberseguridad en Infraestructuras críticas", la que debe exponer frente a una comisión evaluadora.

El objetivo del proyecto de Ciberseguridad: Es elaborar un proyecto de desarrollo de mejoramiento de Ciberseguridad de Infraestructura crítica de una institución, ministerio y/o empresa atendiendo a la solución de un problema tecnológico focalizado.

El Proyecto de Ciberseguridad: Representa un producto de insumo tecnológico final de cierre de programa elaborado de manera grupal (máximo 3 estudiantes), cuyo formato de presentación será establecido por la Dirección del Programa.

Tiempo máximo de elaboración: 06 meses (2do. año del Programa).

Profesor Guía / Metodólogo: Será determinado por la Dirección del Programa y tendrá la labor de apoyar la elaboración del Proyecto de Ciberseguridad de Infraestructuras Criticas en áreas institucionales, ministeriales y/o empresa.

En caso de reprobación del Proyecto, los estudiantes tendrán sólo una segunda oportunidad en un plazo no superior a 04 meses ante una comisión designada por las autoridades de la Escuela de Post Grado.

**B.3.b CÁLCULO DE NOTA DE EGRESO:**

La nota final se calculará en base a la sumatoria de ponderación de las siguientes notas:

| **Ítem** | **Porcentaje** |
|---|---|
| Promedio notas asignaturas | 60 % |
| Nota Trabajo de Titulación | 40% (20 % Proyecto + 20 % Exposición) |

## C. METODOLOGÍA Y ESTRUCTURA CURRICULAR

### C.1 METODOLOGÍA GENERAL

La metodología del Máster está basada en la enseñanza online y a distancia. Esto permite al estudiante seguir el curso cualquiera que sea su lugar de residencia. Compatibilizar el aprendizaje con sus responsabilidades familiares y laborales y aprender sin necesidad de desplazamientos.

Esta metodología de aprendizaje conduce a una adecuada formación mediante el empleo de material didáctico digitalizado, diseñado especialmente para este programa,

compuesto por textos, ilustraciones, vídeos, glosarios, enlaces y ejercicios. Además, considera una permanente tutoría y atención al estudiante.

La forma de evaluación por cada Módulo será la siguiente:

| | |
|---|---|
| 15% | Participación (en foros, debates, chats, etc.) |
| 35% | Pruebas sumativas |
| 50% | Examen final |

**Prueba Formativa:** Cada actividad del módulo será evaluada con una batería de preguntas tipo quiz, para poder constatar el nivel de aprendizaje esperado versus el logrado.

**Pruebas Sumativas:** A finalizar cada módulo se realizará una prueba tipo test con una batería de preguntas y ejercicios de desarrollo.

**Características generales de la modalidad online:**

- Acceso a plataforma durante 24 horas al día, 7 días a la semana.
- Tutoría online disponible durante la realización del programa.
- Disponibilidad del programa completa 24 horas y 7 días a la semana.
- El programa incluye material didáctico, ejemplos y ejercicios prácticos.

La metodología tiene una orientación teórico - práctica en relación con las áreas propias del programa, poniendo énfasis en el trabajo en equipo generando apoyos individualizados y grupales para favorecer los aprendizajes de la diversidad de estudiantes. Se enfatiza en la solución de problemas presentes en el campo de estudio y se caracteriza por la aplicación de estudios de casos, resolución de problemas en contextos multidisciplinarios.

**C.2 MALLA CURRICULAR**

- El Máster en Ciberseguridad en Infraestructuras Criticas, tiene una duración de 3 semestres lectivos (18 meses).
- Está estructurado por 20 asignaturas o módulos
- Cada módulo tiene una duración de 24 horas pedagógicas
- En total en Máster tiene una carga académica de 480 horas pedagógicas,

