ABAST

Seguridad en las PYMEs

Servicios de auditoría y consultoría de seguridad para mediana empresa

www.abast.es

Cada vez es más complicado gestionar la seguridad de la información en nuestra organización. La tecnología cada vez es más compleja y cambiante. Nuestra organización cada vez es más extensa, ampliando sus límites tradicionales para dar acceso y comunicarse con proveedores, clientes, socios, empleados, etc. La aparición de nuevas tecnologías sociales y el cloud complican la gestión de la seguridad de nuestros datos, que pueden estar en cualquier sitio. Además, los requerimientos legislativos y regulatorios cada vez son más exigentes.

En las PYMEs la consciencia de los riesgos y de la necesidad de tomar medidas para gestionar correctamente la seguridad suele ser menor que en las grandes empresas, cuando las amenazas, en realidad, son similares. Desde ABAST le ofrecemos nuestros servicios de auditoría y consultoría de seguridad con un enfoque práctico y adecuado a las características y necesidades de una mediana empresa.

Los riesgos a los que se enfrentan las PYMEs no son menores

Por ejemplo, desde el punto de vista de la **ciberseguridad**, muchas empresas pequeñas y medianas creen que, al no ser un banco o una aseguradora, o al no tener su página web conectada con sus sistemas, no son un blanco de los hackers y están libres del riesgo de sufrir ataques por parte de estos. No es así, hemos de tener en cuenta que las motivaciones de éstos pueden ser muy diversas. En este sentido, algunas empresas han acudido a nosotros tras sufrir lo que se conoce como **ataques "man in the middle"**. El hacker había interceptado las comunicaciones entre la empresa y el proveedor o cliente de manera que, en un momento determinado consiguió desviar hacia él pagos cifrados entre decenas y centenas de miles de euros.

Otro ejemplo, éste desde el punto de vista del cumplimiento legal. Con el código penal de 2010 se establece que toda persona jurídica (empresas) se enfrenta a los riesgos penales y podrá responder penalmente por los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho y de derecho (consejeros) o por quienes estando sometidos a la autoridad de las personas físicas que ejercen la dirección, hayan podido realizar los hechos por no haberse ejercido sobre ellos el debido control atendidas las concretas circunstancias del caso (empleados). Esto significa que el administrador podría ser imputado como responsable penal de un delito sólo por no haber ejercido el debido control sobre lo que ocurre en su empresa.

Para 2015 está prevista la obligatoriedad por parte de las empresas de definir un Modelo o Plan de Prevención del Delito que trate de impedir la comisión de estos delitos y que sirva como atenuante en caso de que se produzca uno.

¿Qué hay que hacer?

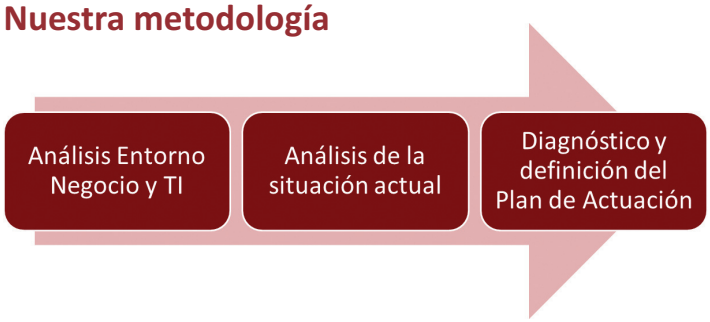
Implementar un **nivel de seguridad adecuado** (la palabra adecuado es muy importante) en función de los **riesgos** a los que está expuesta la empresa (financieros, operativos, legales, comerciales, medioambientales...) y de los **requisitos legales, regulatorios y contractuales** que tenga que cumplir.

Todo ello a través de un sistema de control basado en la implementación de **medidas de seguridad** que pueden ser **técnicas, organizativas y procedimentales**.

Beneficios de alcanzar un grado de madurez óptimo en la gestión de la seguridad de la información:

- **Reducción de riesgos.** Minimizar o eliminar los riesgos para el negocio, resultantes de la materialización de las amenazas existentes sobre la seguridad de la información.
- **Ahorro de costes.** Racionalización de los recursos en base a la eliminación de inversiones innecesarias o ineficientes debidas a la infra o sobreestimación de los riesgos.
- **Cumplimiento con la legislación vigente.** Aseguramiento del cumplimiento del marco legal que protege a la empresa eliminando los riesgos y sanciones asociadas.
- **Mejora de la competitividad en el mercado.** Mejora de la confianza en el negocio entre clientes, proveedores y socios con los que se intercambia y/o comparte información.

Nuestra metodología



1. Análisis del entorno de negocio y TI

A nivel de Negocio.

a. Procesos de negocio claves
b. Tipos de información y flujos clave
c. Servicios que se dan y reciben de terceros
d. Requerimientos legales, normativos
e. Personal clave

A nivel de TI.

a. Servicios de TI (ej.: correo electrónico)
b. Activos deTI (PCs, servidores, ...)
c. Entorno físico (CPD, etc...)

2. Análisis de la situación actual

Análisis de Riesgos

a. Identificando vulnerabilidades y amenazas
b. Determinando el riesgo (probabilidad x impacto)
c. Estableciendo criterios de gestión del riesgo

Auditoría técnica de seguridad (+ Pentesting)

a. Análisis vulnerabilidades
b. Pentesting (acceso a información...)
c. Auditoría configuración, capacidad y rendimiento

Auditoría de Cumplimiento

a. LOPD, LSSI, código penal, PCI ...

3. Diagnóstico y definición del plan de actuación

- Definir las recomendaciones para mejorar la seguridad mediante la implementación de un conjunto de medidas o controles
- Establecer un Plan de Acción priorizado para la implementación de los mismos en base a:

a. El nivel de riesgo que trata o las carencias que resuelve.
b. El nivel de riesgo aceptado por la organización
c. Una estimación del coste necesario para su implementación

ABAST – Área de Seguridad TI

ABAST cuenta con un área especializada que ofrece uno de los portfolios de servicios y soluciones de Seguridad TI más completos del mercado español, pues cubre todos los aspectos relacionados con infraestructura de seguridad TI, continuidad y disponibilidad, auditoría y control, y gobierno de la seguridad TI.

Aportamos una gran experiencia en la realización de planes de contingencia de TI, planes de continuidad del negocio y planes directores de seguridad; en auditorías y consultorías relacionadas con ISO2700X, LOPD, ENS y otros estándares o regulaciones; y en auditorías de seguridad basadas en test de intrusión (hacking ético).

Estos servicios y soluciones podemos ofrecérselos también como servicio gestionado bajo el concepto de Oficina de Seguridad.

Para más información:
seguridad@abast.es

ABAST

BARCELONA
C/Equador 39-45
08029 Barcelona
Tel. 933 666 900
Fax 933 666 901
abs_bcn@abast.es

MADRID
C/ de la Basílica, 19 9ºB
28020 Madrid
Tel. 914 061 601
Fax 914 061 604
abs_mad@abast.es