TECNOideas2.0 ciberseguridad y formación.

TECNOideas2.0 es una empresa que **presta servicios de ciberseguridad ofensiva**, que incluye test de intrusión —físicos, sistemas o webs—, auditoría de seguridad en industria 4.0, análisis forense junto con pericia judicial, consultoría legal en tecnologías de la información, y también ofrece formación, tanto a nivel de seguridad para empleados y directivos de empresas en general, como una formación específica más técnica para personal de tecnologías de la información.

TECNOideas2.0 nace en **el año 2009** ofreciendo servicios informáticos generales, como venta y mantenimiento de redes y equipos, gestión de proyectos, etc. a todo tipo de clientes y en sectores muy diversos.

En 2018 decidimos especializarnos en ciberseguridad, por el aumento de la demanda en estos servicios por parte de nuestros clientes, y por la experiencia **de nuestro personal** en estos temas.

Contamos con personal con **una dilatada experiencia en el ámbito tecnológico, informático, industrial y empresarial, todos ellos** especialistas en ciberseguridad.

Teniendo también en nuestras filas **docentes requeridos en universidades como la de Castilla-La Mancha, centros como el Basque Cybersecurity Centre y son conferenciantes de los mejores eventos de España.**

Nuestros métodos no incluyen el uso de grandes plataformas de software, o las típicas listas de ISOS o departamentos de tecnología de algún ente o gobierno, aunque también las podemos seguir bajo petición.

Crecemos y nos nutrimos de los fallos, el conocimiento compartido del hacking ético. Investigamos y acotamos nuestras investigaciones previas, para luego buscar agujeros en los sistemas.

Hacemos *pentesting* (test de penetración) y cualquier acción dentro del **hacking ético**, para probar sus sistemas. Y repetimos todas las auditorías, cuando se suponen solucionado los fallos, para su total seguridad y confianza.

Ética. SOMOS ÉTICOS: hemos enfocado nuestra visión empresarial en esa palabra. Cuando detectamos problemas, no vendemos al mejor postor los servicios de terceros, sino que recomendamos empresas que también nos prestan servicios, o que consumimos nosotros, ya que el ejemplo es la mejor demostración de calidad.

¿Por qué? Creemos que no es ético indicar a los clientes los problemas que tienen, solucionarlos y luego certificar que lo hemos solucionado.
Sin embargo, no dejamos a los clientes, sino que les ayudamos a buscar a los mejores profesionales y las mejores soluciones, nos comprometemos a hacer un seguimiento e ir de la mano con ellos en todo el proceso.

Ante todo, **claridad de conceptos**. Nos gusta que los clientes nos entiendan, por eso queremos definir tres palabras que se repiten constantemente en este sector:

Hacker: últimamente se ha desfigurado esta definición y se la hace sinónimo de delincuentes informáticos.
Un *hacke*r es alguien que busca conocimiento, probarse día a día, compartirlo, y demostrar donde ha llegado, por ejemplo, mostrándole a una empresa donde tiene vulnerabilidades en sus sistemas para que le pongan solución.

Si lo hace para beneficio propio, secuestrando datos, haciendo que una empresa no pueda trabajar, o en definitiva buscando un lucro económico, es un **ciberdelincuente**.

Si lo que hace es vulnerar un software o hardware, para copiarlo y revenderlo por su cuenta, es un ***cracker***.

Pentesting o test de penetración: acciones técnicas concretas para poder entrar en un sistema informático sin las claves adecuadas.

***Hacking ético*:** análisis de los sistemas y software informáticos, para encontrar posibles vulnerabilidades y, como no, sus soluciones, a través de la especialización técnica, del conocimiento compartido.

- II. FORMACIÓN

Y como no podía ser de otro modo, para completar nuestra oferta en ciberseguridad, ofrecemos también diversos niveles de formación, ya que es otro de nuestros puntos fuertes.

Es imprescindible una buena concienciación por parte de las empresas y de sus trabajadores de los riesgos reales que existen en temas de ciberseguridad.

¿QUÉ OFRECEMOS?

• **Pequeñas charlas de concienciación** general o de temas más concretos y sus soluciones.

• **Charlas a medida de las necesidades de su empresa**.

• **Formaciones *in company***. Nos desplazamos a su empresa para ofrecer cursos o píldoras formativas, a trabajadores y directivos, para concienciar y proteger los activos, o formas seguras de trabajar.

• **Cursos para profesionales** de tecnologías de la información, tanto para los que están activos como para los que se quieran reciclar. Son formaciones a diferentes niveles dentro de la ciberseguridad.

• **Todos nuestros cursos son bonificables** para trabajadores en activo a través de **Fundae** (Fundación Estatal para la Formación y el Empleo).

• Casi todas nuestras formaciones **pueden realizarse de forma presencial o en línea.**

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Esta es nuestra principal oferta formativa:

- **Ciberseguridad para empleados**
  Curso de 2-4 horas.
  Después de este curso, los empleados sabrán porque es tan importante ser muy estrictos en seguridad personal y tecnológica, y el motivo de los protocolos empresariales. Serán capaces de evaluar, distinguir amenazas, y corregir malos hábitos.

  TEMARIO
  - Protección personal y de dispositivos
  - Identificación de phishing y correos maliciosos
  - Wifis (gratuitas y dispositivos personales en redes corporativas)
  - Dispositivos USB
  - Robos de credenciales (hacking social)

- **Ciberseguridad para mandos intermedios y directivos**
  Curso de 2-4 horas.
  No todo el mundo trata el mismo tipo de información, la misma presión o responsabilidad, por ello hacemos hincapié en los problemas más comunes a los que se pueden enfrentar los mandos intermedios y los directivos.

  TEMARIO
  - Definición de phishing, spamming, carding...
  - RGPD - Reglamento General de Protección de Datos
  - Explicación de ataques y vulnerabilidades
  - Factor humano y organizativo en la seguridad de la información.

  OBJETIVOS
  - Comprender los principales retos de la gestión de la seguridad de la información.
  - Análisis de las principales amenazas y tipos de ataques a la seguridad de la información.
  - Resumen de soluciones tecnológicas para implantar controles de seguridad en las organizaciones.
  - Análisis de los problemas de privacidad y de seguridad en dispositivos móviles (smartphones y tabletas) y de otros dispositivos conectados o compartidos.

- **Ciberseguridad en el teletrabajo**
  Curso de 4 horas.
  Curso que tiene por objetivo el adquirir hábitos "saludables" en el ámbito de la ciberseguridad, para trabajar de forma segura desde casa, proteger la wifi y protegernos de ataques de phishing.

- **BYOD - *Bring Your Own Devices***
  (Trae tu propio dispositivo)
  Curso de 4 horas.
  Estudiaremos la problemática de esta política empresarial según la cual se permite a los empleados usar sus propios dispositivos personales para trabajar.
  Explicaremos como hacerla servir con seguridad y como protegernos al usar los dispositivos personales para trabajar y conectarse a las redes de la empresa y viceversa.

- **Ciberseguridad en e-commerce**
  Curso de 12 horas.
  Se detallarán las diferentes vulnerabilidades en los sistemas de comercio online, enseñando como configurar los diferentes entornos y CMS más ampliamente utilizados.

  TEMARIO
  - Niveles de seguridad, prácticas y medidas
  - Storage de datos de clientes
  - GDPR sobre e-commerce
  - Gestión de usuarios y contraseñas
  - Check de enlaces a nuestro sitio
  - Actualizaciones y updates
  - Cumplimiento de la legislación nacional
  - Procesos de autenticación
  - PCI y PSD2
  - Certificados SSL.

- **Hacking ético iniciación**
  Curso de 20 horas.
  Nos introducimos en el apasionante mundo de la ciberseguridad bajo la perspectiva ofensiva, del hacking ético.

  TEMARIO
  - Presentación
  - Conceptos de Hacking
  - Virtualización
  - Comandos básicos Linux
  - Técnicas de ocultamiento
  - Auditoría Redes Wifi
  - Password cracking
  - Malware

- **Hacking ético avanzado**
  Curso de 20 horas.
  Curso destinado a adquirir los diferentes conocimientos avanzados, para pentesting, tanto en defensa como en ataque.
  Conocer algunas herramientas específicas para realizar pentesting en entornos controlados, y también desarrollar los scripts propios para realizar ataques.
  Tiene un reparto de tiempo 60/40 teórico/práctico.

  TEMARIO
  - Presentación
  - Scripts en Python
  - Metasploit
  - Análisis del trafico
  - Auditoría Redes Wifi II
  - Password cracking II
  - Forense de dispositivos

- **Hacking ético intensivo**
  Curso de 24 horas.
  Juntamos los dos cursos de hacking ético para las personas que no tienen tanta disponibilidad o tiempo libre.

- **Iniciación al pentesting con PowerShell**
  Curso de 20 horas.
  Aprenderemos el uso de una potente herramienta como es PowerShell. Utilizando esta suite, aprenderemos a programar scripts para ataques y auditoria sobre sistemas Windows.

  TEMARIO
  - Qué es PowerShell y su utilidad
  - Administración máquinas, usuarios y servicios con PowerShell
  - Desarrollo scripts en PowerShell para automatizar tareas
  - Metodología de pentesting usando PowerShell
  - Escaneado de máquinas y servicios
  - Ejecución exploits desde PowerShell
  - Post-explotación

- **Pentesting con Metasploit 100%**
  Curso de 20 horas.
  Aprenderemos el uso de una potente herramienta como es Metasploit. Utilizaremos este framework para las diferentes fases de un proceso de auditoria.

  TEMARIO
  - Qué es Metasploit y su utilidad
  - Uso de payloads
  - Desarrollo scripts en Metasploit para automatizar tareas
  - Metodología de Pentesting usando Metasploit
  - Escaneado de máquinas y servicios
  - Ejecución exploits desde Metasploit
  - Post-explotación

- **Pentesting con Python**
  Curso de 20 horas.
  Aprenderemos el uso de uno de los lenguajes más potentes y extendidos como es Python. Utilizaremos este lenguaje para las diferentes fases de un proceso de auditoria y utilización de librerías específicas para ello.

  TEMARIO
  - Introducción al Python
  - Datos funciones y clases
  - Recolección de información (I)

- Recolección de información (II)
- Análisis de vulnerabilidades
- Ataques red local

- **Transformación digital de la industria**
  Curso de 12 horas.
  Un curso para ver las ventajas de la tecnificación de la industria, y de la ciberseguridad en ella.

  TEMARIO
  - Por qué y cómo afrontar la transformación digital de la industria
  - Cultura digital
  - El qué o la visión
  - El cómo o los procesos
  - Tus clientes
  - Adaptando servicios y productos
  - Tu modelo de negocio
  - Personas y digitalización en la industria: introducción al Agile Talent
  - Introducción a las tecnologías IoT para la industria
  - Fabricación 3D: prototipos para el sector productivo

- **Ciberseguridad industrial**
  Curso de 25 horas.
  Conoceremos qué es, de qué se compone, cuáles son las principales vulnerabilidades y cómo se realiza una auditoria en sistemas de control industrial.

  TEMARIO
  - Visión general y conceptos más importantes de la ciberseguridad industrial.
  - Entender las principales diferencias existentes en entornos IT /OT
  - Principales vulnerabilidades y amenazas en entornos industriales
  - Tipología de los diferentes ataques en una red OT o una infraestructura crítica
  - Principales vectores de ataque
  - Auditoría de un sistema OT

- **Auditorías de sistemas de control industrial**
  Curso de 12 horas.
  Curso para adquirir conocimientos sobre las estructuras y funcionamientos de las redes OT, protocolos, equipos, instrumentación, vulnerabilidades y obsolescencia de los equipos, que los conforman.

  TEMARIO
  - Presentación
  - Entornos industriales
  - Protocolos industriales
  - Infraestructuras criticas
  - Legislación vigente
  - Auditoría OT
  - Convergencia IT/OT
  - Ataques reales

- **Forense industrial iniciación**
  Curso de 20 horas.
  Aprende las diferentes técnicas forenses para la recolección y tratamiento de evidencias digitales en equipamiento y dispositivos industriales.
  Consta de un 75% de práctica y un 25% de teoría.