| Semestre I<br>Inteligencia Básica | Semestre II<br>Inteligencia Especializada | Semestre III<br>Inteligencia Avanzada |
|---|---|---|
| **Modulo 1.** | **Modulo 7.** | **Modulo 13.** |
| - Ámbito y Dimensión del Ciberespacio | - Gestión de Ciberseguridad. Normas y Leyes | - Recuperación ante Desastres y Continuidad de Negocios |
| **Modulo 2.** | **Modulo 8.** | **Modulo 14.** |
| - Marco Jurídico y Políticas de Ciberseguridad | - Ciberseguridad en Redes, Internet y Telefonía | - Testing de Seguridad |
| **Modulo 3.** | **Modulo 9.** | **Modulo 15.** |
| - Gestión y Conectividad en Redes Escalables | - Comunicaciones Móviles y Voz sobre IP | - Ingeniería Social |
| **Modulo 4.** | **Modulo 10.** | **Modulo 16.** |
| - Infraestructura Crítica de Información | - Arquitectura de Ciberseguridad en Entornos TI | - Ingeniería Forense y Hacking Ético |
| **Modulo 5.** | **Modulo 11.** | **Modulo 17.** |
| - Proceso y Análisis de Incidentes Informáticos | - Ciberseguridad en Sistemas Operativos Aplicaciones y BD | - Juego Aplicado de Ciberseguridad Infraestructura Crítica |
| **Modulo 6.** | **Modulo 12.** | **Modulo 18.** |
| - Criptografía Aplicada | - Aplicaciones Web (OWASP) | - Metodología de la Investigación y Tesis de Grado |
| **Diplomado en CSIRT** | **Diplomado en Ciberseguridad** | **Diplomado Hacking Ético** |
| | **Seminario I** | **Seminario II** |
| | **Proyecto de Titulación** | |

## 7.1. DIPLOMADO EN CSIRT (Mención Gestión de incidentes informáticos).

### Módulo 1. Ámbito y Dimensión del Ciberespacio.

- El ámbito y dimensión del actual contexto, entorno y escenarios cibernéticos.
- Evolución histórica del ciberespacio desde la II Guerra mundial hasta nuestros días.
- Consignara características, fundamentos tecnológicos, principios, términos conceptuales, experiencias y lecciones aprendidas informáticas.
- Identificación de las amenazas que se originan desde el ciberespacio a los sectores estratégicos para la seguridad de las instituciones, ministerios y empresas del estado.

### Módulo 2. Marco Jurídico y Política Internacional de Ciberseguridad.

- Regulación legal del ciberespacio y su protección a base de los actuales derechos de protección tecnológica.
- Marco de leyes normativo-nacionales e internacionales: Tratado de Budapest y Manual de Tallin.
- Políticas de ciberseguridad internacionales y su proyección 2021. Normas ISO internacionales.

### Módulo 3. Gestión y Conectividad en Redes Escalables.

- Los conceptos básicos del funcionamiento de una red de comunicaciones, sus protocolos y estándares asociados a las distintas capas de los modelos OSI y TCP/IP.
- Las principales técnicas de conmutación tanto a nivel de capa 2, como de capa 3, también conocer los paquetes Ipv4 e Ipv6.
- Como segmentar una Red de datos tanto división con clase, como sin clase (VLSM). La implementación de protocolos de enrutamiento, tanto estáticos como dinámicos.
- La implementación de listas de control de acceso y traducción de direcciones de Red para Ipv4.

### Módulo 4. Infraestructura Crítica de Información.

- Conceptos, contenidos y aplicaciones para el estudio, identificación y ponderación de las infraestructuras de información de una organización.
- El proceso de planificación que permita establecer “criticidad” en función de las datas que fluyen en el Ciberespacio y que son constituyentes de condiciones de riesgo y amenaza cibernética contra tales infraestructuras
- Aplicar procesos de análisis organizacional y de arquitectura de sistemas de redes.
- Una matriz para ponderar la criticidad de procesos y procedimientos organizacionales y de la arquitectura del sistema de redes, previamente analizados y categorizados.

**Módulo 5. Proceso y Análisis de Incidentes Informáticos.**

- El marco conceptual del proceso y análisis de incidentes informáticos ocurridos en el Ciberespacio y su accionar en los sistemas de plataformas de comunicaciones críticas de información.
- Las fases del Proceso de análisis de los riesgos y amenazas cibernéticas a los que se ven expuestas las arquitecturas críticas del sistema de redes y ordenadores de las instituciones, organizaciones públicas y privadas del estado.
- El ciclo del proceso de análisis, integración e Interpretación aplicados a las actividades que fluyen en el Ciberespacio y las amenazas para la infraestructura critica de informaciones.

