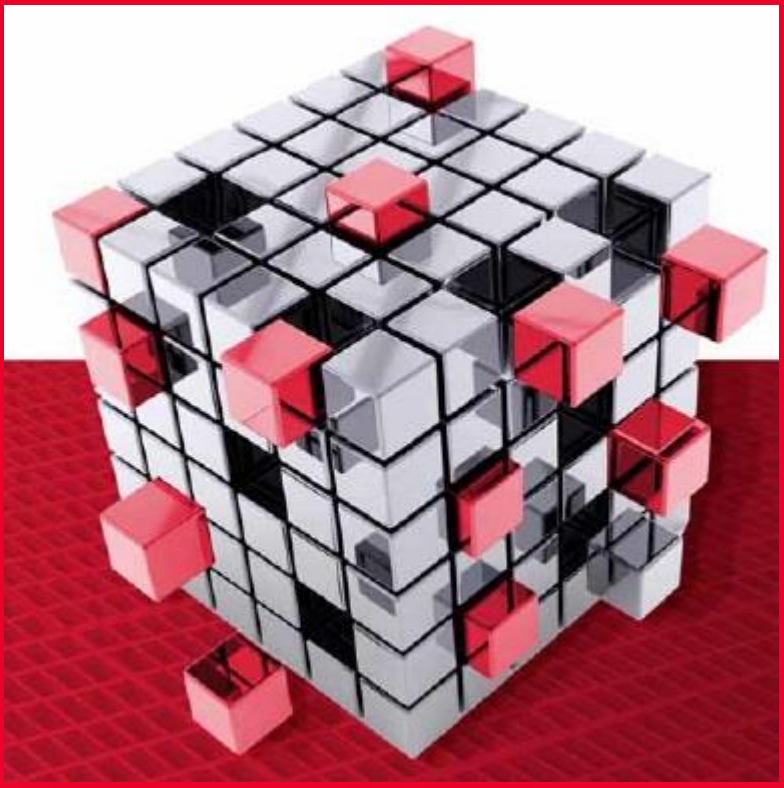


Altabir
consulting

www.altabir.es

Servicios **especializados** para un mundo digital

Altabir
www.altabir.es
Consultoría de Empresas desde 1996

Grupo CFI
Ciberseguridad y Protección de datos

¿Por qué con Grupo Altabir?

1. Porque es una consultora creada en 1996, especializada en formación, ciberseguridad y protección de datos.
2. Porque cuenta con una gran experiencia, avalada por los profesionales certificados en el Esquema de la Agencia Española de Protección de Datos.
3. Porque entidades de todos los sectores han confiado y confían en Grupo Altabir para gestionar la ciberseguridad y la protección de datos.

Ayuntamientos
Clínicas
Comunidades
Panaderías
Librerías
Talleres
Asociaciones
Sindicatos
Arquitectos y Decoradores
Constructoras
Centros de Formación
Asesorías y Gestorías
Consultorías de Servicios a empresas (PRL, Calidad, Marcado CE)
Corredurías de Seguros
Fábricas
Comercios al Por Mayor y al Por Menor
Estancos
Peluquerías y Centros de Estética
Programadores y Diseñadores Web
Restaurantes y Cafeterías
Supermercados
Fotógrafos
Empresas de Mensajería
Autoescuelas
Clubs Deportivos…

Nosotros

Grupo Altabir es una empresa creada en 1996, **especializada** en **Formación**, **Protección de datos y Ciberseguridad y**. Cuenta con una gran experiencia, avalada por los años que lleva prestando servicios en este ámbito

Proporciona **servicio a nivel nacional**, dando una **importancia fundamental** a la **formación** de todos sus profesionales, los cuáles cuentan con las certificaciones más prestigiosas dentro de estos ámbitos (AENOR, EC-Council, APEP, etc.).