  TEMARIO
  - Presentación
  - Qué es la ciencia forense
  - Legislación estatal
  - RFC 3227
  - Adquisición de firmare
  - Reversing de firmware
  - Búsqueda de amenazas
  - Informe forense

- **Forense industrial avanzado**
  Curso de 20 horas.
  Aprende las diferentes técnicas forenses para la recolección y tratamiento de evidencias digitales en equipamiento y dispositivos industriales, así como la protección de estos.
  Consta de un 75% de práctica y un 25% de teoría.

  TEMARIO
  - Presentación
  - Qué es la ciencia forense
  - Legislación estatal
  - RFC 3227

- Adquisición de firmare
- Reversing de firmware
- Threat hunting en redes OT
- Configurando un IDS y reglas específicas para OT
- Informe forense

- **Forense informático iniciación**
  Curso de 20 horas.
  Aprende las diferentes técnicas forenses para la recolección y tratamiento de evidencias digitales en sistemas Linux y Windows, así como una introducción a diferentes herramientas.
  Consta de un 75% de práctica y un 25% de teoría.

  TEMARIO
  - Presentación
  - Qué es la ciencia forense
  - Legislación estatal
  - RFC 3227
  - Volcados de memoria Windows/Linux
  - Recogida de evidencias
  - Cadena de custodia
  - Informe forense
  - Forense informático avanzado

- **Forense informático avanzado**
  Curso de 15 horas.
  Avanzaremos en las diferentes técnicas forenses para la recolección y tratamiento de evidencias digitales en formato avanzado en sistemas Linux y Windows, principalmente servidores.
  Consta de un 75% de práctica y un 25% de teoría.

  TEMARIO
  - Presentación
  - Legislación judicial
  - 40 puntos de control Windows
  - Destripando Linux
  - Autopsy
  - Cain
  - Santoku

- **Forense de dispositivos móviles**
  Curso de 15 horas.
  Conoceremos diferentes herramientas y su utilización para realizar un informe forense a partir de la adquisición de evidencias.

  TEMARIO
  - Presentación
  - Legislación judicial
  - Adquisición de memoria.
  - Principales directorios
  - Extracción de evidencias
  - Autopsy

- **Auditorías de dispositivos móviles**
  Curso de 25 horas.
  Conoceremos una poderosa herramienta, capaz de extraer los datos de cualquier evidencia, con el fin de generar un completo informe forense.

  TEMARIO
  - Herramientas y metodología OWASP
  - Rooteo de dispositivos
  - Escaneo y recolección de información
  - Análisis y descompresión de aplicaciones
  - Análisis de trafico
  - Volcados y análisis de memoria
  - Examen final práctico

- **Iniciación a Autopsy**
  Curso de 15 horas.
  Conoceremos una poderosa herramienta, capaz de extraer los datos de cualquier evidencia, con el fin de generar un completo informe forense.

  TEMARIO
  - Metodología forense
  - Análisis de datos extraídos
  - Cronología
  - Flujos de trabajo
  - Fuentes de datos
  - Análisis automáticos
  - Instalación de módulos de terceros
  - Reporting

- **Iniciación al Blockchain**
  Curso de 12 horas.
  Conoceremos de qué trata la tecnología Blockchain y los diferentes campos de aplicación.

  TEMARIO
  - Introducción en el mundo de Blockchain y criptomonedas
  - ¿Qué son y cómo se crean las criptomonedas?
  - ¿Qué futuro tienen?
  - ¿Son una burbuja?
  - ¿Para qué sirven?
  - ¿Cómo me puedo beneficiar de ellas?

Principales certificaciones de TECNOideas2.0

Nuestra profesionalidad y buen hacer queda patente en las siguientes certificaciones obtenidas por nuestra empresa y nuestros profesionales.

Formamos parte desde 2019 del Catálogo del Incibe, el [Instituto de Ciberseguridad de España.]

Poseemos la máxima certificación profesional (nivel **Negro**) del **[Centro de Ciberseguridad Industrial.]**

Y además poseemos estas **certificaciones internacionales**:

EC-Council

CEH Certified Ethical Hacker
ETHICAL HACKER
PRACTICAL

CISSP®
Certified Information Systems Security Professional

Information Security Management System
ISO 27001
Certified
Lead Auditor

ISO 27001
INFORMATION SECURITY
MANAGEMENT SYSTEM