**Módulo 6. Criptografía Aplicada**

- Los principales métodos y algoritmos criptográficos, cómo utilizarlos de la manera correcta. Beneficios y vulnerabilidades de los sistemas criptográficos.
- Conceptos de sistemas criptográficos Métodos criptográficos.
- Algoritmos simétricos y asimétricos. Hashes. Firmas digitales. Infraestructura de claves públicas.
- Implementación de sistemas criptográficos y vulnerabilidades.

**7.2. <u>DIPLOMADO EN CIBERSEGURIDAD</u> (Mención Ciberseguridad).**

**Módulo 1. Gestión de ciberseguridad. Normas y leyes.**

- Los principales conceptos y aspectos a tener en cuenta para la creación de un plan de seguridad informática y su implantación en una organización, basado en normas y teniendo en cuenta la gestión de riesgos, incidentes y la posterior auditoria.

**Módulo 2. Ciberseguridad en Redes, Internet y Telefonía**

- Diseñar infraestructuras de red enfocadas en la seguridad.
- Identificar vulnerabilidades en los distintos niveles de la red de una organización e implementar controles para evitarlos.
- El funcionamiento de los firewalls, VPNs, IDS/IPS.
- Conocer los principales problemas en redes VoIP y cómo protegerlas.

**Módulo 3. Comunicaciones Móviles y Voz sobre IP**

- Los conceptos básicos del funcionamiento de las redes celulares e inalámbricas, su infraestructura, historia y evolución tecnológica de sus principales estándares.
- Comprender las principales soluciones que se implementan hoy en día para proyectos con VoIP para comprender cuál es la que se adapta mejor a su organización.

**Módulo 4 Arquitectura de Ciberseguridad en Entornos TI**

- Las diferentes arquitecturas empresariales y cómo guiar desde el punto de vista tecnológico al ambiente empresarial.
- Cómo mantener una mejora continua en la forma en que la organización conduce su negocio, optimizando el uso de los recursos tecnológicos a partir del uso de buenas prácticas.
- Los principales conceptos asociados a la seguridad, estándares existentes.
- Modelos existentes de seguridad, así como para el control de acceso, y los principios y factores fundamentales de evaluación y selección.
- Diseñar y supervisar los procedimientos de instalación, configuración y mantenimiento de los recursos de una red de comunicaciones para proveer servicios de voz, datos y multimedia a los usuarios y realizar la integración de los recursos ofrecidos por los sistemas de transmisión y conmutación.
- Reglamentaciones y organismos de estandarización y Proyecto telemático Herramientas para el desarrollo de un proyecto telemático
- Integración de servicios de comunicaciones, voz, datos, multimedia, pasarelas. Administración de recursos y servicios.

**Módulo 5. Ciberseguridad en Sistemas Operativos, Aplicaciones y BD**.

- Identificar problemas de seguridad en sistemas operativos.
- Cómo garantizar la seguridad durante el proceso de desarrollo de software y de los datos almacenados en bases de datos.
- Cuáles herramientas pueden utilizarse para garantizar la seguridad en estos aspectos.

**Módulo 6. Aplicaciones Web (OWASP).**

- Los conocimientos y recursos necesarios para evaluar la seguridad de aplicaciones Web, mediante la comprensión de la teoría y buenas prácticas descritas y provista por la organización OWASP.
- Los riesgos y debilidades que se inyectan al código, en el ciclo de vida del software SDLC.
- El enfoque y proyectos globales de OWASP para desarrollo seguro. La teoría y buenas prácticas descritas en metodologías OWASP.
- Los estándares OWASP para identificar y clasificar vulnerabilidades críticas en aplicaciones Web.
- Estrategias para implementar las medidas correctivas que sean necesaria.

**7.3. <u>DIPLOMADO HACKING ÉTICO</u> (Mención Hacking)**

**Módulo 1. Recuperación ante Desastres y Continuidad de Negocios**

- Los conocimientos y herramientas necesarias que son parte fundamental del proceso de implementación de Planes de Continuidad de Negocios y Recuperación ante Desastres de

la disciplina de Business Recovery: BIA, RA, RTO, RPO, Estrategias de Continuidad y podrán ser capaces de realizar un BCP (Business Continuity Plan).

- Conceptos Básicos y especializados de recuperación ante desastres y continuidad de negocios.
- El Plan de continuidad de negocios (BCP) El Plan de recuperación ante desastres

**Módulo 2. Testing de Seguridad.**

- El proceso de testing profesional de seguridad TI basado en la OSSTMM, ISO 27008.
- El Manual de Metodología para Pruebas de Seguridad de Código Abierto (OSSTMM).
- La metodología de las reglas éticas relacionadas.
- La planificación de una auditoria técnica básica.
- La configuración de las herramientas necesarias para ejecutar una auditoria.

**Módulo 3. Ingeniería social.**

- Conceptos fundamentales relacionados con la Ingeniería social basada procesos de ingeniería utilizando principios de diseño seguros
- Modelos de ingeniería social y técnicas de evaluación de seguridad. Capacidades de seguridad de los sistemas de información.
- Arquitecturas de seguridad, diseños y elementos de solución vulnerabilidades, vulnerabilidades de los sistemas basados en la Web y sistemas móviles.
- Análisis de dispositivos embebidos y vulnerabilidades de los sistemas ciber-físicos, criptografía, principios de diseño de seguridad de las instalaciones.

**Módulo 4. Ingeniería forense y Hacking ético.**

- Principales aspectos asociados al análisis forense.
- Aplicar metodologías y técnicas existentes usando herramientas de soporte. Uso de técnicas anti forenses para proteger la información.
- Conceptos, principios y usos del análisis forense. Ética y aspectos legales. Evidencia digital.
- Tipos de análisis forense. Metodologías y técnicas existentes. Herramientas de soporte.
- Técnicas anti forenses.

**Módulo 5. Juego Aplicado Ciberseguridad Infraestructura Crítica.**

- La situación del juego aplicado de ciberseguridad en infraestructuras críticas de informaciones.
- La problematización de la temática del juego, para organizar y aplicar los roles de gestión de Csirt, Ciberseguridad y hacking conforme al caso aplicado de Ciberseguridad.
- Aplicaciones técnicas, tecnológicas y procedimientos teórico práctica de ciberseguridad para mitigar vulnerabilidades en infraestructura críticas.

**Módulo 6. Seminario y Tesis de Grado.**

- Las diferentes etapas cualitativa y cuantitativa de las metodologías de la investigación.
- Los principales aspectos metodológicos de un anteproyecto de tesis y normas APA para desarrollar el tema de tesis para su aprobación.
- Trabajo individual y/o grupal de desarrollo de los contenidos del proyecto de tesis bajo la supervisión de un profesor guía.

## 8. BIBLIOGRAFÍA OBLIGATORIA Y COMPLEMENTARIA

**Obligatoria:**


- Botnets: The Killer Web Application, Craig Schiller ISBN 1-59749-135-7
- Managing an Information Security and Privacy Awareness and Training Program, Rebecca Herold ISBN 0-8493-2963-9
- The CISO Handbook: A Practical Guide to Securing Your Company, Michael Gentile ISBN 0-8493-1952-8
- Google Hacking for Penetration Testers, Volume 1, Johnny Long ISBN 1-93183-636 -1
- Know Your Enemy: Fast Flux Service Networks: http://www.honeynet.org/papers/ff
- DDoS Cheat Sheet http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf
- Ibáñez de la Corte Luis & Navarro Blanco José Maria. "Seguridad Nacional, Amenazas y Respuestas". Editorial LID. 1° Edición. Madrid. España. Año 2014. Pp. 115 – 130, 267 – 281.
- Fernández Díaz M. Antonio "Diccionario Inteligencia y Seguridad". Editorial LID. 1° Edición. Madrid. España. Año 2014. Pp 25 – 277.
- Aguilar Joyanes Luis, Bejarano Caro José María, Clotet Salom Juan, Durán del Río Díaz, Juan, Romero Candau Javier. "Centro Superior de Estudios de la Defensa Nacional de España". Monografía 126. Ciberseguridad: Retos y Amenazas a la Seguridad Nacional en el Ciberespacio". Editorial NIPO. 1° Edición. Madrid. España. Año 2013. Pp 09 – 309.
- Corredera Casar Ramón José, Ortega Feliu Luis, González Enríquez Carlos, Sánchez y de Turiso López Javier, de Agreda Gómez Ángel. Acosta Pastor Óscar, Cortés Pérez Manuel. "Centro Superior de Estudios de la Defensa Nacional de España ". Monografía 126. Ciberespacio Nuevo Escenario de Confrontación". Editorial NIPO. 1° Edición. Madrid España. Año 2013. Pp. 05 – 353.


