UNIVERSIDAD Piloto DE COLOMBIA

Diplomado en

CIBERSEGURIDAD

Diplomado en

CIBERSEGURIDAD

Este Diplomado contribuye a formar personas con capacidades técnicas para apoyar las áreas de tecnología en temas de ciberseguridad de cualquier organización pública o privada.

Información general

Duración
140 horas

Horario
100% Virtual*

Metodología y sedes
100% Virtual*

Justificación

El ritmo acelerado de los ataques y la aparente tendencia hacia más vulnerabilidades parecen sugerir que la brecha entre los ataques y la protección de datos se está ampliando a medida que nuestra capacidad para lidiar con ellos parece disminuir por la falta de recurso humano con conocimientos detallados para cerrar dicha brecha, es por ello que el diplomado en Ciberseguridad contribuye a formar personas con capacidades técnicas para apoyar las áreas de tecnología de cualquier organización pública o privada.

Diplomado Virtual en

CIBERSEGURIDAD

Perfiles de ingreso

Este diplomado está dirigido a personal técnico de áreas de tecnología de cualquier organización, preferiblemente con estudios técnicos, tecnológicos o profesionales en sistemas o telecomunicaciones.

Propósitos de formación

Este diplomado tiene como propósito socializar los conocimientos básicos relacionados con la protección de la información y los entornos tecnológicos como herramientas claves de ciberseguridad. Igualmente, contribuir en el desarrollo de las destrezas y habilidades para; apoyar procesos de implementación de sistemas de gestión de la seguridad, análisis de riesgos y mitigación de vulnerabilidades tecnológicas.

Competencias a desarrollar

Al finalizar el Diplomado, el participante habrá desarrollo las capacidades para:

- Identificar los principales tipos de ataque o ciberataques.
- Identificar definiciones básicas claves relacionadas con la ciberseguridad.
- Identificar, elegir y aplicar los modelos existentes para la implementación de un programa de ciberseguridad y de un modelo de gestión de riesgos en ciberseguridad.
- Apropiar y aplicar los mecanismos que les permitan a las organizaciones enfrentar los ataques del mundo real a través de un plan de ciberseguridad orientado a la atención de incidentes.
- Identificar los elementos vulnerables en un entorno tecnológico.
- Describir los factores que contribuyen a las vulnerabilidades.
- Mitigar las vulnerabilidades existentes.

Plan de estudios

Módulo 1

FUNDAMENTOS DE CIBERSEGURIDAD

Al finalizar el módulo el participante habrá desarrollo las capacidades para:

- Definir claramente que es ciberseguridad.
- Identificar los principales tipos de ataque o ciberataques
- Identificar definiciones básicas claves relacionadas con la ciberseguridad.

- Definiciones.
- Ciberdefensa: axiomas de la ciberdefensa.
- Ciberataques.
- Ciberatacantes: amenazas básicas, hacktivistas, crimen organizado, espionaje, ciberguerra.

Módulo 2

FRAMEWORKS DE CIBERSEGURIDAD

Al finalizar el módulo el participante habrá desarrollo las capacidades para:

- Identificar, elegir y aplicar los modelos existentes para la implementación de un programa de ciberseguridad.
- Identificar, elegir y aplicar los modelos existentes para la implementación de modelo de gestión de riesgos en ciberseguridad.

- El programa de ciberseguridad: elementos para un programa efectivo de ciberseguridad.
- Estándares (NIST / ISO).
- Gestión del riesgo: (ISO 27001 / NIST – SP 800-53, 2020 / MAGERIT).

Los Conferencistas

- Álvaro Escobar Escobar.

Diplomado Virtual en

CIBERSEGURIDAD

Módulo 3

LA CIBERDEFENSA

Al finalizar el módulo el participante habrá desarrollo las capacidades para apropiar y aplicar los mecanismos que les permitan a las organizaciones enfrentar los ataques del mundo real a través de un plan de ciberseguridad orientado a la atención de incidentes.

- El ciberataque tipos y etapas: tipos (dirigidos y no dirigidos), etapas de un ataque.
- La ciberdefensa efectiva: elementos de una ciberdefensa efectiva.

Módulo 4

VULNERABILIDADES EN CIBERSEGURIDAD

Al finalizar el módulo el participante habrá desarrollo las capacidades para:

- Identificar los elementos vulnerables en un entorno tecnológico.
- Describir los factores que contribuyen a las vulnerabilidades.
- Mitigar las vulnerabilidades existentes.

- Identificación.
- Evaluación.
- Gestión.
- Herramientas: herramientas de evaluación de vulnerabilidades, programa de gestión de vulnerabilidades.

Módulo 5

AUDITOR INTERNO ISO 27001

Al finalizar el módulo el estudiante deberá implementar y auditar correctamente, en una organización, un sistema de gestión de seguridad de la información de acuerdo a los lineamientos de la norma ISO 27001.

- Interpretación de la norma desde el enfoque de la auditoría.
- Requisitos de documentación y la diferencia entre varias formas de documentos, sus diferencias y características.
- Tipos de auditorías, sus características distintivas y beneficios.
- Auditoría al Sistema de Gestión de Seguridad de la Información ISO 27001.
- Beneficios de una auditoría de primera parte.
- Papel de un auditor en la planificación, realización, informe y seguimiento de una auditoría a un Sistema de Gestión de Seguridad de la Información y la Ciberseguridad; según directrices de ISO 19011:2018.
- Planificación de una auditoría (incluyendo la elección y dirección de un equipo auditor).
- Realización de una auditoría para la Gestión de Seguridad de la Información.
- Habilidades interpersonales y de entrevistador eficaces adecuadas a una situación de auditoría - rol play en casos prácticos.
- Redacción de hallazgos de la auditoría.
- Seguimiento a la auditoría.
- Preparación para el examen de conocimientos.
- Examen de conocimientos (2 horas).

