Mar del Plata, 21 de agosto de 2020.-

RESOLUCIÓN DEL RECTORADO Nº 281/20

VISTO:

El Proyecto de Desarrollo Tecnológico Social "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI*****"** presentado por el Señor Decano de la Facultad de Ingeniería y;

CONSIDERANDO:

Que el Proyecto de Desarrollo Tecnológico Social - PDTS "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI*****"** ha sido formulado por su director, Ing. Santiago José Trigo por la Facultad de Ingeniería Universidad FASTA, la co-dirección del Dr. Jorge Kamlofsky de la Facultad de Tecnología Informática de la UAI y del Coronel Mayor Ingeniero Macos Horacio Mansilla de la Facultad de Ingeniería del Ejército de la Universidad de la Defensa Nacional;

Que el mencionado PDTS será co-ejecutado por el Grupo de Investigación Informática Forense de la Facultad de Ingeniería de la Universidad FASTA, la Facultad de Tecnología Informática de la Universidad Abierta Interamericana y la Facultad de Ingeniería del Ejército de la Universidad de la Defensa Nacional;

Que la suscripción del proyecto por parte de sus directores implica el compromiso ético del equipo de desarrollo, manifestando explícitamente que su trabajo, objetivos y métodos respetan los códigos de ética profesional nacionales e internacionales y que no contradicen los principios éticos y valores de la Universidad FASTA;

Que la Universidad FASTA ha suscripto los convenios y/o instrumentos necesarios con las partes involucradas en el mencionado PDTS, donde constan los roles y compromisos de cada una;

Que el mencionado PDTS cuenta con el aval de la Secretaria de Investigación de la Facultad de Ingeniería y la Secretaria de Proyección de la Facultad de Ingeniería, que han verificado la factibilidad del proyecto, la disponibilidad del presupuesto y los recursos necesarios al efecto y la pertinencia respecto de la política y las líneas de investigación y extensión definidas en la Unidad Académica.

Que el mencionado PDTS ha sido evaluado por reconocidos especialistas en la temática, convocados al efecto por la Secretaría de Investigación de la Facultad de Ingeniería, que han recomendado su aprobación, conforme los lineamientos y criterios establecidos por la Secretaría de Articulación Científico

Tecnológica del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación Argentina para la acreditación de PDTSs;

Que el mencionado PDTS cuenta con el aval del decano de la Facultad de Ingeniería, que lo eleva para su aprobación, comprometiendo la afectación de los recursos necesarios para el desarrollo del proyecto;

Que el mencionado PDTS cuenta con el aval de la Secretaria de Investigación de la Universidad FASTA, habiendo verificado el cumplimiento de los aspectos metodológicos y formales del proyecto;

Que el mencionado PDTS cuenta con el aval del Vicerrector de Asuntos Económicos de la Universidad FASTA, garantizando la disponibilidad del presupuesto necesario para el desarrollo del proyecto;

Que el mencionado PDTS cuenta con el aval del Vicerrector Académico de la Universidad FASTA, garantizando el cumplimiento del debido proceso del expediente y las conformidades requeridas

Por ello, y en uso de las atribuciones que le confieren los Arts. 28º inc. c) y concordantes del Estatuto Universitario

EL RECTOR DE LA UNIVERSIDAD FASTA

DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMÁS DE AQUINO

R E S U E L V E :

Artículo 1º.- APROBAR el Proyecto de Desarrollo Tecnológico Social "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI*****"** presentado por la Facultad de Ingeniería, que consta en el Anexo I de la presente, y que será co-ejecutado por el Grupo de Investigación Informática Forense de la Facultad de Ingeniería, la Facultad de Tecnología Informática de la Universidad Abierta Interamericana y la Facultad de Ingeniería del Ejército de la Universidad de la Defensa Nacional, bajo la dirección del Ing. Santiago José Trigo por la Facultad de Ingeniería Universidad FASTA, la co-dirección del Dr. Jorge Kamlofsky de la Facultad de Tecnología Informática de la UAI y del Coronel Mayor Ingeniero Macos Horacio Mansilla de la Facultad de Ingeniería del Ejército de la Universidad de la Defensa Nacional.

Artículo 2º.- GARANTIZAR la afectación del presupuesto, las designaciones y los recursos necesarios para llevar adelante el Proyecto de Desarrollo Tecnológico Social "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI*****"** conforme lo previsto en el Anexo I de la presente y los convenios correspondientes.

Artículo 3º.- ELEVAR el Proyecto de Desarrollo Tecnológico Social "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI*****"** a la

Secretaría de Articulación Científico Tecnológica del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación Argentina a efectos de su acreditación.

Artículo 4º.- NOTIFÍQUESE al director del Proyecto de Desarrollo Tecnológico Social "***Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI***"**,** al Sr. Decano de la Facultad de Ingeniería, a la Secretaría de Investigación y vicerrectorados de la Universidad FASTA, y a las entidades involucradas en el proyecto y archívese.

PROF MARCELA S. GREGA de CHACHAGUA
SECRETARIA GENERAL
UNIVERSIDAD FASTA

DR. JUAN CARLOS MENA
RECTOR
UNIVERSIDAD FASTA

ANEXO RESOLUCIÓN DEL RECTORADO N°281/20

PROYECTO de INVESTIGACIÓN

Proyecto de Desarrollo Tecnológico y Social

Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. GUIA-ICI

1. EL PROYECTO DE DESARROLLO TECNOLÓGICO SOCIAL

TÍTULO O DENOMINACIÓN DEL PROYECTO Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales
ACRÓNIMO GUIA-ICI

MES Y AÑO DE INICIO: 08/2020
MES Y AÑO DE FINALIZACIÓN: 07/2023

ÁREA DE CONOCIMIENTO: CIENCIAS TECNOLÓGICAS (33)
SUB-ÁREA DE CONOCIMIENTO: OTRAS ESPECIALIDADES TECNOLÓGICAS (3399)

2. INSTITUCIONES PARTICIPANTES

INSTITUCIÓN/ES EJECUTORA/S DEL PROYECTO: • UNIVERSIDAD FASTA. FACULTAD DE INGENIERÍA. • UNIVERSIDAD ABIERTA INTERAMERICANA. FACULTAD DE TECNOLOGÍA INFORMÁTICA • UNIVERSIDAD DE LA DEFENSA NACIONAL. FACULTAD DE INGENIERÍA DEL EJÉRCITO.
CENTRO/S DE INVESTIGACIÓN EJECUTOR/ES: • UNIVERSIDAD FASTA. LABORATORIO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA EN INFORMÁTICA FORENSE • UNIVERSIDAD ABIERTA INTERAMERICANA. CENTRO DE ALTOS ESTUDIOS EN TECNOLOGÍA INFORMÁTICA. • UNIVERSIDAD DE LA DEFENSA NACIONAL. FACULTAD DE INGENIERÍA DEL EJÉRCITO. LABORATORIO DE REDES Y CIBERSEGURIDAD TI.
INSTITUCIÓN QUE PRESENTA EL PROYECTO: UNIVERSIDAD FASTA

ENTIDAD/ES FINANCIADORA/S DEL PROYECTO: • UNIVERSIDAD FASTA. FACULTAD DE INGENIERÍA • UNIVERSIDAD ABIERTA INTERAMERICANA. FACULTAD DE TECNOLOGÍA INFORMÁTICA. • UNIVERSIDAD DE LA DEFENSA NACIONAL. FACULTAD DE INGENIERÍA DEL EJÉRCITO.
INSTITUCIÓN/ES ADOPTANTE/S DEL PROYECTO: • TREND INGENIERÍA • COMANDO CONJUNTO DE CIBERDEFENSA (ELEMENTO OPERATIVO) • DIRECCIÓN DE CIBERDEFENSA DEL EJÉRCITO (ELEMENTO OPERATIVO) • FACULTAD DE INGENIERÍA DEL EJÉRCITO (DIFUSOR DEL CONOCIMIENTO CIENTÍFICO - TECNOLÓGICO DE CIBERDEFENSA Y CIBERSEGURIDAD EN EL EJÉRCITO ARGENTINO)
INSTITUCIÓN/ES DEMANDANTE/S DEL PROYECTO • TREND INGENIERÍA • DIRECCIÓN NACIONAL DE CIBERSEGURIDAD (JEFATURA DE GABINETE DE MINISTROS, PRESIDENCIA DE LA NACIÓN)
INSTITUCIÓN/ES PROMOTORA/S DEL PROYECTO *(si la/s hubiera)*:

3. DIRECTOR

NOMBRE Y APELLIDO DEL DIRECTOR DEL PROYECTO: ING. SANTIAGO TRIGO
DIRECCIÓN DE CONTACTO DEL DIRECTOR (TELEFÓNICA Y/O ELECTRÓNICA): SANTIAGOTRIGO@UFASTA.EDU.AR **(0223)570 3825**
NOMBRE Y APELLIDO DEL CO-DIRECTOR: DR. JORGE KAMLOFSKY
DIRECCIÓN DE CONTACTO DEL CO-DIRECTOR (TELEFÓNICA Y/O ELECTRÓNICA): JORGE.KAMLOFSKY@UAI.EDU.AR **(011) 5742 4180**
NOMBRE Y APELLIDO DEL CO-DIRECTOR: CORONEL MAYOR (R) **INGENIERO MARCOS HORACIO MANSILLA**
DIRECCIÓN DE CONTACTO DEL DIRECTOR (TELEFÓNICA Y/O ELECTRÓNICA): MHMANSILLA@FIE.UNDEF.EDU.AR **(011) 58722459**

4. EQUIPO DE TRABAJO

NOMBRE Y APELLIDO	INSTITUCIÓN –UNIDAD/ES ACADÉMICA/S	FUNCIÓN(
Santiago Trigo	UFASTA - Facultad de Ingeniería	Director
Jorge Kamlofsky	UAI - Facultad de Tecnología Informatica	Co-Director

Marcos Mansilla	UNDEF - FIE	Co-Director
Bruno Constanzo	UFASTA - Facultad de Ingeniería	Investigador
Hugo Curti	UFASTA - Facultad de Ingeniería	Investigador
Juan Alberdi	UFASTA - Facultad de Ingeniería	Investigador
Gonzalo Ruiz de Angeli	UFASTA - Facultad de Ingeniería	Investigador
Leandro Ferrari	UFASTA - Facultad de Ingeniería	Investigador
Enrique Belaustegui	UAI- Facultad de Tecnología Informática	Becario
Pedro Hecht	UAI - Facultad de Tecnología Informática	Investigador
Claudio Milio	UAI - Facultad de Tecnología Informática	Investigador
Oscar Romero	UAI - Facultad de Tecnología Informática	Investigador
Pablo Croci	UNDEF - FIE	Investigador
Nicolás Díaz País	UNDEF - FIE	Investigador
Rafael Olivieri	UNDEF - FIE	Investigador
Juan Ignacio Raffo Triacca	UNDEF - FIE	Desarrollador / Tecnólogo
Ignacio Omaechevarría	UNDEF - FIE	Desarrollador / Tecnólogo

5. CARACTERIZACIÓN DEL PROYECTO

PROBLEMA O NECESIDAD A RESOLVER (*máximo 150 palabras de descripción*):

La automatización de los procesos industriales se ha convertido en un proceso clave en la industria, y ha abierto las puertas a la Industria 4.0. En Argentina, la automatización industrial se encuentra presente en varios procesos, como por ej.: Semaforización, Luz eléctrica, Agua corriente, entre otros, muchos de los cuales forman parte de la denominada “infraestructura crítica”, tanto en el ámbito privado como del Estado.

Estos sistemas de automatización y control de procesos no pueden apagarse, lo que podría generar que su sistema operativo no se actualice y podría generar una puerta de entrada tanto para el robo de información como para la modificación de procesos, entre otros.

Las infraestructuras críticas industriales, ante esta situación, precisan contar con una guía que contemple tanto una evaluación del riesgo, como recomendaciones para mitigarlo e instrucciones de actuación básica de primera respuesta a incidentes y análisis forense básico en automatización Industrial.

PRODUCTO O PROCESO A GENERAR (*máximo 150 palabras)*

El proyecto busca desarrollar una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales compuesta por tres secciones:

- Evaluación de Riesgos de Seguridad Informática en Sistemas de Automatización.

- Recomendaciones para Mitigar los riesgos de Sistemas de Automatización.
- Actuación para dar Respuesta a Incidentes y Análisis Forense en Sistemas de Automatización.

