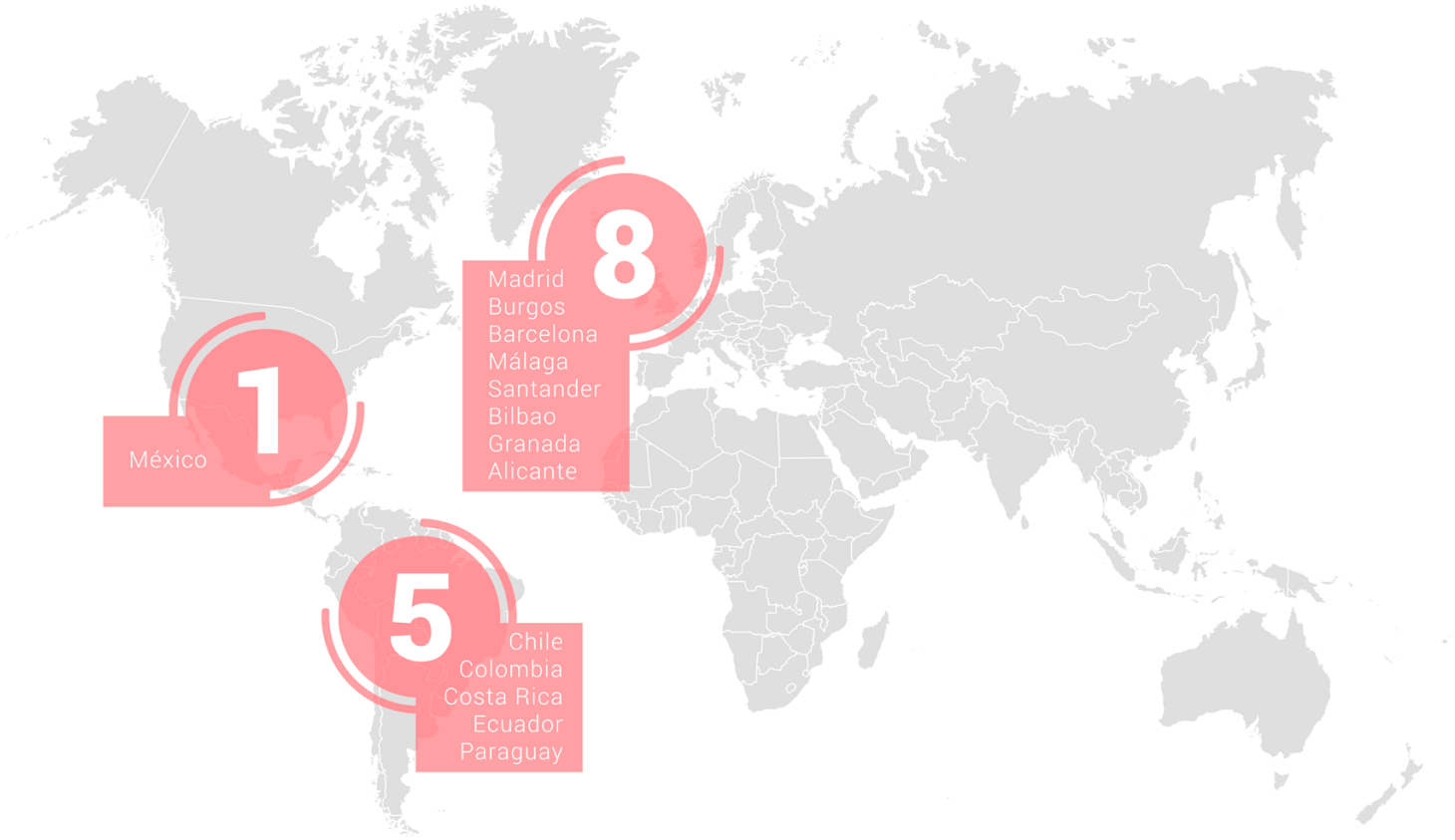
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Auditoría Seguridad Informática



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

EnGrupo ACMSpodemos asesorarle si necesita un servicio de auditoría de Seguridad Informática Hacking Ético Profesional. Rellene el formulario de contacto y nos pondremos en contacto con su organización.

Auditoría Seguridad Informática

Actualmente tanto las empresas como las organizaciones son dependientes casi al 100% de infraestructuras tecnológicas y ello está generando vulnerabilidades en los sistemas informáticos.

Nuestros servidores, archivos, directorios, dispositivos, etc. son susceptibles de sufrir robos de información confidencial, ciberataques por parte de delincuentes informáticos y necesitamos la experiencia y la ayuda de expertos informáticos que hagan pruebas en las propias redes para descubrir posibles fisuras.

Sin un servicio de consultoría hacking ético profesional personalizado para su empresa es imposible detectar los problemas de seguridad.

La labor de un buen hacker ético es averiguar cuáles son los mecanismos de ataque que han utilizado los delincuentes informáticos en nuestra Red y a partir de ahí bloquearlos y buscar soluciones prácticas y efectivas.

¿Cuál es el objetivo de una Auditoría de Seguridad Informática para prevenir ataques informáticos?

