

Diplomado en

SEGURIDAD DE LA INFORMACIÓN

100 horas



Diplomado



| PRESENTACIÓN

Este diplomado tiene como objetivo **brindar a los participantes conceptos sólidos asociados a la seguridad de la información** que les permitan **identificar activos de información, gestionar los riesgos asociados a los mismos e implementar controles para su adecuado tratamiento, con el fin de garantizar la confidencialidad, disponibilidad e integridad de dichos activos.**

Para ello, con un enfoque práctico, el diplomado aborda los marcos de referencia más importantes para la gestión de la seguridad de la información, a los que se suman un amplio abanico de controles y herramientas avanzadas para la gestión y prevención de los incidentes de seguridad de la información.

I JUSTIFICACIÓN

La pandemia aceleró la transformación digital de la sociedad y con ello los riesgos a los que están expuestos los activos de información, tanto en el entorno familiar como laboral. Esta nueva realidad plantea la necesidad de desarrollar competencia en materia de seguridad de la información en todos los niveles.

En este sentido el presidente ejecutivo de la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, señaló textualmente en el Informe Tendencias del Cibercrimen en Colombia 2019-2020, que: “los ciberataques a nuestras empresas pueden generar una serie de efectos colaterales que incluyen reducir su productividad, causar daños reputacionales e incluso pueden llegar a generar demandas y otros retos de carácter legal por fuga de información privilegiada y datos sensibles de clientes y proveedores, entre otros” (CCIT, 2019, p. 4).



OBJETIVO GENERAL



Desarrollar en los participantes competencias en el manejo de la seguridad de la información.

OBJETIVOS ESPECÍFICOS

Lograr que los participantes apropien los conocimientos y desarrollen las habilidades necesarias para una gestión eficiente de la seguridad de la información en sus entornos más inmediatos.

Dar a conocer a los participantes los marcos de referencia más importantes para la gestión de la seguridad de la información, junto con un amplio abanico de controles y herramientas avanzadas para la gestión y prevención de los incidentes de seguridad de la información.

Ofrecer a los participantes los conceptos claves asociados a la protección de datos personales en Colombia, para que los puedan aplicar de acuerdo al marco legal en cualquiera de sus posibles roles (titulares, responsables o encargados del tratamiento de datos).

I PERFIL DEL ASPIRANTE

El programa está dirigido a bachilleres, técnicos, tecnólogos y profesionales con conocimientos básicos en el uso de computadores y manejo de internet, interesados en desarrollar competencias en materia de seguridad de la información.



I METODOLOGÍA

El enfoque del diplomado será práctico y con ejercicios dentro de cada módulo, que permitan la aplicación de los conceptos abordados en cada uno de ellos.

El diplomado aplica una metodología participativa, activa y dinámica que permite a los participantes la apropiación de conocimiento para construir su propio saber desde su realidad, entorno a los conceptos de seguridad de la información y su gestión eficiente. Se realizan talleres grupales para fomentar la aplicación de los citados conceptos en el orden temático.

Además, a partir de la intervención activa de los participantes y la creación de espacios para el análisis y reflexión sobre la importancia de conceptualizar se busca reconocer su ámbito de competencia para la construcción de nuevos escenarios para el aprovechamiento de la seguridad de la información en la protección de activos de información.

COMPETENCIAS A DESARROLLAR



Comprende los conceptos básicos de la seguridad de la información.



Reconoce los controles asociados a la seguridad de redes, sistemas, aplicaciones y datos.



Identifica los aspectos claves que intervienen en la gestión e implementación de un sistema de gestión de seguridad de la información.



Comprende los conceptos básicos de la protección de datos personales en Colombia y el principio de responsabilidad demostrada.



CONTENIDO TEMÁTICO

MÓDULO UNO

Introducción a la seguridad de la información (20 horas)

- * Ciclo de vida de la información.
- * Características de la información (integridad, confidencialidad y disponibilidad).
- * ¿Qué es la seguridad de la información?
- * Objetivos de la seguridad de la información.
- * Diferencias entre seguridad de la información, seguridad informática, seguridad digital y la ciberseguridad.
- * El cubo de McCumber.
- * Gobierno de la seguridad de la información.
- * Políticas de seguridad de la información.
- * Roles de la seguridad de la información.
- * Certificaciones de seguridad de la información.

MÓDULO DOS

Conceptos de seguridad de la información (20 horas)

- * Partes interesadas.
- * Activos de información.
- * ¿Qué es el riesgo en el contexto de la seguridad de la información?.
- * Gestión del riesgo e ISO/IEC 27005.
- * Vulnerabilidades
- * Amenazas.
- * Técnicas y tipos de ataque.
- * Aplicaciones en la industria de alimentos.
- * Código malicioso (malware) y ransomware.
- * Eventos de amenaza no adversos.
- * Agentes de amenaza.
- * Riesgos en la computación en la nube y la telefonía móvil.

CONTENIDO TEMÁTICO

MÓDULO TRES

Controles de la seguridad de la información (20 horas)

- * Arquitectura de seguridad de la información.
- * El modelo OSI y el modelo TCP/IP.
- * Seguridad de redes, sistemas, aplicaciones y datos.
- * Controles de procesos.
- * Seguridad física.
- * Anexo A – Norma ISO/IEC 27001.
- * Norma ISO/IEC 27002.
- * Tendencias avanzadas de controles.

MÓDULO CUATRO

Implementación de la seguridad de la información (20 horas)

- * Marcos de referencia de la seguridad de la información.
- * Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000.
- * Tipos de políticas, procesos y procedimientos de seguridad de la información.
- * Gestión de incidentes de seguridad.

CONTENIDO TEMÁTICO

MÓDULO
CINCO

Protección de datos personales (20 horas)

- * Privacidad y protección de datos personales.
- * Régimen de protección de datos en Colombia.
- * Implementación del principio de responsabilidad demostrada.
- * Reporte de bases de datos personales a la Superintendencia de Industria y Comercio (SIC).
- * Norma ISO / IEC 27701.

9

REQUERIMIENTOS

El participante debe disponer de un equipo de cómputo para realizar las prácticas de laboratorio y contar con conexión a internet.

Diplomado



Universidad de
América
Código SNIES 1715

Diplomado en

**SEGURIDAD DE
LA INFORMACIÓN**

100 horas

www.uamerica.edu.co
www.uniamerica.edu.co



Más información:

Oficina de Mercadeo y Admisiones
educacion.continua@uamerica.edu.co

☎ 310 869 6885 ☎ 314 218 1547

☎ 316 629 0450

EcoCampus de Los Cerros: Avenida Cincunvalar No 20 -53

Tel: (60 1) 3376680 / Fax: (60 1) 3362941

Sede Norte: Calle 106 No. 19-18

Tel: (60 1) 6580658

Bogotá D.C., Colombia.