tecnolearning

Personas que forman a Personas

C/ Navarra, 24. Bis · 913830641 · 28039 Madrid · info@tecnolearning.com · www.tecnolearning.com
https://www.facebook.com/tecnolearning/ · https://www.linkedin.com/company-beta/2943254/

¡CIBERSEGURIDAD!

- Un dossier sobre la importancia de la seguridad en el ámbito informático de las empresas, sus características, ataques y protección.
- Los cursos más adecuados para estar al día en las más modernas herramientas.
- Software de Backup.

La Seguridad:

La seguridad informática, también conocida como **ciberseguridad** o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La formación en **ciberseguridad** está enfocada a la protección de las infraestructuras e información de su empresa, tanto software como aquellas herramientas a las que su organización confiera un valor critico en su negocio, contra la pérdida de control, robo o destrucción de las mismas.

Se utilizan una serie de estándares, protocolos, normas, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos con el objetivo final de utilizar técnicas destinadas a conseguir un sistema de información seguro y confiable.

Cursos:

Hacking Ético:

- Aprender y profundizar en todas las fases que involucran un Test de Intrusión
- Conocer las herramientas y técnicas más importantes de obtención de información, descubrimiento de sistemas y servicios y posterior explotación de los problemas que afectan a los sistemas analizados.
- Conocer técnicas de hacking más importantes que se aplican en sistemas, entornos web y entornos wireless.
- Obtener conocimientos detallados sobre malware, tipos de malware, elementos de arquitectura de red, y seguridad de red.

Ciberseguridad para departamentos de Desarrolladores:

- **Redes**
  - Teoría de redes
  - Protocolos de red y su implementación
  - Implementación de Sistemas de cifrado en red
  - Librerías de protocolos y cifrados en red
- **Desarrollo de Código Seguro**
  - Buena Praxis en la codificación
  - Sesiones, Accesos, autentificación
  - Practicas criptográficas para almacenamiento temporal
  - Proteccion de datos contra Man in the middle
  - Seguridad en base datos, archivos y memoria.
  - Librerías criptográficas y su implementación
  - Criptografía Básica y avanzada
  - Integración de certificados, tokens, etc. (FrontEnd / BackEnd)
  - OWASP
  - Herramientas para desarrollo seguro
  - Auditoria De Seguridad orientada al Código
  - Técnicas de Testing, entornos y buenas practicas
  - Errores y Logs (Gestión segura)
  - Pentesting de aplicaciones (preproducción)
  - Ofuscación de código contra ingeniería inversa
  - Configuración Segura Entornos IIS / Apache, etc.
  - Métodos comunes de ataque al código, exploiting
  - Programación segura en Java
  - Programación segura en .NET
  - Codigo Javascript Seguro
  - Desarrollo Aplicaciones Pentesting con Python
  - Entorno Legal

☞ Ciberseguridad para departamentos de Sistemas

- **Redes**
  - Teoría de redes (Arquitecturas)
  - Modelos y protocolos (Implantaciones, capas lógicas y físicas)
  - Manipulación de la red (teoría hacking y herramientas)
  - Sistemas de cifrado (Protección del tránsito en la red)
  - Monitorización y análisis
  - Seguridad Wifi (Protección de la infraestructura)
  - Protocolo e infraestructura 3G/4G
  - Implementación IPv6
  - Teoría de Firewalls
  - Balanceo y enrutamiento
  - Protección frente a DDOS y similares
  - TCP/IP, DNS, HTTPS, etc.

- **Sistemas de intrusión y contramedidas**
  - Ingeniería social
  - Captura de paquetes, análisis y herramientas
  - Escaneo de puertos
  - Malware en red y troyanos
  - DLP (fuga de datos) Cryptolocker (secuestro de datos)
  - GPO y similares
  - Sistemas de autentificación e identificación
  - Administración de entidades de certificación
  - Configuraciones incorrectas de la red
  - Contramedidas de hardware y arranque de SO
  - Auditorias de acceso y uso
  - Herramientas Office y similares, vulnerabilidades
  - Intrusión por correo electrónico
  - Técnicas básicas de hacking ético
  - Técnicas básicas de intrusión y ataque
  - Footprinting / Fingerprinting y vectores de ataque
  - Test De Intrusión y Exploiting
  - Análisis Forense de amenazas
  - XSS, RFI, LFI, Inyección, etc
  - ROOTKITS

☞ Ciberseguridad para departamentos de Dirección:

- **Implementación y planificación**
  - Sistemas de intrusión y contramedidas en la organización
  - Auditorias de seguridad
  - Análisis y gestión de riesgos
  - Seguridad perimetral en la organización
  - Amenazas internas y externas
  - Gestión de identidades y control de accesos
  - Políticas en dispositivos BYOD y corporativos
  - Planificación de Respuesta a incidentes
  - Implantar Departamentos SOC / CERT
  - Mejoras en materia de ciberseguridad en los Dptos. de desarrollo
  - Mejoras en materia de ciberseguridad en los Dptos. de sistemas

- **Teoría**
  - Malware en red y troyanos
  - Protección de activos
  - DLP (fuga de datos) Cryptolocker (secuestro de datos)
  - Concienciación en ciberseguridad y modos de protección
  - Utilidad de los sistemas SIEM
  - Introducción a los MDM
  - Criptografía básica
- **Normativas**
  - Ley española en materia de ciberseguridad
  - Entorno Legal, Protección de datos, LSSI
  - Estrategia de ciberseguridad nacional
  - INCIBE
  - CCN-CERT

☞ Seguridad de la Información. ISO 27001:

- Adquirir los conocimientos, habilidades y aptitudes necesarias para planificar, desarrollar e implementar un sistema de gestión de la seguridad.
- Información de una organización basándose en los estándares internacionales aplicables de acuerdo a la normativa ISO 27001.
- Aprender, planificar y documentar debidamente un Sistema de Gestión de Seguridad de la Información utilizando los diferentes
- Instrumentos de análisis e información que permitan realizar correctamente una auditoría SGSI.

