CONSEJO NACIONAL DE RECTORES
Oficina de Planificación de la Educación Superior
División Académica

Dictamen sobre la creación de la Maestría Profesional en Ciberseguridad Industrial (MACIBI) de la Sede Regional Chorotega de la Universidad Nacional

Katalina Perera Hernández

OPES; no. 01-2025

378.2
P437d

Perera Hernández, Katalina.
Dictamen sobre la creación de la maestría profesional en ciberseguridad industrial (MACIBI) de la Sede Regional Chorotega de la Universidad Nacional. [Recurso electrónico] / Katalina Perera Hernández -- San José, C.R. : CONARE - OPES, 2025.
(OPES; no. 01-2025) 1 recurso en línea (40 páginas): archivos de texto PDF, 500 KB

ISBN 978-9977-77-646-0

1. CIBERSEGURIDAD INDUSTRIAL. 2. MAESTRÍA UNIVERSITARIA. 3. PERFIL PROFESIONAL. 4. PLAN DE ESTUDIOS. 5. PERSONAL DOCENTE. 6. UNIVERSIDAD NACIONAL (COSTA RICA). SEDE REGIONAL CHOROTEGA. I. Título. II. Serie.

LRD

PRESENTACIÓN

El estudio que se presenta en este documento (OPES; no. 01-2025) se refiere al Dictamen sobre la creación de la Maestría Profesional en Ciberseguridad Industrial (MACIBI) de la Sede Regional Chorotega de la Universidad Nacional, propuesta por la Sede Regional Chorotega de la Universidad Nacional (UNA).

El dictamen fue elaborado por la Dra. Katalina Perera H. investigadora y jefa de la División Académica de la Oficina de Planificación de la Educación Superior (OPES), con base en el resumen ejecutivo del posgrado de Maestría Profesional en Ciberseguridad Industrial para la Sede Chorotega remitido por la UNA.

La revisión integral del documento estuvo a cargo de la Mag. Ana Yancy Alfaro, investigadora de la División Académica y la edición del documento fue realizada por Licda. Sandra Guillén Guardado, asistente de la División citada.

El presente dictamen fue aprobado por el Consejo Nacional de Rectores en la sesión No. 3-2025, artículo 8, celebrada el 28 de enero de 2025, comunicado a la universidad mediante acuerdo CNR-17-2025.

Gastón Baudrit Ruiz
Director a.i de la OPES

Tabla de contenido

1. Introducción

La solicitud de creación de la Maestría Profesional en Ciberseguridad Industrial fue enviada al Consejo Nacional de Rectores (CONARE) por el señor Francisco González Alvarado, Rector de la Universidad Nacional mediante nota UNA-R-OFIC-2849-2024 con el objeto de iniciar los procedimientos señalados en el documento Lineamientos para la creación y rediseño de carreras universitarias estatales[a].

Para la creación de una carrera de posgrado se utiliza lo determinado en los Lineamientos para la creación y rediseño de carreras universitarias estatales (p.18). Los principales temas que constituyen la base del estudio realizado por la Oficina de Planificación de la Educación Superior (OPES) contiene:

- Datos generales
- Autorización de la unidad académica para impartir posgrados
- Objeto de estudio
- Justificación
- Desarrollo académico en el campo de estudios del posgrado
- Objetivos académicos
- Perfil académico-profesional
- Campo de inserción profesional
- Contextos donde puede laborar el profesional graduado
- Datos de empleabilidad según resultados del OLaP
- Oferta académica aprobada en relación con la disciplina
- Requisitos de ingreso
- Requisitos de graduación
- Requisitos de permanencia
- Descripción de los cursos
- Correspondencia del equipo docente con los cursos asignados

A continuación, se detalla cada uno de estos aspectos.

[a] Aprobado por el Consejo Nacional de Rectores en la sesión Nº41-2022 celebrada el 18 de octubre de 2022.

2. Datos generales

La Maestría Profesional en Ciberseguridad Industrial (MACIBI) de la UNA se encontrará adscrita a la Sede Regional Chorotega (Campus Liberia y Campus Nicoya) de la Universidad Nacional. Este posgrado tiene como objetivo formar profesionales en el campo de la Ciberseguridad Industrial con habilidades estratégicas y operativas que les permitan abordar los retos actuales en ciberseguridad aplicados a entornos industriales, promoviendo la protección de sistemas de control, de infraestructuras industriales y la continuidad operacional mediante el análisis de riesgos frente a amenazas cibernéticas y diseño de estrategias de seguridad, tanto a nivel nacional como internacional.

Modalidad y duración:

Esta maestría se desarrollará en modalidad virtual. La duración total de la maestría abarca 6 cuatrimestres, distribuidos en ciclos lectivos de 15 semanas cada uno. El plan contempla un total de 5 promociones.

Créditos y titulación:

El plan de estudios tiene una carga de 66 créditos, distribuidos en 6 ciclos (3 ciclos por año) que contemplan 12 cursos obligatorios, un proyecto de investigación aplicada y dos cursos optativos, distribuidos de la siguiente manera:

- Dos ciclos de 12 créditos cada uno.
- Dos ciclos de 9 créditos cada uno.
- Un ciclo de 13 créditos.
- Un ciclo de 11 créditos.

Al concluir la maestría, las personas estudiantes obtendrán el título de Magister en Ciberseguridad Industrial.

Gestión administrativa y recursos:

La orientación general del posgrado está a cargo del Comité de Gestión Académica (CGA) de la Sede Chorotega, el cual está integrado por el coordinador del posgrado, por el decano de la Sede Regional Chorotega, por 3 miembros profesores del programa y por 1 representante estudiantil del programa. Asimismo, el posgrado contará con el apoyo logístico del personal de la Sede.

En cuanto a infraestructura y talento humano, según indica la UNA, la Sede Chorotega, campus Liberia y Nicoya dispone de los recursos, infraestructura, equipos y herramientas tecnológicas requeridas para desarrollar las actividades académicas, complementarias y de apoyo a la formación virtual. Cuenta con un sistema de bibliotecas actualizadas (física y electrónica), laboratorios de cómputo e instalaciones con amplias zonas verdes y dispone de conectividad a Internet basado en Fibra Óptica con una capacidad de 2 Gpbs de ancho de banda y en proceso de expansión a 10 Gbps.

Asimismo, dispone de una Plataforma de Aprendizaje Virtual (LMS), laboratorios virtuales y simuladores de ciberseguridad, herramientas de colaboración y comunicación en línea, software de ciberseguridad, herramientas de análisis y recursos bibliográficos físicos y digitales.

3. Autorización de la unidad académica para impartir posgrados

Según la normativa, para autorizar a una unidad académica para impartir un posgrado, resulta indispensable recabar información detallada sobre los (as) docentes de dicha unidad. Esto incluye el grado académico, su dedicación, los años de experiencia acumulada en el ámbito de la Educación Superior y el dominio del idioma aparte del español.

La unidad base de la Maestría en Ciberseguridad Industrial es la Sede Chorotega de la Universidad Nacional, la cual ya cuenta con la autorización para impartir posgrados a partir de la creación de la Maestría en Turismo y Desarrollo Sostenible, según consta en el OPES 17-2022.

4. Objeto de estudio

El objeto de estudio de la Maestría en Ciberseguridad Industrial (MACIBI) es la ciberseguridad industrial, aplicada de forma holística en infraestructuras computacionales industriales y todo lo tecnológico relacionado con estas, haciendo énfasis en la protección cibernética de: hardware especializado industrial, sistemas de software de control y supervisión industrial y redes industriales críticos contra amenazas cibernéticas, que garanticen su funcionamiento seguro y continuo basado en normas y estándares industriales internacionales. (Plan de estudios de Maestría en Ciberseguridad Industrial (MACIBI), UNA, p.23).

5. Justificación

En resumen, para la propuesta de la Maestría en Ciberseguridad Industrial se plantea que Latinoamérica experimenta un crecimiento significativo en innovación tecnológica y adopción de tecnologías industriales avanzadas que conlleva la necesidad urgente de proteger sistemas de control industrial y datos sensibles contra ciber amenazas. Tomando en cuenta el desarrollo y liderazgo tecnológico de Costa Rica en la región, surge la propuesta de la maestría en Ciberseguridad Industrial con el objetivo de formar profesionales altamente capacitados para enfrentar estos retos y fortalecer la seguridad nacional y regional.

En cuanto a las dimensiones externa e Interna de la Maestría en Ciberseguridad Industrial, se indica que la ciberseguridad industrial ha emergido como una prioridad global frente a la creciente digitalización y automatización de sistemas industriales. Este panorama exige planes de estudio que integren aspectos esenciales como normativas internacionales, gestión de riesgos, respuesta a incidentes y colaboración internacional. Organismos como INTERPOL y foros internacionales, entre ellos el Foro Económico Mundial, lideran esfuerzos para mitigar amenazas cibernéticas, mientras que estándares y ejercicios internacionales, como "Cyber Europe" o normativas como la Directiva NIS 2 y

la ISA/IEC 62443, se establecen como referencias imprescindibles para fortalecer la protección de infraestructuras críticas.

