Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

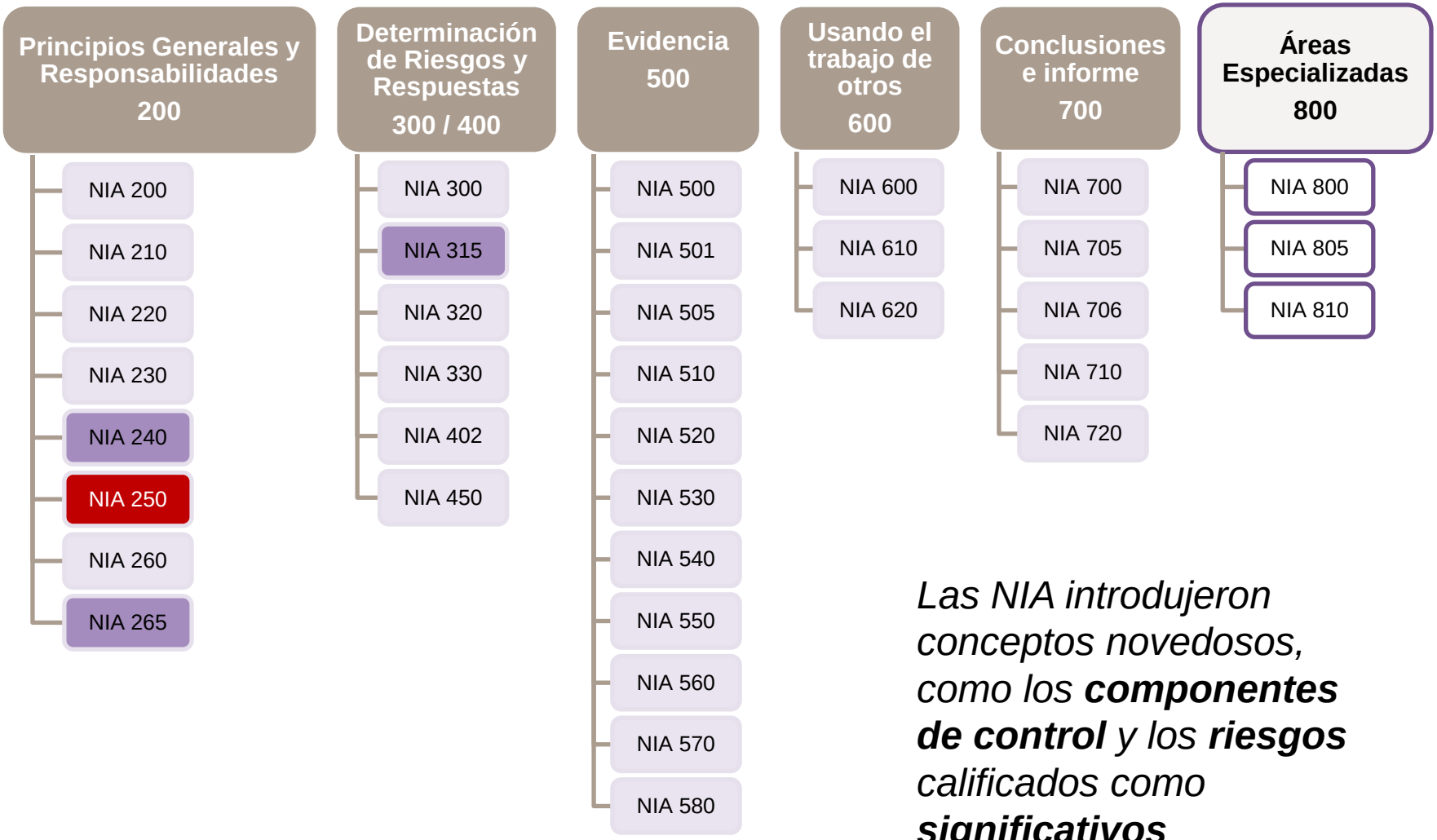
Los retos de los modelos de compliance con la seguridad

(Parte I)

Juan Luque
Socio de MAZARS

Las NIA y el Cumplimiento Normativo

NORMAS INTERNACIONALES DE AUDITORÍA (NIA)



*Las NIA introdujeron conceptos novedosos, como los **componentes de control** y los **riesgos** calificados como **significativos***

DEFINICIÓN DE INCUMPLIMIENTO NORMATIVO NIA - 250

Acciones u omisiones de la entidad, intencionadas o no, que son **contrarias a las disposiciones legales y reglamentarias vigentes**, realizadas por:

- la **entidad**, o en su nombre,
- por **cuenta de la entidad**, por los **responsables de su gobierno**, la **dirección** o los **empleados**.

