PRESENTACIÓN

TECNOideas2.0 es una empresa que presta servicios de ciberseguridad, tanto industrial como informática..

¿Qué hacemos?

- Test de intrusión —físicos, sistemas o webs— , en sistemas informáticos.
- Auditoría de seguridad en industria 4.0
- Análisis forense junto con pericia judicial
- Consultoría legal en tecnologías de la información
- Formación. Cursos de seguridad para empleados; para directivos de empresas en general y también una formación más técnica para personal de tecnologías de la información.

TECNOideas2.0 tiene más de diez años de experiencia.

Nacimos 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**.

TECNOideas2.0 posee personal cualificado.

Nuestro personal **es especialista en ciberseguridad** y posee una dilatada experiencia en el ámbito tecnológico, informático, industrial y empresarial.

Para impartir formación, tenemos **docentes reconocidos**. Nuestros expertos no sólo tienen los conocimientos técnicos, sino que son **profesores universitarios y del Basque Cybersecurity Center** y dictan conferencias en los mejores eventos de ciberseguridad de España.

En TECNOideas2.0 tenemos un método propio de trabajo.

Nuestro sistema se basa en los principios del hacking ético, creciendo y nutriendonos de los fallos y el conocimiento compartido. Investigamos el entorno, buscamos los defectos y agujeros de los sistemas; en definitiva nos ponemos en la piel de un delincuente.

Nuestros métodos en auditorías informáticas **no incluyen el uso de grandes plataformas de software,** pero para industría podemos seguir listados de Isos, recomendaciones sectoriales, gubernamentales, o cualquier otra que sea acorde con las necesidades del cliente.

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

En TECNOideas2.0 somos éticos.

Hemos enfocado nuestra visión empresarial en esa palabra.
Analizamos y detectamos los fallos en los sistemas de nuestros clientes.
Les informamos de lo que deben hacer.
Proponemos las empresas que pueden realizarlo. Suelen ser empresas que también nos prestan esos 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, siempre ayudamos a los clientes en esta etapa. Buscamos los mejores profesionales y soluciones, nos comprometemos a hacer un seguimiento e ir de la mano con ellos en todo el proceso.

En TECNOideas2.0 hablamos vuestro idioma.

Nos gusta que los clientes nos entiendan. **Claridad de conceptos.** Por eso queremos definir tres palabras que se repiten constantemente en este sector:

Hacker: desde siempre 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***.

Test de intrusión o pentesting o test de penetración: son un conjunto de ataques simulados dirigidos a un sistema informático para detectar posibles debilidades o vulnerabilidades, para que sean corregidas y no puedan ser explotadas.

***Hacking ético*:** análisis en el que se realizan una serie de pruebas acordadas con el cliente, con el fin de descubrir fallos de seguridad que pueda afectar a la empresa y a su producción.

CIBERSEGURIDAD INDUSTRIAL

- **Industria 4.0**

La Ciberseguridad industrial ya no puede ignorarse.

Los responsables de IT/OT **necesitan evaluar la seguridad de los sistemas de control industrial y sistemas conjuntos** (Entornos IT clásicos).

La cuarta revolución industrial ya ha llegado, e incluye dispositivos digitales y de comunicaciones en el entorno productivo o logístico.
Estos dispositivos son esenciales para el buen funcionamiento industrial, son **elementos críticos y al estar conectados a Internet, también son vulnerables.**

En TECNOideas2.0 somos expertos en dispositivos industriales y poseemos la máxima certificación para ello.

¿Qué ofrecemos?
Servicios de ciberseguridad industrial que mejoran y se adaptan a los más exigentes requerimientos de calidad.

Aplicamos normativas y estándares nacionales e internacionales para poder cumplir con todas las normativas, incluso las impuestas de forma sectorial.

¿Cuál es el problema?
Identificamos los elementos críticos que precisan protección inmediata:

1. **Gestión de los permisos.**
   Antes, la mayoría de los sistemas estaban aislados. Ahora **las redes IT y OT están interconectadas**, con la famosa "integración IT/OT".
   Es necesario aplicar técnicas e implementaciones de ciberseguridad en OT.
   >> Hay que determinar los privilegios para cada usuario autorizado.
   >> Hay que bloquear los accesos a los no autorizados.

2. **Actualización de sistemas operativos: el hardware y el software**. Algunos sistemas hardware y software son anteriores al concepto de ciberseguridad.
   Hay que garantizar la compatibilidad con las protecciones modernas.
   >>Software antivirus.
   >>Tecnologías de escaneado de amenazas.
   >>Plantear buenas políticas de *update* y parcheado de los sistemas.

3. **Identificar los activos inseguros, y los accesibles por IP desde el exterior.**
   Es el caso, por ejemplo, de los sensores e indicadores de presión, plc's. hmi's, scada, etc.
   Los datos en estos dispositivos **pueden ser manipulados**, lo que impacta en la seguridad y fiabilidad de todo el sistema.

Estos sistemas son indexados por buscadores, que informarán de las diferentes vulnerabilidades de los sistemas y su disponibilidad.
Ejemplo ***www.shodan.io***

4. **Buenas prácticas en la programación, desarrollo e implementación**. A menudo se usa y se incorpora software a medida, pero **programado con escasa atención a las técnicas de ciberseguridad**: el sistema OT queda expuesto a los ataques.
   Hay que mantener una buena praxis en todas las fases de desarrollo e implementación de los sistemas.

5. **Políticas de registro de incidentes**.
   Las empresas que establecen un proceso para la notificación y comunicación de eventos del sistema pueden usar estos datos para detectar irregularidades e implementar medidas de seguridad.
   Hay que monitorizar la actividad de la empresa con herramientas de supervisión, IDS, IPS, etc.

6. **Segmentación de la red**.
   Una buena y bien definida segmentación de la red, es la clave para el éxito en materia de ciberseguridad.
   Muchas organizaciones no han separado todavía sus redes en diferentes segmentos funcionales.
   Sin esta segmentación, los datos y las aplicaciones infectadas pueden expandirse de un segmento a otro y los atacantes que consiguen traspasar las defensas perimetrales pueden, fácilmente, moverse transversalmente por la red sin ser detectados.

7. **Plan de recuperación operacional y respuesta ante incidentes**.
   En el caso de un ataque, se necesita un proceso documentado para evaluar los daños, reparar sistemas y máquinas y restablecer sus operaciones.
   Los simulacros regulares de seguridad también ayudan a los operadores a adoptar una recuperación rápida y eficiente.
   El plan debe establecer prioridades, personal afectado, definición de cada rol dentro la recuperación del desastre y

retro-alimentación del mismo.

8. **Formación en materia de OT**.
   Muchas empresas carecen de formación en materia OT, la cual es imprescindible a la hora de establecer políticas de seguridad en estos sistemas, y cumplir con las normativas existentes.

¿Cómo lo hacemos?

Auditamos estos sistemas, que no suelen estar tan bien protegidos como deberían.
HMI's, scadas, sensores, etc. suelen ser antiguos, y por ello no cuentan con una capa de protección adecuada en su diseño original.

Actuamos en cualquier sector y sea cual sea el tamaño de la empresa.

¡LEEDNOS!

Tenemos una serie de artículos tanto en **nuestro blog** como en **Linkedin**, para reforzar la concienciación que realizamos en cuanto a ciberseguridad industrial:

https://tecnoideas20.com/2020/02/06/exposicion-de-activos-ot/

https://tecnoideas20.com/2020/05/18/el-riesgo-cibernetico-por-sectores-salud-parte-i/

https://tecnoideas20.com/2020/05/07/el-riesgo-cibernetico-por-sectores-salud-parte-ii-farmaceuticas/

¡VEDNOS!

Y también podéis visitar nuestro **canal de Youtube**, donde vamos colgando presentaciones, webinars, cursos, etc.

https://www.youtube.com/channel/UC7FRpS61xNxPUkIDCO8JuZw
FORMACIÓN

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 en el teletrabajo**
  Curso básico de 4 horas de duración.

- **Hacking ético, básico y avanzado**
  Cursos de 20 horas duración.

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

- **Auditorías de sistemas de control industrial**
  Curso de iniciación de 10 horas de duración.

- **Iniciación a forensia industrial**
  Curso de iniciación de 20 horas.

- **Forense informático avanzado**
  Curso de nivel medio de 20 horas.

- **Aplicando machine learning a la ciberseguridad**
  Curso de 25 horas.

- **Y muchos más cursos cada mes. A medida también realizamos formaciones según las necesidades de su personal.**

Más información sobre nuestros cursos, AQUÍ.

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