Se indica, además, que en Costa Rica, campo de la ciberseguridad industrial, se ha vuelto indispensable la profundización en conocimientos técnicos especializados en áreas como la seguridad en redes industriales, la gestión de sistemas de control industrial como ICS/SCADA, y la protección integral de infraestructuras críticas. Estos conocimientos no solo abren la puerta a la comprensión de complejas arquitecturas tecnológicas, sino que también capacitan a los profesionales para salvaguardar los recursos más valiosos de la industria y responder a las crecientes demandas del sector.

Por otro lado, se expone que la Sede Regional Chorotega (SRCH) de la Universidad Nacional ha evolucionado desde 1973 y se ha consolidado como una respuesta a las necesidades del desarrollo regional.

La justificación detalla la estructura funcional y de gestión con que cuenta la sede y describe los programas de alto nivel con que cuentan, a saber: el Centro Mesoamericano de Desarrollo Sostenible del Trópico Seco (CEMEDE), el Centro de Recursos Hídricos para Centroamérica y el Caribe (HIDROCEC), el Observatorio Regional y el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE). Estos programas son innovadores en áreas como sostenibilidad, recursos hídricos, ciberseguridad, así como en investigación y desarrollo en seguridad digital.

La Sede Regional Chorotega (SRCH) de la Universidad Nacional también se ha consolidado como referente académico al impartir la carrera de Ingeniería en Sistemas de Información y organizar eventos destacados en ciberseguridad, como congresos y simposios de impacto regional y nacional. Estas experiencias refuerzan la pertinencia y capacidad de la Sede de ofrecer una maestría en Ciberseguridad Industrial que atienda tanto las necesidades locales como las mesoamericanas.

Igualmente relevante, se señala que la propuesta de la Maestría en Ciberseguridad se enmarca en el Plan Estratégico 2023-2027 de la SRCH, que busca liderar la transformación digital y la educación STEM, comprometida con la excelencia académica, la sostenibilidad y la incidencia en políticas públicas. Asimismo, la propuesta de la Maestría se alinea con la misión y visión institucional de la UNA, enfocada en la inclusión, equidad y desarrollo regional, integrando objetivos académicos con estrategias de impacto regional y nacional, en respuesta a las demandas actuales y futuras de la ciberseguridad. (Resumen ejecutivo posgrado en Ciberseguridad Industrial, UNA, s.p).

A partir de lo planteado, se colige que la Maestría en Ciberseguridad Industrial se enmarca en un contexto de creciente interconexión tecnológica y desafíos en ciberseguridad. Su diseño responde a necesidades globales y regionales para fortalecer las capacidades en ciberseguridad y contribuir a la protección de infraestructuras críticas y sistemas industriales de los sectores estratégicos del país. Por ello, se considera que la justificación para la creación de la Maestría propuesta es apropiada.

6. Desarrollo académico en el campo de estudios del posgrado

En lo relativo al desarrollo académico en el campo de la Ciberseguridad, la Sede regional Chorotega de la Universidad Nacional indica lo siguiente:

> Experiencias académicas de la SRCH relacionadas con Ciberseguridad.
>
> En el área de la Ciberseguridad, se ha aprovechado que la Sede imparte desde el año 2008, la carrera de Ingeniería en Sistemas de Información, la cual se ha colocado como una de las carreras más demandadas, con el respaldo de Laboratorios de altos estándares de calidad, plantel docente bien cualificado y estudiantes comprometidos, competentes e intelectualmente inquietos. Se han desarrollado durante estos años eventos académicos de alto nivel relacionados al ámbito de la Ciberseguridad, tales como: talleres de entrenamiento para instructores de seguridad informática en conjunto con Registro de Direcciones de Internet de América Latina y Caribe (LACNIC, por sus siglas en inglés), simposios y conferencias entorno al Día de la Seguridad Informática, cursos a la comunidad estudiantil relacionados con Seguridad Informática, el Congreso de Ciberseguridad y Sociedades Hiperconectadas (CICSOH, 2019) (Memoria: https://repositorio.una.ac.cr/handle/11056/18014), el Congreso Nacional de Ciencia, Tecnología y Sociedad (2017) (Memoria: https://repositorio.una.ac.cr/handle/11056/25756). El I Simposio Internacional de Ciberseguridad y Sociedades Hiperconectadas (2023). (Resumen ejecutivo posgrado en Ciberseguridad Industrial, UNA, s.p).

Por otra parte, se indica que la Sede cuenta con el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE), el cual impulsa proyectos de investigación, desarrollo e innovación en Ciberseguridad, mediante recurso humano especializado y tecnología científica en la Universidad Nacional (UNA), en aspectos relacionados con ciberseguridad, la atención a incidentes, la preservación de la privacidad y construcción de herramientas de software. (Resumen ejecutivo posgrado en Ciberseguridad Industrial, UNA, s.p).

7. Objetivos académicos

Objetivo general:

- Brindar una formación profesional superior de la capacidad estratégica y operativa en Ciberseguridad Industrial a nivel nacional y regional, mediante la comprensión fundamental de los principios y prácticas de ciberseguridad aplicables a entornos industriales, basados en normativas y estándares internacionales que permitan la implementación de estrategias en la protección de estos sistemas contra amenazas cibernéticas.

Objetivos específicos:

- Desarrollar habilidades de liderazgo, creatividad, ética, comunicación y gestión, para que el profesional esté preparado en la toma de decisiones que permitan la

gobernanza de la ciberseguridad industrial en obediencia a la ley y regulaciones relacionadas.

- Desarrollar habilidades en investigación aplicada en ciberseguridad industrial, para la creación de evaluaciones de riesgos más precisas y detalladas, identificando posibles puntos de fallo y áreas de vulnerabilidad en sistemas industriales.
- Desarrollar habilidades técnicas en ciberseguridad industrial que contribuyan a la mejora continua de la postura de seguridad, permitiendo el análisis forense de incidentes aplicando medidas correctivas que eviten futuros ciberataques. (Resumen ejecutivo posgrado en Ciberseguridad Industrial, UNA, s.p).

Los objetivos planteados están acordes con el grado y nombre de la carrera propuesta. Además, mantienen coherencia con el objeto de estudio y perfil académico profesional.

8. Perfil académico-profesional

La Maestría en Ciberseguridad Industrial de la UNA presenta un perfil académico profesional por resultados de aprendizaje: conceptuales, procedimentales y actitudinales, tal como se detalla a continuación:

Tabla 2: Perfil académico-profesional de la Ciberseguridad Industrial (MACIBI) de la UNA

Saberes	Resultados de aprendizaje
Saber conceptual	Dominará conceptos de ciberseguridad en sistemas de control industrial y protección de infraestructuras críticas.
	Comprenderá a identificar amenazas y vulnerabilidades de los sistemas de control industrial reconociendo sus riesgos.
	Desarrollará conocimientos de ciberseguridad en la gestión de software industrial.
	Conocerá conceptos legales y regulatorios de la información nacionales e internacionales que le permitan tomar decisiones basadas en la legalidad y la ética profesional.
Saber procedimental	Aplicará herramientas para formular sistemas de gestión de la seguridad de la información basados en las mejores prácticas de la industria.
	Aplicará herramientas para desarrollar soluciones ante incidentes de ciberseguridad usando metodologías forenses informáticas.
	Demostrará el desarrollo de habilidades para el diseño de marcos de gestión de ciberseguridad adecuados en las Infraestructuras Críticas y entornos industriales.
	Logrará planificar e implementar estándares de industria y recomendaciones aplicables al entorno industrial correspondiente a su área laboral.

	Integrará aspectos organizacionales y de gestión relevantes de ciberseguridad industrial y gestión de procesos tecnológicos de planta en ambientes industriales. Poseerá la capacidad para analizar y evaluar eventos de seguridad industrial de manera crítica para tomar decisiones informadas, especialmente bajo presión.
Saber actitudinal	Desarrollará su capacidad para trabajar en equipos multidisciplinarios, locales, nacionales o internacionales. Entablará adecuadas relaciones humanas de respeto mutuo. Desplegará una ética centrada en el desarrollo humano. Será líder en su grupo de trabajo y desarrollará la habilidad para comunicar riesgos de seguridad, incidentes y necesidades de manera clara a una variedad de audiencias, incluyendo a aquellos sin un trasfondo técnico. Asumirá como parte integral de su quehacer, los aspectos éticos, tanto en el plano personal como en el profesional. Se actualizará de manera permanente en ciberseguridad industrial y las áreas afines que afecten su entorno laboral. Tendrá disposición para resolver problemas con un enfoque meticuloso y orientado a la legalidad.

Fuente: Resumen ejecutivo Posgrado en Ciberseguridad Industrial (MACIBI), UNA.

El perfil académico profesional planteado para la Maestría profesional en Ciberseguridad Industrial (MACIBI) mantiene congruencia con el objeto de estudio y los objetivos de la carrera.