El **incumplimiento no incluye conductas personales inapropiadas** (no relacionadas con las actividades empresariales de la entidad)

DEFINICIÓN DE FRAUDE NIA - 240

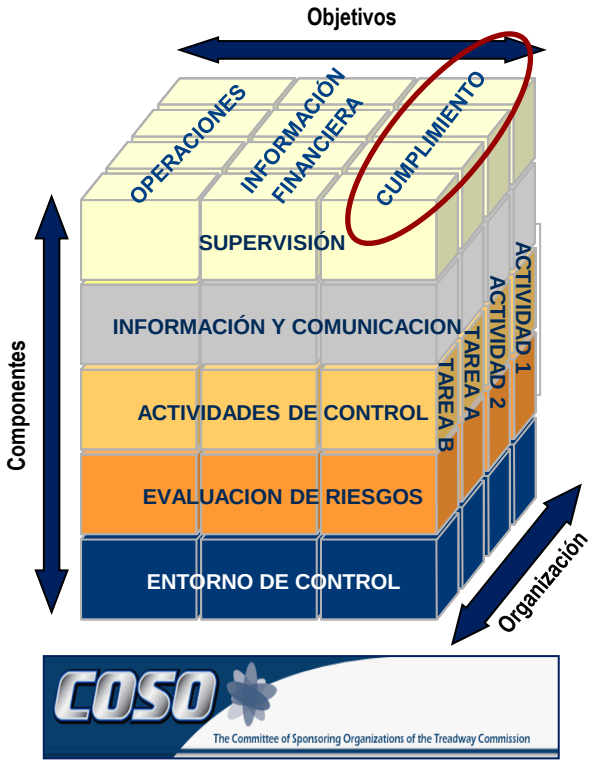
Acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la **utilización del engaño** con el fin de conseguir una **ventaja injusta o ilegal**.

El Triangulo del Fraude".Doctor Donald Cressey (1961)

DEFINICIÓN DE CONTROL INTERNO NIA - 315

Proceso diseñado, implementado y mantenido por los **responsables del gobierno** de la entidad, la dirección y otro personal, con la finalidad de proporcionar una **seguridad razonable** sobre la consecución de los objetivos de la entidad relativos:

- la eficacia y eficiencia de las operaciones
- la fiabilidad de la información financiera
- el **cumplimiento de las disposiciones legales y reglamentarias** aplicables



NORMAS INTERNACIONALES DE AUDITORÍA (NIA)

NIA 250 CONSIDERACIÓN DE LAS **DISPOSICIONES LEGALES Y REGLAMENTARIAS**

OBJETIVOS

1. **Obtener evidencia** suficiente y adecuada del cumplimiento de las disposiciones legales y reglamentarias **con efecto directo** estados financieros
2. **Aplicar procedimientos** para identificar otras disposiciones legales y reglamentarias que deben cumplirse pero **sin efecto directo** sobre los estados financieros de la entidad
3. **Responder** adecuadamente al incumplimiento o indicios de incumplimiento de disposiciones legales y reglamentarias identificadas en la auditoría

REQUERIMIENTOS

1. **Consideración** por el auditor del **cumplimiento** de las **disposiciones legales y reglamentarias**
2. **Procedimientos** de auditoría cuando se identifican que **existen indicios de incumplimiento**
3. **Comunicación de incumplimientos** identificados o existencia de indicios de un posible incumplimiento
4. **Documentación**

NORMAS INTERNACIONALES DE AUDITORÍA (NIA)

NIA 240 RESPONSABILIDADES DEL AUDITOR CON RESPECTO AL **FRAUDE**

NIA 250 CONSIDERACIÓN DE LAS **DISPOSICIONES LEGALES Y REGLAMENTARIAS**

- **Responsabilidad** del **gobierno** de la entidad y la **dirección**:
  - La prevención y detección del **fraude**.
  - Asegurar que las **actividades de la entidad** se realizan de **conformidad con las disposiciones legales y reglamentarias.**

- **Responsabilidad del auditor:**

  Obtener una **seguridad razonable** de que los estados financieros considerados en su conjunto **están libres de incorrecciones materiales debidas a fraude** o **error**.

