ABASTsystems

Workshops Formativos

Para Responsables de Seguridad de TI
CIOs/CISOs

Enero 2015

v.1.0

Workshops Formativos
para Responsables de Seguridad de TI

1. **Objetivo y marco de trabajo**
2. Workshop 1: entendimiento del negocio
3. Workshop 2: riesgos y marcos de gestión de la seguridad
4. Workshop 3: cumplimiento legal y TIC
5. ROSI (Retorno de la inversión en seguridad de la información) y resultados

© 2014 Abast Systems, S.A.

Objetivo

Formar y analizar a alto nivel, cómo complementar los objetivos de negocio con un **nivel adecuado (responsable) del riesgo y de la seguridad** de los sistemas y tecnologías de la información, que considere el **impacto económico** asociado.

El enfoque basado en riesgos permite decidir qué, dónde, cuándo y cómo proteger el negocio, así como el coste de hacerlo.

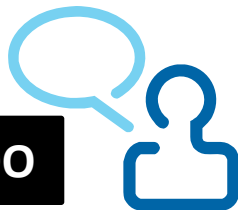
© 2014 Abast Systems, S.A.

Marco de trabajo

1

Principales preocupaciones negocio:

- Pérdida reputación/confianza clientes
- Parada en la operativa del negocio
- Violación de cumplimiento
- Pérdida financiera



CEO/CFO/COO

2

3 Pilares

- Negocio
- Madurez Tecnológica
- Capacidades Disponibles

3

Riesgo

Cumplimiento (Riesgo Legal)

Controles:

- Técnicos
- Procedimentales
- Organizativos

4

Entorno Económico (Global o particular)

CONSERVADOR:

Focalizarse en los requerimientos mínimos

CRECIMIENTO:

Proporcionar valor al negocio a través de la implementación de capacidades robustas y mejoradas

© 2014 Abast Systems, S.A.

Workshops Formativos

para Responsables de Seguridad de TI

1. Objetivo y marco de trabajo
2. **Workshop 1: entendimiento del negocio**
3. Workshop 2: riesgos y marcos de gestión de la seguridad
4. Workshop 3: cumplimiento legal y TIC
5. ROSI (Retorno de la inversión en seguridad de la información) y resultados

© 2014 Abast Systems, S.A.

Workshop 1: Entendimiento del Negocio

- **Sesión TEÓRICA (2h)**
  - Una manera de conocer el negocio es a través del conocimiento de su modelo. Se explicará la técnica de modelado de negocio conocida como **Business Model Canvas**.
- **Sesión PRÁCTICA (4h)**
  - **Sesión de trabajo** donde aplicaremos el modelaje de negocios a la organización con el objetivo de conocer sus **proveedores, actividades, productos, servicios y canales clave así como los costes e ingresos principales y su origen**.

- **Resultados:**
  - **Business Model Canvas del Negocio**
  - **Establecimiento a alto nivel de las principales preocupaciones / riesgos en seguridad del negocio**

Análisis Modelo Negocio

1

Principales preocupaciones negocio:
- Pérdida reputación/confianza clientes
- Parada en la operativa del negocio
- Violación de cumplimiento
- Pérdida financiera

CEO/CFO/COO

2

3 Pilares

Negocio | Madurez Tecnológica | Capacidades Disponibles

- ¿Quiénes son nuestros **Proveedores/socios** clave?
- ¿Qué **recursos clave estamos adquiriendo** de ellos?
- ¿Qué actividades clave desempeñan?
- ¿Qué **actividades clave/ recursos clave** requieren nuestras propuestas de valor, canales de distribución, relaciones con los clientes, fuentes de ingresos?

- ¿Qué valor ofrecemos a los clientes?
- ¿Cuál de los problemas de nuestros clientes estamos ayudando a resolver?
- ¿Qué paquetes de **productos y servicios** estamos ofreciendo?
- ¿Qué necesidades del cliente estamos satisfaciendo?

CÓMO	QUÉ	QUIÉN
COSTES		INGRESOS

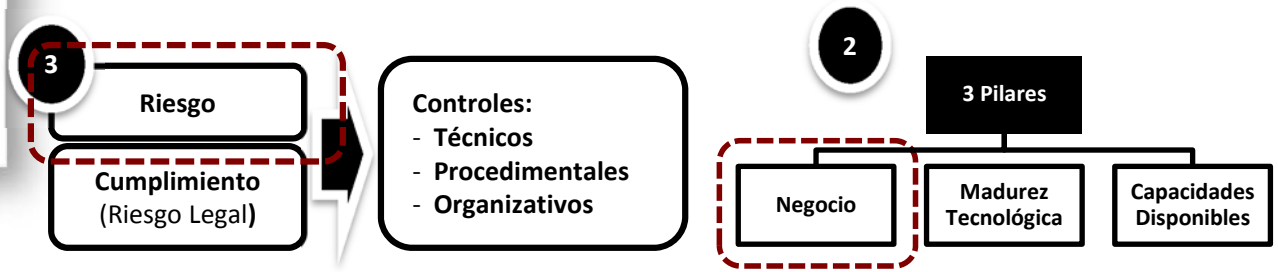
- ¿Quiénes son nuestros **clientes** más importantes?
- ¿Qué tipo de relación tenemos con ellos?
- ¿Cómo los tenemos segmentados?
- ¿Cómo estamos llegando a ellos? ¿A través de qué **canales**?
- ¿Cómo se integran nuestros canales?
- ¿Cuáles son los mejores?
- ¿Cuáles son los más rentables?

- ¿Cuáles son los **costos** más importantes inherentes a nuestro modelo de negocio?
- ¿Qué **recursos** clave son los **más caros**?
- ¿Qué **actividades** clave son las **más caras**?

- ¿Por qué **valor están pagando** nuestros clientes?
- ¿Cómo están pagando actualmente?
- ¿Disponemos de otras fuentes de ingresos adicionales?

© 2014 Abast Systems, S.A.

Análisis Riesgos Negocio



- No disponibilidad de un Proveedor/Recurso clave
- Qué puede afectar la relación con un proveedor clave, cómo puede verse afectada, qué impacto económico
- Impacto asociado a temas de cumplimiento legales

- Efectos temporales de la no disponibilidad de un, producto, servicio, actividad clave
- Cómo afectaría una disminución de la calidad de los productos y/o servicios
- Pérdida de conocimiento/talento y su impacto en la capacidad/competencia

CÓMO	QUÉ	QUIÉN
COSTES	INGRESOS	

- Eventos o factores podrían afectar la relación con los clientes
- Impactos económicos, legales, etc, en y con los clientes de las interrupciones en la prestación de servicios
- Dependencia frente a la autonomía de sus canales
- posición relativa (apalancamiento) a través de los diferentes canales

- Impacto potencial de las variaciones en los componentes de los costes más importantes
- Condiciones en el mercado que puede tener un impacto en los flujos de costes
- Vulnerabilidades de seguridad que faciliten el soborno o fraude y afecten a los costes ¿Cómo y cuánto?

- Eventos, condiciones del mercado o dinámica de la competencia que pueda afectar las ventas y lo que los clientes estarán dispuestos a pagar
- ¿Pueden las vulnerabilidades de seguridad o fraude afectar sus ingresos? ¿Cómo y cuánto?

© 2014 Abast Systems, S.A.

Workshops Formativos
para Responsables de Seguridad de TI

1. Objetivo y marco de trabajo
2. Workshop 1: entendimiento del negocio
3. **Workshop 2: riesgos y marcos de gestión de la seguridad**
4. Workshop 3: cumplimiento legal y TIC
5. ROSI (Retorno de la inversión en seguridad de la información) y resultados

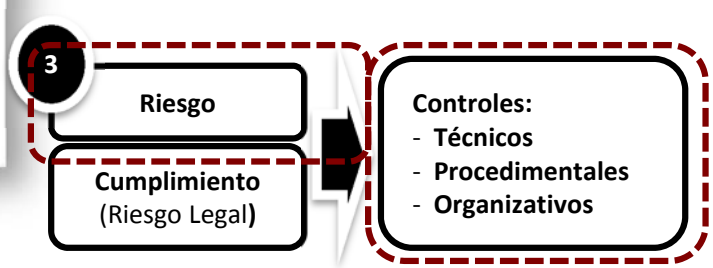
© 2014 Abast Systems, S.A.

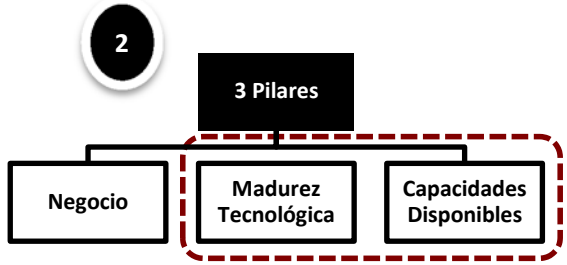
Workshop 2:
Riesgos y Marcos de Gestión de la Seguridad

- **Sesión TEÓRICA (2h)**
  - Explicación de las metodologías **análisis y gestión de riesgos (ISO 31000/ ISO 27005)**.
  - Explicación de los **marcos de gestión de la seguridad de TI como ISO 27001/2 y SANS**, así como los **objetivos de control y controles de seguridad** que proponen.
- **Sesión PRÁCTICA (4h)**
  - **Sesión de trabajo** sobre cómo los servicios de TI soportan el negocio y sobre el nivel de madurez tecnológica y capacidades disponibles de la organización tomando como base los marcos de gestión de la seguridad explicados.
  - **Sesión de trabajo** sobre qué riesgos de TI es prioritario gestionar en función del análisis anterior y del conocimiento del negocio analizado en el workshop 1.

- **Resultados:**
  - **Informe a alto nivel (de situación) del estado de madurez de seguridad de TI y capacidades asociadas disponibles**

Análisis Madurez Tecnológica y Capacidades Disponibles





Gestión de Riesgos
- Analizar los riesgos y establecer una estructura de gestión eficaz de los mismos.
- Obtener el apoyo y compromiso de la Dirección.
- Producir políticas de apoyo a la gestión de riesgos de la información.

Movilidad y Trabajo remoto
- Establecer políticas
- Adherir a los usuarios
- Proteger los datos en tránsito

Concienciación y Educación Usuarios
- Políticas de uso seguro de los recursos
- Programa de formación
- Concienciación riesgos cibernéticos

Gestión Incidencias
- Establecer capacidades recuperación incidencias y desastres (formación incluida)
- Crear y probar los planes de respuesta y recuperación

Gestión Privilegios Usuario
- Establecer procesos
- Limitar cuentas privilegiadas
- Restringir privilegios usuarios
- Controlar y auditar accesos

Control Dispositivos y Medios
- Política de control dispositivos
- Tipos de dispositivos a utilizar
- Control antimalware de ellos

Monitorización
- Definir estrategia monitorización
- Seguimiento sistemas y redes
- Análisis registros de actividad inusual

Configuración Segura
- Gestión de parches de seguridad
- Asegurar configuraciones seguras
- Disponer de un inventario de sistemas

Protección Antimalware
- Establecer políticas
- Disponer de soft antimalware
- Análisis de soft malicioso

Seguridad de Redes
- Filtrado de acceso y contenido malicioso
- Protección contra ataques externos e internos
- Administración del perímetro
- Monitorización y prueba de los controles

© 2014 Abast Systems, S.A.

Workshops Formativos
para Responsables de Seguridad de TI

1. Objetivo y marco de trabajo
2. Workshop 1: entendimiento del negocio
3. Workshop 2: riesgos y marcos de gestión de la seguridad
4. **Workshop 3: cumplimiento legal y TIC**
5. ROSI (Retorno de la inversión en seguridad de la información) y resultados

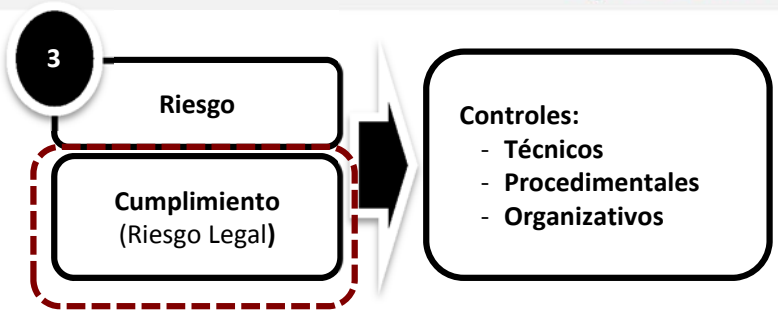
© 2014 Abast Systems, S.A.

