Maestría

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: 20232122

RVOE
EDUCACIÓN SUPERIOR

tech universidad tecnológica

tech universidad tecnológica

Maestría

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: **20232122**
Fecha de RVOE: **24/07/2023**
Modalidad: **100% en línea**
Duración: **20 meses**
Acceso web: www.techtitute.com/mx/informatica/maestria/maestria-gestion-politicas-seguridad-informatica-empresa

Índice

01

Presentación

En un mundo digitalizado e informatizado es esencial que las compañías cuenten con Políticas de Seguridad para evitar la pérdida de datos o el robo de información confidencial que provoquen pérdidas financieras, de reputación y de clientes. Por esta razón, en los últimos años estas acciones de protección cobran vital transcendencia en el día a día de las organizaciones. En este sentido, es esencial contar con perfiles profesionales especializados y con capacidad de liderazgo capaz de implementar estrategias adecuadas en aras de evitar ataques externos a los sistemas informáticos. Así, nace esta titulación 100% online que ofrece al alumnado el conocimiento más actual y avanzado en este campo a través de un temario elaborado por auténticos expertos.

Posiciónate como un director líder en la implementación de Políticas de Seguridad Informática en tu empresa"

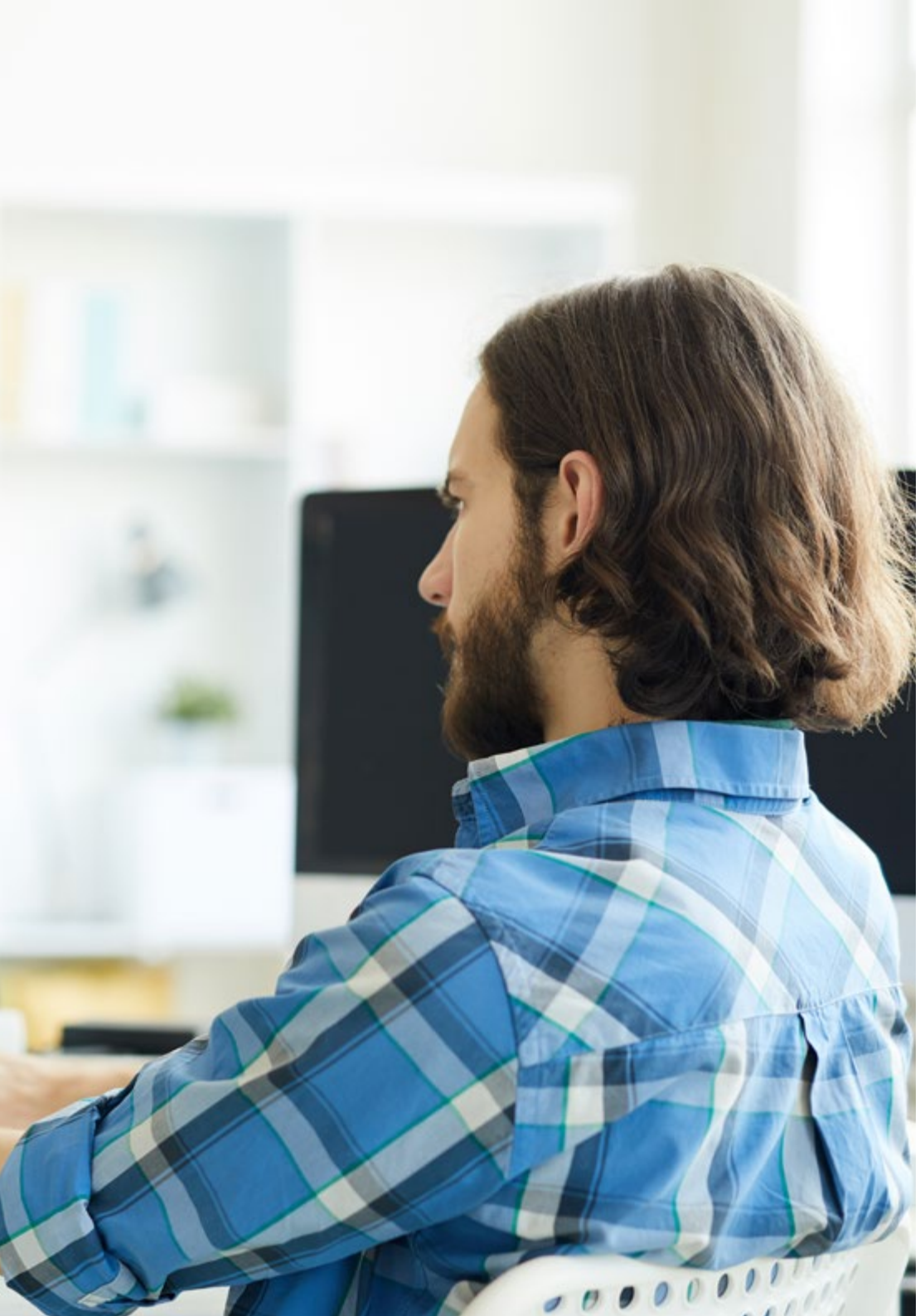
La constante evolución de la tecnología y el proceso constante de digitalización de todos los sectores socioeconómicos hace indispensable la adopción de medidas de protección ante ataques cibernéticos o pérdida de datos cruciales. En este sentido, la labor de dirección de estas Políticas se presenta hoy en día como indispensable en toda organización.

En este sentido, la cultura de seguridad debe partir de la más alta dirección e integrar al resto de miembros de la compañía, quienes deben ser consciente de la trascendencia de contar con dichas medidas para evitar pérdidas económicas y de clientes. Dada su trascendencia, TECH ha diseñado esta Maestría con RVOE y una metodología 100% online que aporta flexibilidad para cursarla.

Se trata de un programa avanzado que contiene un temario elaborado por un excelente equipo de especialistas en Ciberseguridad y sus áreas afines. De esta manera, el alumnado a lo largo de este itinerario académico adquirirá un aprendizaje esencial para trazar las estrategias más efectivas en Políticas de Seguridad Informática. Para ello, dispone de recursos didácticos innovadores y un enfoque teórico-práctico que le resultará de gran utilidad para su desempeño diario.

Asimismo, gracias al método *Relearning*, basado en la reiteración continuada de los conceptos clave, el egresado conseguirá obtener una enseñanza mucho óptima y disminuir las largas horas de memorización.

Sin duda, una opción académica inigualable que irrumpe en el ámbito académico con una pedagogía efectiva y acorde a los tiempos actuales. Y es que, el alumnado tan solo necesita de un dispositivo digital con conexión a internet para visualizar, en cualquier momento del día, el temario alojado en la plataforma virtual. Así, sin presencialidad, ni clases con horarios fijos, el egresado tendrá una mayor libertad para autogestionar su tiempo de estudio.



TECH brinda la oportunidad de obtener la Maestría en Gestión de Políticas de Seguridad Informática en la Empresa en un formato 100% en línea, con titulación directa y un programa diseñado para aprovechar cada tarea en la adquisición de competencias para desempeñar un papel relevante en la empresa. Pero, además, con este programa, el estudiante tendrá acceso al estudio de idiomas extranjeros y formación continuada de modo que pueda potenciar su etapa de estudio y logre una ventaja competitiva con los egresados de otras universidades menos orientadas al mercado laboral.

Un camino creado para conseguir un cambio positivo a nivel profesional, relacionándose con los mejores y formando parte de la nueva generación de futuros directores de Políticas de Seguridad Informática capaces de desarrollar su labor en cualquier lugar del mundo.

Matricúlate ya en una titulación con validez oficial en México y convalidable en otros países”

02

Plan de estudios

Este programa de alto nivel ha sido diseñado por un grupo profesionales con elevadas competencias en el sector de la Seguridad Informática. Su experiencia, así como su profundo conocimiento en este campo, le permitirá al alumnado estar al tanto de las últimas tendencias y avances en la protección de información y sistemas cruciales para las organizaciones. Para ello, TECH facilita herramientas pedagógicas en las que ha empleado la última tecnología aplicada a la enseñanza.

Accede cuando lo desees, desde tu Tablet con conexión a internet a la información más actual en Seguridad Informática"

El plan de estudios de esta titulación se imparte en un formato pedagógico exclusivamente en línea y sin clases con horarios encorsetados. Una flexibilidad, que permite al alumnado conciliar sus responsabilidades profesionales y personales más exigentes con una Maestría de calidad.

Todo esto, además, será posible gracias a la multitud de recursos pedagógicos basado en vídeo resúmenes de cada tema, vídeos en detalle, simulaciones de casos de estudio y lecturas especializadas con las que el estudiante podrá extender aún más la información facilitada en esta titulación. Instrumentos todos ellos, que dan un plus a este dinámico y atractivo aprendizaje, que conducirá al alumno a progresar en su carrera de manera notoria.

Con esta enseñanza serás capaz de tomar decisiones mucho más certeras ante los posibles riesgos de la exposición de datos de una empresa"

Módulo 1	Sistema de gestión de seguridad de información
Módulo 2	Aspectos organizativos en Políticas de Seguridad de la Información
Módulo 3	Políticas de Seguridad para el análisis de amenazas en sistemas informáticos
Módulo 4	Implementación de Políticas de Seguridad en software y hardware
Módulo 5	Políticas de gestión de incidencias de seguridad
Módulo 6	Implementación de Políticas de Seguridad física y ambiental en la empresa
Módulo 7	Políticas de comunicaciones seguras en la empresa
Módulo 8	Implementación de Políticas de Seguridad ante ataques
Módulo 9	Herramientas de monitorización en Políticas de Seguridad de los sistemas de información
Módulo 10	Políticas de recuperación de desastres de seguridad

Dónde, cuándo y cómo se imparte

Esta Maestría se ofrece 100% en línea, por lo que alumno podrá cursarla desde cualquier sitio, haciendo uso de una computadora, una tableta o simplemente mediante su smartphone.

Además, podrá acceder a los contenidos tanto online como offline. Para hacerlo offline bastará con descargarse los contenidos de los temas elegidos, en el dispositivo y abordarlos sin necesidad de estar conectado a internet.

El alumno podrá cursar la Maestría a través de sus 10 módulos, de forma autodirigida y asincrónica. Adaptamos el formato y la metodología para aprovechar al máximo el tiempo y lograr un aprendizaje a medida de las necesidades del alumno.

Sumado al contenido académico más riguroso y actualizado del mercado, encontrarás las mejores herramientas tecnológicas de aprendizaje"

Módulo 1. Sistema de gestión de seguridad de información

1.1. Seguridad de la información. Aspectos Clave
- 1.1.1. Seguridad de la información
- 1.1.2. Confidencialidad
- 1.1.3. Integridad
- 1.1.4. Disponibilidad
- 1.1.5. Medidas de seguridad de la información

1.2. Sistema de gestión de la seguridad de la información
- 1.2.1. Modelos de Gestión de Seguridad de la Información
- 1.2.2. Documentos para implantar un Sistema de Gestión de Seguridad de la Información (SGSI)
- 1.2.3. Niveles y controles de un Sistema de Gestión de Seguridad de la Información (SGSI)

1.3. Normas y estándares internacionales
- 1.3.1. Estándares internacionales en la seguridad de la información
- 1.3.2. Origen y evolución del estándar
- 1.3.3. Estándares internacionales gestión de la seguridad de la información
- 1.3.4. Otras normas de referencia

1.4. Normas ISO/IEC 27000
- 1.4.1. Objeto y ámbito de aplicación
- 1.4.2. Estructura de la norma
- 1.4.3. Certificación
- 1.4.4. Fases de acreditación
- 1.4.5. Beneficios de las Normas ISO/IEC 27000

1.5. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.1. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.2. Fases de Implantación de un Sistema General de Seguridad de Información
- 1.5.3. Plan de Continuidad de Negocio

1.6. Fase I: diagnóstico
- 1.6.1. Diagnóstico preliminar
- 1.6.2. Identificación del nivel de estratificación
- 1.6.3. Nivel de cumplimiento de estándares/normas

1.7. Fase II: preparación
- 1.7.1. Contexto de la organización
- 1.7.2. Análisis de normativas de seguridad aplicables
- 1.7.3. Alcance del Sistema General de Seguridad de Información
- 1.7.4. Política del Sistema General de Seguridad de Información
- 1.7.5. Objetivos del Sistema General de Seguridad de Información

1.8. Fase III: planificación
- 1.8.1. Clasificación de activos
- 1.8.2. Valoración de riesgos
- 1.8.3. Identificación de amenazas y riesgos

1.9. Fase IV: implantación y seguimiento
- 1.9.1. Análisis de resultados
- 1.9.2. Asignación de responsabilidades
- 1.9.3. Temporalización del Plan de Acción
- 1.9.4. Seguimiento y auditorias

1.10. Políticas de Seguridad en la gestión de incidentes
- 1.10.1. Fases
- 1.10.2. Categorización de incidentes
- 1.10.3. Procedimientos y gestión de incidentes

Módulo 2. Aspectos organizativos en Políticas de Seguridad de la Información

2.1. Organización interna
- 2.1.1. Asignación de responsabilidades
- 2.1.2. Segregación de tareas
- 2.1.3. Contactos con autoridades
- 2.1.4. Seguridad de la información en gestión de proyectos

2.2. Gestión de activos
- 2.2.1. Responsabilidad sobre los activos
- 2.2.2. Clasificación de la información
- 2.2.3. Manejo de los soportes de almacenamiento

2.3. Políticas de seguridad en los procesos de negocio
  2.3.1. Análisis de los procesos de negocio vulnerables
  2.3.2. Análisis de impacto de negocio
  2.3.3. Clasificación procesos respecto al impacto de negocio
2.4. Políticas de seguridad ligada a los Recursos Humanos
  2.4.1. Antes de contratación
  2.4.2. Durante la contratación
  2.4.3. Cese o cambio de puesto de trabajo
2.5. Políticas de Seguridad en Dirección
  2.5.1. Directrices de la Dirección en seguridad de la información
  2.5.2. Analizando del impacto en el negocio
  2.5.3. Plan de recuperación como política de seguridad
2.6. Adquisición y mantenimientos de los sistemas de información
  2.6.1. Requisitos de seguridad de los sistemas de información
  2.6.2. Seguridad en los datos de desarrollo y soporte
  2.6.3. Datos de prueba
2.7. Seguridad con Suministradores
  2.7.1. Seguridad informática con suministradores
  2.7.2. Gestión de la prestación del servicio con garantía
  2.7.3. Seguridad en la cadena de suministro
2.8. Seguridad operativa
  2.8.1. Responsabilidades en la operación
  2.8.2. Protección contra código malicioso
  2.8.3. Copias de seguridad
  2.8.4. Registros de actividad y supervisión
2.9. Gestión de la seguridad y normativas
  2.9.1. Gestión de la seguridad y normativas
  2.9.2. Cumplimiento de los requisitos legales
  2.9.3. Revisiones en la seguridad de la información
2.10. Seguridad en la gestión para la continuidad de negocio
  2.10.1. Seguridad en la gestión para la continuidad de negocio
  2.10.2. Continuidad de la seguridad de la información
  2.10.3. Redundancias

Módulo 3. Políticas de Seguridad para el análisis de amenazas en sistemas informáticos

3.1. La gestión de amenazas en las Políticas de Seguridad
  3.1.1. La gestión del riesgo
  3.1.2. El riesgo en seguridad
  3.1.3. Metodologías en la gestión de amenazas
  3.1.4. Puesta en marcha de metodologías
3.2. Fases de la gestión de amenazas
  3.2.1. Identificación
  3.2.2. Análisis
  3.2.3. Localización
  3.2.4. Medidas de salvaguarda
3.3. Sistemas de auditoria para localización de amenazas
  3.3.1. Sistemas de auditoría para la localización de amenazas
  3.3.2. Clasificación y flujo de información
  3.3.3. Análisis de los procesos vulnerables
3.4. Clasificación del riesgo
  3.4.1. Tipos de riesgo
  3.4.2. Cálculo de la probabilidad de amenaza
  3.4.3. Riesgo residual
3.5. Tratamiento del riesgo
  3.5.1. Tratamiento del riesgo
  3.5.2. Implementación de medidas de salvaguarda
  3.5.3. Transferir o asumir
3.6. Control de riesgo
  3.6.1. Proceso continuo de gestión de riesgo
  3.6.2. Implementación de métricas de seguridad
  3.6.3. Modelo estratégico de métricas en seguridad de la información
3.7. Metodologías prácticas para el análisis y control de amenazas
  3.7.1. Catálogo de amenazas
  3.7.2. Catálogo de medidas de control
  3.7.3. Catálogo de salvaguardas

3.8. Norma ISO 27005
- 3.8.1. Identificación del riesgo
- 3.8.2. Análisis del riesgo
- 3.8.3. Evaluación del riesgo

3.9. Matriz de riesgo, impacto y amenazas
- 3.9.1. Datos, sistemas y personal
- 3.9.2. Probabilidad de amenaza
- 3.9.3. Magnitud del daño

3.10. Diseño de fases y procesos en el análisis de amenazas
- 3.10.1. Identificación elementos críticos de la organización
- 3.10.2. Determinación de amenazas e impactos
- 3.10.3. Análisis del impacto y riesgo
- 3.10.4. Metodologías

Módulo 4. Implementación de Políticas de Seguridad en software y hardware

4.1. Implementación práctica de Políticas de Seguridad en software y hardware
- 4.1.1. Implementación de identificación y autorización
- 4.1.2. Implementación de técnicas de identificación
- 4.1.3. Medidas técnicas de autorización

4.2. Tecnologías de identificación y autorización
- 4.2.1. Identificador y contraseña de un único uso
- 4.2.2. Token o tarjeta inteligente
- 4.2.3. La llave "Confidencial Defensa"
- 4.2.4. Tecnología RFID (identificación por radiofrecuencia) Activo

4.3. Políticas de seguridad en el acceso a software y sistemas
- 4.3.1. Implementación de políticas de control de accesos
- 4.3.2. Implementación de políticas de acceso a comunicaciones
- 4.3.3. Tipos de herramientas de seguridad para control de acceso

4.4. Gestión de acceso a usuarios
- 4.4.1. Gestión de los derechos de acceso
- 4.4.2. Segregación de roles y funciones de acceso
- 4.4.3. Implementación derechos de acceso en sistemas

4.5. Control de acceso a sistemas y aplicaciones
- 4.5.1. Norma del mínimo acceso
- 4.5.2. Tecnologías seguras de inicios de sesión
- 4.5.3. Políticas de seguridad en contraseñas

4.6. Tecnologías de sistemas de identificación
- 4.6.1. Directorio activo
- 4.6.2. Contraseña dinámica
- 4.6.3. Protocolo de autenticación por desafío mutuo
- 4.6.4. Protocolo de autentificación de contraseña
- 4.6.5. Protocolos de autentificación KERBEROS, DIAMETER, NTLM

4.7. Controles críticos de seguridad informática para bastionado de sistemas
- 4.7.1. Controles básicos
- 4.7.2. Controles fundamentales
- 4.7.3. Controles organizacionales

4.8. Seguridad en la operativa
- 4.8.1. Protección contra código malicioso
- 4.8.2. Copias de seguridad
- 4.8.3. Registro de actividad y supervisión

4.9. Gestión de las vulnerabilidades técnicas
- 4.9.1. Vulnerabilidades técnicas
- 4.9.2. Gestión de vulnerabilidades técnicas
- 4.9.3. Restricciones en la instalación de software

4.10. Implementación de prácticas de Políticas de Seguridad
- 4.10.1. Implementación de prácticas de Políticas de Seguridad
- 4.10.2. Vulnerabilidades lógicas
- 4.10.3. Implementación de políticas de defensa

Módulo 5. Políticas de gestión de incidencias de seguridad

5.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
- 5.1.1. Gestión de incidencias
- 5.1.2. Responsabilidades y procedimientos
- 5.1.3. Notificación de eventos

5.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 5.2.1. Datos de funcionamiento del sistema
- 5.2.2. Tipos de sistemas de detección de intrusos
- 5.2.3. Criterios para la ubicación de los IDS/IPS

5.3. Respuesta ante incidentes de seguridad
- 5.3.1. Procedimiento de recolección de información
- 5.3.2. Proceso de verificación de intrusión
- 5.3.3. Equipo de respuesta ante emergencias informáticas

5.4. Proceso de notificación y gestión de intentos de intrusión
- 5.4.1. Responsabilidades en el proceso de notificación
- 5.4.2. Clasificación de los incidentes
- 5.4.3. Proceso de resolución y recuperación

5.5. Análisis forense como política de seguridad
- 5.5.1. Evidencias volátiles y no volátiles
- 5.5.2. Análisis y recogida de evidencias electrónicas
- 5.5.3. Importancia de las evidencias electrónicas

5.6. Herramientas de sistemas de detección y prevención de intrusiones (IDS/IPS)
- 5.6.1. Sistema de detección de intrusos Snort
- 5.6.2. Motor de detección de amenazas de red Suricata
- 5.6.3. Software SolarWinds

5.7. Herramientas centralizadoras de eventos
- 5.7.1. Administración de la seguridad de la información
- 5.7.2. Administración de la seguridad de los eventos
- 5.7.3. Administración de la seguridad de eventos e información

5.8. NIST SP800-61
- 5.8.1. Capacidad de respuesta ante incidentes de seguridad informática
- 5.8.2. Manejo de un incidente
- 5.8.3. Coordinación e información compartida

5.9. Norma ISO 27035
- 5.9.1. Norma ISO 27035. Principios de la gestión de incidentes
- 5.9.2. Guías para la elaboración de un plan para la gestión de incidentes
- 5.9.3. Guías de operaciones en la respuesta a incidentes

Módulo 6. Implementación de Políticas de Seguridad física y ambiental en la empresa

6.1. Áreas seguras
- 6.1.1. Perímetro de seguridad física
- 6.1.2. Trabajo en áreas seguras
- 6.1.3. Seguridad de oficinas, despachos y recursos

6.2. Controles físicos de entrada
- 6.2.1. Controles físicos de entrada
- 6.2.2. Políticas de control de acceso físico
- 6.2.3. Sistemas de control físico de entrada

6.3. Vulnerabilidades de accesos físicos
- 6.3.1. Vulnerabilidades de accesos físicos
- 6.3.2. Principales vulnerabilidades físicas
- 6.3.3. Implementación de medidas de salvaguardas

6.4. Sistemas biométricos fisiológicos
- 6.4.1. Huella dactilar
- 6.4.2. Reconocimiento facial
- 6.4.3. Reconocimiento de iris y retina
- 6.4.4. Otros sistemas biométricos fisiológicos

6.5. Sistemas biométricos de comportamiento
- 6.5.1. Reconocimiento de firma
- 6.5.2. Reconocimiento de escritor
- 6.5.3. Reconocimiento de voz
- 6.5.4. Otros sistemas biométricos de comportamientos

6.6. Gestión de riesgos en biometría
- 6.6.1. Gestión de riesgos en biometría
- 6.6.2. Implementación de sistemas biométricos
- 6.6.3. Vulnerabilidades de los sistemas biométricos

6.7. Implementación de políticas en dispositivos anfitriones
- 6.7.1. Instalación de suministro y seguridad de cableado
- 6.7.2. Emplazamiento de los equipos
- 6.7.3. Salida de los equipos fuera de las dependencias
- 6.7.4. Equipo informático desatendido y política de puesto despejado

6.8. Protección ambiental
- 6.8.1. Sistemas de protección ante incendios
- 6.8.2. Sistemas de protección ante seísmos
- 6.8.3. Sistemas de protección antiterremotos

6.9. Seguridad en centro de procesamiento de datos
- 6.9.1. Puertas de seguridad
- 6.9.2. Sistemas de videovigilancia (CCTV)
- 6.9.3. Control de Seguridad

6.10. Normativa Internacional de la Seguridad Física
- 6.10.1. IEC 62443-2-1 (europea)
- 6.10.2. NERC CIP-005-5 (EE.UU.)
- 6.10.3. NERC CIP-014-2 (EE.UU.)

Módulo 7. Políticas de comunicaciones seguras en la empresa

7.1. Políticas de Comunicaciones Seguras en la Empresa
- 7.1.1. Gestión de la Seguridad en las Redes
- 7.1.2. Control y monitorización de red
- 7.1.3. Segregación de redes
- 7.1.4. Sistemas de seguridad en redes

7.2. Protocolos Seguros de Comunicación
- 7.2.1. Modelo de protocolos de red TCP/IP
- 7.2.2. Conjunto de Protocolos IPsec (seguridad del protocolo de Internet)
- 7.2.3. Protocolo de Seguridad de la Capa de Transporte (TLS)

7.3. Protocolo TLS 1.3
- 7.3.1. Fases de un proceso TLS 1.3
- 7.3.2. Protocolo Handsake
- 7.3.3. Protocolo de registro
- 7.3.4. Diferencias con TLS 1.2

7.4. Algoritmos criptográficos
- 7.4.1. Algoritmos criptográficos usados en comunicaciones
- 7.4.2. Algoritmo de protección de red Cipher-suites
- 7.4.3. Algoritmos Criptográficos permitidos para TLS 1.3

7.5. Funciones Digest de resumen de archivo
- 7.5.1. Importancia
- 7.5.2. Herramienta de seguridad MD6
- 7.5.3. Algoritmo de Hash Seguro

7.6. Infraestructura de Clave Pública o PKI
- 7.6.1. PKI y sus entidades
- 7.6.2. Certificado digital
- 7.6.3. Tipos de certificados digital

7.7. Comunicaciones de túnel y transporte
- 7.7.1. Comunicaciones túnel
- 7.7.2. Comunicaciones transporte
- 7.7.3. Implementación túnel cifrado

7.8. Protocolo y programa Secure Shell o SSH
- 7.8.1. Cápsula Segura
- 7.8.2. Funcionamiento de SSH
- 7.8.3. Herramientas SSH

7.9. Auditoria de sistemas criptográficos
- 7.9.1. Auditoría de sistemas criptográficos
- 7.9.2. Pruebas de integridad
- 7.9.3. Testeo Sistema criptográfico

7.10. Sistemas criptográficos
- 7.10.1. Sistemas Criptográficos
- 7.10.2. Vulnerabilidades sistemas criptográficos
- 7.10.3. Salvaguardas en criptografía

Módulo 8. Implementación de Políticas de Seguridad ante ataques

8.1. Detección de vulnerabilidades de seguridad
- 8.1.1. Características e importancia
- 8.1.2. Riesgos y vulnerabilidades
- 8.1.3. Contramedidas

8.2. Sistemas operativos en servicios
- 8.2.1. Importancia en los servicios
- 8.2.2. Riesgos y vulnerabilidades
- 8.2.3. Contramedidas

8.3. Pérdida de sesión
- 8.3.1. Características
- 8.3.2. El proceso
- 8.3.3. Contramedidas

8.4. Evasión de sistemas de detección de intruso, sistemas de protección "Firewalls y Honeypots"
- 8.4.1. Evasión de los sistemas de protección
- 8.4.2. Técnicas de evasión
- 8.4.3. Implementación de contramedidas

8.5. Intrusión en servidores web
- 8.5.1. Características
- 8.5.2. Ataques a servidores webs
- 8.5.3. Implementación de medidas de defensa

8.6. Intrusión en aplicaciones
- 8.6.1. Características
- 8.6.2. Ataques a aplicaciones web
- 8.6.3. Implementación de medidas de defensa

8.7. Intrusión en internet inalámbrico
- 8.7.1. Ataque a red inalámbrica
- 8.7.2. Vulnerabilidades Redes Wifi
- 8.7.3. Implementación de Medidas de defensa

8.8. Intrusión en plataformas móviles
- 8.8.1. Ataque a plataformas móviles
- 8.8.2. Vulnerabilidades a plataformas móviles
- 8.8.3. Implementación de contramedidas

8.9. Intrusión mediante bloqueadores o Ramsonware
- 8.9.1. Características de los Rams Ramsonware onware
- 8.9.2. Vulnerabilidades causantes del Ramsonware
- 8.9.3. Implementación de contramedidas

8.10. Ingeniería Social
- 8.10.1. Ingeniería Social
- 8.10.2. Tipos de Ingeniería Social
- 8.10.3. Contramedidas para la Ingeniería Social

Módulo 9. Herramientas de monitorización en Políticas de Seguridad de los sistemas de información

9.1. Políticas de monitorización de sistemas de la información
- 9.1.1. Monitorización de sistemas
- 9.1.2. Métricas
- 9.1.3. Tipos de métricas

9.2. Auditoria y registro en sistemas
- 9.2.1. Auditoría y registro en sistemas
- 9.2.2. Auditoria y registro en Windows
- 9.2.3. Auditoria y registro en Linux

9.3. Protocolo Simple de Administración de Red
- 9.3.1. Características
- 9.3.2. Funcionamiento
- 9.3.3. Herramientas

9.4. Monitorización de redes
- 9.4.1. Monitorización de redes
- 9.4.2. La monitorización de red en sistemas de control
- 9.4.3. Herramientas de monitorización para sistemas de control

9.5. Sistema de monitorización de Redes Nagios
- 9.5.1. Características de Nagios
- 9.5.2. Funcionamiento de Nagios
- 9.5.3. Instalación de Nagios

9.6. Sistema de monitorización de Redes Zabbix
- 9.6.1. Características de Zabbix
- 9.6.2. Funcionamiento de Zabbix
- 9.6.3. Instalación de Zabbix

9.7. Sistema de Monitorización de Redes Cacti
- 9.7.1. Características de Cacti
- 9.7.2. Funcionamiento de Cacti
- 9.7.3. Instalación de Cacti

9.8. Sistema de monitorización de Redes Pandora
- 9.8.1. Características de Pandora
- 9.8.2. Funcionamiento de Pandora
- 9.8.3. Instalación de Pandora

9.9. Sistema de monitorización de Redes SolarWinds
- 9.9.1. Características de SolarWinds
- 9.9.2. Funcionamiento de SolarWinds
- 9.9.3. Instalación de SolarWinds

9.10. Normativa sobre monitorización
- 9.10.1. Normativa sobre monitorización
- 9.10.2. Controles sobre auditoria y registro
- 9.10.3. NIST 800-123

Módulo 10. Políticas de recuperación de desastres de seguridad

10.1. Plan de Recuperación de Desastres o DRP
- 10.1.1. Objetivo de un DRP
- 10.1.2. Beneficios de un DRP
- 10.1.3. Consecuencias de su ausencia o no actualizado

10.2. Guía para definir un Plan de Recuperación de Desastres
- 10.2.1. Alcance y objetivos
- 10.2.2. Diseño de la estrategia de recuperación
- 10.2.3. Asignación de roles y responsabilidades
- 10.2.4. Realización de un Inventario de hardware, software y servicios
- 10.2.5. Tolerancia para tiempo de inactividad y pérdida de datos
- 10.2.6. Establecimiento de los tipos específicos de DRP que se requieren
- 10.2.7. Realización de un Plan de formación, concienciación y comunicación

10.3. Alcance y objetivos de un Plan de Recuperación de Desastres
- 10.3.1. Garantía de respuesta
- 10.3.2. Componentes tecnológicos
- 10.3.3. Alcance de la política de continuidad

10.4. Diseño de la Estrategia de un Plan de Recuperación de Desastre
- 10.4.1. Estrategia de Recuperación de Desastre
- 10.4.2. Presupuesto
- 10.4.3. Recursos Humanos y Físicos
- 10.4.4. Posiciones gerenciales en riesgo
- 10.4.5. Tecnología
- 10.4.6. Datos

10.5. Continuidad de los procesos de la información
- 10.5.1. Planificación de la continuidad
- 10.5.2. Implantación de la continuidad
- 10.5.3. Verificación evaluación de la continuidad

10.6. Alcance de un Plan de Continuidad Empresarial
- 10.6.1. Determinación de los procesos de mayor criticidad
- 10.6.2. Enfoque por activo
- 10.6.3. Enfoque por proceso

10.7. Implementación de los procesos garantizados de negocio
- 10.7.1. Actividades prioritarias
- 10.7.2. Tiempos de recuperación ideales
- 10.7.3. Estrategias de supervivencia

10.8. Análisis de la organización
- 10.8.1. Obtención de información
- 10.8.2. Análisis de Impacto sobre negocio (BIA)
- 10.8.3. Análisis de riesgos en la organización

10.9. Respuesta a la contingencia
- 10.9.1. Plan de Crisis
- 10.9.2. Planes Operativos de Recuperación de Entornos
- 10.9.3. Procedimientos técnicos de trabajo o de incidentes

10.10. Norma Internacional ISO 27031
- 10.10.1. Objetivos
- 10.10.2. Términos y definiciones
- 10.10.3. Operación

Con esta titulación serás capaz de integrar la cultura de Seguridad en las diferentes áreas de tu empresa”

