REGISTRADO

Firmado digitalmente por: AUBURIEL PABLO ARIEL
Fecha y hora: 30.08.2022 18:51:59
JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

Ministerio de Educación
Universidad Tecnológica Nacional
Rectorado

APRUEBA CURSO DE ACTUALIZACIÓN DE POSGRADO

Buenos Aires, 10 de agosto de 2022

VISTO la Resolución Nº 345/22 del Consejo Directivo de la Facultad Regional Villa María, a través de la cual solicita la aprobación y autorización de implementación del Curso de Actualización de Posgrado "Análisis Forense de Evidencias Digitales e Incidentes de Ciberseguridad", y

CONSIDERANDO:

Que el Curso propuesto responde a la necesidad de brindar a docentes y graduados de la Universidad, conocimientos, metodologías y herramientas que les permitan comprender acerca del rol, alcance y responsabilidades de quienes deseen actuar como Perito Informático y/o Analista Forense Digital.

Que la Facultad Regional Villa María cuenta con un plantel de profesores de elevado nivel académico y profesional, además de una prolongada y amplia experiencia en el dictado de cursos y seminarios vinculados al propuesto.

Que la Comisión de Posgrado de la Universidad ha analizado los antecedentes que acompañan la solicitud y avala la presentación, y la Comisión de Ciencia, Tecnología y Posgrado recomienda su aprobación.

Que el dictado de la medida se efectúa en uso de las atribuciones otorgadas por el Estatuto Universitario.

Por ello,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD TECNOLÓGICA NACIONAL

ORDENA:

REGISTRADO

PABLO A. HUEL

JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

Ministerio de Educación
Universidad Tecnológica Nacional
Rectorado

ARTÍCULO 1°.- Aprobar el currículo del Curso de Actualización de Posgrado "Análisis Forense de Evidencias Digitales e Incidentes de Ciberseguridad", que figura en el Anexo I y es parte integrante de la presente Ordenanza.

ARTÍCULO 2°.- Autorizar el dictado del mencionado curso en la Facultad Regional Villa María y avalar la propuesta del Cuerpo Docente que figura en el Anexo II y es parte integrante de la presente Ordenanza.

ARTÍCULO 3°.- Establecer que la propuesta mencionada en el Articulo precedente quedará supeditada al cronograma de dictado de las correspondientes actividades académicas de la Facultad Regional.

ARTÍCULO 4°.- Regístrese. Comuníquese y archívese.

ORDENANZA Nº 1884

UTN
l.p.
p.f.d.
m.m.m.

ING. RUBÉN SORO
RECTOR

ING. PABLO ANDRÉS ROSSO
Secretario del Consejo Superior

REGISTRADO

PABLO A. HUEL
JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

Ministerio de Educación
Universidad Tecnológica Nacional
Rectorado

ORDENANZA Nº 1884

ANEXO I

CURSO DE ACTUALIZACIÓN DE POSGRADO

"ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES E INCIDENTES DE CIBERSEGURIDAD"

1. FUNDAMENTACIÓN Y JUSTIFICACIÓN

Las tecnologías de la información y de las comunicaciones (TIC) han invadido todas las áreas de la sociedad. El quehacer diario de las personas está vinculado de una forma u otra a las tecnologías informáticas, ya sea como usuario final mediante un celular, una PC o una Tablet, o como entidad que cumple un rol social, económico o comunitario, en el cual exige a sus integrantes una interacción virtual.

Esta inclusión de las tecnologías en la sociedad ha posibilitado importantes mejoras en las actividades en general, notándose su mayor impacto en el ámbito de las comunicaciones interpersonales mediante las redes sociales, la mensajería instantánea y el correo electrónico.

Pero de igual forma, así como ha favorecido la vida de las personas, también se utiliza para el desarrollo de actividades delictivas, en las cuales las TIC participan con idéntica fuerza que en el resto de los quehaceres sociales.

Ubicados en el contexto legal, a partir de 1990 surge la necesidad de convocar a peritos informáticos para que actúen como auxiliares de la justicia cuando se presenta una prueba digital. Con el transcurso del tiempo, y la evolución de las tecnologías, esta primera acción del profesional informático que solo hacía un aporte técnico pasó a convertirse en una rama de la disciplina informática con entidad propia.

Proveniente de la Informática aplicada, el desarrollo de la Informática Jurídica tuvo una variante distintiva cuando se abordaron las pericias informáticas. Así, surge primeramente la Informática Forense y se transforma en lo que hoy se conoce como Forensia Digital.

A partir del año 2000, comienzan a surgir los ataques a la seguridad informática, lo que produce un crecimiento en las normas y procesos necesarios para atender la problemática de hacking e intrusión sobre los sistemas informáticos. Ya en el 2005, con la incorporación de aplicaciones web, se hace más crítica la cuestión de la seguridad y resguardo de los datos, al punto de tener que generar esquemas de seguimiento y búsqueda de vulnerabilidades. Aparecen nuevas formas de la seguridad informática (hacking ético, por ejemplo) y allí se formaliza la Forensia Digital, para dar una respuesta al análisis de los incidentes de seguridad informática.

Por su parte, la Informática Forense toma para sí las herramientas y métodos de la Forensia Digital y le agrega algunos de los procedimientos propios de la criminalística como la cadena de custodia.

Se toma como definición de Informática Forense la propuesta por el Grupo de Investigación en Sistemas Operativos e Informática Forense de la UFASTA (Di Ioro et al., 2017) que dice: La Informática Forense es considerada una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital.

Asimismo, se adhiere a la definición de Forensia Digital propuesta por (Zuccardi et al., 2006) que dice: Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?,

¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Luego del 2020, y como producto de la virtualización de las actividades comerciales y sociales debido a la situación de la pandemia COVID-19, se observó un crecimiento alarmante de los ciberdelitos con el surgimiento de Nuevos Escenarios Virtuales para Comisión de Delitos que, en términos de la Seguridad Informática, están requiriendo de Analistas Forenses capacitados en el manejo de la evidencia, cuando se trabaja en la gestión de incidentes de Ciberseguridad.

La Forensia Digital se aplica principalmente en dos áreas: en el ámbito de la justicia mediante las pericias informáticas con la inclusión de las evidencias digitales, y en el ámbito empresarial cuando se considera la gestión de incidentes de ciberseguridad.

Con la intención de iniciar al asistente en la realización del Análisis Forense Digital, se presenta el contexto de la Forensia Digital y se lo capacitará dotándolos de conocimientos, metodologías y herramientas que les permitan comprender acerca del rol, alcance y responsabilidades de quienes deseen actuar como Perito Informático y/o Analista Forense Digital.

Se abordarán cuestiones pluridisciplinarias que promueven un análisis forense más eficiente cuando se aborda desde el campo judicial, conformando equipos de trabajo con profesionales del área del derecho, la criminalística y las fuerzas de seguridad. Y también se brindará una base de conocimiento adecuada y suficiente sobre gestión de incidentes de ciberseguridad.

2. OBJETIVOS

Al finalizar el curso se pretende que el asistente sea capaz de:

- Conocer acerca del estado del arte de la Forensia Digital
- Desarrollar y explicar las características básicas del contexto de las Pericias Informáticas y de los incidentes de Ciberseguridad
- Comprender el proceso de tratamiento de la evidencia digital en todas sus etapas (identificación, adquisición, análisis, preservación y presentación)
- Identificar y aplicar el proceso de tratamiento de la evidencia digital en todas sus etapas.
- Conocer acerca de la aplicación del Análisis Forense en el contexto de la Justicia y en la gestión de incidentes de Ciberseguridad
- Conocer acerca de las cuestiones básicas del Derecho Procesal aplicable a la realización de pericias
- Comprender y desarrollar las guías metodológicas más usuales para realizar el análisis forense digital.
- Utilizar y evaluar diferentes herramientas forenses.

3. CONTENIDOS MÍNIMOS

Unidad I - Forensia Digital: definición, conceptos fundamentales vinculados a la Seguridad de la Información, Seguridad Informática, Ciberseguridad y Auditoría Forense. Antiforensia. Principios del Derecho y legislación relacionada con la Forensia Digital.

Unidad II - Delitos Informáticos: Legislación Nacional e Internacional. Tipificación de los Delitos Informáticos. El Delincuente Informático. Roles del Experto Informático en la Forensia Digital.

Unidad III - Metodologías de la Forensia Digital: Protocolos y Normas de uso internacional. Familia de Normas ISO/IEC 27000:2015. Metodologías propias de la Forensia Digital y

REGISTRADO

PABLO A. HUEL

JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

Ministerio de Educación
Universidad Tecnológica Nacional
Rectorado

propias de la Ciberseguridad.

Unidad IV – Actuación Forense: La Ética del Analista Forense y el desempeño profesional. Deberes, derechos y responsabilidades del Analista Forense. Los puntos de pericia en la actuación judicial. Informe Pericial / de Análisis Forense. La Contrapericia. Regulación profesional de la actividad forense digital.

Unidad V – Evidencia Digital: Evidencia y Prueba Digital. Tipos de evidencia digital. La Cadena de Custodia. Valor probatorio del Documento Electrónico. Evidencia y hallazgos de Auditoría Forense.

Unidad VI – Dispositivos Soporte de la Evidencia Digital: Dispositivos Digitales (H+S+D). Estructura interna de la Evidencia Digital: memoria, disco, artefactos, redes, correo electrónico, imágenes, bases de datos, entornos IoT.

Unidad VII – Escenarios Forenses: Escenarios delictivos en los entornos virtuales. Plataformas Digitales de Negocios. Plataformas Digitales de Industrias 4.0. Escenarios Forenses Complejos: Aplicaciones para Reuniones Virtuales, Redes Sociales, OSINT.

Unidad VIII – Herramientas Forenses: Taxonomía NIST. Herramientas Forenses propias de cada tipo de evidencia. Herramientas Forenses Integradas. Kits de herramientas del Analista Forense. Aportes de la Informática Aplicada a la Forensia Digital.

Unidad IX - Talleres de Herramientas Forenses: Operatividad de herramientas forense de acceso libre. Prácticas en modalidad taller de: Recuperación de Archivos Borrados, Volcado de Memoria, Forensia de Correos Electrónicos, Forensia de Teléfonos Celulares y Forensia de Imágenes.

Unidad X – Taller de Análisis Forense de Incidentes de Ciberseguridad: Casos de estudio. Gestión de Incidentes de Ciberseguridad. Planificación del Análisis Forense. Informe de Respuesta, Lecciones Aprendidas y Recomendaciones de Mejoras.

REGISTRADO

PABLO A. HUEL

JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

4. DURACIÓN

El curso tendrá una duración de SESENTA (60) horas.

5. METODOLOGÍA

El curso se llevará a cabo modalidad presencial, complementado con utilización de las herramientas virtuales necesarias (webinar, foros, actividades prácticas, etc.).

Las clases expositivas sobre las temáticas centrales de la unidad, se combinarán con tutorías personalizadas, a fin de establecer una comunicación particular con cada asistente, con el objetivo de realizar un seguimiento sobre las actividades pautadas y a las que el asistente no pudo asistir o completar.

6. EVALUACIÓN Y APROBACIÓN

Para la aprobación del curso se requerirá, además del 80% de asistencia, la ejecución de los trabajos prácticos y talleres, y la aprobación de un examen final individual.

REGISTRADO

PABLO A. HUEL
JEFE DE DEPARTAMENTO - APOYO AL CONSEJO SUPERIOR

Ministerio de Educación
Universidad Tecnológica Nacional
Rectorado

ORDENANZA Nº 1884

ANEXO II

CURSO DE ACTUALIZACIÓN DE POSGRADO

"ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES E INCIDENTES DE CIBERSEGURIDAD"

FACULTAD REGIONAL VILLA MARÍA

Cuerpo Docente

- Dra. Herminia Beatriz PARRA DE GALLO (DNI 12.007.512)

Ministario de Educación de la Nación
Universidad Tecnológica Nacional
Firmado digitalmente por: ROSSO Pablo Andres
Secretario Consejo Superior.
Sarmiento 440. CP 1041. CABA.
Fecha y hora: 24.08.2022 09:20:48
Email: pabloarosso@gmail.com

Firmado Digitalmente por:

Ing. RUBEN SORO
RECTOR
UNIVERSIDAD TECNOLOGICA NACIONAL