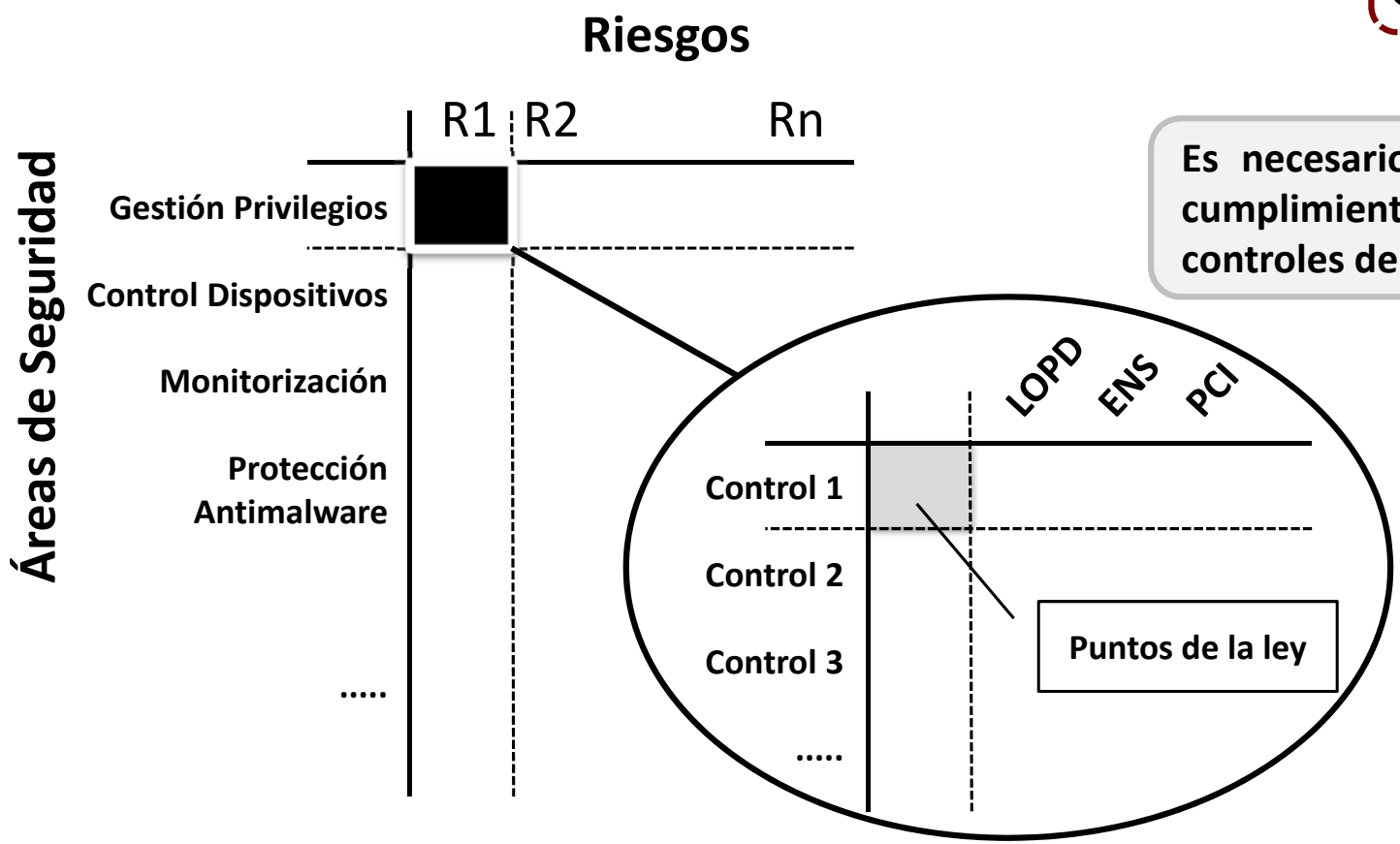
Workshop 3:
Cumplimiento Legal y TIC

- **Sesión TEÓRICA (2 h)**
  - Explicación de la tendencia asociada a la gestión de riesgos legales. Explicación de marcos de cumplimiento como la nueva ISO 19.600 (soft law). Implicación de leyes existentes como el código penal (responsabilidad penal de las personas jurídicas y debido control), la LOPD y venideras como la nueva regulación europea sobre protección de datos (Data Privacy Officer, Privacy Impact Analisys…) (law).
- **Sesión PRÁCTICA (4 h)**
  - **Sesión de trabajo** sobre los requerimientos legales que afectan al negocio y su relación con los riesgos de TI existentes y los controles de seguridad.

- **Resultado:**
  - **Informe a alto nivel (de situación) del estado de madurez de seguridad en cuanto a cumplimiento legal se refiere.**

Influencia de los temas de cumplimiento legal en las TIC





Es necesario tener en cuenta los temas de cumplimiento legal y sus implicaciones en los controles de seguridad a implementar

© 2014 Abast Systems, S.A.

Workshops Formativos
para Responsables de Seguridad de TI

1. Objetivo y marco de trabajo
2. Workshop 1: entendimiento del negocio
3. Workshop 2: riesgos y marcos de gestión de la seguridad
4. Workshop 3: cumplimiento legal y TIC
5. **ROSI (Retorno de la inversión en seguridad de la información) y resultados**

© 2014 Abast Systems, S.A.

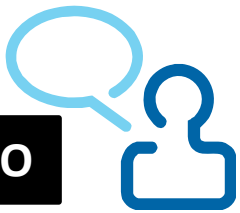
ROSI. Retorno de la Inversión en Seguridad

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

1

Principales preocupaciones negocio:

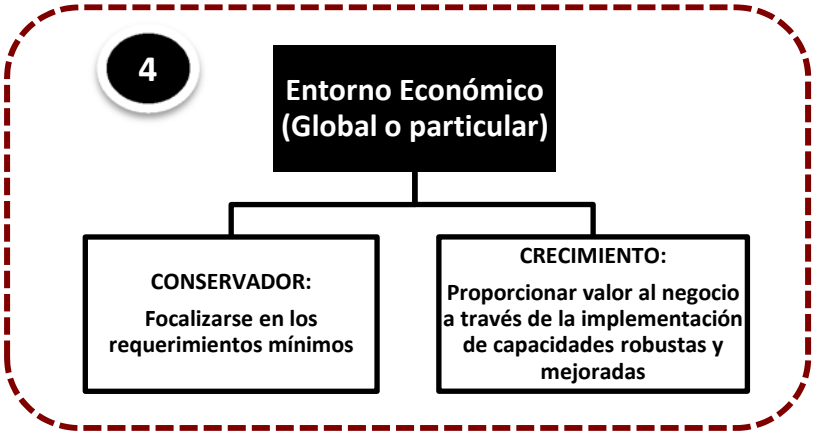
- **Pérdida reputación/confianza clientes**
- **Parada en la operativa del negocio**
- **Violación de cumplimiento**
- **Pérdida financiera**



CEO/CFO/COO

© 2014 Abast Systems, S.A.

Resumen Workshops Condiciones



Resultado final:

- **Mapa de Ruta para desarrollar una estrategia de seguridad acorde con el negocio e impacto económico asociado**

- Los workshops se realizarán in-situ, en casa del cliente.
- Podrán participar más de una persona en ellos.
- La información se obtendrá en base a entrevistas y uso de cuestionarios (preguntas clave).

LEÍDO Y CONFORME

	ABAST SYSTEMS, S.A.
	
Firmado:	**Firmado:** David Ortega Resp. Área Consultoría TI

- **Condiciones y Estimación económica:**

1. Importe económico (sin IVA): **2.500 €**
2. Facturación y forma de pago:
   - Facturación a la aceptación de los servicios
   - Pago por transferencia bancaria a 60 días f.f.

© 2014 Abast Systems, S.A.