



teasaConsulting

ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT



Gestión de Riesgos

CONTROL Y COMPLIANCE

¿Qué entendemos por Compliance?

Es el **Sistema que implementan las sociedades para asegurar** no sólo el cumplimiento de las disposiciones legales y normativas que le aplican, sino también el **cumplimiento de las normas internas éticas y de comportamiento de los miembros de la Organización.**

La función de Compliance abarca tres ámbitos:

- **Governance:** conjunto de mecanismos para asegurar un Modelo de Gobierno que garanticen que las decisiones se toman con total información y que se establecen los controles adecuados para confirmar que las instrucciones y la estrategia se están desarrollando correctamente.
- **Gestión de Riesgos.**
- **Compliance:** se encarga no sólo del cumplimiento de las regulaciones y leyes que resulten aplicables, sino también de la redacción y aprobación de las políticas, compromisos y valores internos y de las funciones de control y supervisión.

¿Y por gestión de riesgos?

La **Gestión de Riesgos** es el proceso de identificación, análisis y evaluación de cualquier actuación, hechos o proceso (riesgo) que pueda **afectar de forma adversa a la estrategia de la organización**, su capacidad de operar y el cumplimiento de los objetivos económicos o reputacionales, ya sean **riesgos corporativos o penales**.

La gestión de estos riesgos **se puede realizar a través de su mitigación** (reducir impacto o probabilidad), **prevención** (evitar el riesgo), **aceptación** según apetito al riesgo, **o compartirlos**, por ejemplo póliza de seguros.

¿Por qué lo necesito?

- **Se aplica a todas las empresas independientemente del sector y tamaño**, si bien se especifica que el Sistema se adecuará precisamente a estas circunstancias
- **Son requerimientos que cada vez están más exigiendo las compañías** para operar comercialmente con Terceros, ya sea como proveedor o clientes.
- **Su correcta implementación comporta exenciones o reducciones de la responsabilidad penal de la persona jurídica y de los administradores y directivos**, así como reducción o eliminación de sanciones económicas y administrativas.
- **Se valora mucho en el Mercado junto con los criterios ESG** (Medio Ambiente, Social y Personas), **Governance** (Compliance) **y refuerza la Compañía.**

¿Cómo lo haremos?

Utilizamos metodología contrastada siguiendo las directrices establecidas en diferentes Normas ISO y UNE de aplicación ISO 37001 Gestión de Riesgos, ISO 37301 Sistema de Gestión de Compliance, UNE 19601 Sistema de Gestión de Compliance Penal.

Ejemplos de necesaria aplicación:

- **¿Qué tipo de controles tiene establecidos** una empresa de reciclaje para **controlar las compras de materias primas (por ejemplo cobre)?**
- **¿Cómo gestiona una empresa la identificación, análisis y valoración de la integridad de los Terceros** con los que mantenemos o queremos iniciar relaciones comerciales?
- **¿La compañía tiene implementadas medidas o políticas anticorrupción y contra el fraude?**
- **¿La empresa dispone de políticas en el área de RRHH contra el acoso, plan de igualdad en su caso?**
- **¿La Pyme tiene actualizado el canal de denuncia según la L2/2023?**



01 Punto de partida de la empresa

01 Punto de partida de la empresa

Posibles escenarios en los que se puede encontrar su empresa u organización:

- La empresa NO tiene implementado un **Sistema de Gestión de Riesgos**.
- No existen responsabilidades asignadas en cuestiones **de riesgos, ni en las funciones de control y supervisión**.
- **Han trabajado los riesgos y controles, pero disponen de un mapa de riesgos no actualizado:** NO hacen seguimiento.
- **Si tienen un Sistema de Gestión de Riesgos:** Se necesitaría una Auditoría y una revisión del Modelo.



02 Objetivos

02 Objetivos

El proyecto persigue alcanzar **cuatro objetivos**:

