Curso Profesional Inicial de Ciberseguridad

Autor

Seguridad de la Información de Agesic

Fecha de creación

02/04/2024

Tipo de publicación

Fichas

Resumen

Curso preparatorio para certificación Security+ de compTIA

Organizan:

Estado Mayor de la Defensa (ESMADE), Escuela de Guerra Naval (ESGUE) y Agencia de Gobierno Electrónico, Sociedad de la Información y el Conocimiento (Agesic)

Objetivo, requisitos y perfil de egreso

Objetivo

- **El curso tiene como finalidad preparar a las personas para desarrollarse en cualquier tarea relativa a ciberseguridad y validar que se encuentren en condiciones de dar el examen de certificación internacional Security+ de CompTIA.**
- **Se cubrirán todas las áreas de la ciberseguridad, con niveles de profundidad variables según los conocimientos previos en ciertos temas. Algunas áreas serán más técnicas que otras en función de esto.**
- **Security + de CompTIA es una certificación vendor neutral, de nivel inicial y es las certificaciones de ciberseguridad más reconocida a nivel internacional. Acredita que una persona tiene claro los principios y prácticas que rigen la ciberseguridad y que podrá desempeñarse de forma satisfactoria en cualquier área relativa a esta temática. Además, la certificación CompTIA Security+ es la puerta de entrada a diferentes certificaciones en ciberseguridad.**

Requisitos

CompTIA recomienda esta certificación para aquellas personas que desempeñan tareas en roles como:

- Administradores de Sistemas.
- Administradores de Ciberseguridad.
- Especialistas de Ciberseguridad.
- Ingeniero de Ciberseguridad.
- Administradores de redes.
- Auditores de TI.
- Penetration tester.
- Consultores de Ciberseguridad.
- Quien aspire a realizar el curso deberá tener conocimientos comprobados de redes (networking) de al menos dos años.

Perfil de egreso

La persona que realice el curso podrá desarrollarse en cualquier tarea relativa a ciberseguridad y estará lista para rendir la certificación CompTIA Security+.

Duración, modalidad, y equipo docente

Duración

- **El curso se dicta en modalidad híbrida y cuenta con una duración aproximada de 9 meses, distribuido en dos clases semanales de una una hora y media cada una. Cualquier excepción se comunicará de forma oportuna.**

Modalidad

- Presentación inicial del curso y la modalidad de estudio que se debe adoptar ante una certificación internacional.
- Durante el curso, se realizarán evaluaciones parciales a fin de analizar el progreso de cada estudiante y su estado para presentarse a la certificación.
- Se programará un período final para sesiones de preguntas, respuestas y simulacros de examen.
- En temas puntuales, en los cuales se entienda que la temática tiene cierta complejidad, se brindará una presentación durante la clase.
- El curso se aprobará con un nivel mínimo de 80% en cada evaluación.

Equipo docente

- ESMADE: CN Claudio López.
- AGESIC: Juan Pablo García y Adrián Marrero.

Contenido, materiales y programa del curso

Contenido

- **El curso está basado en el texto Comptia Security+, Studie Guide by Mikke Chaple SYO-701, fuente primaria recomendada por la propia CompTIA.**
- **Si bien las clases se dictarán en idioma español, todo el material de referencia se encuentra en inglés.**
- **El examen de la certificación podrá realizarse en idioma español.**

Materiales

- Comptia Security+, Studie Guide by Mikke Chaple (Recomendado)
- CompTIA Security+ All-in-One Exam Guide by by Wm. Arthur Conklin
- CompTIA Security+ (SY0-701) Complete Course & Exam by Jason DION
- Videos de youtube o material relativos a temas particulares
- Exámen de Certificación CompTIA.
- Aplicación móvil oficial de CompTIA para la respuesta de pregunta de certificación.

Programa del curso

Tema	Clases	Modalidad
Presentación	1	Presencial
1. Profesional de la seguridad actual	1	Remota
2. Panorama de las amenazas a la ciberseguridad	2	Remota
3. Código malicioso	2	Remota
4. Ciberataques: ingeniería social, ataques físicos y a identidades	2	Remota
5. Análisis y test de seguridad	2	Remota
6. Código seguro	4	Remota
Evaluación General	2	Remota
7. Criptografía e infraestructura de clave pública	5	Remota
8. Gestión de acceso e identidad	5	Remota

9. Resiliencia y seguridad física	4	Remota
Evaluación General	2	Remota
10. Seguridad en la nube y la virtualización	2	Remota
11. Seguridad en el endpoint	4	Remota
Evaluación General	4	Remota
12. Seguridad de la red	2	Remota
13. Seguridad inalámbrica y móvil	4	Remota
14. Respuesta a incidentes	4	Remota
15. Análisis forense digital	2	Remota
16. Gobernanza en ciberseguridad	3	Remota
17. Gestión de riesgos y privacidad	2	Remota
Entrenamiento en Cyberrange	1 (3h)	Presencial
Preguntas de examen	8	Híbrida
Total	67 clases 34 semanas	

1. Profesional de la seguridad actual

- Visión global de la Ciberseguridad, definiendo sus pilares: CIA. confidencialidad, integridad y disponibilidad de los datos de su organización.
- Aprenderá sobre los tipos de riesgo que enfrentan las organizaciones y el uso de herramientas gerenciales, operativas y controles técnicos de seguridad para gestionar esos riesgos.

