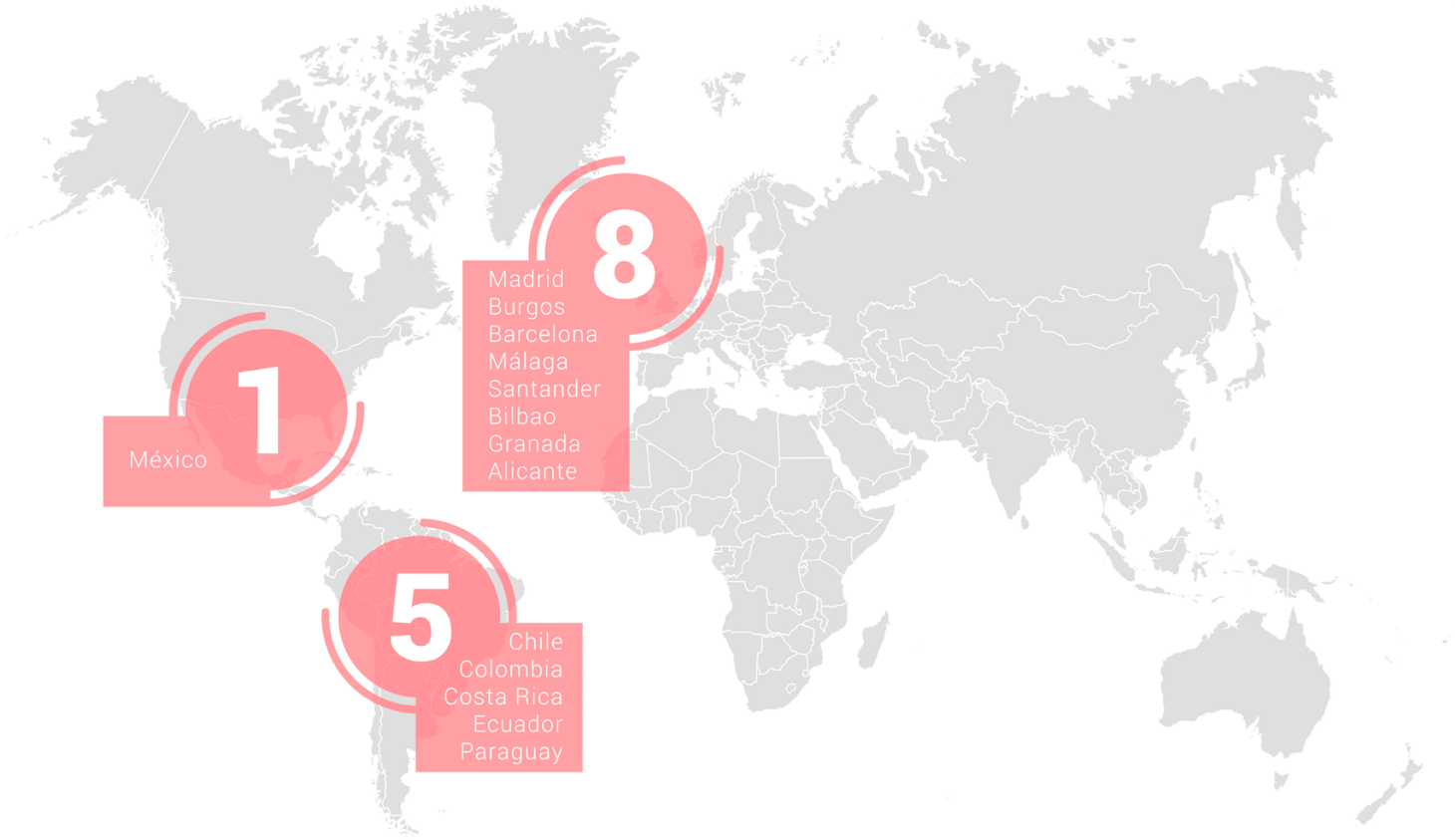
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Forense Digital Análisis: Principios y técnicas



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)

Grupo ACMS Consultores está especializado en el Análisis Forense Digital.Rellene el formulario de contacto y nos pondremos en contacto con su organización.

¿Qué es un análisis forense digital?

Cada vez hay más datos de carácter privado en la red y poco a poco las nuevas tecnologías han invadido nuestro espacio en las empresas.Ello ha supuesto un incremento de ataques informáticos a nuestros sistemas y servidores llevados a cabo por delincuentes informáticos.

Esta situación ha dado lugar a un tipo de delito que se denomina Cibercrimen de los sistemas informáticos. Estamos, por tanto, ante delitos relacionados con las tecnologías de la información y las comunicaciones.Algunos ejemplos: amenazas como la Intrusión no autorizada, piratería de software, acciones maliciosas, hacking, spam, phishing, etc.

El Análisis Forense Digital es una combinación de principios y técnicas que conforman los procesos de adquisición, conservación, documentación, análisis y presentación de evidencias. Esta información puede aportarse en un proceso.

¿Qué importancia tiene la figura del forense informático?

El Forense informático es la figura legal que tiene como objetivo aunar pruebas para perseguir delitos relacionados con las tecnologías de la información y las comunicaciones.

Los delitos, que se consideran ciberataquesse producen cuando se vulneran ciertos derechos que se contemplan en la Constitución Española y si se incumplen legislaciones como Decretos y Leyes Orgánicas aprobadas y vigentes en el estado español que pretenden garantizar la seguridad de los datos personales en Internet.

En la Constitución Española encontramos el artículo 18.1 donde se garantiza el derecho a la intimidad personal y el Artículo 18.4 donde se realiza una limitación del uso de la informática para así poder garantizar el derecho al honor y el derecho a la intimidad personal de los ciudadanos.

A través del análisis Forense se inicia un estudio sobre cualquier soporte físico que pueda contener información ya sean teléfonos móviles, memorias USB, discos duros? para encontrar evidencias del ataque informático.

¿Qué es un incidente de seguridad informática?

Llamamos incidente de seguridad informática a la violación o intento de violación de la política de seguridad de una empresa, de las políticas del uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.Unos Ejemplos de Incidentes de seguridad informática podrían ser los Incidentes de denegación de servicios, incidentes de código de carácter malicioso, incidente de acceso no autorizado, uso inapropiado, incidentes múltiples...

¿Qué aporta a una empresa realizar este tipo de análisis?

El Análisis Forense Digital iniciado nos brinda las técnicas y los principios imprescindibles para desarrollar una investigación que nos posibilite identificar, recuperar, reconstruir y analizar las evidencias de lo sucedido.

Fases del Análisis

En un Análisis Forense Digital pueden identificarse las siguientes fases:

Fase I

Identificar el incidente: averiguando cuales son las marcas de ataque.

Fase IIRecopilar evidencias: que podemos encontrar en la caché, en la memoria, en las conexiones de red, en los procesos en ejecución, en discos duros, etc.

Fase IIIConservar dichas evidencias: haciendo copias, etiquetando, etc.

Fase IVAnalizar las evidencias: reconstruir la secuencia temporal del ataque, descubrir cuáles han podido ser las causas del inicio del ataque informático, intentar identificar al autor del delito y evaluar el impacto causado en el sistema informático?

Fase VDocumentar y presentar resultados: a través de los informes técnicos y de los informes de ejecución.

¿Necesita servicios de consultoría en materia de ciberseguridad?

En Grupo ACMS Consultores nos avalan más de 25 años de experiencia. Si necesita asesoramiento en materia de seguridad de la información, consúltenos sin compromiso

Entidades de certificación de prestigio: AENOR, SGS, Bureau Veritas,TÜV Reinhland, Control Unión, Oca Global, DNV.

Instituto Nacional de Ciberseguridad:Incibe

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