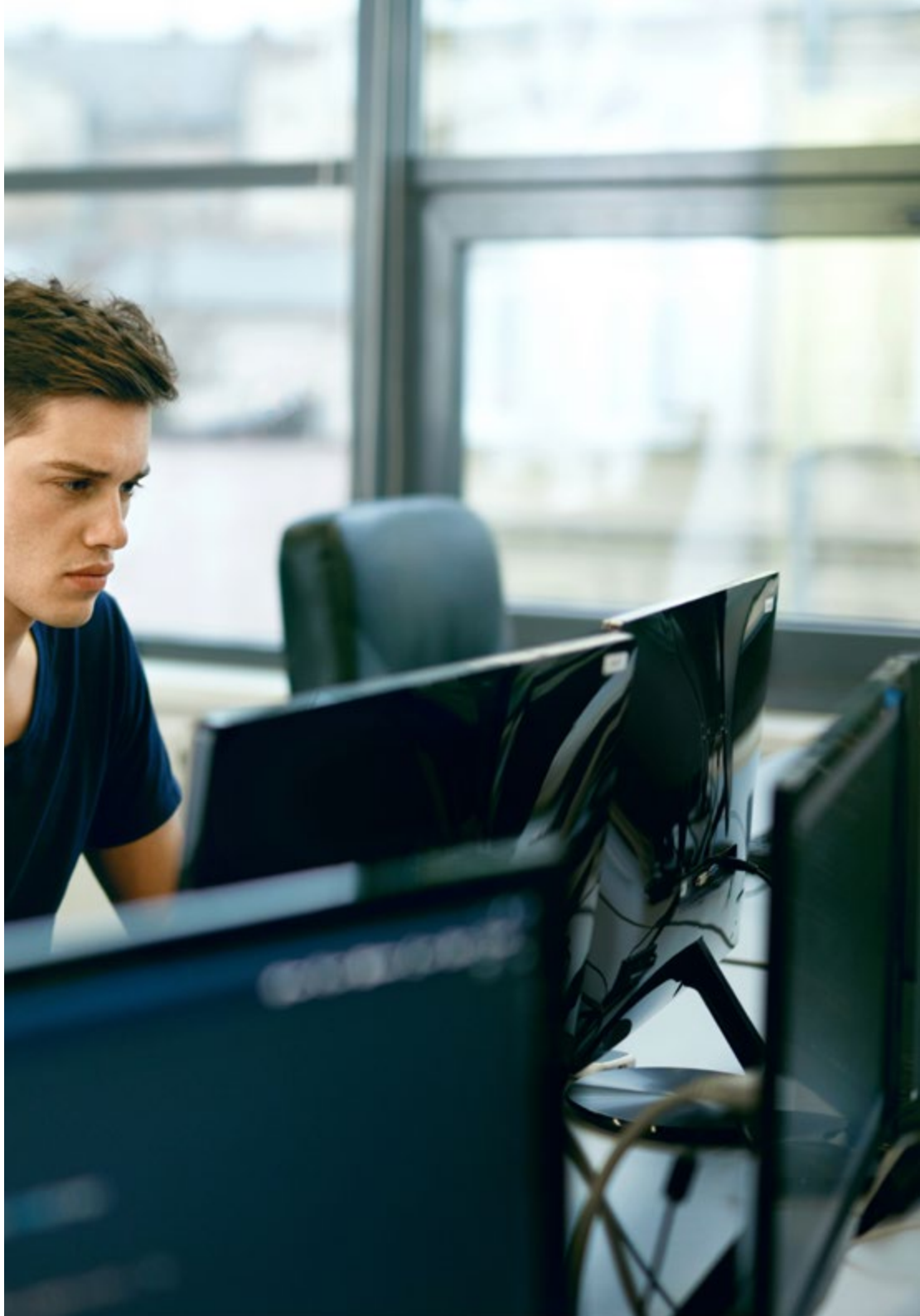
03
Objetivos

La finalidad de esta Maestría es proporcionar al profesional el conocimiento necesario para poder gestionar adecuadamente la seguridad informática es fundamental para evitar brechas de seguridad y sus consecuencias negativas. Además, potenciará dichas competencias y sus habilidades para la dirección de equipos y departamentos involucrados en las tareas de mantener la protección de la empresa y evitar riesgos indeseados.

Conoce las últimas tendencias en Seguridad Informática de la mano de auténticos expertos en este campo. Matricúlate ahora"

Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Analizar las normativas y estándares aplicables en la actualidad a los SGSI
- Implementar un SGSI en la empresa
- Determinar qué departamentos debe abarcar la implementación del sistema de gestión de seguridad
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Determinar qué es la autenticación e identificación
- Analizar los distintos métodos de autenticación que existen y su implementación práctica
- Implementar la política de control de accesos correcta al software y sistemas
- Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Analizar el término de área segura y perímetro seguro
- Analizar los distintos algoritmos de cifrado utilizados en redes de comunicaciones
- Determinar los distintos ataques reales a nuestro sistema de información
- Evaluar las distintas políticas de seguridad para paliar los ataques
- Desarrollar el concepto de monitorización e implementación de métricas
- Generar conocimiento especializado sobre el concepto de continuidad de la seguridad de la información
- Determinar qué es la Criptografía y tipos de Criptografía



Objetivos específicos

Módulo 1. Sistema de gestión de seguridad de información

- Ampliar el concepto de seguridad de la información a través del estudio de las normativas y estándares aplicables a este sector en la actualidad, comprendiendo las fases necesarias para implementar un sistema de seguridad de información
- Ponerse al día de los procedimientos de gestión de incidentes de seguridad y determinando sus implicaciones en la organización interna de la entidad
- Ser capaz de explicar las fases que permiten el desarrollo y la implantación de un Sistema de Gestión de Seguridad de la Información

Módulo 2. Aspectos organizativos en Políticas de Seguridad de la Información

- Profundizar en las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información y qué medidas deben ser observadas con suministradores y mantenimientos de sistemas de información
- Estudiar las contramedidas de seguridad necesaria en la operativa, considerando el papel del departamento de recursos humanos en materia de seguridad informática
- Definir las políticas de seguridad en la empresa y la normativa relacionada con todo el proceso para gestionar los activos en materia de seguridad de la información

Módulo 3. Políticas de Seguridad para el análisis de amenazas en sistemas informáticos

- Ampliar el concepto de amenazas informáticas, así como las fases de una gestión preventiva de las mismas
- Ahondar en la comprensión de las diferentes metodologías que permiten un análisis exhaustivo, diferenciando las metodologías de auditoría con el fin de ser capaz de clasificar las amenazas por impacto y gravedad
- Definir políticas de seguridad para el tratamiento preventivo de amenazas

Módulo 4. Implementación de Políticas de Seguridad en software y hardware

- Comprender los conceptos de autenticación e identificación a través del estudio de los distintos métodos y tecnologías que existen actualmente y su operatividad en la empresa
- Ahondar en los sistemas de Directorio Activo y los distintos sistemas de autenticación con el propósito de ser capaz de definir políticas efectivas de control de accesos a redes y servicios y de control de código malicioso para la seguridad en hardware y software

Módulo 5. Políticas de gestión de incidencias de seguridad

- Dominar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad informática a través del estudio de las distintas herramientas utilizadas en el tratamiento y prevención de incidencias y explicando las distintas fases de una gestión de eventos en el área
- Ponerse al día de la normativa ISO 27035, valorando la necesidad de un análisis informático para el estudio en profundidad de las incidencias registradas y asimilando los protocolos estandarizados para el tratamiento de incidencias de seguridad

Módulo 6. Implementación de Políticas de Seguridad física y ambiental en la empresa

- Analizar los conceptos de área y perímetro seguro a través del estudio de los elementos que componen la biometría y los sistemas biométricos que hacen posible el control de acceso físico
- Actualizar la normativa vigente sobre el tema con el propósito de definir políticas de seguridad física correctas y los sistemas de control de acceso físico en Centros de Procesamiento de Datos

Módulo 7. Políticas de comunicaciones seguras en la empresa

- Explicar los elementos que componen una red de comunicaciones mediante la división de la misma, a través del estudio de los distintos algoritmos de cifrado utilizados en redes de comunicaciones, así como las diversas técnicas de cifrado en la red
- Actualizar el concepto de Criptografía y sus tipos con el propósito de contar con los conocimientos requeridos que permitan implementar una red segura y establecer el funcionamiento de una Infraestructura de Clave Única

Módulo 8. Implementación de Políticas de Seguridad ante ataques

- Reflexionar sobre las vulnerabilidades de las plataformas móviles y del internet de las cosas y las estrategias para evitarlas a través de estudio de los distintos ataques a los sistemas de información
- Ahondar en la importancia de la detección de vulnerabilidades de seguridad
- Definir medidas técnicas para mitigar las principales amenazas y conocer contramedidas para evitarlas en los servidores web y en las aplicaciones web

Módulo 9. Herramientas de monitorización en Políticas de Seguridad de los sistemas de información

- Explicar los conceptos de monitorización e implementación de métricas mediante la configuración de los registros de auditoría en los sistemas de monitorización de las redes
- Ahondar en el manejo de las herramientas más actuales existentes en el mercado con el propósito de adquirir los conocimientos que permitan la instalación y seguimiento del Protocolo Simple de Administración de Red

Módulo 10. Políticas de recuperación de desastres de seguridad

- Analizar el concepto de continuidad de la seguridad de la información mediante el estudio de las características de un plan de continuidad de negocio y de recuperación de desastres
- Considerar los distintos tipos de proyectos de continuidad con el propósito de asimilar los conocimientos que permitan un análisis de impacto de negocio para averiguar cuáles son los activos más vulnerables y con mayor impacto en su pérdida

Alcanza tus metas profesionales y personales más ambiciosas, gracias a los contenidos más completos y las herramientas educativas más avanzadas"