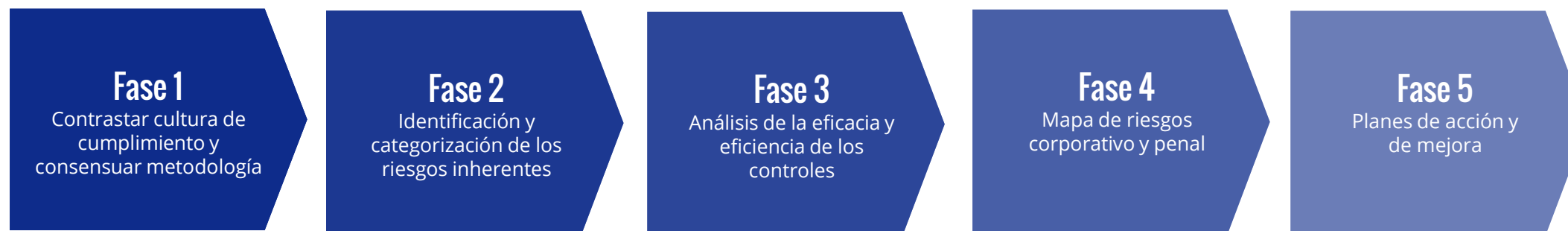
- **Identificar los riesgos inherentes y residuales:** análisis, valoración y evaluación.
- **Análisis, eficacia y eficiencia de los controles:** valoración del sistema de control interno.
- **Elaborar el Mapa de Riesgos:** corporativo y penal.
- **Establecer planes de revisión y mejora en la gestión de riesgos:** implementar controles.



03 Desarrollo del Proyecto

03 Desarrollo del Proyecto

El proyecto se desarrolla en **5 fases** y en **4 formatos de trabajo** diferentes:



Sesión presencial



Sesión digital

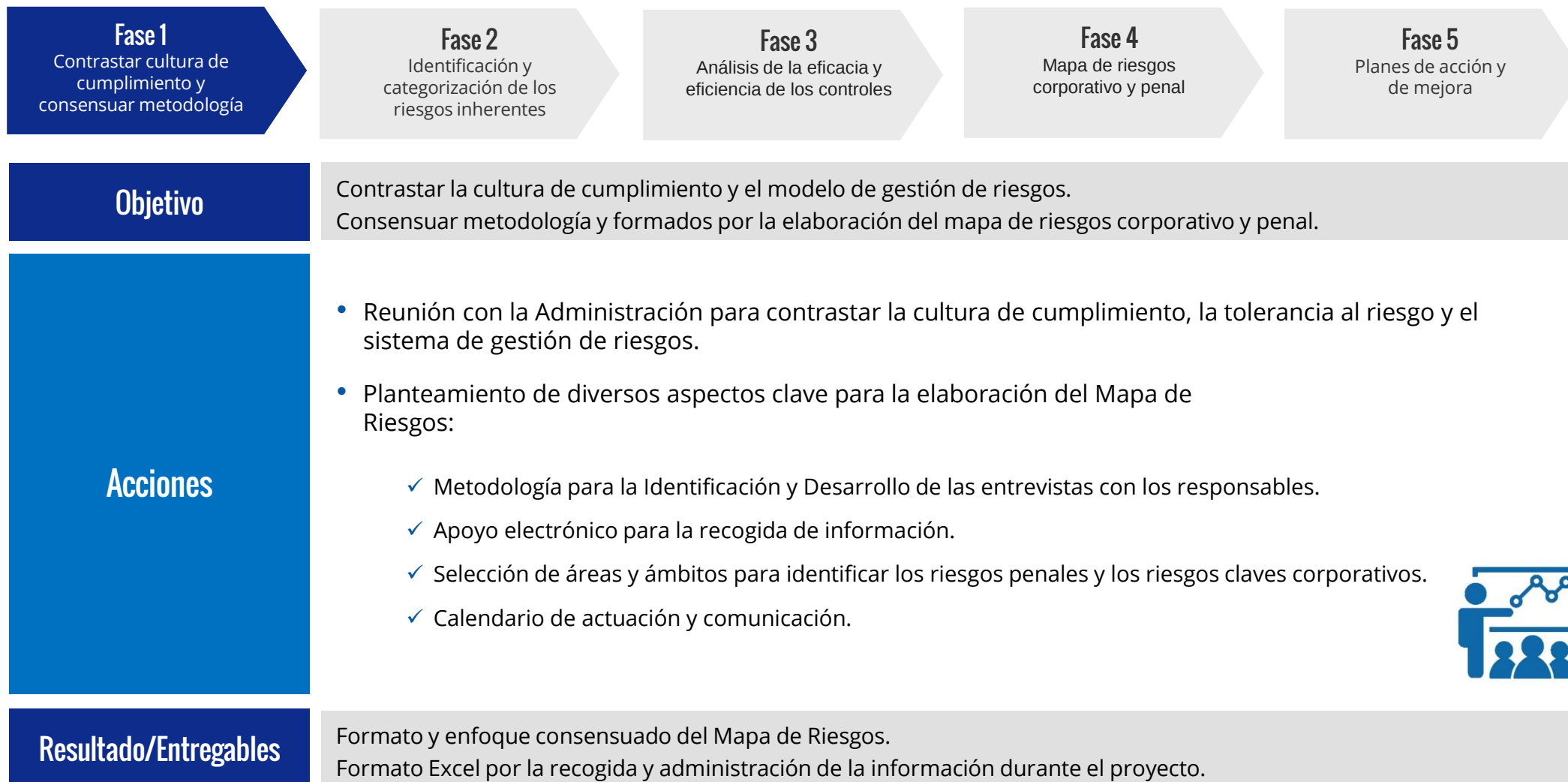


Trabajo interno empresa

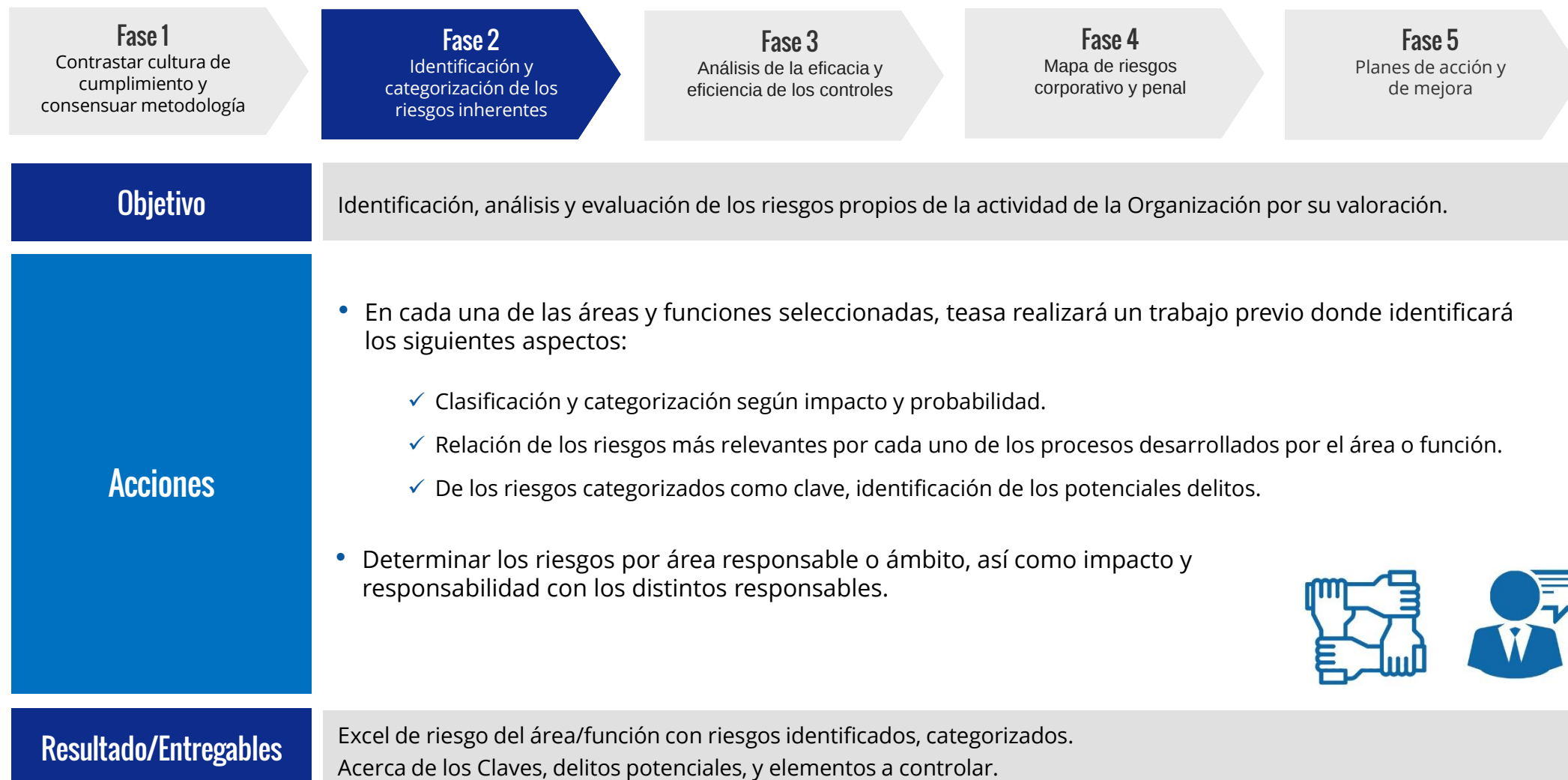


Trabajo consultor

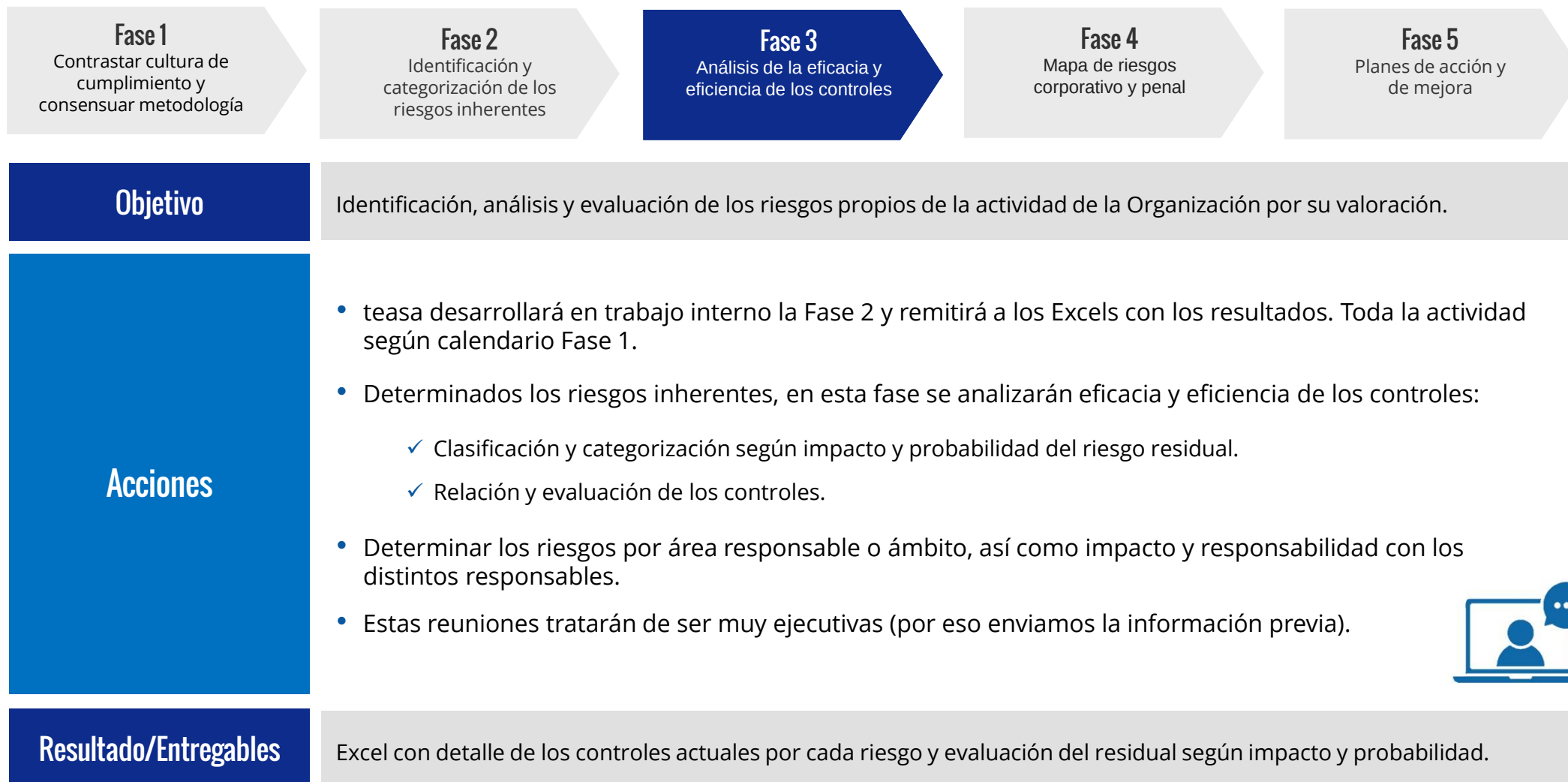
03 Desarrollo del Proyecto



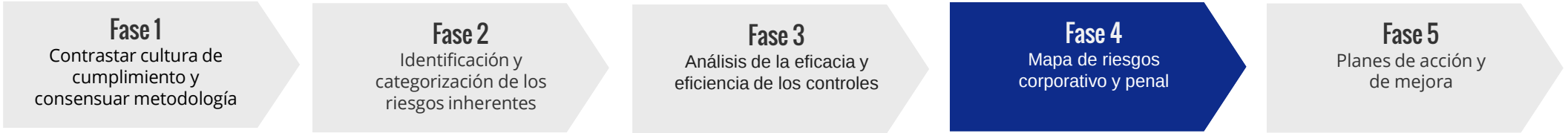
03 Desarrollo del Proyecto



03 Desarrollo del Proyecto



03 Desarrollo del Proyecto



Objetivo

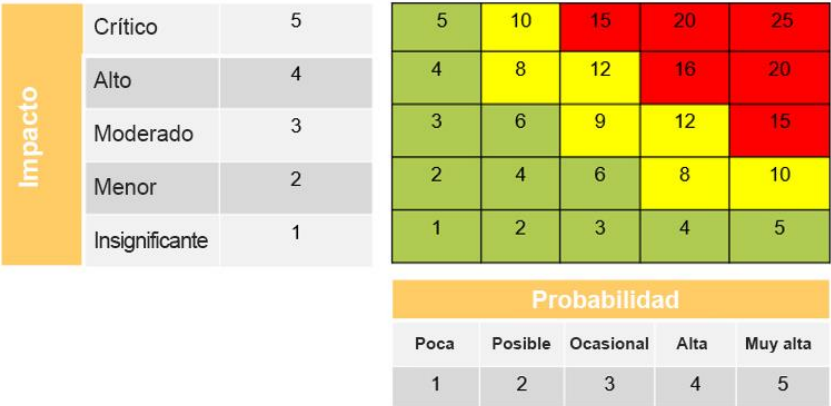
Elaborar Mapa de riesgos penales y corporativos.

Acciones

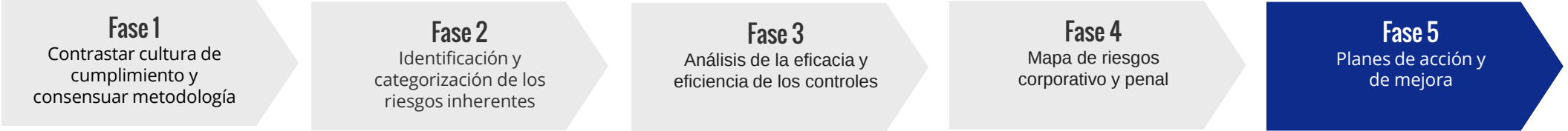
Resultado/Entregables

Excel con Mapa de riesgos corporativos y Mapa de color de riesgos penales.

Descripción del riesgo	Categoría del riesgo	Tipología del riesgo	Exposición	(Ex qué dentro Impacto)	Impacto	Probabilidad	Resultado de la evaluación	Control Mitigador preventivo	Impacto tras control	Probabilidad tras control	Resultado de la evaluación	Nivel de riesgo residual	Área/Departamento responsable	Riesgo asociado
Falta de política de seguridad IT (no documentada)	Operativo	Tecnológico	NO		4. Alto	3. Ocasional	12	Está elaborada Política. Se aprueba por el responsable del Departamento. El Director de Área decide los acciones	4. Alto	2. Posible	8		Departamento de Sistemas	
Falta de Política de uso de medios tecnológicos documentada (dispositivos, acceso personal,...)	Operativo	Tecnológico	No		4. Alto	4. Alta	16		4. Alto	3. Ocasional	12		Departamento de Sistemas	
Obsolescencia externa o "roscuro" de información/sistemas	Operativo	Tecnológico	SI	Dentro Tecnológico	5. Crítico	5. Muy alta	25	Financiar de acciones, acceso red no autorizado, todo documentado	5. Crítico	3. Ocasional	15		Departamento de Sistemas	
Incumplimiento de la Ley de Protección Datos Personales	Operativo	Tecnológico	SI	Dentro contra la intimidad y/o por revelación datos	4. Alto	2. Posible	8	CPD independiente para garantizar la seguridad de la información y evitar que ataques externos afecten la confidencialidad del negocio. Actualizar	3. Moderado	1. Poco probable	3		Departamento de Sistemas	SI
Pérdida de datos o información asociada a sistemas. Seguridad de la información.	Operativo	Tecnológico	SI	Dentro Tecnológico	5. Crítico	5. Muy alta	25		3. Moderado	1. Poco probable	3		Departamento de Sistemas	SI



03 Desarrollo del Proyecto



Objetivo

Presentación del Mapa de Riesgos penales y corporativos y los planes de acción y mejora en la gestión de los riesgos.

Acciones

Plan de acción Mecanismo control adicional	Responsable	Fecha máxima realización	Estado situación



Resultado/Entregables

Mapa de riesgos penal (mapa de color) y los riesgos corporativos (Excel) con los Planes de acción y mejora.

Gracias



C/ Sardenya, 397-399 2n 5a

08025 Barcelona

Tel. 934 874 260

Email: teasa@teasa.es

www.teasa.es



teasa*Consulting*

ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT



teasatech

TRANSFORMACIÓN DIGITAL | INDUSTRIA 4.0 | INNOVACIÓN