Esta guía permitirá trabajar tanto ex ante (prevención) como ex post (actuación, remediación, análisis forense) en el abordaje de incidentes de ciberseguridad en infraestructuras que requieren una gestión de extrema seguridad, por su condición de criticidad para la propia organización y la población en general; especialmente, en instalaciones industriales del Estado o de empresas que brindan servicios esenciales (agua, energía, comunicaciones, combustibles, etc). Un problema de seguridad en estas instalaciones puede significar el colapso de servicios vitales para la población. De ahí la importancia de desarrollar un producto tecnológico de soporte a la gestión.

RESUMEN, DETALLANDO OBJETIVOS Y ACTIVIDADES DEL PROYECTO *(máximo 250 palabras)***:**

El proyecto tiene el objetivo de desarrollar una guía basada en tres aspectos básicos: la evaluación de riesgos de seguridad en infraestructuras críticas industriales, las recomendaciones para mitigar estos riesgos y las instrucciones de actuación para dar respuesta a los incidentes de seguridad detectados y para el análisis forense.

El tiempo previsto de desarrollo es de 36 meses, conforme a la siguiente planificación:

Etapa 1: Relevamiento y análisis de documentos y guías de buenas prácticas en la temática.

Etapa 2: Extracción de Requerimientos de la Guía de Evaluación de Riesgos.

Etapa 3: Desarrollo de la Guía de Evaluación de Riesgos.

Etapa 4: Aplicación, prueba piloto y validación de la Guía de Evaluación de Riesgos por parte del adoptante.

Etapa 5: Extracción de Requerimientos de la Guía de Recomendaciones.

Etapa 6: Desarrollo de la Guía de Recomendaciones para mitigación de Riesgos.

Etapa 7: Aplicación, prueba piloto y validación de la Guía de Mitigación de Riesgos por parte del adoptante.

Etapa 8: Extracción de Requerimientos de la Guía de Actuación para Respuesta a Incidentes y Análisis Forense Básico.

Etapa 9: Desarrollo de la Guía de Actuación.

Etapa 10: Aplicación, prueba piloto y validación de la Guía de Actuación para dar respuesta a incidentes y análisis forense básico en Infraestructuras críticas industriales por parte del adoptante.

Etapa 11: Ajustes a las guías. Conclusiones e informe final del proyecto.

Las pruebas se realizarán Tred Ingeniería para aplicarlas, luego de validadas en ese terreno, en las infraestructuras críticas de los adoptantes del Estado nacional.

NOVEDAD U ORIGINALIDAD LOCAL EN EL CONOCIMIENTO *(máximo 250 palabras)*[)]**:**

La conexión de una instalación industrial a Internet requiere de ciertas garantías de seguridad; más aún cuando se trata de infraestructuras críticas, ya que son un blanco fácil para ataques informáticos, sobre todo si estos dispositivos deben permanecer en funcionamiento 7x24 y su mal funcionamiento o ataque puede ocasionar perjuicios a la población como en los sistemas industriales de potabilización de agua, energía, comunicaciones, salud, etc.

No existen guías ni protocolos pensados para el abordaje de las cuestiones de ciberseguridad en Infraestructuras Críticas a nivel general. La Dirección Nacional de Ciberdefensa los requiere y demanda con urgencia para cumplir su misión. Este proyecto pretende desarrollar una guía aplicable a cualquier sistema de automatización industrial de misión crítica, lo que requiere del desarrollo de algoritmos de verificación y control ad hoc con un enfoque multidisciplinario y multidimensional inédito que significa, por sí mismo, un avance cognitivo importante para el país en la temática. Además, permite que este conocimiento sea estrictamente ajustado a la Estrategia Nacional de Ciberseguridad y la normativa relacionada, garantizando una solución concreta y pertinente en función de la realidad y demanda nacional.

Esta herramienta, de suma utilidad para responsables de ciberseguridad en instalaciones industriales y que no tiene precedentes en Argentina, permitirá no solo contribuir a la gestión de la ciberseguridad y su fortalecimiento, sino también a la tarea de los organismos de contraloría del Estado que deben verificar las condiciones en las que operan las empresas proveedoras de servicios esenciales.

GRADO DE RELEVANCIA *(máximo 250 palabras)***:**

En el marco de la Estrategia Nacional de Ciberseguridad, la Resolución N°1523/2019 define las infraestructuras críticas como “aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente” y las infraestructuras críticas de información como “las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas.”

