

DIPLOMATURA EN SEGURIDAD INFORMÁTICA Y AUDITORÍA DE SISTEMAS

- INICIO INMEDIATO -

INTRODUCCIÓN

Esta diplomatura capacita al estudiante para entender las funciones, las actividades, la operación y el desarrollo de nuevas técnicas innovadoras y la implementación de estos sistemas y de sus responsables, así como la correcta administración, el aprovechamiento, la seguridad y el control de equipos de cómputo, hardware, software, bases de datos, información, periféricos y de todos los componentes relacionados con los sistemas informáticos.

OBJETIVOS

- Entender los conceptos básicos de ciberseguridad y seguridad de la información.
- Poder participar en la creación de programas de seguridad de la información.
- Aumentar la seguridad de la información de su organización o institución al conocer los conceptos y políticas.
- Elaborar estrategias para lograr una correcta privacidad informática.

MODALIDAD 100% ONLINE

VALORACIÓN DE
NUESTROS ESTUDIANTES

4,8 / 5

Hacé click aquí para ver las opiniones

ESEP
ESCUELA SUPERIOR
DE ESTUDIOS PROFESIONALES



AULA VIRTUAL

Disponible los 365 días del año, las 24 hs. Podés ingresar desde cualquier dispositivo, en tu casa, en el trabajo o donde quieras. También podrás descargar o imprimir el material.



DOCENTES PROFESIONALES

La capacitación tiene como tutor un docente experimentado en la materia, quien te guiará y ayudará durante todo el proceso de aprendizaje.



DÍAS Y HORARIOS FLEXIBLES

Vos decidís cuando estudiar en función de tus tiempos libres, tus días y horarios disponibles.

- Interpretar los controles de los sistemas de información, las técnicas disponibles y el rol del Auditor.
- Desarrollar los conocimientos necesarios para, que al detectar riesgos y/o debilidades en los sistemas evaluados, pueda efectuar recomendaciones orientadas a fortalecer las debilidades detectadas.
- Interpretar un informe de auditoría, de manera de poder implementar sus recomendaciones.

DESTINATARIOS

Quien busque una rápida salida laboral en el ámbito de la auditoría o contadores o auditores que quieran especializarse esta rama.

Profesionales y entusiastas de la tecnología, técnicos en informática, personas que trabajan en áreas de sistemas, estudiantes de ingeniería y carreras relacionadas, público en general con conocimientos básicos de informática interesado en esta temática.

Además, quien busque un cambio de pensamiento superador para el uso de herramientas o instrumentos básicos, con el fin de considerar las acciones informáticas en los sistemas diarios de la organización.

DURACIÓN

Dependerá del ritmo de estudio del alumno. Son 12 unidades, se estima un promedio de 3 meses.

ESEP
ESCUELA SUPERIOR
DE ESTUDIOS PROFESIONALES



CERTIFICADO

Una vez finalizada la cursada, podrás descargar una certificación digital que acredita los conocimientos adquiridos. También tendrás la posibilidad de acceder a una certificación profesional adicional.



ORIENTADO AL MERCADO LABORAL

Basado y actualizado en función de los requerimientos del mercado laboral. Totalmente práctico para que sepas qué hacer y cómo hacerlo en cada situación que se te presente.



BOLSA DE EMPLEOS

Descubrí oportunidades laborales que se ajusten a tus intereses y metas profesionales.

PLAN DE ESTUDIOS

Seguridad Informática

Unidad 1: Seguridad de la Información. Concepto, Concepción de la Seguridad de la Información. Principios Básicos: Confidencialidad, Integridad y Disponibilidad. Autenticación o autentificación, Tipos de autenticación, Características y Mecanismos de la autenticación.

Unidad 2: Seguridad de la Información. Servicios de Seguridad, Protocolos de Seguridad de la Información. La Seguridad de la Información, según la Norma ISO/IEC-27001. Elementos o Fases para la Implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Implementando la Norma ISO/IEC-27001. Política General de Seguridad de la Información. Análisis y Evaluación de Riesgos. Método de Análisis, Evaluación y Tratamiento del Riesgo. Auditorías para la Norma ISO/IEC-27001. Beneficios de la Norma ISO/IEC-27001. Sistema de Gestión de la Seguridad de la Información utilizando O-ISM3.

Unidad 3: Seguridad Informática. Objetivos y Tipos de Seguridad Informática: Seguridad Informática de Hardware, de Software y de Red. Métodos de Seguridad Informática de Red. Seguridad Informática de Red en la Nube Concepto de Amenazas. Algunos Tipos de Amenazas: Malware, Spyware, Ransomware, Spoofing, Troyan Horse, Worms, BackDoor, Botnets, Spam, Trashing. Ingeniería Social. Tipos de Ataques de Ingeniería Social: Hunting y Farming. Técnicas de Ingeniería Social: Pretextos, Shoulder Surfing, Phishing, Masquerading, Baiting, Scavening y Vishing.

ESEP
ESCUELA SUPERIOR
DE ESTUDIOS PROFESIONALES



Unidad 4: Seguridad Informática. Algunos Tipos de Ataques Informáticos: Ataque por Denegación de Servicio, Ataque por Técnicas de Escaneo de Puertos, Ataque por Suplantación de Identidad ARP, Ataque por Saturación de ICMP, Ataque a través de Intermediario, Ataques para Secuestro de Datos, Ataques por Ingeniería Social, Ataque por Determinación de Sistema Operativo, Ataque por Grabación de Teclas Oprimidas y Ataque por Virus Informáticos. Amenazas Informáticas del Futuro. Prácticas Útiles para Aplicar en Seguridad Informática. Algunos Consejos de Seguridad Informática. Aspectos para Seleccionar el mejor Software de Seguridad Informática.

Auditoría de Sistemas

Unidad 1. Conceptos básicos de la auditoría de sistemas de información. Tecnología de Información. Qué es la información. Clasificación de la información. Información estratégica. Información para el control de gestión. Información técnica u operacional. Información contable y financiera. Atributos de la información. Necesidad de la Auditoría Informática. Clasificación de los tipos de Auditorías según el lugar de aplicación. Auditoría externa. Auditoría interna. Auditoría por su lugar de origen. Auditoría externa. Auditoría interna. Auditoría de sistemas informáticos con y sin la computadora. Auditoría a la gestión informática. Auditoría al sistema de cómputo. Auditoría alrededor de la computadora. Auditoría en la seguridad de los sistemas informáticos. Auditoría a los sistemas de redes. Auditoría integral a los centros de cómputo. Auditoría ISO-9000 a los sistemas informáticos. Auditoría outsourcing. Auditoría ergonómica de sistemas informáticos.

Unidad 2. Objetivos de la auditoría de sistemas. Marco esquemático. Hardware. Software. Ejemplo de relevamiento de datos en Hw y Sw. Gestión informática. Información. Diseño de sistemas. Base de datos. Seguridad. Redes Especializadas.

ESEP
ESCUELA SUPERIOR
DE ESTUDIOS PROFESIONALES



Unidad 3. Metodología y Alcance en la Auditoría de Sistemas. Metodología de trabajo. Etapas. Herramientas y Técnicas para la Auditoría. CRMR (Computer Resource Management Review). Evaluación de la gestión de recursos informáticos. Metodología CRMR. Áreas de Aplicación. Objetivos. Alcance. Información necesaria para la evaluación CRMR. Información necesaria para la realización CRMR. Caso Práctico de una Auditoría de Seguridad Informática. Alcance de la auditoría.

Unidad 4. Análisis de Riesgos. Concepto. Enfoques. Amenazas. Vulnerabilidad. Análisis. Políticas de Seguridad. Etapas de seguridad. Riesgos de auditoría. Tipos de Riesgo en la Auditoría de Sistemas.

Unidad 5. Control Interno Informático. Concepto. Tipos de control interno. Objetivos principales del CII. Función del control interno. Áreas de aplicación del CII. Controles generales organizativos. Controles de desarrollo y mantenimiento de SI. Controles de explotación de SI. Controles en aplicaciones. Controles en sistemas de gestión de BD. Controles informáticos sobre redes. Controles sobre computadores y redes. Herramientas del CII. Implantación de un sistema de CII.

Unidad 6. El planeamiento, la ejecución y el dictamen de las auditorías. Etapas de la fase de planeamiento. Ejecución de las auditorías. Presentación de una auditoría tipo. Técnicas de recopilación de evidencias. Vista preliminar. Contacto inicial con personal del área. Identificación preliminar de la problemática. Objetivos Específicos. Determinar los puntos que serán evaluados en la Auditoría. Evaluación de las funciones y actividades del personal del área. Planilla proforma del plan de Auditoría. Guía del Plan de Auditoría. Diseño de un formulario tipo para encuesta al coordinador del aula informática. Ejecución. Dictamen. Conclusión de la Auditoría.

ESEP
ESCUELA SUPERIOR
DE ESTUDIOS PROFESIONALES



Unidad 7. El informe en la auditoría. Características del Informe de Auditoría. Características fundamentales. Característica de fondo. Característica de forma. Característica de la presentación del Informe. Características importantes para el lector del IA. Procedimientos para elaborar el IA. Instrumentos de recopilación. Importancia del uso de herramientas. Estructura del Informe de Auditoría. Desarrollo de la estructura del IA. Situaciones detectadas. Anexo modelo. Ejemplo de Auditoría.

Unidad 8. Organismos, normas y certificaciones de auditoría de sistemas de información: ISO, ISACA, COSO, CISA, COBIT, etc. ¿Qué es ISACA? Objetivos. Normas ISO. ISO 17799. BS 7799. ISO/IEC 27002. COBIT. ISC2. CISM. CISSP. COSO. NIA 315.

La Escuela Superior de Estudios Profesionales (ESEP), en conjunto con el Instituto de Estudios Superiores de Buenos Aires (ESBA), unen su experiencia y trayectoria para ofrecerte esta capacitación que te introducirá al mundo de la Seguridad Informática y la Auditoría de Sistemas de una manera clara, didáctica y sencilla, que te permitirá obtener importantes conocimientos en esta temática iniciando desde cero, en clases virtuales, sin días ni horarios fijos de cursada, acompañados por docentes profesionales en la materia y a tu propio ritmo.

ESEP ESCUELA SUPERIOR DE ESTUDIOS PROFESIONALES

ESBA ESTUDIOS SUPERIORES DE BUENOS AIRES

www.esep.com.ar

11 3384-7000

contacto@esep.com.ar

ESEP ESCUELA SUPERIOR DE ESTUDIOS PROFESIONALES