2. Panorama de las amenazas a la ciberseguridad

- Se aborda el panorama de las amenazas a la seguridad cibernética, ayudará a comprender amenazas presentes en el ambiente y vectores de ataque.
- Aprenderá sobre el uso de fuentes de inteligencia de amenazas para mejorar su organización, programa de seguridad y los problemas de seguridad que surgen de los diferentes tipos de vulnerabilidad.

3. Código malicioso

- Se explora un amplio rango de código malicioso que se puede encontrar: gusanos, virus, troyanos, bots, las redes de mando que utilizan atacantes para controlarlos, y una gran cantidad de otros tipos de malware.
- Además, se abordarán nuevas amenazas, como los ataques contra la inteligencia artificial y los sistemas de aprendizaje automático, así como la manera en que atacantes emplean scripts y lenguajes de programación como parte de sus estrategias, además del malware.

4. Ciberataques: ingeniería social, ataques físicos y a identidades

- La ingeniería social explora el lado humano para centrarse en cómo responden las personas a diversas técnicas como la autoridad, la intimidación y la confianza, y cómo pueden aprovechar esas respuestas tanto atacantes como probadores de penetración.
- Explorará siete principios fundamentales y una variedad de ingeniería social para influir en las técnicas de campaña.
- Se describirán los ataques a contraseñas más comunes tales como; ataques de fuerza bruta, ataques de diccionario y pulverización de contraseñas.
- Además, aprenderá cómo son los ataques físicos y cómo pueden afectar a una organización.

5. Análisis y test de seguridad

- Explora los diferentes tipos de evaluaciones y pruebas de seguridad, procedimientos que puede utilizar para evaluar la eficacia de su programa de seguridad.
- Aprenderá sobre las diferentes técnicas de evaluación utilizadas por profesionales de la ciberseguridad y la realización adecuada de pruebas de penetración en una variedad de entornos.
- Además, aprenderá cómo desarrollar un programa de evaluación que cumple con los requisitos de seguridad de su organización.

6. Código seguro

- El curso cubre la seguridad y los problemas que pueden surgir dentro del código de la aplicación y los indicadores asociado con ataques de aplicaciones.
- Reconocimiento de ataques web: SQL injection, XSS, CSRF, etc.
- Aprenderá sobre el uso de desarrollo, implementación y automatización de aplicaciones seguras y descubrirá cómo puede ayudar a su organización a desarrollar e implementar códigos que sean resistentes frente a las amenazas.

7. Criptografía e infraestructura de clave pública

- El curso explica el rol crítico que la criptografía juega en los programas de seguridad al facilitar comunicación y almacenamiento seguro de datos. Se presentarán los conceptos criptográficos básicos y cómo pueden usarlos para proteger datos en su propio entorno.
- Además, aprenderá acerca de los ataques comunes criptográficos que podrían usarse para socavar su control.
- Se explicará qué es una infraestructura de claves públicas y a partir de ahí el caso de uso de la Firma Electrónica Avanzada y la Identificación Digital en Uruguay.

8. Gestión de acceso e identidad

- El curso explica el uso de la identidad como una capa de seguridad para las organizaciones modernas. Aprenderá sobre los componentes de una identidad, el funcionamiento de la autenticación y la autorización, y las tecnologías comúnmente implementadas. Además, comprenderá cómo el inicio de sesión, la federación y los directorios contribuyen a la infraestructura de autenticación y autorización.
- Además, también aprenderá sobre la autenticación multifactor y la biometría como métodos para garantizar una autenticación más segura. Además, explorará el papel de cuentas, control de acceso, esquemas y permisos.
- Identidad Digital y Firma Digital en Uruguay.

9. Resiliencia y seguridad física

- El curso guía a través de los conceptos de seguridad física. Sin seguridad física, una organización no puede garantizar un ambiente seguro.
- Aprenderá a construir infraestructura resiliente y resistente a desastres utilizando copias de seguridad y redundancia.
- Explorará los controles de respuesta y recuperación que ayudan a que las organizaciones vuelvan a la funcionalidad cuando suceden fallan y ocurren desastres.
- Aprenderá sobre una amplia gama de controles de seguridad física para garantizar la protección de instalaciones y sistemas contra ataques y amenazas presenciales.
- Además, el curso abarca, qué hacer cuando los dispositivos y los medios alcanzan el final de su vida útil y necesitan ser destruidos o eliminados apropiadamente.

10. Seguridad en la nube y la virtualización

- Explora el mundo de la computación en la nube y la virtualización de la seguridad, ya que muchas organizaciones implementan negocios a través de aplicaciones en la nube y utilizan estos entornos para procesar información delicada.
- Aprenderá cómo las organizaciones hacen uso de la nube y sus servicios disponibles. Además, se explorará cómo construir arquitecturas en la nube que satisfagan las necesidades definidas.
- Además, también aprenderá a gestionar el riesgo de ciberseguridad de los servicios en la nube mediante el uso de una combinación de controles tradicionales y específicos para estos ambientes.

11. Seguridad en el endpoint

- El curso proporciona una descripción general de los muchos tipos de “puntos finales” que se pueden necesitar, abarcando los sistemas embebidos, sistemas de control industrial y los dispositivos que usan IoT o Internet de las Cosas, entre otros.
- Aprenderá sobre las consideraciones especiales a tener en cuenta en un diseño de seguridad, como encriptación y procesos de arranque seguro, y también explorará sus detalles.
- Además, aprenderá sobre algunas de las herramientas utilizadas para evaluar y proteger la seguridad de “puntos finales”.

12. Seguridad de la red

- El curso abarca la red seguridad, desde la arquitectura y el diseño, hasta los ataques a la red y defensas.
- Explorará técnicas comunes de ataque a la red y amenazas, aprenderá sobre protocolos, tecnologías, diseño, conceptos y técnicas de implementación para redes seguras para contrarrestar o evitar esas amenazas.
- Además, también aprenderá a descubrir dispositivos de red, así como los conceptos básicos de captura de paquetes de red y repetición.

13. Seguridad inalámbrica y móvil

- El curso explorá el mundo de la seguridad inalámbrica y móvil.
- Explorará cómo funciona una variedad cada vez mayor de tecnologías inalámbricas, desde GPS y bluetooth hasta Wi-Fi. Aprenderás sobre algunos ataques inalámbricos comunes y cómo diseñar y construir un entorno inalámbrico seguro.
- Además, también aprenderá sobre las tecnologías y el diseño utilizado para asegurar y proteger redes inalámbricas y dispositivos, incluyendo la administración de dispositivos móviles y métodos de implementación.

14. Respuesta a incidentes

- Aprenderá sobre incidentes, las políticas, procedimientos y técnicas de respuesta, dando una guía de acción.
- También aprenderá dónde y cómo obtener la información que necesita para los procesos de respuesta, y qué herramientas se usan comúnmente.
- Por último, el curso revisa medidas de mitigación y las técnicas que se utilizan para controlar los ataques y remediar los sistemas.

15. Análisis forense digital

- El curso explora las técnicas y herramientas digitales forenses.
- Aprenderá a descubrir pruebas como parte de las investigaciones, y verá herramientas y procesos forenses claves, y cómo se pueden utilizar juntos para determinar qué salió mal.
- Además, también aprenderá sobre los aspectos legales y los procesos probatorios necesarios para llevar a cabo la investigación forense cuando interviene la aplicación de la ley o el asesor legal.

16. Gobernanza en Ciberseguridad

- Explorá el mundo de las políticas, normas y cumplimiento, elementos fundamentales en cualquier programa de ciberseguridad.
- Aprenderá a escribir las políticas y los mecanismos para hacer cumplir las mismas, y explorará sobre personal, capacitación, datos, credenciales y otros asuntos.
- Además, también aprenderá la importancia de comprensión de las reglamentaciones, leyes y normas que rigen una organización y cómo gestionar el cumplimiento de esos requisitos.
- Marco de ciberseguridad de Uruguay.

17. Gestión de riesgos y privacidad

- El curso describe los conceptos de gestión de riesgos y privacidad que son cruciales para el trabajo de profesionales de la ciberseguridad.
- Aprenderá sobre el proceso de gestión de riesgos, incluida la identificación, evaluación y gestión de riesgos.
- Además, aprenderá sobre las consecuencias de las violaciones de la privacidad y los controles que puede poner en marcha para proteger la privacidad de la identificación personal información.

Entrenamiento Cyberrange

Un Cyberrange es una plataforma en la cual estudiantes pueden utilizar el conocimiento previamente adquirido para resolver un escenario simulado de ataque cibernético en infraestructura virtualizada real.

Esta instancia se lleva a cabo en el Cyberrange del CERTuy, donde se seleccionará un escenario acorde a la temática del curso y al nivel de las personas participantes.