La División Académica considera que el perfil académico profesional de las personas graduadas de la Maestría en Ciberseguridad Industrial se adecúa a los Resultados de Aprendizaje esperados para el nivel de Maestría, según lo establecido en el Marco Centroamericano de Cualificaciones para la Educación Superior Centroamericana (MCESCA)[b]. Este marco de cualificaciones fue adoptado por el CONARE como referente para la formulación de planes de estudio en las Instituciones de Educación Superior Universitario Estatal mediante acuerdo CNR-338-2018.

9. Campo de inserción profesional

La UNA establece los cargos, espacios laborales y funciones por desempeñar las personas graduadas de la Maestría en Ciberseguridad Industrial (MACIBI).

A continuación, el detalle:

[b] Marco de Cualificaciones para la Educación Superior Centroamericana. Resultados de Aprendizaje para los niveles Técnico Superior Universitario, Bachillerato Universitario, Licenciatura, Maestría y Doctorado, Consejo Superior Universitario Centroamericano, 2018.

Tabla 3: Contextos donde puede laborar el profesional graduado

Espacios laborales	Cargos por ocupar	Funciones por desempeñar
Empresas de Producción Eléctrica. Manufactura y producción industrial. Sector transporte. Sector municipal, área de acueductos. Empresas de telecomunicaciones.	Ingeniero de Seguridad en Sistemas de Control Industrial (ICS)	- Especializado en la protección de sistemas de control industrial como SCADA. Estos ingenieros comprenden tanto la tecnología operativa (OT) como la tecnología de la información (IT).
Empresas de Producción Eléctrica. Manufactura y producción industrial. Sector transporte. Sector municipal, área de acueductos. Empresas de telecomunicaciones. Sector salud.	Auditor de Ciberseguridad Industrial	- Realiza auditorías de seguridad cibernética para evaluar el cumplimiento de normativas y estándares de seguridad en entornos industriales, identificando áreas de mejora.
Empresas de Producción Eléctrica. Manufactura y producción industrial. Sector transporte. Sector municipal, área de acueductos. Empresas de telecomunicaciones. Sector salud.	Consultor de Ciberseguridad Industrial	- Proporciona asesoramiento experto a empresas en la implementación de medidas de seguridad cibernética específicas para entornos industriales, evaluando riesgos y recomendando soluciones.
Empresas de Producción Eléctrica. Manufactura y producción industrial. Sector transporte. Sector municipal, área de acueductos. Empresas de telecomunicaciones. Sector salud. Sector bancario y finanzas.	Analista de Seguridad de la Información	- Responsable de monitorear y analizar las amenazas cibernéticas, identificar vulnerabilidades y tomar medidas correctivas para mitigar riesgos.

Empresas de Producción Eléctrica. Manufactura y producción industrial. Sector transporte. Sector municipal, área de acueductos. Empresas de telecomunicaciones.	Administrador de Proyectos de Ciberseguridad Industrial	- Planificación y Gestión de Proyectos - Análisis de Riesgos y Vulnerabilidades - Implementación de Controles de Seguridad - Gestión de Incidentes y Continuidad del Negocio - Capacitación y Concientización

Fuente: Resumen ejecutivo Posgrado en Ciberseguridad Industrial (MACIBI), UNA.

a. Datos de empleabilidad según resultados del OLaP

De conformidad con el acuerdo del Consejo Nacional de Rectores CNR-498-2022, inciso b, sesión 41-2022, celebrada el 18 de octubre de 2022, se deben indicar datos relacionados con el *Estudio de seguimiento de las personas graduadas de posgrado 2017-2019 de las* universidades *estatales costarricenses* (OPES; no. 03-2023) elaborado por el Observatorio Laboral de Profesiones (OLaP) de la OPES, CONARE, el cual se puede acceder en el siguiente enlace: https://hdl.handle.net/20.500.12337/8449

En este caso, se realiza la comparación con los datos obtenidos en el Estudio de seguimiento de las personas graduadas de posgrado 2017-2019 de las universidades estatales costarricenses, elaborado en la OPES publicado en 2023 mediante el Observatorio Laboral de Profesiones (OLaP), se investigaron tres conceptos básicos de empleo, a saber:

- Desempleo: Se considera desempleado a quien no encuentra trabajo, aunque busca conseguirlo.

- Subempleo por horas: Se considera subempleado por horas a quien trabaja menos de tiempo completo porque no consigue una jornada mayor.

- Trabajo con poca relación con la carrera que estudió: Incluye a aquellas personas graduadas cuyo trabajo tiene poca o ninguna relación con la carrera cursada porque no encuentran empleo relacionado con dicha carrera.

Con base en lo descrito, se presentan los resultados de ese estudio para las personas graduadas universitarias 2017-2019 a nivel general y para la disciplina de Ciencias de la Computación, en donde se ubica la propuesta de la Maestría Profesional en Ciberseguridad Industrial.

Situación laboral de los graduados de la disciplina en Ciencias de la Computación	Hombres	Mujeres	Total
Desempleo	1,0%	0,8%	0,9%
Subempleo por horas	0,0%	0,0%	0,0%
Poca relación con la carrera que estudió	0,0%	0,0%	0,0%

Fuente: CONARE-OLaP, (2023), Estudio de Seguimiento de la Condición Laboral de las Personas Graduadas 2017-2019 de las Universidades Costarricenses.

Al momento de la encuesta, el campo de Ciencias de la Computación presenta una baja tasa de desempleo (0.8%) y una alta tasa de empleo (98.4%), por lo que, los datos del estudio citado muestran un panorama favorable para las personas profesionales en Ciencias de la Computación, ya que reflejan una alta demanda laboral y una rápida inserción en el mercado.

b. Oferta académica aprobada en relación con la disciplina

De conformidad con el acuerdo del Consejo Nacional de Rectores CNR-498-2022, inciso b, sesión 41-2022, celebrada el 18 de octubre de 2022, se indican los datos relacionados con la oferta académica aprobada en relación con la disciplina propuesta.

Se detalla a continuación la información sistematizada de la oferta académica de posgrado relacionada con ciberseguridad. En esta sistematización se contemplan las variables: carrera, grado académico, universidad, sede y año de creación.

Tabla: Listado de carreras de grado o posgrado aprobadas en universidades públicas y privadas según grado académico, universidad y año de creación

Carrera	Grado académico	Universidad	Sede	Año
Ciberseguridad	Maestría Profesional	Instituto Tecnológico de Costa Rica	TEC	2021
Ciberseguridad	Maestría Profesional	Instituto Tecnológico de Costa Rica	TEC-CASJ	2021
Ciberseguridad	Maestría Profesional	Instituto Tecnológico de Costa Rica	TEC-LM	2021
Ciberseguridad	Maestría Profesional	Instituto Tecnológico de Costa Rica	TEC-SIA	2021
Ciberseguridad	Maestría Profesional	Instituto Tecnológico de Costa Rica	TEC-SRSC	2021
Ciberseguridad	Maestría Profesional	Universidad Cenfotec	CENFOTEC	2014

Fuente: Base de datos División Académica, OPES-CONARE, 2024

10. Requisitos de ingreso y de graduación

a. Requisitos de ingreso

El perfil de acceso recomendado o idóneo será el de Grado, Ingeniería o Licenciatura en Informática, o en Telecomunicaciones. Se podrá acceder con otro título de grado como Ingeniería o Licenciatura en disciplinas afines, como Estadística, Matemáticas o Física, si se acredita experiencia profesional en las TIC.

Las personas solicitantes con titulaciones cuyas competencias sean diferentes a las anteriores serán evaluados por el Comité de Gestión Académica (CGA) del Posgrado basándose en las materias cursadas y las evidencias de capacidades y aprovechamiento.

El perfil competencial del estudiantado de entrada incluye necesariamente conocimientos de técnicas y herramientas informáticas, redes de comunicaciones

y programación informática, así como conocimientos matemáticos, al menos del nivel de un primer año de ingeniería. (Resumen ejecutivo Posgrado en Ciberseguridad Industrial (MACIBI), UNA).

b. Requisitos de graduación

Para graduarse cada estudiante deberá cumplir con los requisitos siguientes:

- Haber aprobado todos los cursos y actividades que demande el plan de estudios.
- No tener pendientes financieros con ninguna instancia de la UNA.
- Elaboración, presentación y aprobación del trabajo final de graduación acorde con el Reglamento de Trabajos Finales de Graduación de la maestría.

Se debe cumplir con los demás requisitos administrativos que establezca la Universidad Nacional.

En cuanto a los requisitos de ingreso y graduación, la División Académica indica que lo planteado por la UNA cumple con la normativa vigente.

11. Listado de los cursos

El listado de las actividades académicas que desarrollará este programa se presenta en forma detallada en el Anexo A (Plan de estudios)

El programa comprende un total de 66 créditos y cumple con lo establecido en la normativa vigente.

12. Descripción de los cursos

Los programas de los cursos y demás actividades académicas se muestran en el Anexo B y cumplen con lo establecido en la normativa.

13. Correspondencia del equipo docente con los cursos asignados.

En el Anexo C se indica el nombre de los profesores de cada uno de los cursos de la Maestría en Ciberseguridad Industrial.