Nuestra Filosofía Está Basada En El Engranaje De Tres Bases Fundamentales

RENTABILIDAD – TRANQUILIDAD – SEGURIDAD

Porque sólo de esta manera es posible que el mundo de la empresa participe del desarrollo de nuestra sociedad

Vamos Donde nuestros clientes nos necesitan

Como Consultoría de Protección de Datos asumimos la responsabilidad de la implantación de las empresas que nos contratan sus servicios firmando la documentación pertinente como Consultores responsables de dicha implantación y nos encargamos de llevar en regla toda la documentación y de estar junto al responsable asignado por la empresa para que todo quede correctamente.
Estamos en contacto directo con nuestros clientes los 365 días del año para comunicar cualquier modificación que haya sufrido la empresa a la AGPD y no esperar a la Auditoría.
Contamos con la representación del Delegado De Protección de Datos para incluir este servicio dentro de las empresas a las que la normativa les exige esta figura.

Trabajamos por todo el territorio nacional utilizando herramientas que nos permitan estar al lado de nuestros clientes en cualquier momento y en cualquier circunstancia.

Misión

Ayudar a nuestros clientes a gestionar de forma excelente la protección de los datos personales y la seguridad de la información que manejan, así como la ciberseguridad de sus sistemas informáticos, de forma que dicha información se mantenga protegida ante su difusión no autorizada, manipulación, robo o pérdida.

Visión

Ser el grupo nacional líder en el ámbito de la ciberseguridad y la protección de datos personales, reconocidos por la excelencia y calidad del trabajo desarrollado.

Valores

Profesionalidad

Calidad

Rigor

Honestidad

Confianza

Implantación de la LOPD

- Hacemos un análisis exhaustivo de la empresa para llevar a cabo la implantación correspondiente

- Elaboramos toda la documentación para el cumplimiento de la normativa – entregando a la empresa toda la documentación en formato papel y de forma automatizada y analizando con los responsables cada documento para saber qué hacer y cómo proceder en cada momento (clausulas – información para soportes electrónicos –contratos – fichas para recogida de consentimiento- carteles informativos….)

- Contamos con una plataforma acreditada para dicho cumplimiento

- Formamos a todo el personal con acceso a datos, tanto en modalidad online, con certificación acreditada para los responsables designados para la empresa, como en modalidad presencial para todos los usuarios con acceso a datos.

- Designamos un DPO responsable de la lopd (independientemente del sector o tamaño de la empresa)

- Llevamos todo el mantenimiento anual con los correspondientes análisis de riesgo y evaluaciones de impacto que cada empresa requiere + auditorias.

- Gestionamos cualquier tipo de incidencia tramitando toda la documentación, tanto con la aepd como con los usuarios afectados

- Gestionamos y tramitamos la solicitud de los diferentes derechos que las empresas reciben.

- Somos intermediarios entre la empresa que contrata nuestros servicios y cualquier usuario insatisfecho que desea poner algún tipo de reclamación.
- Entregamos a nuestros clientes un boletín mensual con las últimas noticias y novedades en materia de protección de datos

Auditoría de la LOPD

Un a**uditor externo cualificado** realizará la auditoría en tus instalaciones y emitirá el correspondiente **Informe de Auditoría**

¿Qué es la auditoría LOPD?

Es una revisión de la efectividad de las medidas de seguridad que debe tener implementadas una organización cuando trata datos personales.

¿Por qué debe realizarse?

Para determinar si se han establecido, si son adecuadas y se cumplen las medidas de seguridad que la organización ha implantado para proteger los datos personales.

¿Quién debe realizarla?

Debe realizar la auditoría todas las organizaciones, en especial las que tratan datos sensibles.

En cuanto a la persona que audita, debe tener conocimientos y experiencia en el ámbito jurídico, informático y de auditoría. Puede ser externa a la empresa o interna.

¿Cuándo se debe hacer?

De forma ordinaria cada año y de forma extraordinaria siempre que se realicen modificaciones sustanciales en los sistemas de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

¿Cómo hay que hacerla?

Un auditor debe establecer los tratamientos a auditar, sistemas, procedimientos, etc. así como las medidas de seguridad implantadas y dictaminar sobre su efectividad.

Resultado

El resultado de la auditoría debe reflejarse en un Informe de Auditoría, que debe dictaminar sobre:

- Adecuación de las medidas establecidas a lo dispuesto por la LOPDPGDD y el RGPD.
- Identificación de las deficiencias y propuesta de medidas correctoras y complementarias.
- Incluirá datos, hechos y observaciones en los que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Defensa jurídica LOPD

Cuando más se necesita

Abogados especializados en derecho tecnológico **te defenderán** de la forma más profesional y efectiva

¿Te ha denunciado un cliente o trabajador a la Agencia Española de Protección de Datos o has recibido un requerimiento?. Déjalo en las mejores manos.

¿Qué es el servicio de defensa jurídica LOPD?

Disponer de un abogado especializado para defenderte ante la Agencia Española de Protección de Datos (AEPD).

¿Por qué es necesario?

Porque cuando la organización recibe un requerimiento de la AEPD, a instancias de una denuncia o vulneración de la LOPD, la empresa dispone de un tiempo para realizar las alegaciones que crea oportunas a dicho requerimiento.

Contestar adecuadamente desde el primer momento, amplía las posibilidades de éxito en el procedimiento abierto.

¿Quién debe realizarlo?

Un abogado especializado en protección de datos y nuevas tecnologías.

¿Cuándo es necesario?

Cuando la organización recibe un requerimiento de la Agencia Española de Protección de Datos.

¿Cómo hay que hacerlo?

Adecuadamente, siguiendo las formas y plazos establecidos en la normativa.

Resultado

Dispondrás de un abogado especializado que te defenderá de una forma profesional y efectiva.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Adecuación web a la LSSICE

Para los que tienen página web

Adecuamos tu web a la **LSSICE** (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico**)**

¿Tienes una página web para promocionar tu empresa o vender online? Tenemos el servicio idóneo para dar confianza a tus clientes y visitantes.

¿Qué es la LSSICE?

Es la denominación que se le da a la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico.

¿Por qué debe realizarse la adecuación a la LSSICE?

Es un requisito legal imprescindible para todas las páginas web, y en especial para las que realicen comercio electrónico.

¿Quién debe realizarlo?

Aquellas empresas, profesionales y particulares que tienen una página web en la que se realice alguna actividad económica (catálogo de productos o servicios, venta, publicidad, etc.).

¿Cuándo de debe hacer?

En el momento de desarrollar la página web.

¿Cómo hay que hacerla?

Contratando a un profesional especializado que redacte los textos legales necesarios para su adaptación.

Resultado

Tu página web estará adecuada a la LOPD y a la LSSICE, evitando de esta forma
posibles sanciones y dando confianza a tus clientes y visitantes.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Implantación de un **SGSI** (ISO 27001)

Máxima seguridad

Cuando una organización gestiona adecuadamente la seguridad de su información, **minimiza las posibilidades de sufrir un robo**, catástrofe o pérdida de la misma

*Un **SGSI** es un Sistema de Gestión de Seguridad de la Información que se puede certificar bajo la norma **ISO 27001** y garantiza que gestiona la seguridad de su información.*

¿Qué es un SGSI?

Un SGSI es un Sistema de Gestión de Seguridad de la Información que se puede certificar bajo la norma ISO 27001.

Una vez implantado una empresa certificadora realiza la auditoría de certificación y otorga el sello si es superada.

¿Por qué debe realizarse?

Para garantizar, ante terceros, que la organización gestiona la seguridad de la información que almacena.

¿Quién debe realizarlo?