☞ Análisis Forense para móviles:

- Proporciona los conocimientos y las habilidades necesarias para llevar a cabo una investigación sobre teléfonos móviles mediante diversas herramientas, adquiriendo experiencia práctica con las imágenes del teléfono y el análisis de tarjetas SIM y tarjetas de memoria.
- Se desarrollarán los conocimientos, procedimientos y herramientas disponibles, para analizar, de forma efectiva, auditorías de análisis forense específicas. Todo ello adaptado para cada uno de los sistemas operativos disponibles en los dispositivos móviles más utilizados hoy en día, tales como Android o iPhone.

☞ Implementación y configuración segura de redes wifi en organizaciones:

- Se fundamentarán las bases técnicas y conceptos necesarios para entender el funcionamiento de redes inalámbricas. Se aprenderá sobre materiales, electrónica y equipamiento necesario para auditorias y/o test de penetración inalámbricos. Se realizarán prácticas de auditoria y ruptura de seguridad en redes wifi, se analizarán las configuraciones y mecanismos recomendados para su protección.

- **Securizacion y configuración Servidores Linux:**
  - Procesos de Securizacion de equipos Linux, en servidores y clientes, incluidas las ultimas mejoras en seguridad y las nuevas características. Todo de una forma muy práctica, utilizando diferentes laboratorios para la formación.

- **Securizacion y configuración Servidores Windows Server 20XX:**
  - Procesos de Securizacion de equipos Windows, en servidores y clientes, incluidas las ultimas mejoras en seguridad y las nuevas características. Todo de una forma muy práctica, utilizando diferentes laboratorios para la formación.

- **Implementación Desarrollos Seguros c/c++, Java, c# y trabajo con librerías Crypto:**
  - Obtener una visión desde el punto de vista de la seguridad de las aplicaciones web
  - Conocer vulnerabilidades más comunes de las aplicaciones
  - Aprender cómo se realizan los ataques web y como evitarlos.
  - Manejo y uso de herramientas para comprender las distintas vulnerabilidades web.

- **Seguridad en organizaciones y grupos (Análisis y gestión de riesgos):**
  - Mejorar la identificación de oportunidades y de amenazas
  - Establecer una base fiable para la toma de decisiones y la planificación
  - Mejorar el gobierno empresarial
  - Mejorar la seguridad y la confianza de las partes interesadas
  - Asignar y utilizar de manera eficaz los recursos para el tratamiento del riesgo

- **Implementación y organización de respuesta ante incidentes de seguridad:**
  - Sistemas de detección y prevención de intrusiones
  - Implantación y puesta en producción
  - Control de código malicioso
  - Respuesta ante incidentes de seguridad
  - Proceso de notificación y gestión

- Análisis forense
- Estrategias
- Adquisición de evidencias forenses
- Tratamiento de evidencias
- Recuperación de sistemas y medidas mitigadoras

☞ **Auditoria de Seguridad en Desarrollos:**

- Aspectos de seguridad en las diferentes etapas del desarrollo de software, alineadas a las buenas prácticas propuestas por OWASP.
- Señalar las debilidades más comunes de las aplicaciones y los fundamentos de una programación segura para defender la misma de ataques avanzados.
- Proveer al project manager, de los conocimientos necesarios para analizar, cuantificar y calificar los riesgos de seguridad de un proyecto de software.
- Buenas prácticas de desarrollo seguro basándonos en normativas.

☞ **Data Loss Prevention en organizaciones:**

- Protección de los activos de Información
  - Gestión de la Seguridad de la Información: Inventario y clasificación de los activos de Información.
  - Permisos de Acceso a los Sistemas.
  - Controles de Acceso obligatorios y discrecionales.
  - Seguridad de la Información con Terceros.
  - Controles de Acceso: Puntos generales de entrada.
  - Identificación y Autenticación.
  - Ingeniería Social.
  - Autorización y registro (logging).
  - Almacenar, recuperar, transportar y destruir información confidencial.
  - Amenazas a la seguridad de la Red:
    - A la seguridad LAN.
    - A la seguridad Wireless.
    - A la seguridad de Internet.
  - Cifrado.
- Metodología
  - Consideraciones para el éxito de una Auditoría de seguridad.
- Tipo de Auditorías
  - Beneficios de una Auditoría.
  - Metodologías/Estándares de Auditoria mas destacados

❋ Software

☞ XSIbackup (Xerox Servers Inteligently):

XSIbackup (Xerox Servers Inteligently) es una solución de backup **para entornos Vmware ESXi** que permite la realización de backups de forma inteligente y autónoma:

- Herramienta en línea de comando sin dependencias, corre directamente en el hipervisor.
- Programable en el cron de © ESXi.
- Backup en caliente de máquinas virtuales (Hot Backup), sin tiempos de parada.
- Realización de backups desatendidos.
- Provision automática de espacio en discos llenos.
- Informe detallado via e-mail para cada máquina virtual (velocidad, provisión de espacio, tiempos transcurridos, S.M.A.R.T., etc.).
- Logeo de la información de cada sesión de backup

❋ Contacto: