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, y conferenciantes de los mejores eventos de España.**

Nuestros métodos no incluyen 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. No vendemos al mejor postor los servicios que podamos ofrecer de terceros, sino que 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, no dejamos a los clientes, sino que le 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.**

Información previa para presupuestar el ENS

- Administración publica
  - Número de habitantes totales, y núcleos agregados, si existen.
  - Número, tipología y relación directa de las empresas que dependen directamente del entidad.
  - Empresas externas, si hay, que accedan a los datos de la entidad.
  - Sede electrónica, si la gestiona la propia entidad, o una externas.
  - Relación en porcentaje de funcionarios y personal interino, y el nivel de rotación.
- Empresa privada y pública
  - DPD, si es propio, externo (presencial, telemático o a título honorífico).
  - Si ha tenido un incidente de seguridad informática en los dos últimos años.
  - Tipo de centro de datos: propio, físico, cloud, empresa externa, etc.
  - Nivel en porcentaje de teletrabajo y trabajo presencial.
  - Número de formaciones al año en gestión de datos, ciberseguridad, privacidad, etc.
  - Certificaciones anteriores en ENS o ISO27001 si las hubiera, y fechas.
  - Página web, y tipo: informativa, e-commerce, gestión, apartado usuarios…
  - APP's propias que usen datos internos.
  - Redes sociales utilizadas, con cuentas de empresa. Cuales y quien las usa.

Proceso de ejecución del ENS una vez aceptado por el cliente

1. INICIO DEL PROYECTO: designación del comité de seguridad o persona de enlace.
2. REUNIONES: recogida de información a todo nivel, y preferiblemente una visita física a las instalaciones.
3. CATEGORIZAR LOS SISTEMAS: inventario de todos los elemento personales y técnicos y relaciones con terceros.
4. ANÁLISIS DE RIESGOS: análisis exhaustivo de los riesgos inherentes, ERP, backups gestión de credenciales).
5. DECLARACIÓN DE APLICABILIDAD: análisis actual, y nivel de madurez que se quiere adquirir.
6. DEFINICIÓN DEL PLAN DE MEJORA: revisión de las medidas de seguridad a aplicar juntamente con el responsable del proceso de implantación del ENS.
7. ELABORAR EL PLAN DE IMPLEMENTACIÓN: definir los puntos a implementar o mejorar, en base a los datos recopilados y las deficiencias encontradas si existen.
8. PREPARACIÓN Y ENTREGA DE DOCUMENTACIÓN: durante el proyecto se va entregando información, así como si se encuentran puntos críticos se informara de inmediato
9. COMPROBACIÓN DEL SISTEMA: Elaboración de un plan especifico de pruebas de los sistemas revisados.
10. AUDITORIA: definir un plan de auditoria y un proceso de mejora continua.
11. FORMACIÓN: formación dirigida a todo el personal implicado en el ENS sobre política, normativa y procedimientos de seguridad.
12. REVISIÓN Y ENTREGA FINAL DE DOCUMENTACIÓN: entrega de toda la documentación resultante de la implantación del ENS con una ultima revisión conjunta con el cliente.
13. FIN DE PROYECTO: reunión final para el cierre y valoración del proyecto. Se puede dar soporte al proceso de mejora continua y monitorización.

MÍNIMA REVISIÓN PARA NIVEL BAJO

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

Puntos a analizar durante el ENS (75 medidas):

Marco Organizativo:

- Política de seguridad
- Normativa de seguridad
- Procedimientos de seguridad
- Proceso de autorización

Marco operacional:

- Planificación
- Control de acceso
- Explotación

- Servicios externos
- Continuidad del servicio
- Monitorización del sistema

Medidas de protección

- Instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos
- Protección de las comunicaciones
- Protección soportes de la información
- Protección de aplicaciones informáticas
- Protección de la información
- Protección de los servicios

Tiempos aproximados:

- Ayuntamiento de entre 15 y 25000 habitantes, sin empresas externas, unos 20 días aproximadamente.
- Ayuntamientos de más de 25000 habitantes y con empresas externas, entre 30 y 50 días aproximadamente.
- Pymes de entre 1 y 50 trabajadores, 20 días aproximadamente.
- Pymes de entre 50 y 250 trabajadores, entre 30 y 50 días aproximadamente.

NOTAS:

Opción monitorización y seguimiento (aparte), para continuar cumpliendo la base del ENS

***Nosotros ayudamos con el proceso**, a poner orden, y estar preparados, pero después la certificación la realiza **ENAC** o **AENOR,** pero lo podemos gestionar y hacer de interlocutores.

Algunas de las titulaciones de nuestro equipo

- Ingeniería Electrónica Industrial
- Ingeniería Técnico Informático de Sistemas
- Máster dirección de equipos directivos
- Máster Industria 4.0
- ICS security architect
- Perito informático colegiado

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**: