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 sobre la obligatoriedad de que determinadas empresas tengan un responsable de ciberseguridad

MARCO NORMATIVO
Real Decreto 43/2021, de 26 de enero por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, **de seguridad de las redes y sistemas de información**.
Publicado en el BOE del 28 de enero de 2021, páginas 8187 a 8214.

CONTENIDO
Establece que los operadores de servicios esenciales ***deberán nombrar una persona u órgano colegiado responsable de la seguridad de la información*** que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y los Equipos de Respuesta a Incidentes de Ciberseguridad (CSIRT) de referencia.
Este servicio puede ser externalizado.

El objeto de la Ley es:

- Crear un marco estratégico e institucional de seguridad de las redes y sistemas de información.

- La supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales.

- La supervisión del cumplimiento de las obligaciones de seguridad de los proveedores de servicios digitales.

- La gestión de incidentes de seguridad.

Por todo ello, la ley se aplicará:

- A los servicios esenciales dependientes de las redes y sistemas de información de diversos sectores estratégicos.

- A los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

CUANDO
En menos de tres meses a partir de la fecha de publicación en el BOE. Es decir, las empresas implicadas han de tener su responsable de seguridad de la información (CISO) o un servicio externo que cubra este puesto antes del 28 de abril de 2021.

¿QUÉ DEBEN HACER LAS EMPRESAS AFECTADAS?
Es muy importante señalar que la ley específica que **las empresas,** además de tener a este responsable en nómina (a no ser que el servicio esté externalizado) **deben facilitar los medios y poner todo el empeño en realizar sus tareas.**

Entre las muchas tareas que debe cumplir y efectuar destacamos las siguientes:

• Análisis y gestión de riesgos.
• Gestión de riesgos de terceros o proveedores.
• Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
• Gestión del personal y profesionalidad.
• Adquisición de productos o servicios de seguridad.
• Detección y gestión de incidentes.
• Planes de recuperación y aseguramiento de la continuidad de las operaciones.
• Mejora continua.
• Interconexión de sistemas.
• Registro de la actividad de los usuarios.

¿QUÉ ES Y QUÉ HACE EL RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN O CISO?
Las funciones del CISO son muy variadas y esenciales para cumplir con todos los protocolos que marca la ley. Destacamos:

a) Elaborar y proponer para la aprobación de la organización, las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados.

También para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.

(Artículo 6.2 de este real decreto).

b) Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

c) Elaborar el documento ***Declaración de Aplicabilidad de medidas de seguridad***.

(Artículo 6.3 párrafo 2º de este real decreto).

d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

e) Remitir a la autoridad competente, a través del CSIRT (Equipo de Respuesta a Incidentes de Ciberseguridad) de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

f) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

g) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

UN CISO EXTERNO LA MEJOR SOLUCIÓN

¿QUÉ OS PODEMOS OFRECER?
Ventajas

- Ahorro significativo, por la diferencia entre el coste de nuestro servicio y el sueldo que puede llegar a tener un CISO profesional.

- Confianza y competitividad, ya que nuestra empresa cuenta con profesionales cualificados, para prestar todos nuestros servicios con la mayor eficiencia.

- Contacto único, ya que cualquier necesidad en seguridad os la podemos proporcionar nosotros directamente, o a través de nuestros partners, que son los que utilizamos para nosotros.

¿POR QUÉ TECNOideas?

Porque ofrecemos servicios informáticos desde el año 2009.

Porque somos especialistas en ciberseguridad desde el año 2018.

Porque **somos éticos**.

Porque tenemos un equipo de expertos perfectamente formados.

Porque valoramos no solo la técnica, sino el trato humano. Con TECNOideas podréis hablar con un técnico experto: no sólo usamos máquinas para hacer el trabajo.

Porque sabemos escuchar y comprender las **necesidades reales** de una empresa, sea grande o pyme.

Porque podemos ajustar las tarifas a los requerimientos reales de una empresa.

Porque TECNOideas está cualificado para cumplir todos los requisitos que marca la ley.

CONTACTADNOS,

¡QUEREMOS SER VUESTRO CISO!

MÁS INFORMACIÓN:
- BOE https://www.boe.es/eli/es/rd/2021/01/26/43

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**: