Información General del Curso

Título	**Gestión de Ciber-incidentes y Análisis Forense Digital**
Modalidad	Presencial en Tegucigalpa, Honduras
Fechas	21 y 22 de noviembre del 2022
Duración	2 días
Último día para registro	21 de noviembre del 2022
Costo	Gratuito (los participantes deben cubrir sus gastos de viaje)
Descripción	El curso está orientado a capacitar representantes de equipos nacionales de respuestas ante incidentes cibernéticos, revisar conceptos, metodologías y demostraciones prácticas para la gestión de incidentes de ciber-seguridad.
Código del curso	22BD027915AMS-S

1. OBJETIVOS DEL CURSO

Presentar los conceptos, metodologías y experiencias prácticas para la gestión de incidentes de ciber-seguridad. Profundizar en las técnicas de análisis forense digital y en los planes, playbooks y marco normativo para la correcta gestión de incidentes. Entrenar en las distintas herramientas y metodologías de análisis de evidencia digital y la gestión de la comunicación tanto externa como interna durante un incidente de ciber-seguridad.

2. RESULTADOS DEL APRENDIZAJE

Una vez completado este curso, los participantes podrán:

- Tener mayor conocimiento de los conceptos y metodologías sobre gestión de incidentes de ciber-seguridad.
- Replicar experiencias y mejores prácticas sobre las técnicas de análisis forense digital.
- Tener mayor claridad sobre planes, playbooks y marco normativo para la correcta gestión de incidentes de ciberseguridad.
- Tener mayor experiencia en las distintas herramientas y metodologías de análisis y manejo de evidencia digital.
- Gestionar de mejor manera la comunicación tanto externa como interna durante un incidente de ciber-seguridad.

3. A QUIÉN VA DIRIGIDO EL CURSO

Este curso está destinado a Gerentes de Seguridad Informática / Seguridad de la Información / Ciberseguridad, Líderes técnicos de SOC, Analistas técnicos de Ciberseguridad, Personal de CSIRTs privados y nacionales, Auditores de Seguridad de la Información entre otros.

4. REQUISITOS DE ADMISIÓN

Es importante que los participantes trabajen o tengan conocimientos/experiencia en materia de ciberseguridad.
El curso está orientado a Gerentes de Seguridad Informática / Seguridad de la Información / Ciberseguridad, Líderes técnicos de SOC, Analistas técnicos de Ciberseguridad, Personal de CSIRTs privados y nacionales, Auditores de Seguridad de la Información entre otros.

5. TUTORES/INSTRUCTORES

Nombre del(os) Tutor(es)/Instructor(es)	**Información de Contacto**
Sr. Pablo Palacios, UIT/BDT	pablo.palacios@itu.int
Sr. Marwan Ben Rached, UIT/BDT	marwan.benrached@itu.int
Sr. Julio Ardita, Experto UIT	jardita@cybsec.com

6. CONTENIDO DEL CURSO

Los temas a tratarse en esta formación son los siguientes:

1. Introducción a la Gestión de Ciber-Incidentes
   Contexto actual de los ciber-incidentes
   Marco metodológico para la gestión de ciber-incidentes
   Estableciendo capacidades CIR
   Simulaciones de ciber-incidentes
   Tipos de ciber-incidentes
2. Análisis de casos reales
   Análisis de caso: Fuga de información
   Análisis de caso: Fuga de información y extorsión
   Análisis de caso: Ransomware
   Análisis de caso: Fraude a través del sistema Swift
   Lecciones aprendidas
3. Plan y Playbooks de Respuesta ante Ciber-incidentes
   Marco normativo de Gestión de Ciber-incidentes
   Plan de Respuesta ante Ciber-incidentes
   Playbooks técnicos
   Métricas de CIR
4. Análisis forense digital
   Introducción al análisis forense digital
   Buenas Prácticas

Cadena de Custodia
Generación de Imágenes Forenses
Análisis con Herramientas Forenses
Extracción y análisis de Información

5. Análisis de eventos
   Estrategias para el análisis de eventos
   Análisis de logs
   Herramientas de filtrado y análisis de logs
   Análisis de eventos de firewall, proxy
   Análisis de eventos de sistemas operativos
   Análisis de eventos de aplicaciones
6. Comunicación y legales
   Aspectos legales relacionados con incidentes de Seguridad
   Protocolos de Comunicación externa e interna
   Gestión de crisis de ciberseguridad
   Comunicación entre otros teams de CSIRTs

7. CRONOGRAMA DEL CURSO

Sesión	Tema	Ejercicios e interacciones
Día 1 **21 de noviembre del 2022**	• Introduction to Cyber-Incident Management • Analysis of real cases • Cyber-incident Response Plan and Playbooks	• Analysis of real cases
Día 2 **22 de noviembre del 2022**	• Digital forensics • Event analysis • Communication and legal	• Event analysis

8. METODOLOGÍA

Este curso se impartirá en forma presencial. El curso se imparte utilizando diapositivas que se incluyen en la página del curso y materiales de referencia, que han sido seleccionados, que los participantes deben revisar, estudiar, además de participar en las actividades de cada Sesión y realizar autoevaluaciones. Los estudiantes profundizarán su comprensión de los temas estudiados aprovechando sus entornos específicos y se les alienta a consultar, previamente, con sus colegas experimentados que están trabajando en un tema pertinente.

9. EVALUACIÓN Y CALIFICACIÓN

Se realizará un examen al final del Curso. Para obtener el certificado de la UIT se requiere una puntuación total superior al 60%.

Evaluación al final del curso:	80%
Asistencia:	10%
Participación en los ejercicios:	10%

10 COORDINACIÓN DEL CURSO

Coordinador de la Oficina de Área de UIT en Chile: Nombre: Sr. Pablo Palacios Email: pablo.palacios@itu.int	**Coordinador de la Oficina de Área de UIT en Honduras:** Nombre: Sr. Carlos Lugo Email: carlos.lugo@itu.int