Se estima que los ataques a infraestructuras críticas y servicios públicos aumenten en gran medida cada año y que los conflictos entre países estarán basados en ataques informáticos. Entre los ataques más comunes y perjudiciales a las industrias se pueden mencionar el ransomware y el phishing.

Resulta de suma relevancia contar con una guía que contemple las medidas de seguridad informática imprescindibles para el abordaje de la problemática en infraestructuras que puedan generar el colapso de los servicios esenciales para la población, además de reducir los riesgos, ya sean monetarios, de reputación o físicos, que podrían ocasionarse ante un ataque informático.

La adopción de esta guía por parte del Comando Conjunto de Ciberdefensa y la Dirección de Ciberdefensa del Ejército evidencian su relevancia, tanto como producto, como solución, dado que les permitirá dar garantías de seguridad a la Nación en las infraestructuras críticas de sus dependencias y las que controlan (Dirección Nacional de Ciberdefensa).

GRADO DE PERTINENCIA *(máximo 250 palabras)* **:**

El equipo de investigadores de la Universidad FASTA cuenta con una larga trayectoria participando en Proyectos de Desarrollo Tecnológico y Social vinculados a la informática forense, y los investigadores tienen amplia experiencia en seguridad informática.

En el ámbito de la UAI, hay 5 tesis de grado en desarrollo relacionadas con Ciberdefensa en Infraestructuras críticas y otras 3 en sus inicios, todas en marco del proyecto de investigación denominado "Ciberdefensa en Redes Industriales" radicado en el Centro de Altos Estudios en Tecnología Informática. Este proyecto cuenta con una patente y un banco de pruebas de un sistema industrial.

El equipo de investigadores de la FIE tiene formación y experiencia en implementación de seguridad de infraestructuras de TI en el ámbito de las FFAA y en su equipo se integran las capacidades actuales de los laboratorios de Redes y Ciberseguridad TI, y de Informática Forense. Entre los investigadores existe personal con formación tanto del área de Informática como de Electrónica, cuya convergencia es pertinente para el desarrollo del proyecto. Los investigadores con formación en ingeniería militar también tienen formación en operaciones militares sobre infraestructuras críticas militares y operaciones de ciberdefensa.

El trabajo conjunto con Trend Ingeniería (uno de los líderes nacionales en Automatización Industrial) permite contar con experiencia "en el terreno" de las instalaciones industriales y hacer que esta confluya sinérgicamente con la experiencia y conocimientos científicos universitarios para concretar el desarrollo de una solución inédita que permita minimizar los efectos del riesgo constante de este tipo de infraestructuras.

GRADO DE DEMANDA *(máximo 250 palabras)*[j]:

En este PDTS están claramente identificados y formalmente comprometidos los agentes demandantes y adoptantes.

La demanda surge del requerimiento conjunto de Trend Ingeniería a la UAI y de la Dirección Nacional de Ciberseguridad al InFo-Lab para el desarrollo de una solución tecnológica de vital importancia para la ciberseguridad en infraestructuras críticas que la primera gestiona y cuya responsabilidad primaria recae sobre la segunda en aquellas que son instalaciones del Estado o concesionadas de servicios vitales. Luego se suma la FIE al proyecto, que lleva ya más de 6 años de trabajo conjunto con el InFo-Lab. Asimismo, se suman como adoptantes el Comando Conjunto de Ciberdefensa y la Dirección de Ciberdefensa del Ejército Argentino para implementar la guía en las infraestructuras críticas de sus dependencias y las que controlan o verifican.

El resultado que se busca atiende a las necesidades concretas de los demandantes-adoptantes identificables en la industria que requiere del auxilio científico-tecnológico para el desarrollo de una guía que integre algorítmica, procesos, métodos, técnicas y herramientas especialmente desarrolladas, en un único producto que suponga un avance cognitivo importante, sólo posible a partir del trabajo interinstitucional e interdisciplinario.

En síntesis, esta guía será una herramienta clave para sus adoptantes y demandantes, organismos claves del Estado que tienen una responsabilidad vital en lo que hace a la ciberdefensa nacional y les permitirá implementar políticas y medidas innovadoras, con enfoque multidisciplinario y multidimensional, con gran valor agregado de conocimiento para la defensa de nuestro país y su población.