**Complementaria:**


- COBRA. http://www.security-risk-analysis.com
- OCTAVE. http://www.cert.org/octave
- K. van Wyk, R. Forno, Incident Response. O'Reilly. 2001.
- M. West-Brown, D. Stikvoort, Kosakowski, J. Killcrece, R. Ruefle, M. Zajicek, Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon: Software Engineering Institute CMU/SEI-98-HB-001. Segunda edición. 2003. http://www.cert.org/archive/pdf/csirt-handbook.pdf
- ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005)

- Pacheco G. Federico & Jara Héctor. “Ethical Hacking 2.0”. Editorial RedUsers.1° Edición. Buenos Aires. Argentina. Año 2014. Pp. 230 – 292.
- Paising de la Cruz Broy Hegel. “Hacking & Cracking”. Editorial MACRO. 1° Edición. Miraflores. Perú. Año 2013. Pp.19 -20, 141- 142.
- Greenwald Glenn. “Snowden: Sin un Lugar donde esconderse”. Editorial Grupo Zeta. 1° Edición. Barcelona. España., Año 2014. PP. 11 -259.
- Caballero Sierra Francisco. “Ciudadanía, tecnología y Cultura: Nodos Conceptuales para pensar la nueva mediación digital”. Editorial Gedisa. 1° Edición. Barcelona. España.

**D. RECURSOS DE PERSONAL**

**D.1 PERFIL DE LOS DOCENTES DEL PROGRAMA:**

**1.- Dr. ROBERTO DONOSO PINCHEIRA:** Doctor en Educación, Master en Educación, Master en Comunicación, Master en Análisis de Inteligencia Comunicacional, Diplomado en Ciberseguridad y Ciberdefensa en Infraestructuras Criticas de Información, Diplomado en Estrategias de Ciberseguridad, Diplomado en Operaciones de Paz, Diplomado en Seguridad integral Oública, ciudadna y Privada, Académico con experiencia académica en varias universidades nacionales e investigador internacional en la Escuela superior de Economía y Relaciones Públicas (ESERP), de la Universidad de Barcelona España, Centro de Estudios Investigaciones militares (CESIM) y asesor de investigación y analista en el Ejército de Chile, se desempeña como director de los programas académicos de post grados “Master y Diplomado en Análisis de Inteligencia Comunicacional” de la Universidad Mayor le ha correspondido desempeñarse en relatorías internacionales en los siguientes países**:** Panamá, Perú, Argentina, Colombia, EE.UU, China y España. Actualmente se desempeña como asesor e investigador del Comando de Educación y Doctrina del Ejército de Chile.

**2.- Dr GONZALO ZAMBRANO MILLAR:** Psicólogo, Licenciado en Psicología, formación de post grado: Doctor en Procesos Políticos y Sociales en América Latina, Doctor © en Ciencia Política, Magíster en Gestión de Recursos Humanos. Formación de post título: Diplomado en Gestión de Instituciones de Salud, Diplomado en Sistemas de Resolución de Conflictos y Mediación, Diplomado en Gestión Comunitaria, Diplomado en Evaluación de Intervenciones Sociales, Diplomado en Innovación Didáctica para la Educación Superior. Profesional con amplio conocimiento en la Evaluación de Programas Gubernamentales, bajo la Metodología de Marco Lógico, a nivel nacional e internacional. En Chile en la División de Control de Gestión de la Dirección de Presupuestos del Ministerio de Hacienda (DIPRES); y en Latinoamérica en la Comisión Económica para América Latina y el Caribe (CEPAL). Docente Universitario de pregrado, postítulos y posgrado, en modalidad presencial y online (Universidad de Santiago de Chile, Universidad La República, Universidad Católica Silva Henríquez, Universidad Bernardo O’Higgins, Universidad Internacional SEK).