El objetivo de una Auditoría de Seguridad Informática es salvaguardar la seguridad informática de su organización y proteger su infraestructura tecnológica corporativade ataques informáticos.

Contratar los servicios de una Auditoría de Seguridad Informática o Consultoría hacking ético profesional es el Método Fundamental para conocer los riesgos que existen alrededor de su empresa, estudiando su incidencia y aportando soluciones para cubrir las vulnerabilidades detectadas.

Términos relacionados con el Hacking ético

Si quiere adaptarse al mundo virtual, a un mundo donde las mejoras de las Redes y sistemas informáticos evolucionan de una manera imparable y donde los ciberataques están a la orden del día. Le recomendamos que conozca algunos de los términos que escuchará o leerá en noticias y en libros sobre Auditoría de Seguridad, hacking ético profesional o auditor hacking.

Conceptos relacionados con una "Auditoría de Seguridad Informática y Ataques Informáticos".

Ataque de fuerza bruta:

Es el método para averiguar una contraseña probando todas las combinaciones posibles hasta averiguar la combinación correcta.

Autenticación:

Es el método de comprobación que tiene un ordenador o los servicios online para verificar que la persona que intenta acceder es quién dice ser.

Cortafuegos:
Es un sistema de seguridad cuyo objetivo es asegurar que todas las comunicaciones que se produzcan entre nuestra Red e Internet sigan las políticas de seguridad de la empresa.

Exploit:
Es la secuencia de comandos utilizados para ocasionar comportamientos no deseados e imprevistos al ocurrir un fallo de seguridad o vulnerabilidad en el sistema

Gusano:
Es el típico programa malicioso, en inglés malware, que es conocido por su veloz propagación.

IDS:
Es un sistema de detección de intrusos, Intrusión Detection System, que puede descubrir accesos no autorizados a un PC o a una red.

Informática forense:

Es un proceso para detectar toda evidencia que puedan aportarse a un juicio como prueba fidedigna y evidente.

Malware:
Es un software que tiene como propósito perjudicar un sistema de información o infiltrarse en él, sin el consentimiento de su propietario.

Pentest:
Es un ataque a un sistema, ya sea, software o hardware con la intención de localizar vulnerabilidades. La prueba de penetración conlleva un análisis activo de toda vulnerabilidad potencial y de configuraciones inadecuadas.

Puerta trasera:
O en inglés backdoor es cualquier punto débil de un programa o sistema por donde una persona que no está autorizada accede.

Ransomware:
Es el secuestro de información, utilizando para ello el método de la encriptación. Los datos permanecen ilegibles si no se conoce la contraseña para desencriptar y con ello extorsionan a un usuario exigiendo un rescate económico.

SGSI:

Sus siglas significan: Sistema de Gestión de la seguridad de la Información. Se trata de un conjunto de políticas de seguridad de la información. La Norma ISO/IEC 27001 las recoge en su articulado.

Sniffer:
Es un programa que se utiliza para monitorear información que circula por la red con el fin de adueñarse de información.

Spoofing:
Técnica de suplantación de identidad en la Red cuyo autor es el ciberdelincuente

Esta técnica ataca la privacidad de los usuarios y la integridad de sus datos.

Spyware:
Tipo de malware que colecciona información de un ordenador y posteriormente la manda a una entidad remota sin el conocimiento o consentimiento del usuario

Suplantación de identidad:
El delincuente informático se hace pasar por otra persona para realizar fraude o cyberbulling

Troyano:
Es otro tipo de malware, software malicioso que no se auto replica. Generalmente, para su propagación por la Red es necesario utilizar ingeniería social.

Virus:
Programa que cuando se ejecuta se copia a sí mismo adjuntándose en aplicaciones que hay en el equipo y que infecta archivos. Necesita la mano de un usuario para propagarse

Periodos para ejecutar una auditoría de seguridad Informática o Hacking Ético Profesional

Las empresas deberían ejecutar una auditoria de seguridad o Hacking Ético Profesional al menos una vez al año.Proponemos, como mínimo una vez al año, puesto que, nos consta, que aunque, en un primer momento los procesos de Hacking Ético Profesional ayudan e implementan cambios de carácter técnico y organizativo en la empresa e impulsan su actividad con mejoras, incrementando en muchas ocasiones su eficacia, con el tiempo, esa energía inicial desciende a medida que pasan los meses. Para cubrir esa pérdida de fuerza inicial es conveniente realizar más de una auditoría de Hacking Ético Profesional al año.

El resultado del test de Seguridad posibilitará a la Dirección averiguar cuál es su evolución, la capacidad de los procedimientos y sobre todo, analizar si la inversión que está realizando en seguridad informática es realmente adecuada.

Si desea conocer más sobre el Hacking Ético Profesional a continuación le ofrecemos varios contenidos relacionados:

HACKING ÉTICO PROFESIONAL

CONSULTORÍA HACKING ÉTICO PROFESIONAL

PRESUPUESTO HACKING ÉTICO PROFESIONAL

AUDITORIA DE SEGURIDAD INFORMÁTICA

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com