En el Anexo D, se indica el título y grado del diploma respectivo de cada una de las personas docentes.

Además, la normativa establece que cuando la carrera es impartida total o parcialmente de forma virtual se deberá indicar la experiencia de los docentes propuestos en el desarrollo de cursos o actividades académicas con uso de la virtualidad. En este sentido, la UNA indica que la Sede Chorotega cuenta con la siguiente estrategia de capacitación:

> En primer lugar, se considera primordial la actualización en ciberseguridad industrial, dado el dinamismo y la evolución constante de esta área. Para ello, se priorizarán temáticas como las normativas y estándares internacionales (ISO/IEC 62443, NIST), tecnologías emergentes como IoT industrial, blockchain e inteligencia artificial aplicada a ciberseguridad, además de técnicas avanzadas de ataque y defensa, y la seguridad en sistemas SCADA y redes industriales. La modalidad de actualización incluirá cursos y certificaciones internacionales, seminarios y talleres prácticos, así como la creación de comunidades de aprendizaje que fomenten el intercambio de experiencias y recursos entre los docentes.
>
> De igual importancia es el fortalecimiento de las competencias pedagógicas para entornos virtuales, considerando las particularidades del aprendizaje en línea. Este componente se enfocará en la implementación de metodologías activas, como el aprendizaje basado en problemas (ABP) y la simulación, además de herramientas de evaluación formativa y retroalimentación efectiva. Asimismo, se capacitará a los docentes en el uso de plataformas de gestión de aprendizaje (LMS) como Moodle o Canvas, herramientas interactivas como Miro, Kahoot y Mentimeter, y en el diseño de contenidos multimedia que enriquezcan la experiencia educativa. (Resumen ejecutivo Posgrado en Ciberseguridad Industrial (MACIBI), UNA)

La División Académica considera que las normativas vigentes sobre el personal docente se cumplen.

14. Conclusiones

- ✓ La creación de la Maestría Profesional en Ciberseguridad Industrial es oportuna, dado el contexto de transformación digital y las crecientes amenazas cibernéticas.
- ✓ La propuesta cumple con la normativa aprobada por el CONARE en el:
  - Convenio para crear una nomenclatura de grados y títulos de la Educación Superior Estatal[c]

[c] Aprobado por el CONARE y ratificado por los Consejos Universitarios e Institucional. Publicado en La Gaceta (Diario Oficial) 190 de 16 de octubre de 2023, páginas 42 a 46.

- Convenio para unificar la definición de crédito en la Educación Superior[d]
- Lineamientos para la creación y rediseño de carreras universitarias estatales.
- Marco de Cualificaciones para la Educación Superior Centroamericana (MCESCA).

15. Recomendaciones

Con base en las conclusiones del presente estudio, se recomienda:

a) Autorizar la creación de la Maestría Profesional en Ciberseguridad Industrial de acuerdo con lo establecido en este dictamen.

b) Reiterar la autorización de la Sede Chorotega, campus Liberia y Nicoya de la UNA para impartir posgrados con base en la revisión de los requisitos del grado académico, dedicación, años de experiencia en la Educación Superior y dominio de idiomas adicionales al español del personal docente propuesto por la UNA.

c) Que la Sede Chorotega, campus Liberia y Nicoya de la UNA realice evaluaciones internas durante el desarrollo de la carrera con el propósito de garantizar la calidad y relevancia del proceso formativo.

[d] Aprobado por el CONARE el 10 de noviembre de 1976.

16. Ficha para gestión de datos de la División Académica

FICHA DE INFORMACIÓN PARA GESTIÓN DE DATOS DE LA DIVISIÓN ACADÉMICA		
Nombre de la carrera:	Maestría en Ciberseguridad Industrial	
Universidad	Universidad Nacional	
Grado académico	Maestría Profesional	
Nombre de la titulación:	Magister en Ciberseguridad Industrial	
Número de créditos totales: 66	**Número de periodos totales:** 6	**Tipo de ciclo o periodo:** Cuatrimestral
Clasificación Campos de Educación y Formación (CINE-F 2013), UNESCO:		
Campo amplio (área)	**Campo específico (disciplina)**	**Campo detallado (carrera)**
06 Tecnologías de la Información y la Comunicación	061 Tecnologías de la Información y la Comunicación	0612 Diseño y administración de redes y bases de datos
Observaciones Generales	Esta carrera se imparte en la Sede Regional Chorotega, campus Liberia y Nicoya de la Universidad Nacional	

Anexo A

Plan de Estudios de la Maestría Profesional en Ciberseguridad Industrial de la Universidad Nacional

Nivel	Ciclo lectivo	Nombre del curso	Créditos
I	I	Aspectos legales y regulatorios de la información	4
I	I	Ciberseguridad industrial	5
I	I	Optativo I	3
		Subtotal	**12**
I	II	Metodologías éticas para pruebas de seguridad	5
I	II	Seguridad de la información I	4
I	II	Optativo II	3
		Subtotal	**12**
I	III	Investigación aplicada a la Ciberseguridad I	5
I	III	Seguridad de la información II	4
		Subtotal	**9**
II	IV	Investigación aplicada a la Ciberseguridad II	5
II	IV	Seguridad de componentes y redes industriales	4
		Subtotal	**9**
II	V	Software industrial	5
II	V	Análisis de datos industriales	4
II	V	Seguridad humana para ambientes industriales	4
		Subtotal	**13**
II	VI	Análisis forense industrial	5
II	VI	Proyecto de investigación aplicada	6
		Subtotal	**11**
		Total	**66**

Anexo B

Programas de los cursos de la Maestría Profesional en Ciberseguridad Industrial de la Universidad Nacional

I NIVEL

ASPECTOS LEGALES Y REGULATORIOS DE LA INFORMACIÓN

Créditos: 4

Descripción del curso: Este curso le ofrece al estudiante una comprensión integral de los aspectos legales y regulatorios que rigen la gestión de la información, su protección jurídica y la privacidad de los datos; en diferentes contextos organizacionales y jurisdiccionales.

El curso se centra en el estudio e interpretación de legislación internacional, normativas asociadas y jurisprudencia. A lo largo del curso, los estudiantes aprenderán a interpretar estos marcos legales por medio de casos de estudio, para su uso en la implementación de políticas y procedimientos de protección de datos y privacidad.

Objetivos generales:

Desarrollar una comprensión práctica y aplicable de los aspectos legales y regulatorios relacionados a la información y su protección jurídica, incluyendo metodologías de interpretación en legislación internacional, normativas asociadas y jurisprudencia relacionada a la información.

Objetivos específicos:

- Comprender los principios fundamentales de las leyes de protección de datos internacionales, para la aplicación y desarrollo de normativas de privacidad y seguridad de la información dentro de una organización.
- Evaluar el cumplimiento de controles sobre los riesgos legales en la custodia de información en una organización, desarrollando estrategias y planes de acción que los mitiguen y garanticen la conformidad con los marcos regulatorios pertinentes.
- Supervisar el diseño de procedimientos alineados con requisitos legales y cumplimiento normativo, para la protección de datos en un contexto organizacional.

Contenidos del curso:

- Marco Teórico y Normativo:
  - Análisis detallado a la legislación internacional sobre protección de datos.
  - Comparación de normativas de protección de datos en distintas jurisdicciones.

- Aplicación Práctica y Gestión del Cumplimiento:
  - Evaluación de políticas y procedimientos de protección de datos.
  - Aspectos legales en las auditorías de cumplimiento y gestión de riesgos.
  - Desarrollo de estrategias para asegurar el cumplimiento legal.
- Desarrollo e Implementación de Políticas:
  - Supervisión de diseño de políticas internas de protección de datos.
  - Implementación de procedimientos de seguridad y privacidad.
  - Supervisión y mejora continua de prácticas de gestión de información.

CIBERSEGURIDAD INDUSTRIAL

Créditos: 5

Descripción: El curso está diseñado para proporcionar una base sólida en los principios, técnicas y normativas de ciberseguridad aplicables a sistemas de control industrial (ICS).

El enfoque del curso incluye la comprensión de amenazas y vulnerabilidades específicas de los entornos industriales, así como la aplicación práctica de estrategias y medidas de seguridad basadas en la normativa de industria.

Objetivo General

Desarrollar los principios y prácticas de ciberseguridad aplicables a entornos industriales, incluyendo normativas técnicas asociadas, para la implementación de estrategias básicas en la protección de sistemas de control industrial contra amenazas cibernéticas.

Objetivos específicos

- Comprender los conceptos básicos de ciberseguridad industrial, las principales normativas y estándares aplicables, con un enfoque particular en el desarrollo de una estrategia de protección a Tecnologías Operativas.
- Realizar evaluaciones de riesgos y análisis de vulnerabilidades en sistemas de control industrial, utilizando metodologías y herramientas recomendadas por las buenas prácticas de la industria.
- Desarrollar propuestas de medidas de protección cibernética en entornos industriales, incluyendo la segmentación de redes y gestión de accesos, basado en normativa de industria.

Contenidos:

- Conceptos generales

    - Conceptos básicos de ciberseguridad en entornos industriales.
    - Generalidades de amenazas, ataques y vulnerabilidades en ambientes industriales.
- Técnicas y equipamientos para la defensa de los ciberataques
    - Características y funcionalidades de defensa en profundidad y confianza cero.
    - Características y funcionalidades de dispositivos industriales de seguridad.
- Evaluación de Riesgos y Análisis de Vulnerabilidades
    - Metodologías de implementación de planes de tratamiento de riesgos.
    - Herramientas y técnicas de análisis de vulnerabilidades.
- Implementación de Medidas de Protección
    - Técnicas de segmentación de redes.
    - Gestión de accesos y autenticación.
- Estudios de Caso y Aplicaciones Prácticas
    - Análisis de casos reales de ciberseguridad industrial.
    - Talleres prácticos y laboratorios.

METODOLOGÍAS ÉTICAS PARA PRUEBAS DE SEGURIDAD

Créditos: 5

Descripción: El curso de Metodologías éticas para pruebas de seguridad está diseñado para proporcionar a los estudiantes los conocimientos y habilidades necesarios para proteger sistemas industriales críticos contra amenazas cibernéticas. A través de este curso, los estudiantes aprenderán a identificar vulnerabilidades, ejecutar pruebas de penetración y desarrollar estrategias de mitigación específicas para ambientes industriales de Tecnologías de la Información y Tecnologías Operativas, siguiendo las mejores prácticas y estándares internacionales de ciberseguridad industrial.

Objetivo general: Enseñar a los estudiantes en la aplicación ética de metodologías y técnicas de pruebas de seguridad en ambientes industriales, garantizando la continuidad operativa de los sistemas mediante la identificación, análisis y mitigación de vulnerabilidades siguiendo las mejores prácticas de la industria.

Objetivos específicos:

- Realizar evaluaciones de seguridad en sistemas industriales, identificando y clasificando vulnerabilidades potenciales en infraestructuras críticas como SCADA, PLC, IoT, redes de control industrial (ICS); entre otros componentes.

- Ejecutar pruebas de penetración en infraestructuras críticas, utilizando herramientas y metodologías adaptadas a los sistemas industriales.
- Diseñar la implementación de estrategias efectivas de mitigación y respuesta a incidentes, aplicando buenas prácticas y recomendaciones de la industria para proteger sistemas industriales contra ciberamenazas, minimizando el impacto en la continuidad del negocio.

Contenidos:

- Introducción a la Ciberseguridad Industrial:
  - Fundamentos de sistemas industriales (ICS, SCADA, PLC,IoT).
  - Introducción a la ciberseguridad y conceptos clave en entornos industriales.
- Identificación y Análisis de Vulnerabilidades:
  - Herramientas y técnicas para evaluar la seguridad en sistemas industriales.
  - Identificación y clasificación de vulnerabilidades.
- Pruebas de Penetración en Ambientes Industriales:
  - Metodologías y mejores prácticas para pruebas de penetración.
  - Ejecución de pruebas y análisis de resultados.
- Estrategias de Mitigación y Respuesta a Incidentes:
  - Desarrollo de planes de mitigación.
  - Implementación de medidas de seguridad y respuesta a incidentes.
- Normativas y Estándares Internacionales:
  - Revisión de estándares como ISA/IEC 62443 y su aplicación en la ciberseguridad industrial.

SEGURIDAD DE LA INFORMACIÓN I

Créditos: 4

Descripción: El curso de Seguridad de la Información está diseñado para proporcionar a los estudiantes una comprensión profunda de los principios y prácticas necesarias para proteger la información y los sistemas de información.

El curso abarca desde la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) hasta la evaluación de riesgos y la realización de auditorías de seguridad.

Objetivo general: Desarrollar en los estudiantes una comprensión profunda del diseño, implementación y gestión de un-Sistema de Gestión de Seguridad de la Información efectivo, integrando políticas de seguridad robustas; identificando riesgos de manera proactiva y desarrollando estrategias de recuperación ante desastres de ciberseguridad.

Objetivos específicos:

- Elaborar políticas de seguridad de la información que alineen con las normas y estándares internacionales, para la definición de objetivos estratégicos de la organización.

- Desarrollar metodologías de identificación de amenazas físicas y ambientales que pueden afectar la seguridad de la información, diseñando controles y medidas de protección adecuadas para la mitigación estos riesgos.
- Desarrollar planes de recuperación ante desastres de ciberseguridad que garantice la continuidad del negocio y la rápida recuperación de los sistemas de información críticos en caso de incidentes.
- Establecer sistemas de seguimiento y auditoría continua para la evaluación de la efectividad de las políticas y controles de seguridad, realizando ajustes necesarios y mejorando continuamente el SGSI de la organización.

Contenidos:

- Sistema de gestión de seguridad de información
- Aspectos organizativos en Políticas de Seguridad de la Información
- Políticas de Seguridad para el análisis de amenazas en sistemas informáticos
- Implementación de Políticas de Seguridad en software y hardware
- Políticas de gestión de incidentes de seguridad
- Implementación de Políticas de Seguridad física y ambiental en la empresa
- Políticas de comunicaciones seguras en la empresa
- Implementación de Políticas de Seguridad ante ataques
- Desarrollo de herramientas de monitorización en Políticas de Seguridad de los sistemas de información
- Políticas de recuperación de desastres de seguridad

INVESTIGACIÓN APLICADA A LA CIBERSEGURIDAD I

Créditos: 5

Descripción: Este curso está diseñado para proporcionar a los estudiantes una comprensión profunda de las metodologías de investigación aplicadas específicamente al campo de la ciberseguridad industrial. Abarca tanto enfoques teóricos como prácticos, y se centra en el desarrollo de habilidades para llevar a cabo investigaciones rigurosas y aplicadas en entornos industriales.

Objetivo general: Desarrollar el aprendizaje integral en la aplicación de metodologías de investigación cuantitativa, cualitativa y mixta en el campo de la ciberseguridad industrial, capacitando a los estudiantes para el desarrollo de proyectos de investigación que aborden problemas complejos y emergentes en este ámbito.

Objetivos específicos:

1. Capacitar a los estudiantes en el diseño y ejecución de investigaciones cuantitativas en ciberseguridad industrial, abarcando desde la formulación de hipótesis hasta la recolección y análisis de datos utilizando herramientas y técnicas estadísticas avanzadas.
2. Proveer a los estudiantes de las competencias necesarias para llevar a cabo investigaciones cualitativas en ciberseguridad., incluyendo el diseño de estudios cualitativos, la recolección de datos a través de entrevistas, grupos focales y observación, y el análisis e interpretación de estos.
3. Enseñar a los estudiantes a llevar a cabo investigaciones mixtas que combinen enfoques cuantitativos y cualitativos, integrando datos de diversas fuentes y metodologías que proporcionen una comprensión holística y rigurosa de los desafíos de la ciberseguridad industrial.

Contenidos:

- Introducción a la Ciberseguridad Industrial
    - Conceptos básicos y terminología
    - Panorama de amenazas y vulnerabilidades en entornos industriales
- Metodologías de Investigación en Ciberseguridad
    - Enfoque cuantitativo
    - Enfoque cualitativo
    - Enfoque mixto
- Proceso de Investigación Cuantitativa
    - Formulación de hipótesis
    - Diseño experimental y no experimental
    - Recolección y análisis de datos cuantitativos
- Proceso de Investigación Cualitativa
    - Diseño de estudios cualitativos
    - Técnicas de recolección de datos cualitativos (entrevistas, grupos focales, observación)
    - Análisis de datos cualitativos
- Proceso de Investigación Mixta
    - Diseño y ejecución de estudios mixtos
    - Integración de datos cualitativos y cuantitativos
    - Interpretación y validación de resultados
- Desarrollo de la perspectiva teórica y técnica

    - Métodos de construcción del marco teórico y técnico
    - Definición del alcance de la investigación
    - Formulación de la hipótesis
    - Concepción del diseño de la investigación
- Herramientas y Técnicas para la Investigación en Ciberseguridad
    - Herramientas de software específicas para el análisis de seguridad industrial
    - Técnicas de modelado y simulación
- Aplicaciones Prácticas y Estudios de Caso
    - Análisis de casos reales de incidentes de ciberseguridad industrial
    - Proyectos de investigación aplicados.

SEGURIDAD DE LA INFORMACIÓN II

Créditos: 4

Descripción: Este curso ofrece una comprensión profunda de los modelos de madurez en ciberseguridad, destacando su propósito y aplicación en la gestión de la seguridad de la información. Los estudiantes aprenderán a evaluar y mejorar la capacidad de sus organizaciones para gestionar y proteger sus activos de información mediante la aplicación de diferentes modelos de madurez.

El curso se centra en proporcionar a los estudiantes una base sólida en la teoría y práctica de los modelos de madurez en ciberseguridad. Se abordarán modelos reconocidos como el C2M2 (Cybersecurity Capability Maturity Model) y el NIST CSF (Cybersecurity Framework del NIST), entre otros. El enfoque incluye tanto la comprensión conceptual de estos modelos como la aplicación práctica mediante estudios de caso y ejercicios de evaluación.

Objetivo General:

Desarrollar en los estudiantes las habilidades y conocimientos necesarios para la evaluación y mejora de la ciberseguridad de las organizaciones, mediante la comprensión y aplicación de modelos de madurez en ciberseguridad, que incluyan metodologías y herramientas de evaluación de métricas.

Objetivos específicos:

- Comprender el propósito de los Modelos de Madurez en Ciberseguridad en el contexto de la gestión de la seguridad de la información, identificando los beneficios y limitaciones de la utilización de estos modelos en diversas organizaciones.

- Desarrollar el conocimiento para aplicación de modelos de madurez en escenarios prácticos, evaluando el nivel de madurez de ciberseguridad de una organización y desarrollando planes de acción que mejoren su postura de defensa cibernética.
- Aprender la implementación de diversas técnicas y herramientas de evaluación de madurez para diagnosticar el estado de ciberseguridad de una organización, que permitan la evaluación e interpretación de resultados basados en las métricas generadas.

Contenidos:

- Definición y propósito de los modelos de madurez.
  - Beneficios de utilizar modelos de madurez en ciberseguridad.
  - Comparativa de diferentes modelos de madurez.
  - Modelo de Madurez de Ciberseguridad de C2M2
- Visión general del C2M2 (Cybersecurity Capability Maturity Model).
  - Niveles de madurez y dominios de capacidad.
  - Evaluación y mejora utilizando el C2M2.
  - Modelo de Madurez de CMMI
- Introducción al Capability Maturity Model Integration (CMMI).
  - Aplicación del CMMI en la ciberseguridad.
  - Prácticas y procesos de madurez en CMMI.
  - NIST Cybersecurity Framework (CSF)
- Estructura y componentes del NIST CSF.
  - Implementación y evaluación utilizando el NIST CSF.
  - Mapeo de NIST CSF a otros modelos de madurez.
  - ISO/IEC 21827 (SSE-CMM)
- Visión general del Systems Security Engineering Capability Maturity Model.
  - Niveles de madurez y prácticas clave.
  - Evaluación de la seguridad utilizando SSE-CMM.
  - Evaluación y Auditoría de Madurez
- Métodos y herramientas de evaluación de madurez.
  - Realización de auditorías de madurez.
  - Interpretación y utilización de los resultados de la evaluación.
  - Planes de Mejora Continua
- Desarrollo de planes de mejora basados en evaluaciones de madurez.
  - Estrategias para la implementación de mejoras.
  - Monitoreo y revisión continua de la madurez de ciberseguridad.

II NIVEL

INVESTIGACIÓN APLICADA A LA CIBERSEGURIDAD II

Créditos: 5

Descripción: Este curso está diseñado para proporcionar a los estudiantes una comprensión profunda de las metodologías de recolección datos y muestras probabilísticas aplicadas al campo de la ciberseguridad industrial. Abarca tanto enfoques teóricos como prácticos, y se centra en el desarrollo de habilidades para llevar a cabo investigaciones rigurosas y aplicadas en entornos industriales.

Objetivo general:

Desarrollar el aprendizaje integral en la aplicación de las metodologías de recolección datos y muestras probabilísticas aplicadas al campo de la ciberseguridad industrial, capacitando a los estudiantes para el desarrollo de proyectos de investigación que aborden problemas complejos y emergentes en este ámbito.

Objetivos específicos:

1. Capacitar a los estudiantes en el diseño y ejecución de instrumentos de medición cuantitativas en ciberseguridad industrial, durante la recolección y análisis de datos utilizando herramientas y técnicas estadísticas avanzadas.
2. Proveer a los estudiantes de las competencias necesarias para llevar a cabo investigaciones cuantitativas y cualitativas en ciberseguridad, la recolección de datos a través de entrevistas, grupos focales y observación, y el análisis e interpretación de estos.
3. Enseñar a los estudiantes a llevar a cabo investigaciones mixtas que combinen enfoques cuantitativos y cualitativos, integrando datos de diversas fuentes y metodologías que proporcionen una comprensión holística y rigurosa de los desafíos de la ciberseguridad industrial.

Contenidos:

- Selección de la muestra
    - Delimitación de la población
    - Selección de muestra probabilísticas
    - Definición de marcos muestrales
- Recolección de datos cuantitativos
    - Requisitos de un instrumento de medición
    - Construcción de instrumentos de medición
    - Escogencias de escalas de medición

- Análisis de datos
    - Compresión y uso de estadística descriptiva
    - Análisis mediante pruebas estadísticas
    - Preparación de resultados
- Reporte de resultados
    - Recomendaciones de redacción
    - Definición del contexto

SEGURIDAD DE COMPONENTES Y REDES INDUSTRIALES

Créditos: 4

Descripción: Este curso ofrece una comprensión profunda de los puntos clave a tener en cuenta en cualquier proceso de análisis, diseño, desarrollo y mantenimiento de redes industriales y sus componentes.

El curso ofrece a los estudiantes una base sólida en la teoría y práctica de los principales problemas de seguridad informática relacionados con las redes industriales, físicas y lógicas. Asimismo, se busca que los estudiantes obtengan el conocimiento de las principales soluciones técnicas y organizativas que se utilizan hoy en día en la industria para tratar de minimizar los riesgos asociados a tales problemas de seguridad.

Objetivo general:

Desarrollar en los estudiantes las habilidades y conocimientos necesarios para la solución de los principales problemas de seguridad informática relacionados con las redes industriales y sus componentes, que permitan la implementación de soluciones prácticas a tales problemas de seguridad en ambientes industriales.

Objetivos específicos:

- Aplicar conocimientos teóricos adquiridos en el curso en contextos prácticos, realizando ejercicios técnicos que simulen situaciones reales de ciberseguridad en redes industriales.
- Desarrollar proyectos que integren soluciones de seguridad en el diseño y gestión de sistemas de comunicación industrial, que permitan la medición de la efectividad de controles técnicos de la seguridad industrial de redes y sus componentes.
- Comprender en un contexto práctico la implementación de diversas técnicas y herramientas que protejan las redes industriales y sus componentes, para la identificación de las vulnerabilidades y la implementación de mitigaciones.

Contenidos:

- Revisión de aspectos generales de seguridad de redes industriales y sus componentes.
- Gestión de problemas de seguridad en redes industriales y sistemas de control industrial.
- Diseño, arquitectura de red y protocolos en redes industriales.
- Evaluación de vulnerabilidades y riesgos.
- Introducción a la defensa cibernética en redes industriales y sus componentes.
- Monitoreo de la seguridad en redes industriales.

ANALISIS DE DATOS INDUSTRIALES

Créditos: 4

Descripción: Este curso se centra en la seguridad de datos industriales, cubriendo aspectos críticos como la protección de datos, la privacidad y las técnicas de prevención contra accesos no autorizados en entornos industriales. Los estudiantes participarán en laboratorios prácticos y análisis de casos reales para aplicar técnicas de cifrado, gestión de acceso y auditoría de seguridad en datos industriales.

Objetivo General:

Desarrollar un análisis comprensivo de datos industriales que integre la seguridad y gobernanza de datos en la nube, con un enfoque en el aprendizaje automático, analítica de datos, ciberseguridad en IoT e IIoT, y la visualización de datos para la mejora en la toma de decisiones industriales y la integridad de los datos.

Objetivos específicos:

1. Comprender las prácticas de seguridad y gobernanza de datos, enfocándose en políticas de acceso, protección de datos sensibles, y cumplimiento normativo para el aseguramiento de la integridad y calidad de los datos industriales.
2. Implementar técnicas avanzadas de aprendizaje automático y modelos predictivos para el análisis de grandes volúmenes de datos industriales, para la predicción de tendencias, optimización de procesos y la mejora de la eficiencia operativa.
3. Desarrollar estrategias de ciberseguridad en IoT e IIoT, incluyendo la implementación de medidas de seguridad en el ciclo de vida de los datos, auditoría y monitoreo continuo, así como la preparación y respuesta efectiva a incidentes y mitigación de riesgos, asegurando la continuidad del negocio.

Contenidos:

- Introducción a la Seguridad de los Datos y Gobernanza de Datos en la Nube
- Aprendizaje Automático
- Analítica de Datos y Herramientas de Analítica

- Modelos Predictivos y Machine Learning
- Seguridad en el Ciclo de Vida de los Datos
- Visualización de Datos
- Ciberseguridad en IoT e IIoT
- Respuesta a Incidentes y Recuperación
- Auditoría y Monitoreo de Seguridad de Datos
- Integridad y Calidad de los Datos
- Ética y Seguridad de Datos
- Innovaciones y Tendencias en Seguridad de Datos

SEGURIDAD HUMANA PARA AMBIENTES INDUSTRIALES

Créditos: 4

Descripción: Este curso está diseñado para capacitar a los profesionales en la identificación y gestión de los riesgos asociados con las interacciones humanas en los entornos industriales. Se enfocará en cómo las acciones y decisiones humanas pueden comprometer la seguridad de los activos críticos, incluyendo maquinaria, datos y propiedad intelectual. A través de un enfoque multidisciplinario, los estudiantes aprenderán a implementar estrategias de mitigación, promover comportamientos seguros y asegurar la integridad de los activos industriales

Objetivo general:

Capacitar a los participantes para que comprendan y gestionen los impactos de las interacciones humanas en la seguridad de los activos en la industria, desarrollando estrategias efectivas para minimizar riesgos y mejorar la seguridad operacional.

Objetivos específicos:

- **Identificar Interacciones Riesgosas:** Reconocer las acciones humanas que representan riesgos para la seguridad de los activos industriales.
- **Desarrollar Controles de Seguridad:** Diseñar e implementar controles operacionales y administrativos que minimicen los riesgos asociados con el error humano.
- **Implementar Tecnología de Soporte:** Utilizar herramientas tecnológicas para reforzar la seguridad y monitorear las interacciones humanas en los entornos de trabajo.
- **Promover Prácticas Seguras:** Fomentar una cultura de seguridad que incentive comportamientos responsables y conscientes entre los empleados.

Contenidos:

- **Fundamentos de la Seguridad de Activos en la Industria:**
  - Introducción a los activos industriales y su importancia.
  - Tipos de riesgos asociados con el comportamiento humano.
- **Evaluación de Riesgos y Gestión de Seguridad:**
  - Métodos para identificar y evaluar riesgos humanos.
  - Creación de planes de gestión de riesgos personalizados.
- **Desarrollo de Controles y Políticas de Seguridad:**
  - Estrategias para desarrollar e implementar controles eficaces.
  - Políticas que reduzcan la incidencia del error humano y mejoren la respuesta a incidentes.
- **Tecnología y Herramientas de Monitoreo:**
  - Innovaciones tecnológicas para la supervisión y control de las interacciones humanas.
  - Implementación de sistemas de alerta temprana y respuesta automática.
- **Cultura de Seguridad y Responsabilidad:**
  - Métodos para construir una cultura de seguridad robusta y sostenible.
  - Enfoques para fomentar la responsabilidad individual y colectiva en la seguridad de los activos.

ANALISIS FORENSE INDUSTRIAL

Créditos: 5

Descripción: Este curso ofrece una comprensión profunda cómo aplicar buenas prácticas en el análisis forense de sistemas de automatización y control industrial. La variedad de los incidentes que pueden producirse en estos entornos es tan diversa que puede considerarse que cada incidente es único, aun tratándose de la misma infraestructura y equipamiento específico, por lo que este módulo será una herramienta imprescindible para evaluar la necesidad de efectuar un análisis forense en ambientes industriales y determinar los criterios que se deben aplicar en el tratamiento de la evidencia electrónica que se encuentra en sistemas críticos.

Objetivo general:

Desarrollar en los estudiantes las habilidades y conocimientos necesarios para la implementación de un análisis forense en un entorno de automatización y control industrial, tomando en cuenta tipología de delitos tecnológicos en una organización industrial, recolección de los indicios digitales y sus características, así como su custodia.

Objetivos específicos:

- Comprender las principales técnicas y herramientas que se pueden utilizar en el análisis forense de un entorno OT, para la gestión adecuada de los indicios digitales en estos entornos.
- Desarrollar la implementación de los procedimientos basados en estándares de un análisis forense en ambientes industriales, que guíen en la creación de informes periciales.
- Identificar la aplicación correcta de leyes internacionales y normativas relevantes al análisis forense industrial, evaluando su impacto en la práctica forense y asegurando el cumplimiento legal durante las investigaciones.

Contenidos:

- Proceso de análisis forense en sistemas de control industrial:
  - Principio de Locard.
  - Tipos de análisis forenses.
  - Normativa internacional.
  - Cadena de custodia.
  - Funciones Hash.
  - Sistemas de ocultación.
  - Volcado de memoria.
  - Extracción de evidencias volátiles, no volátiles y en tránsito.
  - Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales. Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas.
  - Borrado seguro de soportes.
- Proceso de análisis forense en sistemas de control y controladores lógicos programables:
  - Funciones Hash en sistemas.
  - Extracción de evidencias volátiles, no volátiles y en tránsito en sistemas.
  - Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en sistemas.
  - Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en sistemas.
- Desarrollo del proceso de análisis forense en robótica industrial:
  - Funciones Hash en dispositivos industriales.
  - Sistemas de ocultación en dispositivos industriales.
  - Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos industriales.

- Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos industriales. Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos industriales.
- Borrado seguro en dispositivos industriales.

- Proceso de análisis forense en dispositivos del Internet de las cosas (IoT), de sectores industriales y otros:
  - Funciones Hash en dispositivos.
  - Sistemas de ocultación de dispositivos.
  - Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos.
  - Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos.
  - Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos.
  - Borrado seguro en dispositivos.
- Respuesta ante un incidente de ciberseguridad:
  - Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
  - Implantar capacidades de ciberresiliencia.
  - Tareas de restablecimiento de los servicios afectados por incidentes.
  - Documentación y lecciones aprendidas.
  - Notificación del incidente.
- Seguimiento del incidente.

PROYECTO DE INVESTIGACIÓN APLICADA

Créditos: 6

Descripción: El curso de Proyecto de Investigación Aplicada está diseñado para proporcionar a los estudiantes claridad del objeto de estudio que desea conocer, así como los tipos de métodos y técnicas que necesita para la obtención de los datos.

La complejidad del proceso implica necesariamente el desarrollo de unas competencias particulares para que el estudio tenga pertinencia social, sea realmente un aporte al desarrollo de la disciplina o profesión y tenga toda la rigurosidad científica de un nivel doctoral.

En el contexto de una investigación se conceptualiza a las competencias como habilidades, características desarrolladas por medio de un ejercicio sistemático de reflexión y análisis que trascienden meras destrezas. El investigador aprende a aprender, aprende a pensar y aprende a

hacer investigación. No trabaja con intuiciones solamente, tiene saberes construidos de todo tipo que se convierten en indispensables para la construcción y reconstrucción del conocimiento científico

Objetivo general:

Desarrollar competencias avanzadas en la formulación, ejecución y evaluación de proyectos de investigación aplicada en ciberseguridad industrial, con un enfoque en la solución de problemas reales y la generación de conocimientos que contribuyan al desarrollo científico y tecnológico en dicho campo de estudio.

Objetivos específicos:

1. Adquirir conocimientos teóricos y metodológicos necesarios para diseñar proyectos de investigación aplicada en ciberseguridad industrial, incluyendo la identificación de problemas relevantes, la formulación de hipótesis, y la selección de métodos y técnicas adecuadas para la recolección y análisis de datos de ambientes industriales.

2. Desarrollar habilidades prácticas en la implementación de investigaciones aplicadas a la ciberseguridad de los ambientes industriales, gestionando eficientemente los recursos y tiempos, y aplicando técnicas avanzadas de análisis para interpretar los resultados y generar conclusiones válidas y útiles.
3. Fortalecer la capacidad de comunicación y difusión de los resultados de la investigación, mediante la elaboración de informes técnicos, artículos científicos y presentaciones orales, dirigidos a diferentes audiencias, incluyendo la comunidad académica, los sectores productivos y el público en general.

Contenidos:

- Introducción a la Investigación Aplicada
  - Definición y características de la investigación aplicada.
  - Diferencias entre investigación básica y aplicada.
  - Importancia y aplicaciones de la investigación aplicada en diferentes campos.
- Formulación de Problemas de Investigación
  - Identificación y selección de problemas de investigación relevantes.
  - Planteamiento de preguntas de investigación y objetivos.
  - Revisión de la literatura: cómo realizarla y su importancia en la investigación aplicada.
  - Formulación de hipótesis y/o marco teórico.
- Diseño Metodológico de la Investigación
  - Métodos y enfoques de investigación: cualitativos, cuantitativos y mixtos.
  - Tipos de diseños de investigación aplicada: experimental, cuasi-experimental, estudios de caso, etc.
  - Selección y justificación del diseño metodológico.

    - Consideraciones éticas en la investigación aplicada.
- Técnicas de Recolección de Datos
    - Instrumentos de recolección de datos: encuestas, entrevistas, observación, análisis documental, etc.
    - Diseño y validación de instrumentos.
    - Muestreo: tipos y técnicas.
    - Procedimientos para la recolección de datos.
- Análisis de Datos
    - Introducción al análisis estadístico y cualitativo de datos.
    - Técnicas avanzadas de análisis: análisis multivariante, análisis de contenido, análisis de redes, etc.
    - Uso de software especializado para el análisis de datos.
    - Interpretación de resultados y generación de conclusiones.
- Gestión y Planificación de la Investigación
    - Planificación de proyectos de investigación aplicada: cronogramas, recursos y presupuesto.
    - Gestión de la investigación: supervisión, control de calidad, y manejo de equipos de trabajo.
    - Documentación y registro del proceso de investigación.
- Comunicación y Difusión de Resultados
    - Elaboración de informes técnicos y científicos.
    - Redacción de artículos para revistas científicas.
    - Preparación y presentación de resultados a diferentes audiencias.
    - Estrategias de difusión y transferencia del conocimiento.
- Evaluación y Aplicación de la Investigación
    - Evaluación del impacto de la investigación aplicada.
    - Aplicación de los resultados en la solución de problemas reales.
    - Innovación y desarrollo tecnológico a partir de la investigación.
    - Reflexión crítica sobre los desafíos y limitaciones de la investigación aplicada.
- Estudios de Caso y Talleres Prácticos
    - Análisis de estudios de caso relevantes en el campo de estudio.
    - Talleres de formulación y ejecución de proyectos de investigación aplicada.
    - Simulación y resolución de problemas aplicados.
- Proyecto Final
    - Desarrollo de un proyecto de investigación aplicada desde la identificación del problema hasta la comunicación de los resultados.
    - Evaluación integral del proyecto, incluyendo retroalimentación por parte de pares y docentes.

