sedian

Seguridad Digital
de Andalucía

Ficha técnica

Ciclo de análisis forense

Modalidad: presencial virtualizada

Fecha de inicio: 09 de mayo de 2022

Fecha de finalización: 18 de mayo de 2022

Junta de Andalucía

ÍNDICE

DATOS BÁSICOS DE LA ACCIÓN FORMATIVA....3
DESCRIPCIÓN....3
OBJETIVOS....4
CONTENIDOS....5
TEMPORALIZACIÓN....6
METODOLOGÍA....7
DOCENTE....8
EVALUACIÓN....9
ATENCIÓN AL ALUMNADO....10
OBSERVACIONES....10

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: Ciclo de análisis forense

Modalidad: Presencial virtualizada.

Fecha de Inicio: 09 de mayo de 2022.

Fecha de Finalización: 18 de mayo de 2022.

Sesiones en directo vía streaming:

- 09 de mayo: 09:00 a 11:30 A.M.
- 13 de mayo: 09:00 a 11:30 A.M.
- 18 de mayo: 09:00 a 11:30 A.M.

Fechas para las tutorías:

- 11 de mayo de 04:00 a 05:00 P.M.
- 16 de mayo de 04:00 a 05:00 P.M.

Dirigido a: Responsables de seguridad TIC y personal TIC de la Junta de Andalucía

Número máximo de personas participantes: 30.

2 DESCRIPCIÓN

El constante uso de internet y de dispositivos electrónicos ha supuesto un antes y un después en nuestras vidas.

El uso de los ordenadores, de internet, archivos de fotografías, audios, vídeos, la aparición de soporte de cada vez menor dimensión y mayor capacidad de procesamiento y almacenamiento de información, la comunicación por email, chat, foros, análisis de malware, gestión de incidentes y amenazas, monitorización y análisis, así como el constante aumento de ciberdelitos (fraudes digitales, ataques contra la protección de datos personales, espionaje industrial, phising…) hace que cada vez sea más demandada la figura del Analista Informático Forense especializado en investigación y obtención de pruebas informáticas que sirvan como argumentos judiciales sobre la culpabilidad o inocencia de una de las partes.

3 OBJETIVOS

Generales

- Llevar a cabo procedimientos y metodologías para identificar, asegurar, extraer, analizar y presentar pruebas generadas y guardadas electrónicamente garantizando la integridad de la cadena de custodia.
- Recopilar las evidencias obtenidas durante la investigación con la finalidad de, crear un informe pericial que cumpla con las principales recomendaciones como guía básica de buenas prácticas.

Específicos

- De acuerdo con la RFC 3227, ser capaces de extraer información volátil almacenada tanto en el sistema operativo como en la memoria RAM para su posterior análisis.
- Adquirir una imagen forense bit a bit del sistema para su posterior análisis siguiendo los procedimientos y buenas prácticas, así como conocer las principales técnicas de clonación de discos duros.
- Entender el concepto hash y ponerlo en práctica en para mantener la cadena de custodia de evidencias digitales.
- Comprender como funciona el registro de Windows para posteriormente realizar un análisis exhaustivo del mismo utilizando herramientas específicas y gratuitas.
- Saber utilizar herramientas forenses destinadas a realizar análisis de imágenes forenses, clonaciones y sistemas operativos en vivo.

4 CONTENIDOS

Unidad 1: La informática forense

1. Conceptos básicos
2. Fase de Identificación
3. Fase de adquisición
4. Fase de preservación
5. Fase de análisis
6. Fase de presentación
7. Cadena de custodia

Unidad 2: El analista forense informático

1. Derechos, deberes y obligaciones
2. Fases del encargo

Unidad 3: Función hash

1. Concepto hash
2. Características

Unidad 4: Recopilación de información volátil

1. Concepto de volatilidad
2. Comandos de CMD
3. Recopilación de información volátil con programas portables
4. Uso de Herramientas Triage

Unidad 5: Memoria RAM

1. Volcado de memoria RAM
2. Análisis de memoria RAM

Unidad 6: Imagen forense

1. Imagen forense VS Clonación
2. Características de la imagen forense
3. Métodos de extracción de una imagen forense

Unidad 7: Registro de Windows

1. Entender cómo funcionan los archivos Hive
2. Localizar los principales archivos Hive del registro

3. Conocer las principales claves del registro

4. Analizar el registro con diferentes herramientas forenses

Unidad 8: Herramientas de Análisis forense

1. Utilizar el software forense Autopsy

2. Utilizar el software forense OSForensic

5 TEMPORALIZACIÓN

Sesiones en directo vía streaming:

- 09 de mayo: 09:00 a 11:30 A.M.
- 13 de mayo: 09:00 a 11:30 A.M.
- 18 de mayo: 09:00 a 11:30 A.M.

Fechas para las tutorías:

- 11 de mayo de 04:00 a 05:00 P.M.
- 16 de mayo de 04:00 a 05:00 P.M.

PLANIFICACIÓN HORARIA

Sesión 1	1. La informática forense 2. El analista forense informático 3. Función Hash 4. Recopilar información volátil 5. Memoria RAM Dudas y preguntas.
Sesión 2.	6. Memoria RAM 7. Imagen forense 8. Registro de Windows Dudas y preguntas.
Sesión 3.	9. Herramienta Autopsy 10. Herramienta OSForensic Dudas y preguntas.

6 METODOLOGÍA

La acción formativa se desarrollará en **modalidad Presencial Virtualizada**, es decir, una modalidad de estudio en la que la docente y alumnos/as toman contacto en un entorno digital basado en las TIC y las redes de ordenadores, utilizando las facilidades y herramientas que proporcionan Internet y las tecnologías digitales. Estas herramientas facilitan la alternancia entre formación grupal (en *streaming*) e individual (Tutorías personalizadas virtuales). Para esta alternancia de atención al alumnado, se usarán las siguientes herramientas:

✔ **Sesiones Grupales/Laboratorio.** La herramienta usada para estas sesiones se denomina **GoToWebinar**. El alumnado será convocado por email, recordando día y hora de conexión, así como, facilitando el enlace de acceso.

La forma de trabajo de cada sesión/laboratorio seria la siguiente:

- **Sesión 1:** Exposición de los conceptos básicos y las diferentes fases que se desarrollan en una investigación forense informática. Se realizan ejercicios prácticos para llevar a cabo las fases de identificación, adquisición y preservación de evidencias electrónicas poniendo en prácticas normativas y estándares internacionales.
- **Sesión 2:** Se utilizarán herramientas forenses específicas para llevar a cabo la fase de análisis de evidencias digitales tanto con evidencias volátiles como en imágenes forenses. Se creará una imagen forense bit a bit y se utilizan diferentes herramientas para analizar el registro de Windows.
- **Sesión 3:** Se aprenderá a utilizar diferentes herramientas para analizar imágenes forenses, clonaciones y sistemas operativos.

✔ **Sesiones Tutorías individualizadas.** Este tipo de interacción con el alumnado tendrá como finalidad la atención y resolución individualizada de dudas acerca del temario por parte de la docente. Estas sesiones estarán disponibles a través del recurso BBB, integrado en el propio Aula Virtual. A través de BBB, herramienta que permite accesibilidad, facilidad de uso y por acceder a cámara web, altavoces, micrófonos y compartición de archivos, así como, pizarra virtual.

7 DOCENTE

IMPARTIDO POR: Rosario Tíscar Mata

Más de 10 años de experiencia en el mundo de las nuevas tecnologías y más de 5 años como profesora y analista forense informática. Ingeniera Técnica Colegiada en Informática de Sistemas.

Acceso a su perfil LinkedIn

8 EVALUACIÓN

Para la evaluación de la *Formación Presencial Virtualizada* se tendrán en cuenta

las siguientes variables: la **asistencia,** el **interés** y **valoración cuantitativa** de los conocimientos adquiridos. Para esto, se tendrá en cuenta:

- **Superar los cuestionarios de conocimientos (un tipo test por cada sesión) y *cuestionario final* de evaluación con un porcentaje de acierto del 60% o superior.**

Cada sesión/laboratorio finaliza con la realización practica opcional de un ejercicio. La posterior corrección y evaluación de la misma conlleva una valoración por parte del docente, y aunque se recomienda la realización para un mejor provecho del curso, no computará para la obtención del certificado.

Criterios de evaluación

Evidencias para la evaluación	Peso
Realización y superación de los cuestionarios tipo test (uno por cada unidad) y evaluación final del curso	**100%**

Valoración de Conocimientos.

Indicador obtenido a partir de los *cuestionarios de conocimientos* de 10 ítems sobre aspectos tratados durante *cada sesión* y una *Evaluación Final* de 15/20 ítems para una valoración global de los conocimientos adquiridos.

Si la **Valoración Final Conocimientos** supera el 60% de la valoración general, el/la alumno/a habrá superado esta parte de la evaluación.

9 ATENCIÓN AL ALUMNADO

Para realizar un correcto seguimiento del curso y disponer de los medios necesarios para que los alumnos puedan elevar sus dudas al tutor, se dispondrán de los siguientes canales para tal fin:

1. Mail del tutor. Los alumnos podrán mantener contacto con el/la tutor/a del curso mediante la dirección de mail formacion.sedian@juntadeandalucia.es donde el/la tutor/a dispondrá de un plazo máximo de 48h para responder al alumnado.

2. Videoconferencia mediante GoToWebinar. En la Ficha técnica del curso y en la propia aula virtual el alumnado tiene disponible los días y horarios de las clases en directo, para que los participantes puedan mantener una videoconferencia con el/la tutor/a y así poder resolver las dudas o profundizar en contenidos que requieren una asistencia técnica.

3. Tutorías mediante BigBlueButton. En la Ficha técnica del curso y en la propia aula virtual el alumnado tiene disponible los días y horarios de las tutorías, para que los participantes puedan mantener una videoconferencia con el/la tutor/a y así poder resolver las dudas o profundizar en contenidos que requieren una asistencia técnica.

4. Foro de discusión. Los alumnos disponen de un foro de discusión donde mantendrán una relación colaborativa y podrán mantener contacto con el/la tutor/a.

10 OBSERVACIONES

Los participantes deben tener conocimientos previos en informática a nivel usuario.

Previa al inicio de la acción formativa se realizará un cuestionario de conocimientos previos de carácter voluntario que permita a la docente analizar los conocimientos en la materia del curso de presencia virtualizado.