**3.- Mg. RODRIGO VARGAS VARAS:** Magister en Tecnologías de la Información (Universidad Federico Santa María), Ingeniero Civil en Computación e Informática, Diplomado en Peritaje Informático Forense (Universidad de Santiago), Diplomado en Seguridad de la Información (Academia Politécnica Militar), Diplomado en Conducción Político Estratégica (ANEPE), CISSP desde el año 2005, CSIRT, ITIL v3.1, especialista en seguridad e implementación de soluciones tecnologías en el ámbito Civil y en el área de

la Defensa Nacional, experto en planificación e implementación de políticas y procedimientos de TICs. Se ha desempeñado como académico de la Universidad de Tarapacá, Universidad Central y Actualmente en Duoc UC en las cátedras relacionadas con la Seguridad de la información, USACH y Universidad Mayor.

**4.- Mg. RICARDO GARATE VERA**, Licenciado en Ciencias Jurídicas, Magister en Ciencias Militares en la Academia de Guerra del Ejército de Chile con mención en Planificación y Gestión Estratégica. Diplomado de Postítulo en Ciberseguridad en la Universidad de Chile. Diplomado en Geopolítica en la Universidad Militar Nueva Granada de Colombia. Profesor Militar de Academia de la Academia de Guerra del Ejército de Chile. Diplomado en Gestión y Administración de Recursos y Proyectos de Defensa en la Academia Politécnica Militar del Ejército de Chile. Diplomado en Administración de Empresas en la Universidad Arturo Prat. Académico e Investigador de la Escuela Superior de Guerra de Colombia

**5.- Mg. CARLOS MONDACA SAAVEDRA:** Máster en Dirección en Dirección General de Empresas (MBA). Escuela Internacional de Negocios, Madrid, España. Diplomado en Preparación y Evaluación de Proyectos (DPEP). Facultad de Ciencias Físicas Matemáticas Universidad de Chile, Santiago. Diplomado en Control de Gestión (DCG), Facultad de Ciencias Económicas y Administrativas Universidad Valparaíso, Santiago. Contador Auditor, Universidad Andrés Bello, Santiago. Certificate of Accreditation in Operational Risk Management, Global Risk Management Solution, obtained in Price Waterhouse & Coopers, Buenos Aires Argentina. Certificate of Accreditation in Project Support Office, Global Risk Management Solutions, obtained in Price Waterhouse & Coopers, Buenos Aires, Argentina. International Course of Computer Audit given by the Comptroller General of the Republic (OLACEF). Brazil. Certification of Accreditation in Operational Resilience, obtained in Price Waterhouse & Coopers, São Paulo, Brazil.

**6.- Mg. ESTEBAN ENRIQUE MAURIN SALDAÑA**. Ingeniero Electrónico, Máster en Ciberseguridad de la Universidad Central de Chile, Diploma en Aplicaciones Criptográficas, con más de 15 años de experiencia en el ámbito de la Ciberseguridad y Ciberdefensa.Satellite Software Engineer EADS Astrium para Proyecto satelital de Chile Fasat-Charlie (Años 2008-2009). Big Data and Information Security Specialist (UESTC). Profesor del programa de Magíster en Seguridad, Peritaje y Auditoría de la Universidad de Santiago de Chile. Profesor del Diplomado en Ciberseguridad de la Universidad de Chile (Módulos BCP-DRP). Miembro de la Red Iberoamericana de Criptografía. Consejero del Instituto Chileno de Derecho y Tecnologías. Académico del programa de Diplomado en Ciberseguridad Ofensiva de la Universidad Certificate of Accreditation in BCP Fast Track, obtained in Price Waterhouse & Coopers, São Paulo,
de los Andes.

**7.- Académico PABLO UMANZOR ARANCIBIA**: Ingeniero Electrónico mención Telecomunicaciones Licenciado en Cs de la Ingeniería Universidad Austral, Datacenter & Security Manager SNPC Biblioredes, Académico en la Catedra de Ciberseguridad en el Ejército de Chile, Cisco CCNA. Mikrotik MTCNA – MTCRE, MTCWE, RedHat Linux RHCE, Miembro Level A IEEE, Miembro Lacnic, Asesor en tecnologías de Auditorias en ámbitos de la Salud.

8. **Mg. ALEXIS HERRERO MENA,** Ingeniero Electrónico y Master en TI & Gestión, Jefe de Telecomunicaciones del Ejército de Chile, con experiencia en evaluación de proyectos de TI, evaluación y administración de sistemas criptográficos, evaluación de software de misión crítica. Asesoramiento en la incorporación de nuevas tecnologías de la seguridad de la información, ejecución de auditorías de seguridad informática y en el desarrollo de proyectos de sensores electrónicos. Elaboración de reglamento para el desarrollo de operaciones en redes de sistemas de información (Ciberdefensa). Administrador de proyecto de implementación de una plataforma para la interoperación de sistema de informáticos basada en la solución Oracle "SOA Suite 11g" y en la implementación de una plataforma para la administración de proyectos basada en la solución Oracle "Primavera P6 Professional Project Management". Se desempeña como profesor en cátedras de post-grado, pregrado y cursos, en entidades educacionales del Ejército de Chile y en la Universidad Central.

**9.-Mg. ERIC DONDERS ORELLANA**, Magíster de Seguridad Informática y Protección de la Información de la Universidad Central de Chile (2010) con proyecto de tesis "Formulación de un modelo electrónico y una metodología que permitan diseñar, implantar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) para PYMES". Ingeniero Civil en Computación de la Universidad Central de Chile (1989) con proyecto de título "Diseño e Implementación de Herramientas de Software de Apoyo a la Seguridad del Sistema Operativo Unix", trabajo en tres ámbitos que actualmente sería equivalente a diseño/implementación de un protocolo de autenticación servidor central, diseño/implementación de un servidor de registro de actividades de administradores/usuarios y herramientas de detección de troyanos.

**10.- Mg. ALVARO MELO CHAVEZ**, Ingeniero Militar en Sistemas TICs, mención Informática y Computación, con MBA y certificación CISM - ISACA. Experiencia como consultor, Jefe de CSIRT, Asesor de Gobernanza y Gestión de Ciberseguridad y Jefe de Sistemas Industriales. Lideré diversos equipos de trabajo en áreas de seguridad informática en el Ejército de Chile. Conocimientos y habilidades en dirección y gestión de Ciberseguridad y asesor de Ciberdefensa y Ciberinteligencia del Ministerio del Interior de Chile, competencias en gestión de riesgos en plataformas Tecnológicas de Infraestructuras críticas.

**11.- Académico. SEGUNDO MANCILLA,** Ingeniero de Ejecución en Informática y Licenciado en Ciencias de la Ingeniería, Universidad de las Ciencias Informática, se desempeña como analista forense informático e investigador de delitos del mismo tipo y otros cometidos de consultorías y asesoramiento en el uso de las nuevas tecnologías y la seguridad de la información. Desempeñándose actualmente como Jefe de Agrupación de Investigaciones especiales en Internet de la Policía de Investigaciones de Chile, Por su experiencia académica y policial es expositor permanente sobre delitos tecnológicos e Informática Forense en diferentes lugares y universidades dentro y fuera de Chile. Asiste al IV Curso Internacional Sobre Delitos Tecnológicos, dictado por el Cuerpo Nacional de Policía de España, en Madrid. Como becario JICA (Japan Internacional Cooperation Agency), asiste a los cursos de Infocomunicaciones Policiales y de Informática. Forense. Dictado por JICA e INTERPOL en Tokio, Japón.

**12.- Investigador JOSHUA PROVOSTE ALVAREZ**: Investigador y experto en Ethical Hacker, Developer y Security Researcher con 10 años de experiencia en seguridad ofensiva y hands-on penetration testing. Ha liderado equipos de ingenieros de ciberseguridad en empresas TELCO de Chile y Perú, para la

implementación y mejora de estrategias de desarrollo seguro en diferentes SDLC. Así mismo, tiene a su haber vulnerabilidades informáticas registradas por norma internacional (CVE-2020-10682, CVE-2020-10681, CVE-2020-8788, CVE-2019-12273, CVE-2019-15862 y CVE-2019-15891). Desarrollador de exploits y malware.

**D.2 PERSONAL NO ACADÉMICO Y DE APOYO AL PROGRAMA:**

| **Personal no Académico** | |
|---|---|
| **Cargo** | **Nombre** |
| Director del Programa | Dr. Roberto Donoso Pincheira |
| Coordinador Académico | Mg. Gonzalo Zambrano Millar |
| Coordinador Administrativo | César Alcalá Giménez |