CURSOS OPTATIVOS DE LA MAESTRÍA EN CIBERSEGURIDAD INDUSTRIAL

INTELIGENCIA ARTIFICIAL PARA CIBERSEGURIDAD I

Créditos: 3

Descripción: El curso de Ciberseguridad en Inteligencia Artificial está diseñado para proporcionar a los estudiantes una comprensión integral de cómo la inteligencia artificial (IA) puede ser utilizada para mejorar la ciberseguridad. Se enfoca en la aplicación de técnicas de automatización, aprendizaje de máquina y análisis de patrones para la detección y mitigación de amenazas cibernéticas

Objetivo general:

Desarrollar un análisis comprensivo de la Inteligencia Artificial (IA) en Ciberseguridad Industrial que fortalezcan la ciberseguridad, mediante el uso de técnicas avanzadas de aprendizaje de máquina para la detección y prevención de amenazas, incluyendo la protección de entornos en la nube y la identificación de malware.

Objetivos específicos:

1. Integrar tecnologías de IA con plataformas de gestión de seguridad en la nube para la automatización la respuesta a incidentes y mitigación de riesgos.
2. Comprender los modelos de IA para la identificación y clasificación de diferentes tipos de malware basados en análisis de comportamiento, sus características estáticas y dinámicas, que sirvan en la optimización de procesos industriales.
3. Desarrollar estrategias de comprensión de algoritmos de aprendizaje de máquina para el análisis de grandes volúmenes de datos de red y la detección de patrones de comportamiento anómalo en tiempo real, asegurando la continuidad del negocio.

Contenidos:

- Introducción a la Ciberseguridad y la IA
  - Conceptos básicos de ciberseguridad
  - Introducción a la inteligencia artificial y el aprendizaje de máquina
- Automatización de Procesos en Ciberseguridad
  - Uso de IA para la automatización de tareas de ciberseguridad
  - Casos de uso y herramientas de automatización
- Aprendizaje de Máquina en Ciberseguridad
  - Técnicas de aprendizaje supervisado y no supervisado
  - Aplicación de algoritmos de aprendizaje de máquina para la detección de amenazas
- Detección de Amenazas de Red con IA

- Análisis de tráfico de red y detección de intrusos
- Herramientas y técnicas de detección basadas en IA

- Detección de Malware con IA
  - Técnicas de análisis y clasificación de malware
  - Implementación de modelos de IA para la detección de malware
- Análisis de Patrones y Algoritmos de Aprendizaje
  - Análisis de patrones de comportamiento en redes y sistemas
  - Desarrollo e implementación de algoritmos de aprendizaje para la ciberseguridad

INTELIGENCIA ARTIFICIAL PARA CIBERSEGURIDAD II

Créditos: 3

Descripción: Este curso proporcionará a los estudiantes conocimientos avanzados y habilidades prácticas en la intersección de la ciberseguridad automotriz y la inteligencia artificial (IA). Los estudiantes aprenderán a proteger sistemas automotrices contra amenazas cibernéticas mediante el uso de algoritmos de aprendizaje automático y técnicas de IA.

Objetivo general:

Desarrollar un aprendizaje profundo en ciberseguridad automotriz, utilizando inteligencia artificial para la detección, prevención y mitigación de amenazas cibernéticas, mediante la implementación de controles de seguridad específicos, el cumplimiento del estándar ISO/SAE21434 y la automatización de procesos, garantizando la seguridad y protección de los sistemas automotrices modernos.

Objetivos específicos:

1. Integrar soluciones basadas en IA en sistemas de ciberseguridad automotriz para mejorar la respuesta y mitigación de ataques, evaluando la efectividad de estas soluciones en escenarios de prueba.
2. Comprender las tecnologías de automatización para la realización de pruebas de seguridad y análisis de vulnerabilidades en sistemas automotrices, que optimicen dichos procesos industriales.
3. Desarrollar estrategias de comprensión de los requisitos del estándar ISO/SAE21434 para la gestión de ciberseguridad en el ciclo de vida de los sistemas automotrices.

Contenidos:

- Introducción a la Ciberseguridad Automotriz
  - Historia y evolución de la seguridad en vehículos.

    - Conceptos básicos de ciberseguridad y su importancia en la industria automotriz.
- Automatización de Procesos en la Ciberseguridad Automotriz
    - Introducción a la automatización de procesos.
    - Herramientas y técnicas de automatización en ciberseguridad.
    - Aplicaciones prácticas en sistemas automotrices.
- Ingeniería de la Seguridad Automotriz
    - Principios de ingeniería de seguridad.
    - Arquitectura de seguridad en vehículos.
    - Evaluación y mitigación de riesgos en sistemas automotrices.
- Estándar ISO/SAE21434
    - Descripción del estándar ISO/SAE21434.
    - Implementación de los requisitos del estándar en sistemas automotrices.
    - Casos de estudio y mejores prácticas.
- Modelado de Amenazas para Sistemas Automotrices
    - Introducción al modelado de amenazas.
    - Técnicas de modelado de amenazas específicas para sistemas automotrices.
    - Herramientas de modelado de amenazas y análisis de casos.
- Controles de Seguridad para ECU
    - Introducción a las Unidades de Control Electrónico (ECU).
    - Controles y técnicas de seguridad para proteger las ECU.
    - Implementación práctica de controles de seguridad.
- Algoritmos de Aprendizaje Automático en Ciberseguridad Automotriz
    - Fundamentos de aprendizaje automático.
    - Aplicaciones de IA en la detección y mitigación de amenazas.
    - Desarrollo e implementación de algoritmos de aprendizaje para la ciberseguridad.

Anexo C

Personas docentes de los cursos de la de la Maestría Profesional en Ciberseguridad Industrial de la Universidad Nacional

Nombre del curso	Docentes propuestos
Ciberseguridad industrial, Análisis forense industrial	Randall Barnett Villalobos
Metodologías éticas para pruebas de seguridad, Seguridad humana para ambientes industriales	Rodrigo Calvo Solano
Seguridad de la información I, Optativo I	Alex Villegas Carranza
Investigación aplicada a la Ciberseguridad I, Proyecto de investigación aplicada	Edgar Vega Briceño
Seguridad de la información II, Optativo II	Enrique Gómez Jiménez
Aspectos legales y regulatorios de la información	Roberto Lemaitre Picado
Investigación aplicada a la Ciberseguridad II	Ronny González
Seguridad de componentes y redes industriales	José Ibarra
Software industrial	Pablo López Aguilar
Análisis de datos industriales	Oscar Ramírez

Cursos optativos	Docentes
Inteligencia Artificial para ciberseguridad I	Alex Villegas Carranza
Inteligencia Artificial para ciberseguridad II	Enrique Gómez Jiménez

Anexo D
Personal docente de la Maestría Profesional en Ciberseguridad Industrial de la Universidad Nacional y sus grados académicos

Nombre	Grado académico	Título	Universidad
Randall Barnett Villalobos	Maestría	Máster en computación e Informática	Universidad de Costa Rica (UCR)
Rodrigo Calvo Solano	Maestría	Maestría en Administración de Recursos Informáticos	Universidad Latina de Costa Rica
Alex Villegas Carranza	Maestría	Máster en Ciberseguridad	Universidad CENFOTEC
Edgar Vega Briceño	Maestría	Máster en Administración de Tecnología de Información con Énfasis en Proyectos Informáticos	Universidad Nacional (UNA)
Enrique Gómez Jiménez	Maestría	Máster en Gestión de la Innovación Tecnológica	Universidad Nacional (UNA)
Roberto Lemaitre Picado	Maestría	Máster en Ciencias de la Computación	Universidad de Costa Rica (UCR)
Ronny González Hernández	Maestría	Máster en Administración de Proyectos	Universidad para la Cooperación Internacional (UCI)
Pablo López Aguilar	Maestría	Master en Telemática	Universidad Latina de Costa Rica
Oscar Ramírez Rodriguez	Maestría	Máster en Ciberseguridad Ciberseguridad	Universidad CENFOTEC

CONSEJO NACIONAL
DE RECTORES

UCR

TEC

UNA

UNED

UTN
Universidad
Técnica Nacional