I Escuela de Verano CiberLac

Palacio de Minería, Ciudad de México

25 al 29 de agosto de 2025

Este documento describe el contenido y la estructura de un curso y un taller de entrenamiento en ciberseguridad que investigadores y docentes del grupo de Seguridad Informática de la Facultad de Ingeniería de la Universidad de la República (FING-Udelar), Uruguay, dictarán en la Escuela.

El responsable académico del curso es el Dr. Gustavo Betarte, Profesor Titular del Instituto de Computación de FING-Udelar y el del taller el Dr. Juan Diego Campo, Profesor Adjunto de la misma institución.

El equipo docente está conformado por Betarte, Campo y tres docentes de apoyo (se adjuntan CVs resumidos de todos). Dichos docentes de apoyo serán coordinados por los responsables.

Título del curso

Análisis forense digital y respuesta a incidentes: un enfoque práctico.

Aspectos generales del curso

Modalidad	Curso de dictado presencial
Duración total	8 hs
Cupo	60
Lengua de impartición	Castellano

Resumen general

Los incidentes de seguridad ocurren a pesar de que los equipos de seguridad hacen todo lo posible para evitarlos. Es importante reconocer esta posibilidad y tomar medidas proactivas para evitar ser tomados por sorpresa. Es así que el análisis forense digital y la respuesta a incidentes (DFIR, por sus siglas en inglés) se han convertido en componentes vitales de la seguridad defensiva.

En este curso cubriremos los conceptos básicos relacionados al análisis forense digital y la respuesta a incidentes. Esta disciplina ayuda a los profesionales de la seguridad a identificar las huellas dejadas por un atacante cuando ocurre un incidente de seguridad, utilizarlas para determinar el alcance del compromiso en determinado entorno e identificar las medidas necesarias para restaurarlo a un estado seguro.

Objetivos específicos:

- Presentar los conceptos básicos de la disciplina de DFIR
- Poner en común metodologías de trabajo y procesos de respuesta a incidentes utilizados en la actualidad
- Realizar trabajos prácticos que apliquen los conceptos vistos a lo largo del curso

Temario detallado

El temario base para este curso está constituido por conceptos relacionados al análisis forense digital y fundamentos de la gestión de incidentes. Habrá trabajo práctico y un laboratorio que será desarrollado en formato hands-on simulando situaciones reales.

Introducción al análisis Forense digital

La ciencia forense digital es una rama de investigación centrada en el tratamiento de datos vinculados con medios electrónicos. En el contexto de DFIR, el objetivo es descubrir qué ocurrió durante un incidente de ciberseguridad. Incluye la recopilación de datos de los sistemas de TI (hardware, sistemas operativos y sistemas de archivos); el análisis de la información recopilada; y la utilización de la información en el proceso de respuesta a incidentes. Durante el proceso de recopilación de datos, analistas experimentados identifican y protegen los dispositivos y datos implicados. Luego, dichos datos se someten a un análisis detallado para determinar la causa que da lugar al incidente, el alcance de la infracción y cómo estos datos se vieron afectados. Una vez identificados los detalles, se gestiona el incidente buscando mitigar la situación para así converger a un estado seguro.

Temas a tratar:

- Introducción
  - Motivación, definiciones y objetivos del análisis forense digital
  - Principios del análisis forense

    - Usos del análisis forense
- Evidencia digital
    - Tipos de evidencia
    - Propiedades
    - Fuentes de obtención de evidencias
    - Cadena de custodia
- Metodologías para el análisis forense
    - Identificación
    - Preservación
    - Análisis
    - Presentación

Respuesta a incidentes

La respuesta a incidentes consiste en las acciones tomadas inmediatamente después de un compromiso de seguridad, un ciberataque o una violación a las políticas de seguridad establecidas en una organización. Al igual que la ciencia forense digital, la respuesta a incidentes investiga los sistemas informáticos, con la salvedad que no solo busca descubrir los hechos, intenta además contener la situación y en la medida de lo posible implementar un proceso de recuperación. Debido a la complejidad de estas actividades, este proceso requiere un equipo de profesionales experimentados que entiendan cómo responder a determinadas situaciones.

Temas a tratar:

- Introducción
    - Tipos de incidente
    - El proceso de gestión de incidentes
- Estrategias de gestión
    - Detección
    - Análisis
    - Contención
    - Erradicación
    - Recuperación
- Actividades posteriores al incidente
    - Cuantificar el impacto
    - Generación de informes

El proceso de investigación

En conjunto, la ciencia forense digital y la respuesta a incidentes pueden proporcionar una comprensión más profunda de los incidentes de ciberseguridad a través de un proceso de investigación integral. Los profesionales especializados en ambas disciplinas tienen como objetivo principal responder, de una forma rápida y efectiva, a un incidente de modo que tenga el menor impacto posible.

Normalmente, las actividades realizadas por un equipo de DFIR intenta responder, entre otras, las siguientes preguntas:

- ¿Cómo se llevó adelante la incursión por parte de los atacantes?
- ¿Cuáles son los pasos exactos que se tomaron para poner los sistemas en riesgo?
- ¿Qué datos se perdieron o comprometieron?
- ¿Cuál fue el daño real que causado?

Temas a tratar:

- Investigación de incidentes

    - Identificación del alcance
    - Identificación del impacto
- Monitoreo y detección de anomalías
- Clasificación y procesamiento de incidentes
    - Triaje: priorización y categorización
- Recopilación, análisis y correlación de eventos

Metodología de enseñanza

El curso posee una duración de 8 horas presenciales en modalidad teórico-práctico a realizarse durante el transcurso de la Escuela de Verano de CiberLac 2025. El equipo docente presentará los conceptos teóricos y las guías de los trabajo prácticos. Los estudiantes serán asistidos y supervisados por el equipo docente a lo largo de la ejecución de las prácticas.

Conocimientos previos exigidos y recomendados

- **Conocimientos previos exigidos**: conocimientos de redes de computadoras, sistemas operativos.
- **Conocimientos previos recomendados:** este curso asume como ya adquiridos por el estudiante conceptos básicos de programación. En caso de no contar con éstos, la incorporación de dichos conceptos será responsabilidad única del estudiante.

Cronograma tentativo

	Tema a tratar	**horas**
Clase 1	Introducción al análisis Forense	2
Clase 2	Recolección y análisis de evidencia	*2*
Clase 3	Respuesta a incidentes	2
Clase 4	El proceso de investigación	2

Requerimientos para el dictado

El curso, en lo que respecta al dictado teórico, requiere de equipamiento necesario como para que el docente pueda conectarse con su computador a internet y a un sistema de proyección de imágenes y reproducción de sonido.

Bibliografía

1) Digital Forensics and Incident Response - Second Edition, Johansen, G., Safari, an O'Reilly Media Company, 2020.
2) Hands-on Incident Response and Digital Forensics, Mike Sheward, BCS - The Chartered Institute for IT, 2018.
3) Digital Forensics and Incident Response - An intelligent way to respond to attacks, Gerard Johansen, Packt Publishing Ltd., 2017.

Título del taller

Entrenamiento DFIR en Tectonic

Aspectos Generales

Modalidad	Taller práctico
Duración total	3 horas (y trabajo de preparación previa)
Cupo	60 participantes organizados en equipos de 3 integrantes
Lengua de impartición	Castellano

Resumen General

El taller constará de una sesión de entrenamiento de 3 horas y enfrentará a los participantes a un ejercicio de gestión de incidentes. El escenario de entrenamiento será implementado a través de Tectonic[1].

Tectonic es un *cyber range* que da soporte para realizar entrenamiento práctico en ciberseguridad. El entrenamiento se realiza mediante escenarios realistas conformados por redes, sistemas y aplicaciones, que permiten simular situaciones ofensivas y defensivas. Las funcionalidades clave de la plataforma incluyen gestión del ciclo de vida de los escenarios de entrenamiento, monitoreo en tiempo real del entrenamiento de los usuarios y simulación automatizada de ataques.

En este entrenamiento se plantea una realidad donde una empresa energética que cuenta con una infraestructura crítica de tipo *Supervisory Control and Data Acquisition* (SCADA) sufre un ataque de ciberseguridad. Los participantes deberán llevar a cabo el proceso de gestión del incidente para la correcta resolución del caso.

Los objetivos de aprendizaje son:

- Importancia del manejo de evidencia.
- Tipos de evidencia y análisis de evidencia.
- Proceso y etapas de un incidente de seguridad.
- Importancia de una buena documentación en un incidente de seguridad.

Escenario de Entrenamiento

La empresa Utopía es una multinacional dedicada al sector energético. Cuenta con múltiples plantas de generación de energía como plantas nucleares, parques eólicos y represas hidroeléctricas, repartidas a lo largo de todo América. Recientemente esta empresa ha experimentado comportamiento anómalo en su infraestructura. Si bien no se cuenta con evidencia, la empresa sospecha que ha sido víctima de un ataque cibernético perpetuado por un actor malicioso con el objetivo de obtener información confidencial de la organización.

Para esclarecer este asunto, Utopía contrata a un equipo de gestión de incidentes (CSIRT CiberLac, de acá en más) para realizar la gestión de este potencial incidente. Los participantes tomaran distintos roles dentro del equipo CSIRT CiberLac a lo largo de los distintos ejercicios planteados. En particular, desarrollarán tareas asociadas a la gestión y análisis de evidencia digital, y la aplicación de tareas de contención y recuperación sobre sistemas operativos.

1 https://github.com/GSI-Fing-Udelar/tectonic, https://www.fing.edu.uy/inco/proyectos/tectonic

Conocimientos previos exigidos y recomendados

- Conocimientos previos exigidos: conocimientos de redes de computadoras y sistemas operativos.
- Conocimientos previos recomendados: sería deseable que los estudiantes tengan conocimientos sobre manejo de consolas Linux.

Requerimientos para el dictado

Cada participante deberá contar con un puesto de trabajo (PC o notebook), con acceso a internet para poder realizar las tareas en una infraestructura remota.

Equipo docente

Gustavo Betarte se graduó de Ingeniero de Sistemas en Computación en la Facultad de Ingeniería de la Universidad de la República, Uruguay (FING-Udelar), y obtuvo una maestría y un doctorado en Ciencias de la Computación en la Universidad de Gotemburgo, Suecia. Es Profesor Titular del Instituto de Computación (InCo) e investigador principal y jefe del equipo de Seguridad Informática (GSI) de FING-Udelar. El Dr. Betarte es miembro del Sistema Nacional de Investigadores del Uruguay (SNI, Nivel II) e investigador activo (Grado 5) del Área de Informática de PEDECIBA. Desde 2006 es Director de Consultoría de Tilsor SA, empresa uruguaya de TI y desde 2021 es el responsable del equipo de gestión de incidentes de la empresa, el CSIRT Tilsor.
Sus intereses de investigación incluyen métodos formales, verificación de programas, seguridad de software y sistemas, y fundamentos de la informática. Actualmente trabaja en la aplicación de técnicas de descubrimiento de conocimiento para la seguridad de software adaptativo, la definición formal y la verificación de las propiedades de seguridad de sistemas críticos, y el diseño e implementación de *cyber ranges*. Para más información, consultar su CV completo y la lista de publicaciones en DBLP.

Juan Diego Campo se graduó de Ingeniero en Computación en la Facultad de Ingeniería de la Universidad de la República, Uruguay (FING-Udelar) y obtuvo su doctorado en Ciencias de la Computación del PEDECIBA Informática, Uruguay. Es Profesor Adjunto del Instituto de Computación (InCo) y miembro del equipo de Seguridad Informática (GSI) de FING-Udelar. El Dr. Campo es investigador activo (Grado 3) del Área de Informática de PEDECIBA.
Sus intereses de investigación incluyen métodos formales, verificación de programas, seguridad de software y sistemas, y fundamentos de la informática. Actualmente trabaja en la aplicación de técnicas de descubrimiento de conocimiento para la seguridad adaptativa del software y en el diseño e implementación de *cyber ranges*. Para más información, consulte la lista de publicaciones en DBLP.

Rodrigo Martínez se graduó de Ingeniero en Computación en la Facultad de Ingeniería de la Universidad de la República, Uruguay (FING-Udelar) y obtuvo una Maestría en Ciencias de la Computación del PEDECIBA Informática, Uruguay. Es Profesor Adjunto del Instituto de Computación (InCo) y miembro del equipo de Seguridad Informática (GSI) de FING-Udelar. Trabaja como consultor de seguridad informática en Tilsor SA desde 2009 y forma parte del Equipo de Respuesta a Incidentes de la empresa (CSIRT Tilsor). Desde 2018, es el líder técnico del equipo de seguridad informática de Tilsor.
Sus intereses de investigación incluyen la seguridad de aplicaciones web y de aplicaciones, así como el uso de técnicas de aprendizaje automático aplicadas a la seguridad de aplicaciones web. Para más información, consulte su CV completo.

Marcelo Rodríguez se graduó de Ingeniero en Computación en la Facultad de Ingeniería de la Universidad de la República, Uruguay. Actualmente cursa el Doctorado en Ciencias de la Computación en PEDECIBA Informática, Uruguay. Es Profesor Adjunto del nstituto de Computación (InCo) y miembro del equipo de Seguridad Informática (GSI) de FING-Udelar. Trabaja como consultor de seguridad informática en Tilsor desde 2009 y forma parte del Equipo de Respuesta a Incidentes de la empresa (CSIRT Tilsor). Sus intereses de investigación incluyen la elaboración de perfiles de atacantes en ciberseguridad, el análisis forense digital y el desarrollo de metodologías y herramientas para la correlación de indicadores de amenazas.

Guillermo Guerrero se graduó de Ingeniero en Computación en la Facultad de Ingeniería de la Universidad de la República, Uruguay. Actualmente cursa una Maestría en Ciencias de la Computación del PEDECIBA Informática, Uruguay. Es ayudante de cátedra del Instituto de Computación (InCo) y miembro del equipo de Seguridad Informática (GSI) de FING-Udelar. Trabaja como consultor de seguridad informática en Tilsor desde 2021.
Actualmente trabaja en la aplicación de técnicas de minería de procesos para la evaluación de entrenamientos de ciberseguridad en cyber ranges.

Para más información sobre el Grupo de Seguridad Informática referimos a la página web del equipo (GSI).