ABAST

Responsabilidad Jurídica

Prevención del Delito

www.abast.es

En los últimos años las presiones impuestas por las normativas como Basilea II o Sarbanes-Oxley o bien los requerimientos legales de obligatorio cumplimiento como la LOPD o Blanqueo de Capitales, han supuesto que desde las áreas de Legal y/o Cumplimiento se requiera el conocimiento de los expertos de seguridad TI para incorporar las medidas de seguridad técnicas y organizativas necesarias para cumplir con los requerimientos normativos y legales exigidos.

Principios u objetivos

Desde la reforma del código penal, que entró en vigor el 23 de diciembre de 2010, se ha incorporado en el catálogo de riesgos del negocio y en el marco de cumplimiento de las compañías, los riesgos relacionados con la responsabilidad penal de personas jurídicas y su consecuente impacto en la alineación no solo con el control interno sino también con la seguridad TI.

El nuevo artículo 31bis del Código Penal, establece que toda persona jurídica se enfrenta a dos riesgos penales y podrá responder penalmente por:

1. 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)
2. Los delitos cometidos por cuenta y provecho de la empresa 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)

Es fundamental para cumplir con los requerimientos normativos y legales y potenciar el nivel de control interno exigido, lo cual supone un mayor grado de concienciación por parte de la compañía en el impacto que supone la incorporación del área de seguridad TI como agente de articulación entre los procesos de negocio y las TIC.

Beneficios

El plan de prevención penal como marco estructurado para mitigar los riesgos de delitos penales identificados y analizados tendrá el componente de los controles TI técnicos y organizativos relacionados a cada delito.

El análisis de riesgos realizado por el área legal o de cumplimiento de la compañía estará complementado con la visión de TI al identificar los controles implementados en la infraestructura tecnológica que soporta los procesos del negocio.

Del análisis se obtendrán como resultado aquellas recomendaciones y el plan de acción con las medidas de tipo técnico y organizativo que permitan tener de forma clara la definición de prioridades y el esfuerzo a dedicar para diseñar, desarrollar e implementar las acciones o protocolos que conformaran parta del marco o plan de prevención de delitos de la compañía.

Nuestra Metodología

1. Riesgos

- Analizar los riesgos de delito penal en el ámbito TI identificados realizado por la compañía en el análisis de riesgos.

2. Análisis de los controles implementados

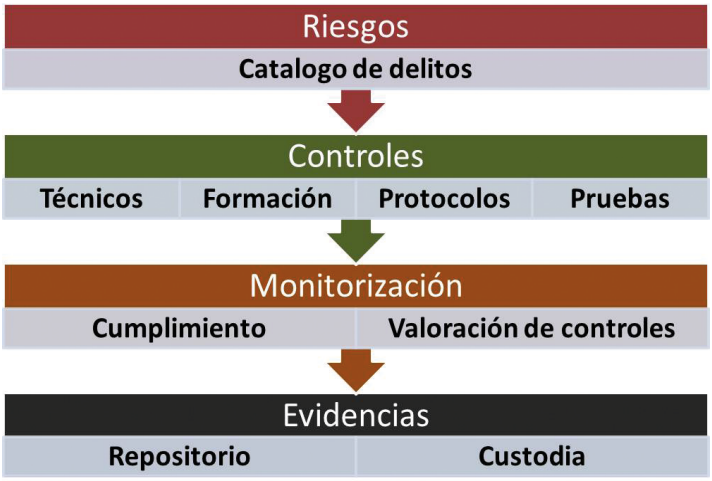
- Realizar entrevistas con los responsables de TI y aplicación de los cuestionarios
- Analizar la documentación existente (procedimientos, políticas), supervisión, ejecución, resguardo de las evidencias o documentación resultado de la ejecución de los controles.
- Revisar las medidas técnicas implementadas en el entorno TI. En esta fase se revisarán de forma limitada los componentes técnicos que conforman la infraestructura.
- Realizar las recomendaciones y el plan de acción con las medidas organizativas y técnicas a implementar. En esta fase de realizarán las recomendaciones con las observaciones identificadas y el riesgo directo. Una vez realizadas las recomendaciones se desarrollará el plan de acción con las medidas priorizadas que deben realizarse para mitigar los riesgos.

3. Desarrollo de controles

- Diseñar y desarrollar los controles técnicos y organizativos (procedimientos, protocolos, políticas TI) para mitigar los riesgos de delito penal identificados. Los controles serán documentados e integrados en el plan de prevención de la compañía.

4. Monitorización

- Diseño del marco de monitorización para la ejecución de los controles. Esta fase comprende el establecimiento del modelo para la ejecución periódica de los controles, la supervisión y el resguardo de las evidencias de la ejecución del control.
- Evaluación de los controles implementados. En esta fase se validará si el control se cumple de acuerdo a su diseño, ejecución periódica y supervisión.



¿Por qué ABAST?

ABAST es una empresa que tiene presencia en el mercado de las TIC desde hace 30 años. Desde el área de Consultoría y Auditoría de TI ofrecemos soluciones de seguridad enfocadas a satisfacer las necesidades técnicas, organizativas y de cumplimiento legal y normativo de nuestros clientes.

El área de Consultoría y Auditoría de ABAST está formada por profesionales con amplia experiencia en la gestión de riesgos de entornos de TI y de negocio, seguridad de datos, auditorías de seguridad, diseño, implementación y monitorización de controles TI. Nuestro objetivo es ayudar a los Directores y Responsables de Seguridad a trasladar los requerimientos de su negocio en servicios y soluciones técnicas, organizativas, procedimentales y jurídicas de una forma práctica, ágil y adaptada a las necesidades y expectativas de nuestros clientes.

El área de Consultoría y Auditoría tiene un equipo estructurado con presencia en Madrid y Barcelona. Los profesionales que forman el área disponen de certificaciones como CISA, PMP, ISO 20.000 e ISO27.000 Lead Auditors, ITIL v2 Service Manager, ITIL v3 Expert, etc. Nuestra práctica de trabajo está basada en metodologías y mejores prácticas nacionales e internacionales como ITIL, CoBIT, ISO, CMMI, etc.

Para más información:
seguridad@abast.es

www.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