04

Competencias

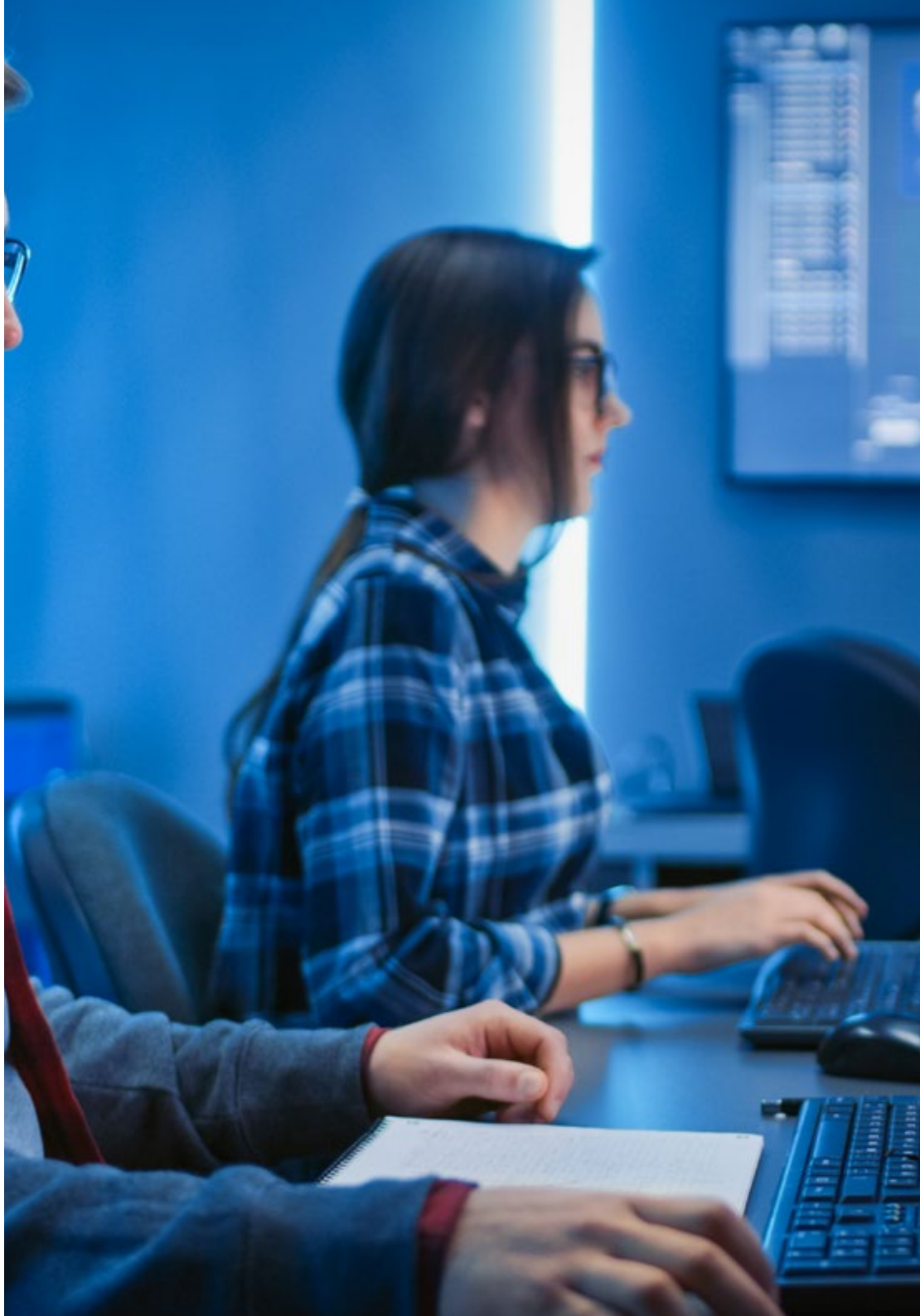
Tras superar las evaluaciones de la Maestría en Gestión de Políticas de Seguridad Informática en la Empresa, el experto habrá desarrollado las habilidades y destrezas necesarias para el ejercicio profesional. Asimismo, también se espera que tenga una visión innovadora del futuro de este campo laboral. Por tanto, este programa es una oportunidad sinigual para todo aquel que quiera adentrarse en esta profesión.

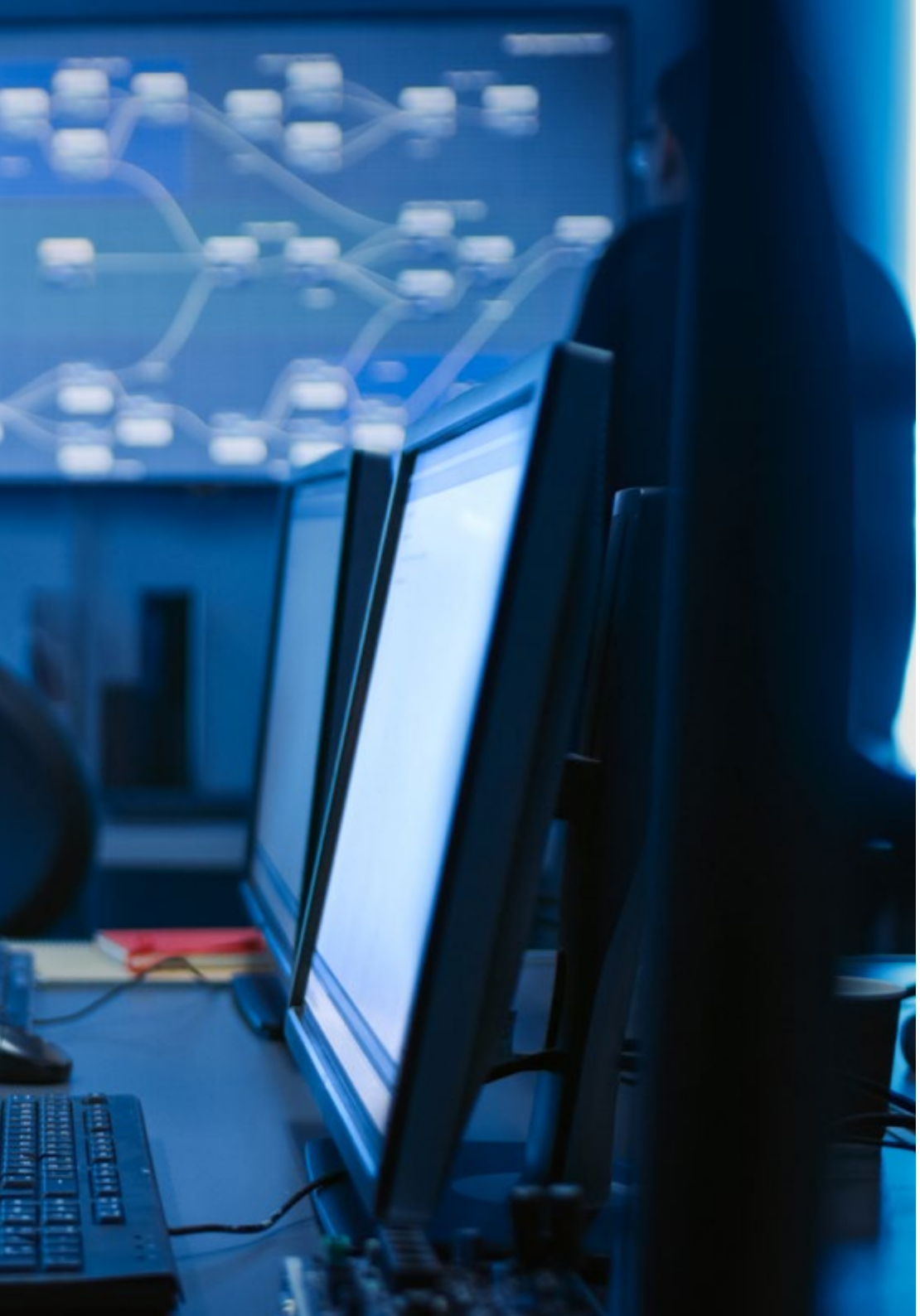
Te damos +

Gracias a esta Maestría implementarás medidas que mitiguen los riesgos ante posibles ataques externos”

Competencias generales

- Determinar la implicación de un SGSI en la organización interna de la entidad, así como su estado
- Establecer las políticas de seguridad en la empresa
- Determinar qué medidas tenemos que implementar con suministradores y mantenimientos de sistemas de información
- Generar conocimiento especializado sobre el control de amenazas
- Determinar las fases de la gestión preventiva de amenazas
- Desarrollar las metodologías para el análisis de amenazas informáticas
- Clasificar las amenazas por impacto y gravedad
- Diseñar una metodología propia para el análisis y control preventivo de amenazas
- Implementar una política correcta de control de accesos a redes y servicios
- Analizar la importancia de un tratamiento correcto en materia de incidencias de seguridad
- Compilar los distintos sistemas biométricos que existen
- Examinar la biometría y sistemas biométricos
- Implementar las distintas políticas de seguridad física correctas y los sistemas de control de acceso físico en CPDs
- Implementar una red segura
- Examinar las vulnerabilidades de las plataformas móviles y de los IoT y cómo evitarlas
- Establecer los tipos de Ingeniera social y aprender a mitigarlos
- Analizar el concepto de monitorización e implementación de métricas
- Determinar la necesidad de la continuidad de la seguridad de la información



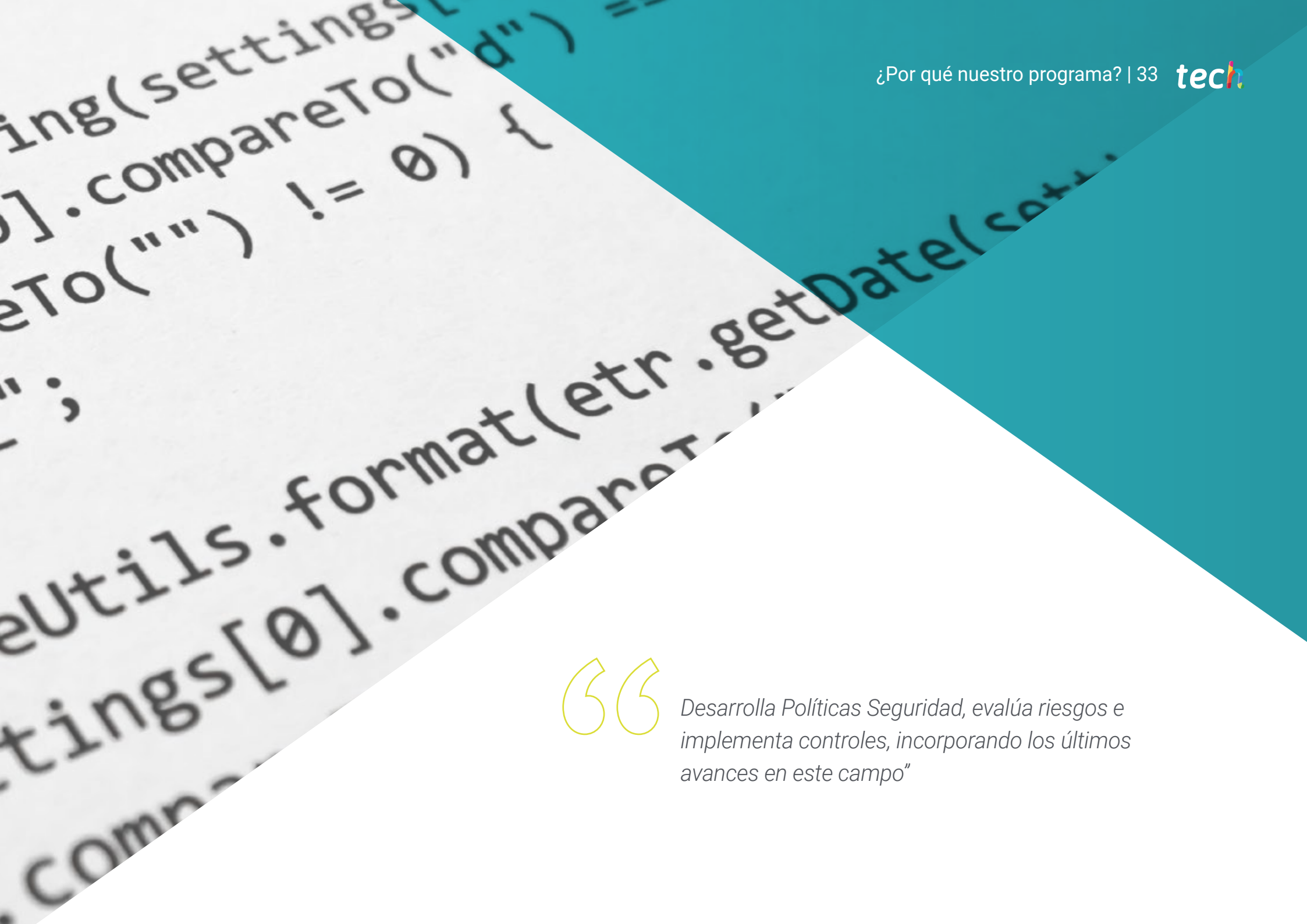


¿Quieres detectar si tu compañía es vulnerable ante ataques informáticos? Obtén el conocimiento que necesitas a través de esta titulación"

05

¿Por qué nuestro programa?

Cursar esta Maestría llevará al egresado a dar un salto importante en su progresión profesional. Y es que contar con una especialización en Seguridad Informática, en un mundo completamente digitalizado, es clave para distinguirse del resto de competidores. Además, este programa aporta un aprendizaje adaptado tanto a las necesidades del alumnado, como a las del sector. De esta forma, ampliará exponencialmente su campo de acción en el mercado laboral.



Desarrolla Políticas Seguridad, evalúa riesgos e implementa controles, incorporando los últimos avances en este campo”

01

Orientación 100% laboral

Con esta Maestría, el estudiante tiene, ante sí, un abanico de posibilidades de progresión profesional ya sea en su empresa actual u otras que requieren de directores de Políticas de Seguridad Informática. Bajo esta premisa ha sido diseñada esta titulación que ofrece al alumnado un enfoque profesionalizante y de gran utilidad práctica para su desempeño profesional diario.

02

La mejor institución

TECH ha realizado una apuesta decidida por la metodología online, ofreciendo al alumnado un amplio catálogo de programas, que le permite incrementar su conocimiento en diversas áreas a través del mejor material didáctico. De esta forma, el alumnado conseguirá progresar profesionalmente desde la comodidad de su hogar y con tan solo un dispositivo electrónico con conexión a internet. Una oportunidad única que tan solo ofrece esta institución, la universidad digital más grande del mundo.

03

Titulación directa

No hará falta que el estudiante haga una tesina, ni examen final, ni nada más para poder egresar y obtener su título. En TECH, el alumno tendrá una vía directa de titulación.

04

Los mejores recursos pedagógicos 100% en línea

TECH Universidad Tecnológica pone al alcance de los estudiantes de esta Maestría la última metodología educativa en línea, basada en una tecnología internacional de vanguardia, que permite estudiar sin tener que asistir a clase, y sin renunciar a adquirir ninguna competencia indispensable en Políticas de Seguridad Informática.

05

Educación adaptada al mundo real

TECH no solo se adapta al alumnado, ofreciendo flexibilidad en la realización de esta Maestría, sino que el contenido de todos sus programas muestra la información más rigurosa y actual. De este modo, el egresado estará al tanto de los avances, tendencias y estrategias más efectivas para dirigir y coordinar Políticas de Seguridad Informática en cualquiera que sea la organización y dimensión que tenga. Una enseñanza vanguardista, acorde a los tiempos académicos presentes.

06

Aprender idiomas y obtener su certificado oficial

TECH da la posibilidad, además de obtener la certificación oficial de Inglés en el nivel B2, de seleccionar de forma optativa hasta otros 6 idiomas en los que, si el alumno desea, podrá certificarse.

07 Mejorar tus habilidades directivas

Gracias a esta titulación, el alumnado potenciará sus habilidades de gestión, liderazgo, comunicación y resolución de problemas. Todas ellas, competencias esenciales, hoy en día, para implementar y mantener Políticas de Seguridad Informática efectivas en una Empresa. Asimismo, será capaz de coordinar diversos departamentos y equipos dentro de una misma organización con éxito.

08 Especialización integral

Esta Maestría va más allá y ofrece al alumnado un conocimiento profundo sobre la detección de intrusos, seguridad de aplicaciones y gestión de incidentes. De esta forma, el egresado obtendrá una especialización mucho más completa que le permita incorporar en las empresas las soluciones técnicas más recientes y optimas en Seguridad Informática.

09 Formar parte de una comunidad exclusiva

Estudiando en TECH, el profesional tendrá acceso a una comunidad de especialistas en ciberseguridad, a grandes compañías del sector y profesores altamente cualificados con una consolidada trayectoria en este campo y en el ámbito docente. Una comunidad única.

06
Salidas profesionales

El perfil de egreso de la Maestría es el de un profesional con altas habilidades para dirigir acciones y estrategias orientadas a la mejora continua de las Políticas de Seguridad Informática en la Empresa. En este sentido, al finalizar el programa, el educador será capaz de gestionar y liderar empresas, organizaciones, consultorías y organizaciones de seguridad cibernética. De esta forma, se convertirá en un directivo solvente, competitivo y con gran capacidad de para implementar actuaciones efectivas.

Logra tus aspiraciones profesionales con una opción académica que te proporciona el mejor material didáctico"

Perfil profesional

El egresado de esta Maestría será un profesional competente y hábil para desempeñarse, de manera responsable en empresas que requieran tener efectivas Políticas de Seguridad Informática. Así, con este programa, el alumnado tendrá las capacidades necesarias para diseñar, implementar y gestionar dichas medidas, adaptadas a las necesidades y requisitos específicos de la empresa.

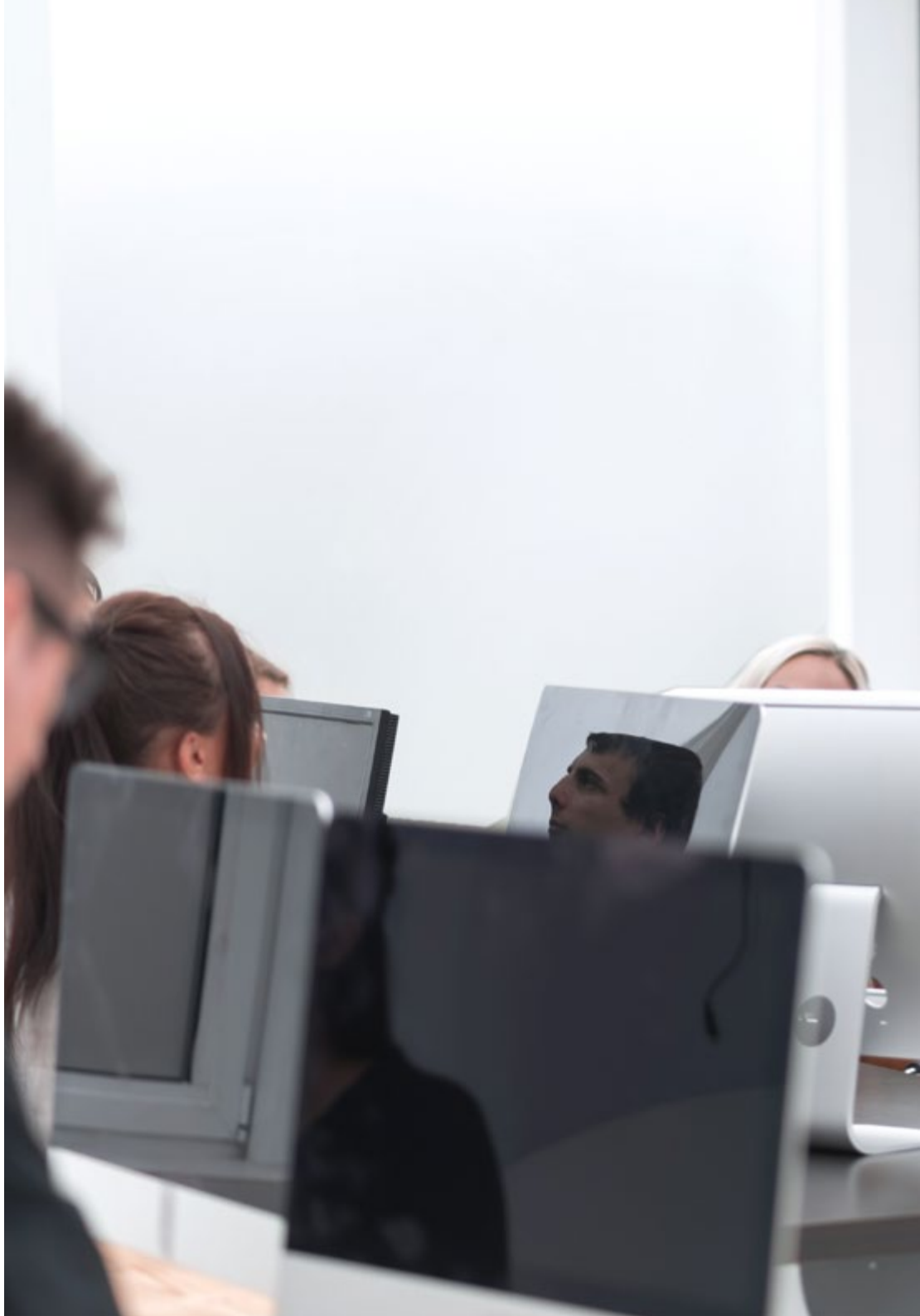
Asimismo, este profesional contará con una gran visión analítica que le llevará a efectuar procesos de evaluación y prevención de los riesgos de seguridad, estableciendo controles adecuados y asegurando el cumplimiento normativo. Todo ello, unido a sus competencias de dirección y de dirección, claves para desarrollar una auténtica cultura de ciberseguridad empresarial.

De esta manera, este programa le permitirá detectar problemas de protección de datos, resolverlos y plantear soluciones alternativas o innovadoras, que realmente cumplan las metas de seguridad cibernética de las compañías. Múltiples cualidades que le darán un impulso a su carrera profesional.

El egresado será, de esta forma, un directivo técnicamente solvente y preparado para desempeñarse profesionalmente en el campo laboral.

Perfil investigativo

Las tecnologías emergentes y la constante evolución digital han llevado en los últimos años a la investigación científica desde diversas disciplinas. Un amplio campo de estudio en el que podrá sumergirse el profesional que curse esta titulación. Y es que, el alumnado que curse este programa tendrá acceso a un conocimiento, que le permitirá profundizar aún más en el campo de la Seguridad Informática.



Perfil ocupacional y campo de acción

Al finalizar este programa, el alumnado habrá alcanzado sus objetivos de aprendizaje y desarrollo personal y profesional. Así, podrá poner en marcha con éxito Políticas de Seguridad, efectuar su planificación, ejecución o bien asesorar a las compañías en el proceso de implementación y seguimiento. Todo ello, además, de forma solvente, lo que le permitirá distinguirse como un auténtico especialista en este campo.

El egresado de TECH en Gestión de Políticas de Seguridad Informática en la Empresa estará preparado para desempeñar los siguientes puestos de trabajo:

- Director de Políticas de Seguridad Informática
- Gestor de Seguridad Informática
- Especialista en Recuperación Práctica de Pérdida de Información
- Auditor de Seguridad Informática
- Perito Forense en Seguridad Informática
- Especialista en Protección de Redes

Conviértete en un especialista en Seguridad Informática y asesora a las principales compañías en su protección digital"

07

Idiomas gratuitos

Convencidos de que la formación en idiomas es fundamental en cualquier profesional para lograr una comunicación potente y eficaz, TECH ofrece un itinerario complementario al plan de estudios curricular, en el que el alumno, además de adquirir las competencias de la Maestría, podrá aprender idiomas de un modo sencillo y práctico.

TECH te incluye el estudio de idiomas en la Maestría de forma ilimitada y gratuita"

En el mundo competitivo actual, hablar otros idiomas forma parte clave de nuestra cultura moderna. Hoy en día, resulta imprescindible disponer de la capacidad de hablar y comprender otros idiomas, además de lograr un título oficial que acredite y reconozca las competencias lingüísticas adquiridas. De hecho, ya son muchos los colegios, las universidades y las empresas que solo aceptan a candidatos que certifican su nivel mediante un título oficial en base al Marco Común Europeo de Referencia para las Lenguas (MCER).

El Marco Común Europeo de Referencia para las Lenguas es el máximo sistema oficial de reconocimiento y acreditación del nivel del alumno. Aunque existen otros sistemas de validación, estos proceden de instituciones privadas y, por tanto, no tienen validez oficial. El MCER establece un criterio único para determinar los distintos niveles de dificultad de los cursos y otorga los títulos reconocidos sobre el nivel de idioma que se posee.

En TECH se ofrecen los únicos cursos intensivos de preparación para la obtención de certificaciones oficiales de nivel de idiomas, basados 100% en el MCER. Los 48 Cursos de Preparación de Nivel Idiomático que tiene la Escuela de Idiomas de TECH están desarrollados en base a las últimas tendencias metodológicas de aprendizaje en línea, el enfoque orientado a la acción y el enfoque de adquisición de competencia lingüística, con la finalidad de preparar los exámenes oficiales de certificación de nivel.

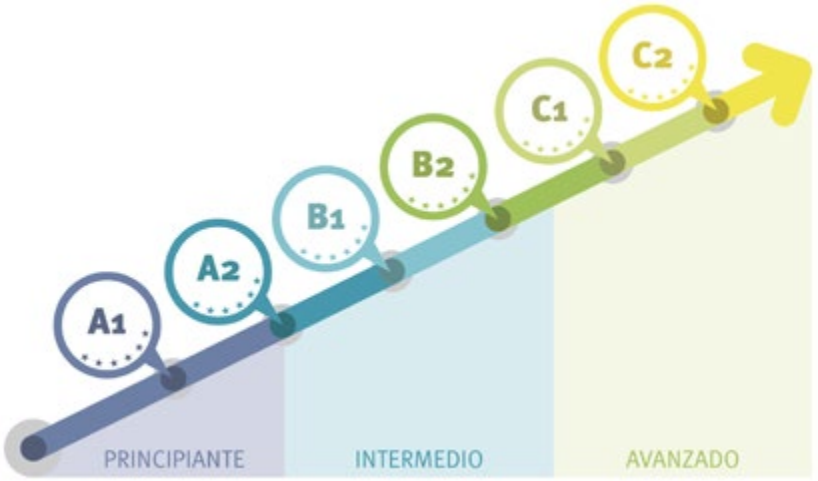
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

Solo el coste de los Cursos de Preparación de idiomas y los exámenes de certificación, que puedes llegar a hacer gratis, valen más de 3 veces el precio de la Maestría"

TECH incorpora, como contenido extracurricular al plan de estudios oficial, la posibilidad de que el alumno estudie idiomas, seleccionando aquellos que más le interesen de entre la gran oferta disponible:

- Podrá elegir los Cursos de Preparación de Nivel de los idiomas y nivel que desee, de entre los disponibles en la Escuela de Idiomas de TECH, mientras estudie la Maestría, para poder prepararse el examen de certificación de nivel
- En cada programa de idiomas tendrá acceso a todos los niveles MCER, desde el nivel A1 hasta el nivel C2
- Cada año podrá presentarse a un examen telepresencial de certificación de nivel, con un profesor nativo experto. Al terminar el examen, TECH le expedirá un certificado de nivel de idioma
- Estudiar idiomas NO aumentará el coste del programa. El estudio ilimitado y la certificación anual de cualquier idioma están incluidas en la Maestría

"48 Cursos de Preparación de Nivel para la certificación oficial de 8 idiomas en los niveles MCER A1, A2, B1, B2, C1 y C2"



08
Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.
Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.

El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

> *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomasen decisiones y emitiesen juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

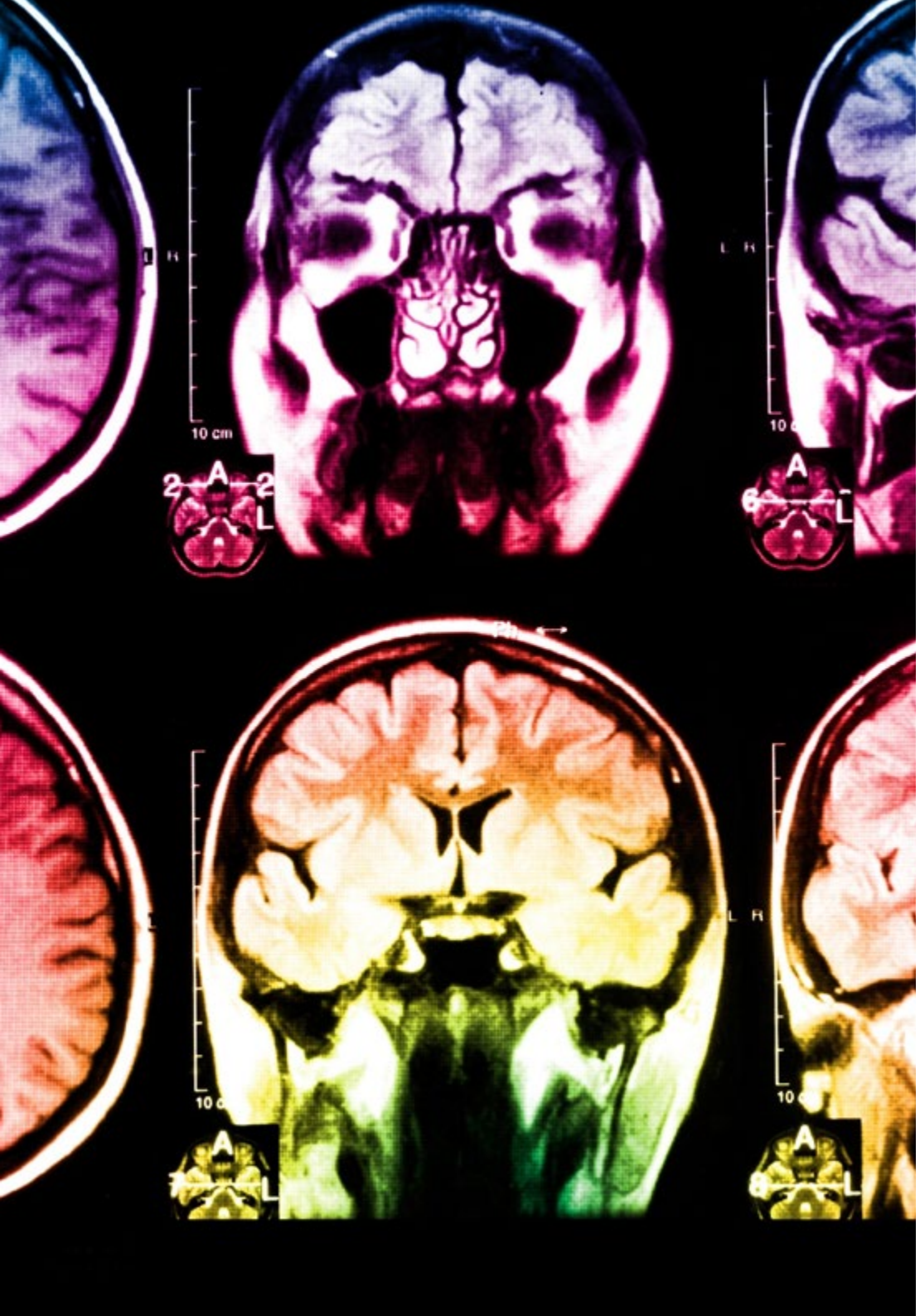
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu capacitación, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

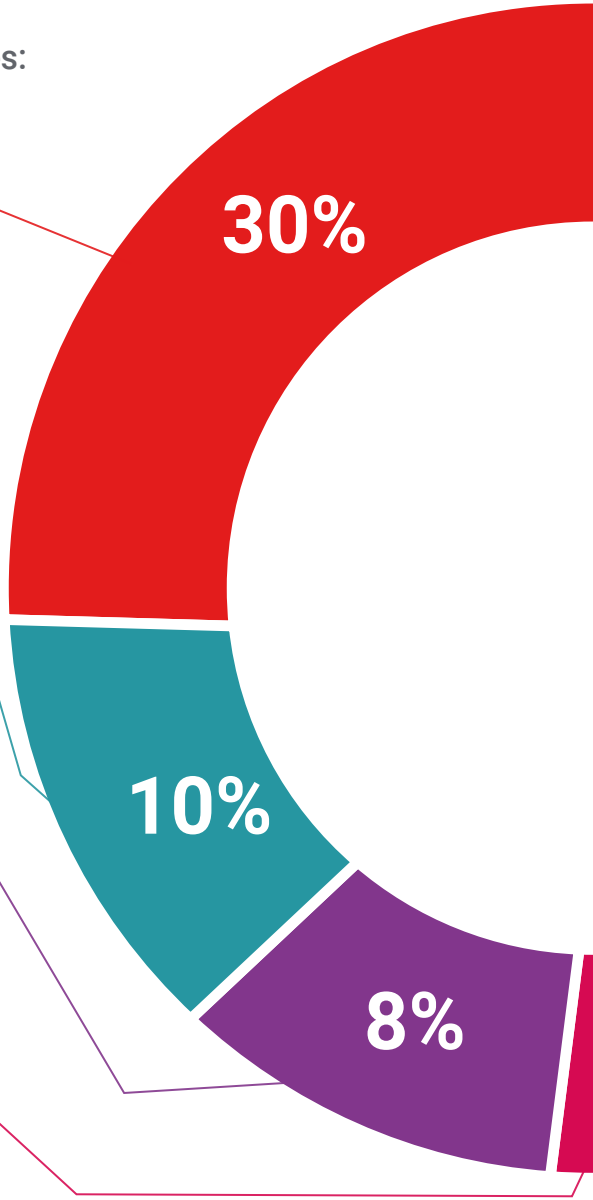
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