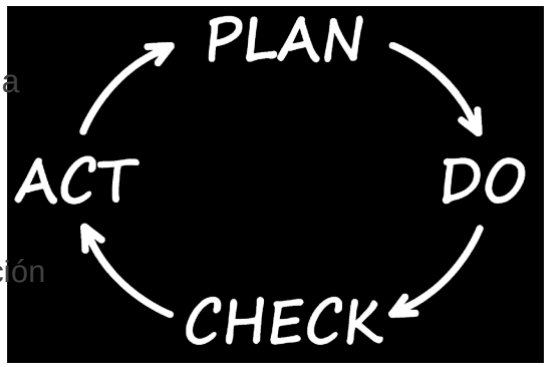
Cualquier organización que necesite, como objetivo de negocio, gestionar la seguridad de la información que almacena y demostrarlo ante terceros.

¿Cuándo se debe hacer?

Cuando se tenga información sensible, ya sea propia o de terceros, que se desee proteger de una forma eficaz y planificada.

¿Cómo hay que hacerlo?

Implantar un SGSI es una tarea compleja, que requiere de la ayuda de un profesional especializado en este ámbito.



Resultado

Un sistema completo que gestiona la seguridad de la información en tu organización que podrás certificar ante terceros.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Implantación de la ISO 27701

Sistema de Gestión de la Seguridad de la Información y Privacidad (SGSIP)

Este sistema **garantiza** que una organización protege **la seguridad de la información y la privacidad de las personas** según establece el Reglamento General de Protección de Datos

La ISO 27701 amplía el alcance de un SGSI basado en la ISO 27001 incorporando controles específicos para proteger también la privacidad de las personas.

¿Qué es la ISO 27701?

Detalla una serie de requisitos de privacidad, controles y objetivos de control adicionales para establecer un Sistema de Gestión de la Seguridad de la Información y Privacidad (SGSIP).

Ha sido desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para que las organizaciones puedan gestionar la seguridad y privacidad de la información y asegurar la conexión entre los actuales requisitos para sistemas de gestión y la actual legislación sobre protección de datos personales.

¿Por qué debe realizarse?

Porque así las organizaciones pueden garantizar que tienen una gobernanza de datos integral y universal que se corresponde con los requisitos legislativos que le son de aplicación.De esta forma, las organizaciones minimizan la posibilidad de acarrear con

cuantiosas sanciones por incumplimiento de la normativa de protección de datos.

¿Quién debe realizarlo?

Aquellas organizaciones que gestionan datos personales.

¿Cuándo se debe hacer?

Cuando la organización trate datos personales y desee disponer de un sistema para garantizar el cumplimiento de los requisitos de la normativa de protección de datos personales.

¿Cómo hay que hacerlo?

La ISO 27701 se apoya y complementa una ISO 27001 que esté implantada en la organización. También pueden implantarse de forma conjunta las dos normas.

Por tanto, es algo complejo que requiere de ayuda profesional experta.

Resultado

La organización dispondrá de un Sistema de Gestión de la Seguridad de la Información y Privacidad (SGSIP) que se puede Certificar para demostrar, ante terceros, que la organización cumple los requisitos establecidos por el Reglamento General de Protección de Datos para el tratamiento de los datos personales.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Implantación del ENS

Confianza digital

Es **exigible** a las **Administraciones públicas** y a determinadas entidades que prestan servicios a dichas Administraciones

El Esquema Nacional de Seguridad (ENS) tiene como objetivo fundamentar la confianza en los sistema de información de las administraciones públicas, de forma que dichos sistemas presten sus servicios y custodien la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

¿Qué es el ENS?

El Esquema Nacional de Seguridad (ENS) es un esquema establecido por el Centro Criptológico Nacional (CCN) para la protección adecuada de la información en el uso de medios electrónicos a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos de las administraciones públicas. Está regulado por el RD 3/2010.

¿Por qué debe realizarse?

Porque es un requisito establecido por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y regulado por el Real Decreto 3/2018, de 8 de enero.

¿Quién debe realizarlo?

El ENS deben implantarlo las Administraciones públicas, así como las entidades externas que prestan servicios a las administraciones públicas que impliquen el acceso a la información que manejan dichas administraciones.

¿Cuándo se debe realizar?

El ENS es exigible desde el año 2016.

¿Cómo hay que hacerlo?

Implantar el ENS es una tarea sumamente compleja, que requiere de la ayuda de un profesional especialmente experimentado en este ámbito.

Resultado

Una vez implantado el ENS, dispondrá de un sistema de gestión de seguridad de la información acorde con los requisitos establecidos y que podrá certificar ante terceros.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Plan de Contingencias y Continuidad de Negocio

¿Estás preparado ante incidentes graves?

Las empresas deben estar **preparadas para prevenir, protegerse y reaccionar** ante **incidentes** que podrían paralizar sus procesos de negocio

Un Plan de Contingencias y Continuidad de Negocio permite a las organizaciones poder dar una respuesta planificada ante un incidente grave, de forma que pueda recuperar sus procesos de negocio en un plazo de tiempo que no comprometa su continuidad.

¿Qué es un Plan de Contingencias y Continuidad de Negocio?

Es un plan que contempla los distintos incidentes de seguridad que pueden afectar a una organización y que podrían impactar en sus procesos de negocio y las tareas que debe realizar dicha organización para poder recuperarse ante un incidente grave en un plazo de tiempo definido previamente.

Un Plan de Contingencias y Continuidad de Negocio puede ayudarnos a:

- Evitar que las actividades de la empresa se interrumpan
- Recuperar la situación inicial antes de la ocurrencia de un incidente
- Establecer un periodo de recuperación definido ante un incidente grave
- Mantener el nivel de servicio en los límites definidos

¿Por qué debe realizarse?

La seguridad al 100% no existe. Las empresas deben estar preparadas protegerse ante posibles desastres que pudieran paralizar su actividad.

Este plan permite disponer de las pautas necesarias para actuar en caso de que un desastre paralice la actividad de la organización, permitiéndola recuperar sus actividades en el menor tiempo posible.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Plan de Contingencias y Continuidad de Negocio

¿Quién debe realizarlo?

Cualquier organización que desee disponer de una respuesta planificada ante los incidentes graves que puedan paralizar sus actividades, especialmente si la organización está prestando un servicio a sus clientes y puede causarles un perjuicio si se paraliza.

¿Cuándo se debe realizar?

En el momento en que la paralización del servicio debido a un incidente pueda ocasionar un perjuicio a terceros.

¿Cómo hay que hacerlo?

El plan se realiza a través de cinco fases definidas que hay que abordar de forma profesional y metódica.

Es necesario conocer en detalle los procesos que se deben proteger, los activos implicados, el análisis de impacto sobre el negocio y el análisis de riesgos.

Con estos datos se determina la estrategia de continuidad, el plan de crisis, los planes operativos de recuperación y las pruebas de mantenimiento y revisión del plan, así como la formación que se debe dar al personal de la organización.

Resultado

La organización dispondrá de un Plan de Contingencias y Continuidad de Negocio, que la permitirá recuperarse, tras un incidente grave, en un plazo de tiempo máximo definido.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Análisis de riesgos

¿Conoces tus riesgos?

Para conocer las **acciones prioritarias a realizar** es necesario **conocer los riesgos** que afectan a **tu información**

Gracias a este servicio conocerás los riesgos a los que se expone tu negocio y qué acciones prioritarias debes realizar para salvaguardar el activo más importante de tu negocio: Tu información.

¿Qué es un análisis de riesgos?

Es determinar, en función del valor de los activos (equipos, software, datos, etc.) y las amenazas a que están expuestos (fuego, fallo de alimentación, virus, Hackers, etc.), el nivel de riesgo que tiene cada activo.

¿Por qué debe realizarse?

Porque muchas veces las organizaciones, por desconocimiento, implantan medidas de seguridad que no son prioritarias y se dejan sin proteger los activos que son críticos para tu negocio.

Un análisis de riesgos permite concentrar los recursos en aquellos activos que son críticos, implantando las medidas y controles de seguridad solo en los recursos que lo requieren. De esta forma ahorrarás dinero al mismo tiempo que proteges lo que realmente importa.

¿Quién debe realizarlo?

Cualquier organización que posea información valiosa para su negocio.

¿Cuándo se debe hacer?

Cuando la organización desee conocer los riesgos para planificar la inversión que debe realizar en seguridad.

¿Cómo hay que hacerlo?

Se debe realizar, de forma metódica, un inventario de activos junto con las amenazas a que está expuesto cada activo.
A continuación, realizamos una matriz para conocer el nivel de riesgo.

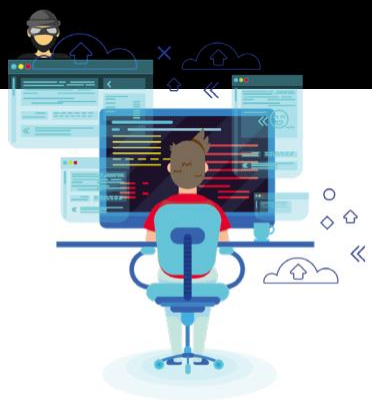
Resultado

Un informe en el que cada activo tiene asignado su nivel de riesgo junto con las medidas y controles que debes implantar para eliminar o minimizar el riesgo.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Análisis de vulnerabilidades



¿Conoces tus puertas traseras?

Gracias a este servicio conocerás las **vulnerabilidades que existen en tus sistemas y redes**

¿Conoces las vulnerabilidades que tiene tu red?, ¿y tus equipos?, ¿sabes que un hacker malintencionado puede explotarlas para acceder a tu información?

¿Qué es un análisis de vulnerabilidades?

Es determinar las vulnerabilidades que existen en routers, software no actualizado, redes, etc., y que pueden ser aprovechadas por un hacker malintencionado para “colarse” en tus sistemas y acceder a su información.

¿Por qué debe realizarse?

Porque todo el software y equipamiento sale de fábrica con defectos que pueden ser aprovechados de forma maliciosa. Posteriormente, según se conocen estos defectos los fabricantes van publicando actualizaciones para subsanarlos. Sin embargo, muchas empresas no las instalan o configuran de forma apropiada, provocando que los sistemas sean vulnerables.

¿Quién debe realizarlo?

Cualquier organización que posea información valiosa para su negocio.

¿Cuándo se debe hacer?

En el momento que la organización desee conocer las vulnerabilidades que tiene en sus sistemas. Es recomendable que sea de forma periódica.

¿Cómo hay que hacerlo?

Analizando de forma metódica, todo el equipamiento y software para detectar las vulnerabilidades que existen en la organización.

Con objeto de automatizar esta tarea, se suele utilizar software extremadamente especializado para detectar estas vulnerabilidades.

Resultado

Un informe en el que están detalladas todas las vulnerabilidades conocidas y la solución que debe aplicarse para solucionarlas.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Pruebas de penetración (hacking ético)

¿Hasta donde puede llegar un hacker?

¿Quieres saber hasta donde podría un hacker malintencionado penetrar en tus sistemas informáticos y a qué información accedería?

Con este servicio realizaremos pruebas de penetración a tu red, e intentaremos acceder a la información que almacena, tal y como haría un hacker con malas intenciones. De este modo descubrirás las vulnerabilidades que un hacker malintencionado podría explotar para acceder a tus datos.

¿Qué son las pruebas de penetración (Pentester)?

Es intentar entrar en los sistemas, no siendo un usuario autorizado, para descubrir las vulnerabilidades que podría explotar un hacker malintencionado para obtener acceso a ellos y hasta dónde podría llegar.

¿Por qué deben realizarse?

Conocer hasta donde podría llegar un hacker malintencionado, va a ayudar a la organización a tapar esas brechas en su seguridad.

Mejor descubrirlo de esta forma, que sufrir las consecuencias una vez que se ha producido el suceso.

¿Quién debe realizarlo?

Cualquier organización que desee descubrir brechas en su seguridad.

¿Cuándo se debe realizar?

En el momento que la organización desee conocer las brechas de seguridad que tiene. Es recomendable que sea de forma periódica.

¿Cómo hay que hacerlo?

Debe ser realizado por un profesional en este ámbito.

Resultado

Un informe que va a mostrar las vulnerabilidades de los sistemas que podrían ser aprovechadas para acceder a los datos, el impacto de su explotación y cómo resolverlas.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Análisis forense de sistemas informáticos

¿Necesitas pruebas informáticas?

¿Sospechas que **un empleado se está llevando información**?
¿Necesitas obtener pruebas de ello para utilizarlas en una negociación o en un proceso judicial?

Necesitas un perito forense digital

Gracias a este servicio, un profesional realizará una reconstrucción de los hechos ocurridos en el ámbito informático. Estos podrán ser utilizados como prueba en un proceso judicial.

¿Qué es un análisis forense de sistemas informáticos?

Reconstruir la secuencia de los hechos acontecidos en un suceso. Por ejemplo, si un empleado se ha llevado datos en una memoria usb, reconstruiríamos la secuencia de sucesos con su fecha y hora, así como en número de serie de la memoria usb en la que se extrajeron los datos.

¿Por qué debe realizarse?

Porque ha habido una “fuga” de datos de la empresa, o se sospecha que alguien está sacando datos o accediendo de forma no autorizada. Un perito forense digital es capaz, siguiendo el rastro electrónico que dejan las operaciones, identificar lo ocurrido y la secuencia de sucesos.

¿Quién debe realizarlo?

Cualquier organización que sospeche que alguien está entrando de forma no autorizada en sus sistemas, que le están robando información o necesite recabar pruebas informáticas para demostrar algún suceso.

¿Cuándo se debe hacer?

Cuando haya ocurrido un incidente o tenga sospechas de comportamientos ilícitos.

¿Cómo hay que hacerlo?

Un análisis forense, para que tenga validez, solo puede ser realizado por un profesional en este ámbito y siguiendo una metodología apropiada.

Resultado

Un informe de la secuencia de los hechos ocurridos, que podrá ser utilizado en una negociación o procedimiento judicial.

Altabir consulting

Grupo CFI
Ciberseguridad y Protección de datos

Formación

Una formación especializada

En formato **presencial, in-company, online** y **vía streaming** en directo a través de Internet

Disponemos de un completo sistema de teleformación en Internet a través del cual el alumno realiza el curso, sigue su evolución, realiza consultas al tutor, etc.

El alumno accede a las decenas de vídeos que componen el curso y a través de los cuales el formador desarrolla su contenido. Esta es la forma más eficiente de impartir formación online, ya que el alumno puede ver los vídeos las veces que desee hasta comprender lo explicado.

Además disponemos de material didáctico en soporte papel y material descargable en otros formatos, como PDF o Word.

Contamos con un catálogo especializado en modalidad presencial distancia y online:

- Experto en el Reglamento General de Protección de Datos de Europa (RGPD)*
- Delegado de Protección de Datos (60h 100h y 180h)*
- Experto en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD)*
- Ciberseguridad Laboral y Personal
- Consultor Especialista LSSICE
- Especialista en Hacking Ético
- Usuario Seguro de Sistemas Informáticos
- Fundamentos ISO 27001
- Desconexión Digital
- Seguridad informática en entornos de teletrabajo
- Seguridad informática para Pymes

Más información: www.altabirformacion.es

www.altabir.es
C/ LUIS AMADOR 26 -GRANADA –
Centro de Negocios Cámara de Comercio de Granada
958 075 564 -- 685 470 834
info@altabir.es – dpo@altabir.es

facebook twitter LinkedIn