GOBIERNO DE EL SALVADOR

SECRETARÍA DE INNOVACIÓN

aecid

PROGRAMA DEL CURSO

Introducción a CompTIA Security+, brindando marcos generales en materia de ciberseguridad

Duración:
20 horas

Facilitador: Ing. Edgar Antonio Peñate Melgar

DESCRIPCIÓN DEL CURSO 01

La transformación digital es una acción inevitable que impulsa a las organizaciones gubernamentales a adoptar estrategias para garantizar su adopción eficiente, lo que conlleva el aprovechamiento acelerado pero seguro de los recursos tecnológicos involucrados en esta misiva.

Con este curso se pretende proporcionar a los participantes los conocimientos en materia de ciberseguridad, a través de los estándares tecnológicos más importantes a nivel internacional. Asimismo, se busca abordar los conceptos de: técnicas de ingeniería social, indicadores para determinar un tipo de ataque a las aplicaciones, indicadores para determinar un ataque de red; reconocer actores, vectores, fuentes de información y los temas de seguridad asociados con diferentes tipos de vulnerabilidades.

De igual forma se hace énfasis para que el participante conozca y sepa explicar la importancia de conceptos de seguridad en entornos empresariales: virtualización y computación en la nube, conocer los conceptos de desarrollo, despliegue y automatización de aplicaciones, autorización, diseño, resiliencia, implicaciones de seguridad en sistemas embebidos, conceptos básicos de criptografía, y la importancia de controles físicos de seguridad.

Además, durante el desarrollo del contenido se dará a conocer la importancia de políticas, procesos y procedimientos para dar respuesta a incidentes, abordando temas como: técnicas de migración, investigación, y evaluación del estado de la seguridad organizacional, regulaciones aplicables, estándares o marcos que afectan la seguridad de la organización, así como los conceptos de procesos de gestión de riesgos y de privacidad y datos sensibles en relación con la seguridad.

Este curso se implementa con la colaboración de la Cooperación Española a través de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) y el Fondo de Fortalecimiento Institucional para el Desarrollo España – El Salvador, en el marco de la implementación del Plan de Acción código 2744 – 91098 "Innovación tecnológica y metodológica para la formación pública en El Salvador, desde la Dirección General de Formación Tecnológica y Gestión Pública / ENAFOP"

OBJETIVO DEL CURSO

02

- Fortalecer los conocimientos en gestión proactiva de la seguridad informática, con énfasis en la identificación de amenazas y vulnerabilidades, principios de seguridad en materia de arquitectura y diseño, manejo operativo y la respuesta a incidentes, así como el poder implementar gobernanza y gestión de cumplimiento mediante el conocimiento de normas y estándares internacionales en materia de seguridad informática.

INDICADORES DE LOGRO

03

- Identificar los conceptos fundamentales de la seguridad informática
- Identificar las amenazas y vulnerabilidades de seguridad
- Manejo de datos, aplicaciones y seguridad del host
- Implementar la seguridad de la red
- Identificar e implementar el control de acceso y las medidas de seguridad de gestión de cuentas
- Identificar e implementar el cumplimiento y medidas de seguridad operativa
- Gestionar el riesgo
- Solucionar y gestionar los incidentes de seguridad
- Plan de continuidad del negocio y recuperación de desastres

04 METODOLOGÍA

Este curso será impartido en modalidad virtual asincrónica a través de la plataforma de Classroom y se pondrá a disposición de los participantes todos los materiales requeridos para que sean gestores de su propio aprendizaje. Asimismo, durante el desarrollo del curso y con la finalidad de facilitar la comprensión de los contenidos se hará uso de un enfoque práctico en el cual se han diseñado actividades de aprendizaje en donde el facilitador procederá a reforzar el proceso de enseñanza aprendizaje mediante sesiones expositivas y demostrativas, de igual manera se compartirán guías de ejercicios prácticos y casos aplicativos con el objetivo de que el participante ponga en práctica los conocimientos adquiridos en el curso y pueda formar un criterio que le permita brindar soluciones a problemas presentados en los entornos reales de acuerdo con los nuevos enfoques de gestión de la tecnología

ACTIVIDADES DE APRENDIZAJE 05

- Evaluación de ingreso al curso para medir los conocimientos previos de los participantes
- Evaluación al finalizar el curso con el objetivo de medir el nivel de aprendizaje por parte de los participantes.
- Cada jornada de capacitación contará con ejercicios prácticos orientados a reforzar los conocimientos teóricos ejecutados
- Sesiones de aprendizaje demostrativas,

CONTENIDO GENERAL

06

- Concepto de ciberseguridad
- Introducción a CompTIA Security+
- Introducción, en el marco de CompTIA Security+
- Ataques, amenazas y vulnerabilidades
- Arquitectura y diseño
- Operaciones y respuesta a incidentes
- Gobernanza, riesgos y cumplimiento

REQUISITOS DE APROBACIÓN DEL CURSO 07

80%

de asistencia

Aprobación de evaluación final con nota mínima de

7.0

CRONOGRAMA DEL CURSO 08

Introducción a CompTIA Security+, brindando marcos generales en materia de ciberseguridad							
MÓDULOS	Día						
	1	2	3	4	5	6	7
Prueba diagnóstica	■						
M.1: Introducción a la seguridad	■						
M.2: Principios de seguridad en el diseño y arquitectura		■					
M.3: Operaciones y respuesta a incidentes			■				
M.4: Gobernanza Riesgos y Cumplimientos				■	■		
Evaluación final						■	■