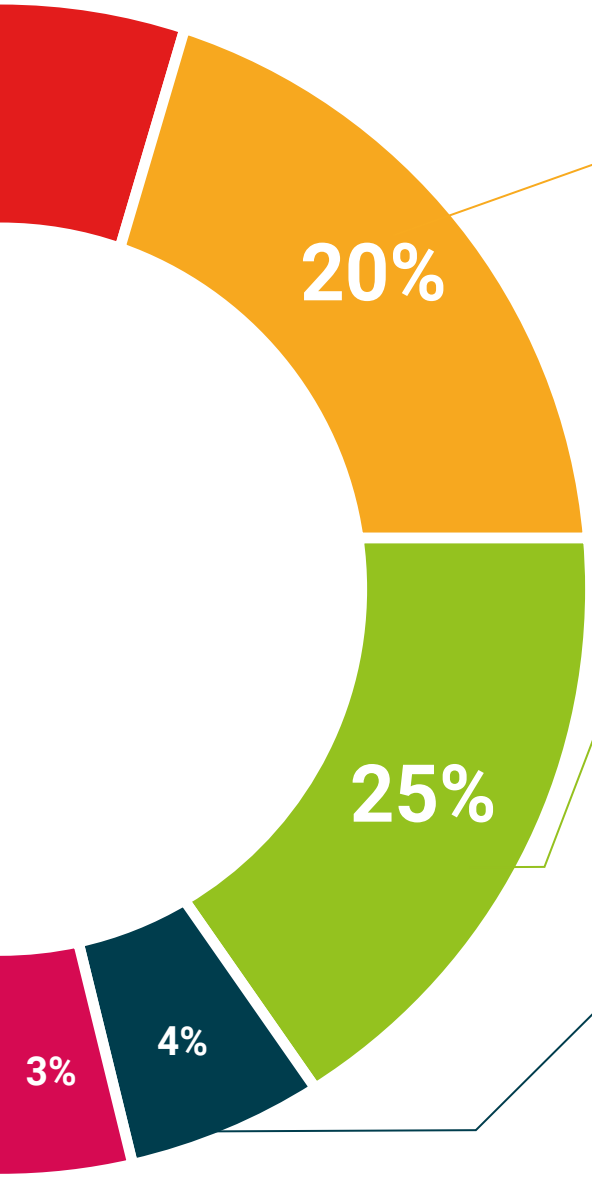
Prácticas de habilidades y competencias

Realizarán actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este exclusivo sistema educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

09
Dirección del curso

En su premisa por ofrecer al alumnado una enseñanza de máxima calidad, TECH ha seleccionado con rigurosidad a todos y cada uno de los docentes que integran esta Maestría. Así, el egresado tendrá a su alcance un programa elaborado por especialistas en diversas áreas de la Seguridad Informática con una amplia experiencia en este sector. De esta forma, el egresado obtendrá la información más actual y rigurosa, de la mano de los mejores expertos.

TECH ha reunido en un mismo programa a los mejores educadores de las Políticas de Seguridad, dispuestos a proporcionarte la información más actualizada y rigurosa"

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional en Informática y Telecomunicaciones
- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Profesores

D. Oropesiano Carrizosa, Francisco

- Ingeniero Informático
- Técnico en Microinformática, Redes y Seguridad en CAS Training
- Desarrollador de Servicios Web, CMS, e-commerce, UI y UX en Fersa Reparaciones
- Gestor de Servicios Web, Contenidos, Correo y DNS en Oropesia Web & Network
- Diseñador Gráfico y de Aplicaciones Web en Xarxa Sakai Projectes SL
- Diplomado en Informática de Sistemas por la Universidad de Alcalá
- Máster en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

D. Peralta Alonso, Jon

- Peralta Alonso, Jon
- Abogado/Asesor jurídico en Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Asesor Jurídico/Pasante en Despacho Profesional: Óscar Padura
- Grado en Derecho por la Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos por EIS Innovative School
- Máster Universitario en Abogacía por la Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil por la Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC

D. Ortega López, Florencio

- Consultor de TIC y Seguridad
- Consultor de Seguridad en Gestión de Identidades en SIA Group
- Consultor de TIC y Seguridad como profesional independiente
- Profesor formador en Sector TI
- Graduado en Ingeniería Técnica Industrial por la Universidad de Alcalá
- Máster en Profesorado por la UNIR
- MBA en Gestión y Dirección de Empresas por IDE-CESEM
- Máster en Dirección y Gestión de Tecnología de la Información por IDE-CESEM
- Certified Information Security Management (CISM) por la ISACA

D. Solana Villarias, Fabián

- Consultor de Tecnologías de la Información
- Creador y administrador de servicios de encuestas en Investigación, Planificación y Desarrollo, S.A.
- Especialista en mantenimiento de mercados financieros y sistemas informáticos en Iberia Financial Software
- Desarrollador web y especialista en accesibilidad en Indra
- Licenciado en Ingeniería Superior de Sistemas por la Universidad de Gales/CESINE
- Diplomado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Gales/CESINE

Dña. López García, Rosa María

- Especialista en Información de Gestión
- Profesora de Linux Professional Institute
- Colaboradora en Academia Hacker Incibe
- Capitana de Talento en Ciberseguridad en Teamciberhack
- Administrativa y gestora contable y financiera en Integra2Transportes
- Auxiliar administrativo en recursos de compras en el Centro de Educación Cardenal Marcelo Espínola
- Técnico Superior en Ciberseguridad y hacking Ético
- Miembro de Ciberpatrulla

10

Requisitos de acceso y proceso de admisión

El proceso de admisión de TECH es el más sencillo de las universidades en línea en todo el país. Podrás comenzar la Maestría sin trámites ni demoras: empieza a preparar la documentación y entrégala más adelante, sin premuras. Lo más importante para TECH es que los procesos administrativos, para ti, sean sencillos y no te ocasionen retrasos, ni incomodidades.

Ayudándote desde el inicio, TECH ofrece el procedimiento de admisión más sencillo y rápido de todas las universidades en línea del país"

Requisitos de acceso

Para poder acceder a los estudios de Maestría en Gestión de Políticas de Seguridad Informática en la Empresa es necesario haber concluido una Licenciatura en Informática; Ingeniería en sistemas; Ingeniería en computación; Ingeniería en informática; Ciencias de la computación; Ingeniería en software; Ingeniería en Sistemas Computacionales; Informática administrativa; Tecnologías y sistemas de la información y la comunicación; Ingeniería en seguridad; Información y sistemas inteligentes; Inteligencia artificial; Ciencias de los Datos; Ingeniería y Programación; Ingeniería en Redes, Ingeniería en Sistemas, Tecnologías de la Información y Telemática, Ingeniería de Software, etc. En caso de que el alumno no cuente con un título en el área mencionada, deberá acreditar documentalmente que cuenta con un mínimo de 2 años de experiencia en el área. Puede consultar requisitos establecidos en el Reglamento de TECH.

Proceso de admisión

Para TECH es del todo fundamental que, en el inicio de la relación académica, el alumno esté centrado en el proceso de enseñanza, sin demoras ni preocupaciones relacionadas con el trámite administrativo. Por ello, hemos creado un protocolo más sencillo en el que podrás concentrarte, desde el primer momento en tu capacitación, contando con un plazo mucho mayor de tiempo para la entrega de la documentación pertinente.

De esta manera, podrás incorporarte al curso tranquilamente. Algún tiempo más tarde, te informaremos del momento en el que podrás ir enviando los documentos, a través del campus virtual, de manera muy sencilla, cómoda y rápida. Sólo deberás cargarlos y enviarlos, sin traslados ni pérdidas de tiempo.

Una vez que llegue el momento podrás contar con nuestro soporte, si te hace falta

Todos los documentos que nos facilites deberán ser rigurosamente ciertos y estar en vigor en el momento en que los envías.

En cada caso, los documentos que debes tener listos para cargar en el campus virtual son:

Estudiantes con estudios universitarios realizados en México

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada de la Clave Única de Registro de Población (CURP)
- Copia digitalizada de Certificado de Estudios Totales de Licenciatura legalizado
- Copia digitalizada del título legalizado

En caso de haber estudiado la licenciatura fuera de méxico, consulta con tu asesor académico. Se requerirá documentación adicional en casos especiales, como inscripciones a la maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Estudiantes con estudios universitarios realizados fuera de México

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada del Título, Diploma o Grado Académico oficiales de Licenciatura que ampare los estudios realizados en el extranjero
- Copia digitalizada del Certificado de Estudios de Licenciatura. En el que aparezcan las asignaturas con las calificaciones de los estudios cursados, que describan las unidades de aprendizaje, periodos en que se cursaron y calificaciones obtenidas

Se requerirá documentación adicional en casos especiales como inscripciones a maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Es del todo necesario que atestigües que todos los documentos que nos facilitas son verdaderos y mantienen su vigencia en el momento en que los envías.

11

Titulación

Este programa te permite alcanzar la titulación de Maestría en Gestión de Políticas de Seguridad Informática en la Empresa obteniendo un título universitario válido por la Secretaría de Educación Pública, y si gustas, la Cédula Profesional de la Dirección General de Profesiones.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este programa te permite alcanzar el grado de **Maestría en Gestión de Políticas de Seguridad Informática en la Empresa**, obteniendo un reconocimiento universitario oficial válido tanto en tu país como de modo internacional.

Los títulos de la Universidad TECH están reconocidos por la Secretaría de Educación Pública (SEP). Este plan de estudios se encuentra incorporado al Sistema Educativo Nacional, con fecha 24 JULIO de 2023 y número de acuerdo de Registro de Validez Oficial de Estudios (RVOE): 20232122.

Puedes consultar la validez de este programa en el acuerdo de Registro de Validez Oficial de Estudios: **RVOE Maestría en Gestión de Políticas de Seguridad Informática en la Empresa**

Para más información sobre qué es el RVOE puedes consultar *aquí:*

RVOE
EDUCACIÓN SUPERIOR

Titulación: **Maestría en Gestión de Políticas de Seguridad Informática en la Empresa**

Nº de RVOE: **20232122**

Fecha de RVOE: **24/07/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Para recibir el presente título no será necesario realizar ningún trámite.
TECH Universidad Tecnológica realizará todas las gestiones oportunas ante las diferentes administraciones públicas en su nombre, para hacerle llegar a su domicilio*:

- Título de la Maestría
- Certificado total de estudios
- Cédula Profesional

Si requiere que cualquiera de estos documentos le lleguen apostillados a su domicilio, póngase en contacto con su asesor académico.
TECH Universidad Tecnológica se hará cargo de todos los trámites.


tech universidad tecnológica

Otorga el presente

GRADO

a

D/Dña _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MAESTRÍA

en

Gestión de Políticas de Seguridad Informática en la Empresa

Con Reconocimiento de Validez Oficial de Estudios de la Secretaría de Educación Pública, según Acuerdo Nº. 20232122 en virtud de que demostró cumplir con los estudios correspondientes y aprobó conforme titulación automática el 24 Julio 2023.

A 24 de julio de 2023

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad tecnológica

Maestría

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: **20232122**

Fecha de RVOE: **24/07/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Maestría

Gestión de Políticas de Seguridad Informática en la Empresa

Nº de RVOE: 20232122

RVOE
EDUCACIÓN SUPERIOR

tech universidad tecnológica