Recursos tecnológicos
requeridos en modalidad virtual

Requerimientos mínimos de la herramienta para un adecuado funcionamiento: Contar con un equipo de cómputo que tenga un sistema operativo en distribución Microsoft Windows 8 como mínimo y en distribución Mac, Mac OS 10.6 como mínimo, el equipo debe contar con tarjeta de sonido con micrófono y altavoces (recomendado el uso de auriculares con micrófono integrado) y cámara web, a su vez el equipo debe tener 1GB de Memoria RAM disponible al momento de realizar la videoconferencia, 40 MB de espacio en el disco duro. Asegúrese de no tener virus que afecten el adecuado funcionamiento.

Se siguiere contar con un ancho de banda de internet mínimo de 5MB para poder compartir archivos, aplicaciones y realizar la videoconferencia sin problema, se recomienda conectarse a internet por cable para tener una mejor conectividad, asegúrese de contar con las últimas actualizaciones de los navegadores de internet como los son: Chrome, Firefox, Safari, del mismo modo se deberá tener actualizada la versión java del equipo.

Para dispositivos móviles se deberá contar con el sistema operativo actualizado y solo podrá ser utilizado como estudiante debido a que no permite la moderación de la videoconferencia.

Recomendaciones
Generales

- Se recomienda que la persona que aspira al programa tenga dominio de software, especialmente Excel, Word, Power Point y navegabilidad en Internet.
- Se dispone de un aula virtual con diferentes recursos educativos y se facilita la interacción entre el participante y el tutor a través de encuentros sincrónicos.
- Los diferentes recursos educativos virtuales podrán ser visualizados desde cualquier dispositivo móvil celular/tablets (Android o IOS), sistema operativo (Windows, Mac, Linux), navegador de internet, (Mozilla, Chrome, Zafari, Explorer) teniendo como único requisito técnico una adecuada conexión a internet.
- El certificado de asistencia de programas virtuales se entrega de manera digital (vía correo electrónico).

*Metodología
Virtual

uso de plataforma virtual para el estudio autónomo del estudiante con encuentros sincrónicos programados para la aclaración de inquietudes. Para determinar la asistencia al diplomado virtual, se realizará con un control a la entrega de las actividades que se tengan planteadas para el programa académico, las cuales pueden incluir: interacción y desarrollo de contenidos de la plataforma virtual, talleres, ejercicios, encuentros sincrónicos, foros, etc., esta información, será tomada como soporte para la determinación de la asistencia al programa. Se otorga certificado digital con el 80% de asistencia y/o participación y entrega de las actividades del diplomado. La duración de un programa virtual estará dada de acuerdo con la fecha final estipulada en el cronograma de actividades, fecha en la cual se dará cierre y se consolida la información para la entrega de los respectivos certificados.

Requisitos para ingreso

- Formulario de inscripción diligenciado y con firma.
- 2 fotografías tipo documento 3×4 fondo blanco.*
- Fotocopia de la cédula de ciudadanía ampliada al 150% o equivalente según el país de origen del estudiante, pasaporte y visa.

* Las fotografías deben ser en alta resolución, no tener más de 6 meses de antigüedad, centrada y enfocada, la cara debe aparecer mirando directamente a la cámara, no de perfil ni mirando por encima del hombro, y no debe haber sombras sobre la cara ni sobre el fondo. No se aceptarán fotos con gafas de fantasía ni con reflejos en los cristales, ni con sombrero, gorro, pañuelo o visera. En caso de traer la documentación por medio físico, se debe tener en cuenta que las fotografías deben ser impresas en papel de calidad fotográfica (no papel común).

Descuentos y Entidades FINANCIERAS

Para mayor información sobre los **DESCUENTOS** que ofrece la Universidad a sus aspirantes y egresados:
http://www.unipiloto.edu.co/descargas/DESCUENTOS_EC.pdf

Aplican convenios con **ENTIDADES FINANCIERAS** vigentes. para mayor información:
http://www.unipiloto.edu.co/descargas/ENTIDADES-FINANCIERAS_2019.pdf

La información estará sujeta a cambios según disposiciones de cada entidad.

Contáctenos

Posgrados y Educación Continuada
Universidad Piloto de Colombia
postgrados@unipiloto.edu.co
www.unipiloto.edu.co

PBX: 580 0968
Whatsapp: 318 280 0923

Calle 45 A No. 9 - 17 | Bogotá - Colombia.

"La Universidad se reserva el derecho de apertura o aplazamiento de los programas en caso de no contar con el número mínimo de inscritos. El grupo docente estará sujeto a cambios según disponibilidad de su agenda al igual que el cronograma y horarios de actividades académicas"

Para todos los efectos, la presentación al proceso de inscripción, admisión y matrícula a cada programa hace constar el conocimiento y aceptación de lo dispuesto en el Reglamento Estudiantil de Posgrados vigente, el cual puede consultar en www.unipiloto.edu.co. Se enfatiza de manera particular el Artículo 28 (Cancelación de matrícula), el Artículo 29 (Abonos y devoluciones) y el Artículo 33 (Asistencia y participación en las actividades curriculares).

VIGILADA MINEDUCACIÓN

Institución de educación superior sujeta a la inspección y vigilancia del Ministerio de Educación Nacional de Colombia. Reconocimiento de personería jurídica como institución de educación superior con Resolución No. 3681 del 27 de noviembre de 1962 del Ministerio de Educación Nacional de Colombia. Código institución: 1815.
Vigencia desde 2024