- Las **NIA-ES 240** y **250** establecen **obligaciones de comunicación sobre:**
  - **fraude** o indicios de fraude,
  - por **incumplimientos de disposiciones legales y reglamentarias** de una entidad auditada, respectivamente.

NORMAS INTERNACIONALES DE AUDITORÍA (NIA)

NIA 265 — **COMUNICACIÓN** DE LAS **DEFICIENCIAS** SIGNIFICATIVAS EN EL **CONTROL INTERNO** A LOS RESPONSABLES DEL GOBIERNO Y, SIGNIFICATIVAS O NO , A LA DIRECCIÓN DE LA ENTIDAD

NIA 315 — **IDENTIFICACIÓN** Y **VALORACIÓN** DE LOS **RIESGOS DE INCORRECCIÓN MATERIAL** MEDIANTE EL CONOCIMIENTO DE LA ENTIDAD Y SU ENTORNO

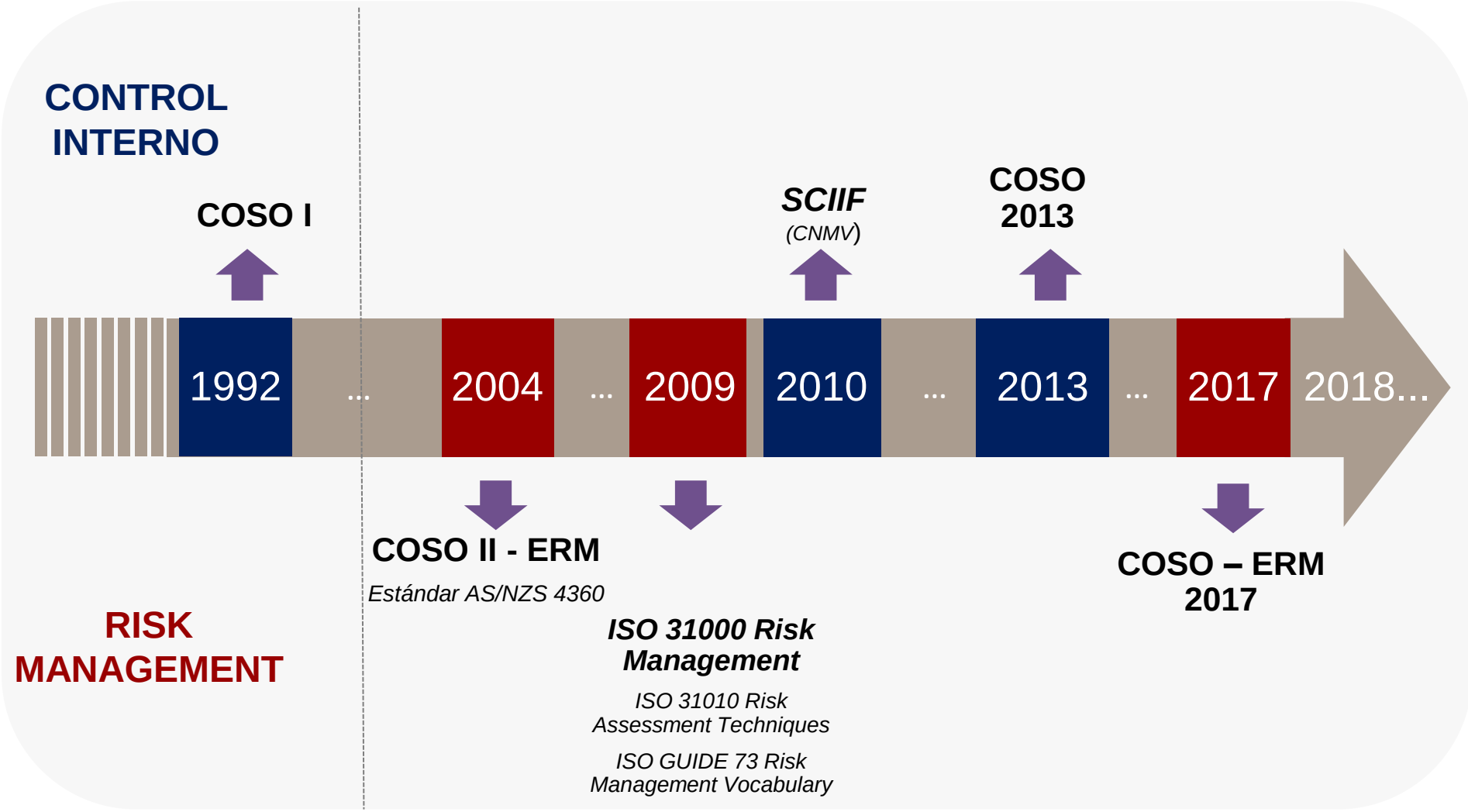
Se requiere obtener información para identificar y valorar riesgos de incorrección material debido a error y fraude que pudieran tener los estados financieros en su conjunto, partiendo del **conocimiento de la entidad**, incluido sus **componentes de control interno**:

- entorno
- proceso de valoración de riesgo de negocio
- sistema de información
- actividades de control relevantes para la auditoría
- seguimiento

} **COSO**

Principales Referenciales en control interno y gestión de riesgos

EVOLUCIÓN PRINCIPALES REFERENCIALES EN CONTROL INTERNO Y GESTIÓN DE RIESGOS



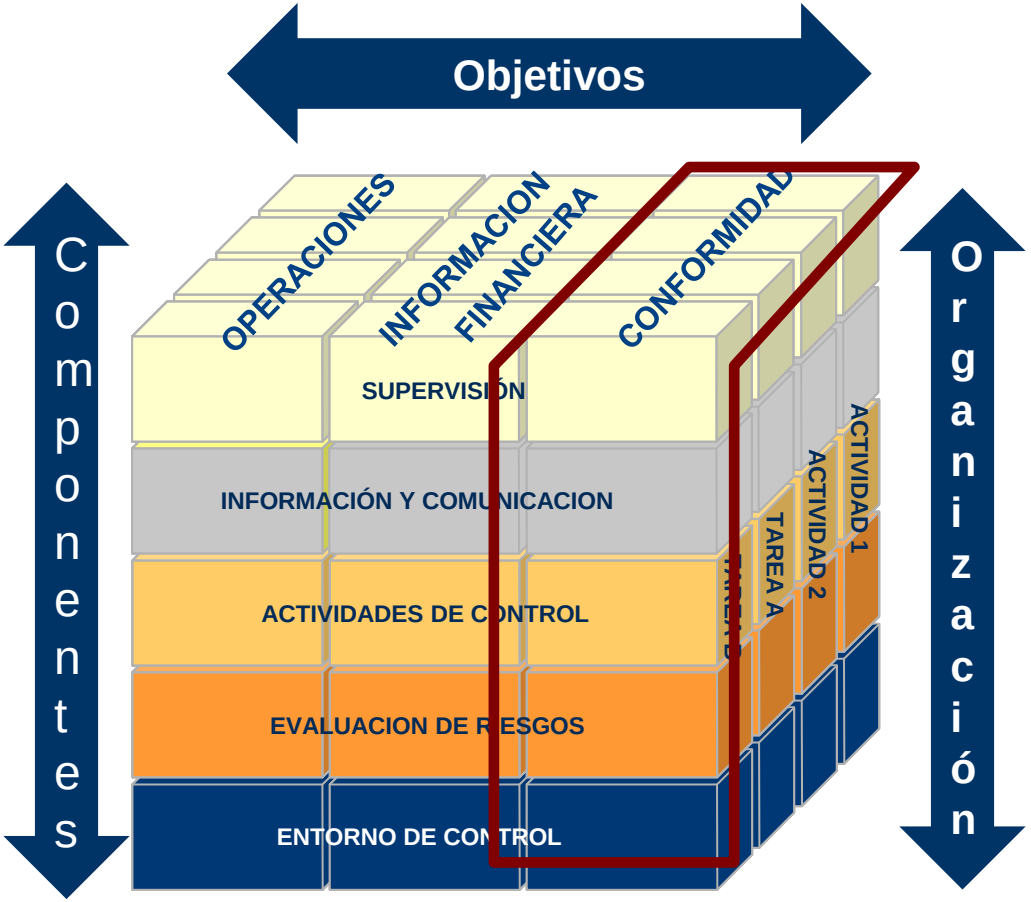
COSO I (1992) – MARCO INTEGRADO DE CONTROL INTERNO

El Marco COSO fue creado para facilitar a las empresas los procesos de evaluación y mejora continua de sus sistemas de control interno

- El modelo COSO se representa con un cubo:
  - 3 objetivos,
  - 5 componentes,
  - Los niveles de organización de la compañía.

- Los 5 componentes deben permitir el cumplimiento
  - … de los 3 tipos de objetivos de la empresa…

    … para cada nivel de organización.



COSO 2013 – UNA EVOLUCIÓN DE COSO I

El Marco de Control Interno (COSO 2013), presentado en mayo de 2013, es una evolución del Marco previo de 1992 para tratar de adaptarse a las sugerencias y retos que se han ido planteando.

Tecnología

- Tiene en cuenta el nuevo entorno tecnológico

Buen Gobierno

- Mayor supervisión del sistema de control interno por los órganos de gobierno

Globalización

- Adaptación a los nuevos modelos de negocio más globales

Objetivos de negocio

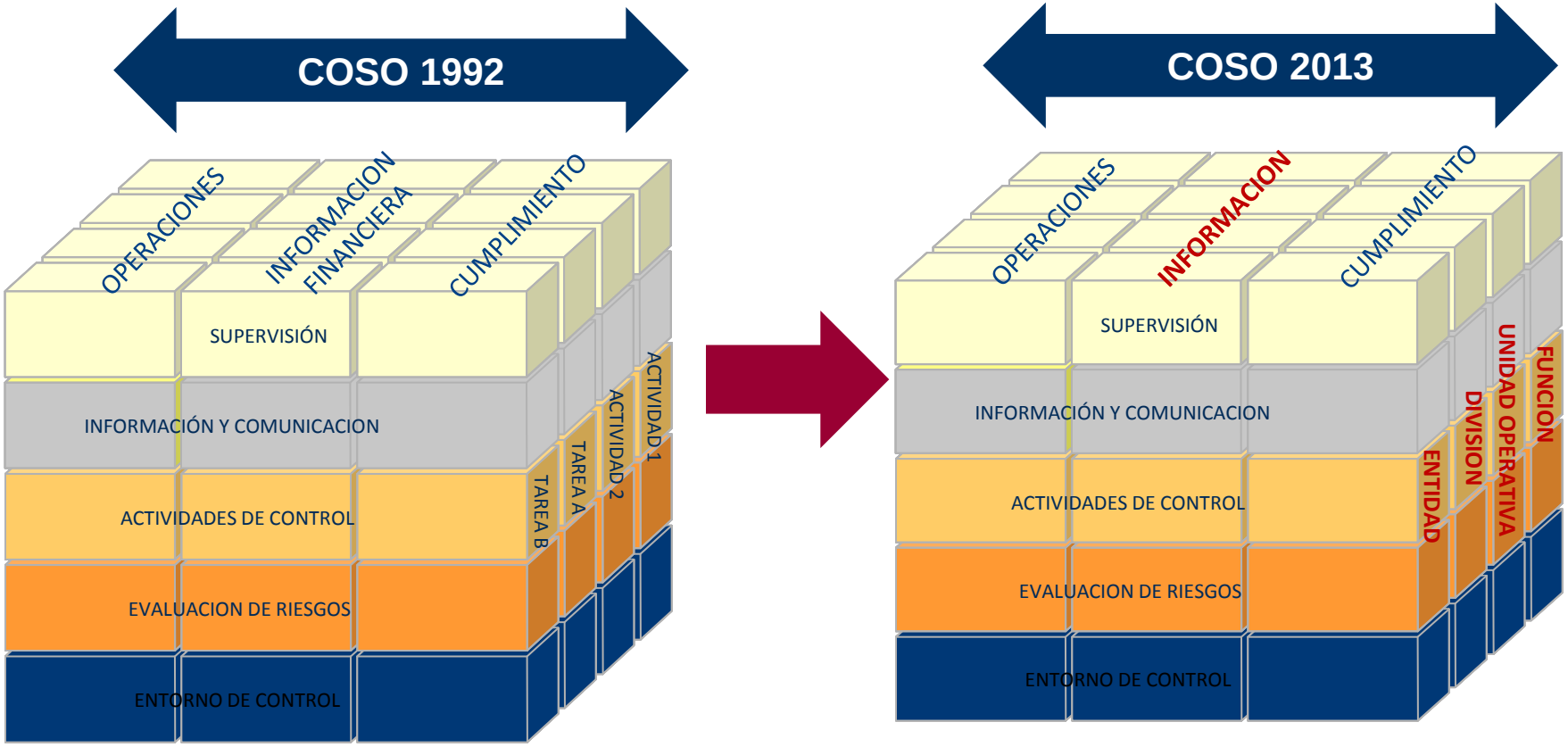
- Necesidad de establecer objetivos de negocio para poder definir los objetivos de control interno

Información

- Objetivo tanto para información financiera como no financiera y tanto a nivel interno como externo

COSO 2013 – UNA EVOLUCIÓN DE COSO I

El cambio más significativo que es que considera que para que los controles internos sean efectivos es necesario que los 5 componentes y los 17 principios relevantes que plantea estén en funcionamiento, operando de forma integrada.



COSO 2013 – UNA EVOLUCIÓN DE COSO I

Entorno de control	1. Demostrar su compromiso con la integridad y los valores éticos. 2. Demostrar independencia en la gestión y ejercer la supervisión del desarrollo y ejecución del control interno. 3. Establecer la estructura, líneas de reportes, autoridad y responsabilidad en la consecución de objetivos. 4. Compromiso para atraer, desarrollar, y retener personas competentes. 5. Disponer de personas responsables para atender sus responsabilidades de Control Interno.
Evaluación de riesgos	6. Especificar los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados. 7. La Organización debe identificar y evaluar sus riesgos. **8. La Organización gestionará el riesgo de fraude**. 9. Identificar y evaluar los cambios importantes que podrían impactar en el sistema de control interno.
Actividades de control	10. Seleccionar y desarrollar actividades de control que contribuyan a la mitigación de los riesgos **11. Seleccionará y desarrollará Controles Generales sobre TI** 12. Implementa sus actividades de control a través de políticas y procedimientos adecuados
Información y comunicación	13. Generar la información relevante. 14. Compartirá internamente la información. 15. Comunicará externamente.
Actividades de monitorización	16. Llevará a cabo evaluaciones continuas e individuales. 17. Evalúa y comunica las deficiencias de control interno.

COSO II (2004) – ENTERPRISE RISK MANAGEMENT – MARCO INTEGRADO

Debido al aumento de preocupación por la Gestión de Riesgos, en septiembre de 2004, se publica el informe denominado Enterprise Risk Management – Integrated Framework, el cual incluye el marco global para la Gestión Integral de Riesgos.

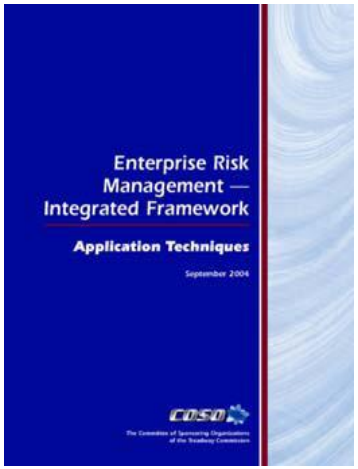
Qué

- 8 componentes interrelacionados

Objetivo Nuevo

Alineado con

- Los objetivos en el contexto de 4 categorías



Dónde

- Considera las actividades de todos los niveles de la organización

COSO 2017 – UNA EVOLUCIÓN DEL COSO II - ERM MARCO INTEGRADO

Este nuevo marco **contempla la gestión de riesgos** como un **aspecto estratégico en toda organización**. Principales aspectos:

- Presenta una **estructura muy simple de 5 componentes y 20 principios** que facilite su implantación en cualquier tipo de empresa
- Impulsa una mejor **cultura organizativa basada en el riesgo**
- **Vincula Riesgo y estrategia**: identificar y valorar adecuadamente los riesgos favorece lograr el éxito en la gestión
- **Vincula los conceptos de riesgo y desempeño organizacional**: a fin de evitar que el concepto de riesgo siga siendo abstracto.
- **Integra la gestión de riesgos con el control interno**: considera los marcos de control interno y gestión de riesgos son plenamente complementarios
- Contempla la **evolución tecnológica** y el **uso del data analysis** como apoyo para la **toma de decisiones**
- **Amplia el reporting** para dar respuesta a las expectativas de más transparencia entre las partes interesadas

COSO 2017 – ENTERPRISE RISK MANAGEMENT MARCO INTEGRADO

Misión, visión y valores fundamentales	Desarrollo de la estrategia	Formulación de los objetivos del negocio	Implementación y perfomance	Valor añadido
Gobierno y cultura	Estrategia y objetivos	Perfomance	Evaluación y Revisión	Información, comunicación y reporting
1. El Consejo supervisa los riesgos	6. Analiza el contexto empresarial	10. Identifica los riesgos	15. Evalúa los cambios sustanciales	18. Aprovecha la información y la tecnología
2. Establece estructuras operativas	7. Define el apetito al riesgo	11. Evalúa la severidad de los riesgos	16. Revisa los riesgos y el desempeño	19. Comunica los riesgos de información
3. Define la cultura deseada	8. Evalúa estrategias alternativas	12. Prioriza los riesgos	17. Propone mejoras en la gestión de los riesgos empresariales	20. Informes sobre riesgos, cultura y desempeño
4. Demuestra compromiso con los valores fundamentales	9. Formula los objetivos empresariales	13. Implementa las respuestas al riesgo		
5. Atrae, desarrolla y retiene individuos competentes		14. Desarrollar un portafolio de riesgos		

Fuente: Enterprise Risk Management Framework: Integrating with Strategy and Performance

Sistemas de Gestión de Compliance

EVOLUCIÓN MARCOS REGULARIOS EN COMPLIANCE

1970-1989

Aprobación FCPA
(Foreing Corrupt Practices Act)

1977

SEC: Investigación sobornos en 400 empresas (pagos irregulares a políticos y partidos)

Caso **Lockheed** (pagos a funcionarios de otros gobiernos: Japón, Holanda, Alemania)

1990- 1999

- **Compliance Programmes** (US Sentencing Comission)
- **Modificación FCPA**

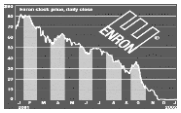
1991 **1998**

Convención anti-corrupción OCDE (41 países) que impulsa la implantación del Compliance en países de cultura no anglosajona

2000-2009

- **SOA- US (2002)**
- **Reforma Guidelines (2004)** (programas de compliance y función cumplimiento)

2002 **2004**



Caso **ENRON** (2002)

Cae **Lehman Brothers (2008)**

Crisis financiera con mayor regulación en los mercados

2010-2018

- **OCDE** (Good Practice Guidance on Internal Controls, Ethics and Compliance)
- **Bribery Act UK**
- **Ley 10/2010 Prev. Blanqueo**
- **Reforma C. Penal L.O 5/2010** (debido control)
- **Ley de Sociedades de Capital (2014)**
- **Reforma C.Penal L.O 1/2015** (modelos compliance)
- **Aprobación GDPR** (aplicación 25/05/2018)

2010 **2014** **2015** **2018**

Aprobación nuevos estándares sobre Sistemas de Gestión en Compliance:

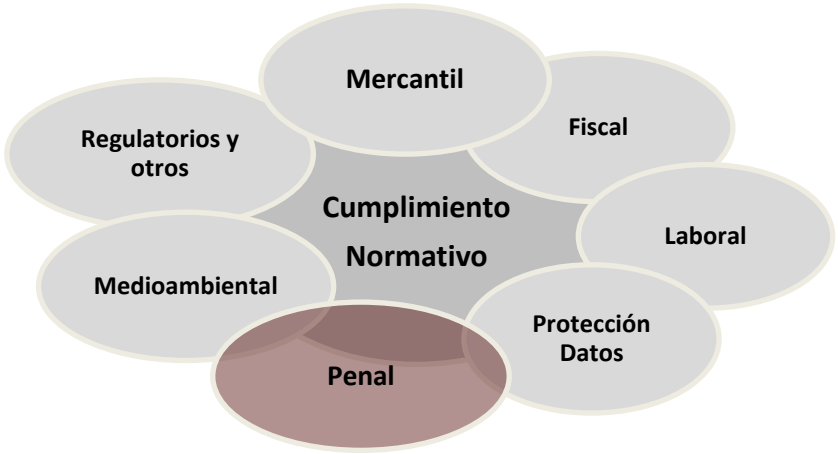
- ISO 19600: 2015 Compliance Management
- ISO 37001: 2016 Anti-Bribery
- UNE 19601:2017 Compliance Penal

EL CUMPLIMIENTO NORMATIVO EN LOS MODELOS DE COMPLIANCE

Las **obligaciones de cumplimiento normativo** en los actuales modelos de compliance incluyen un doble concepto:

- La **normativa regulada** por parte de los poderes públicos de obligado cumplimiento
- Las que se establecen **voluntariamente**

Cumplimiento externo

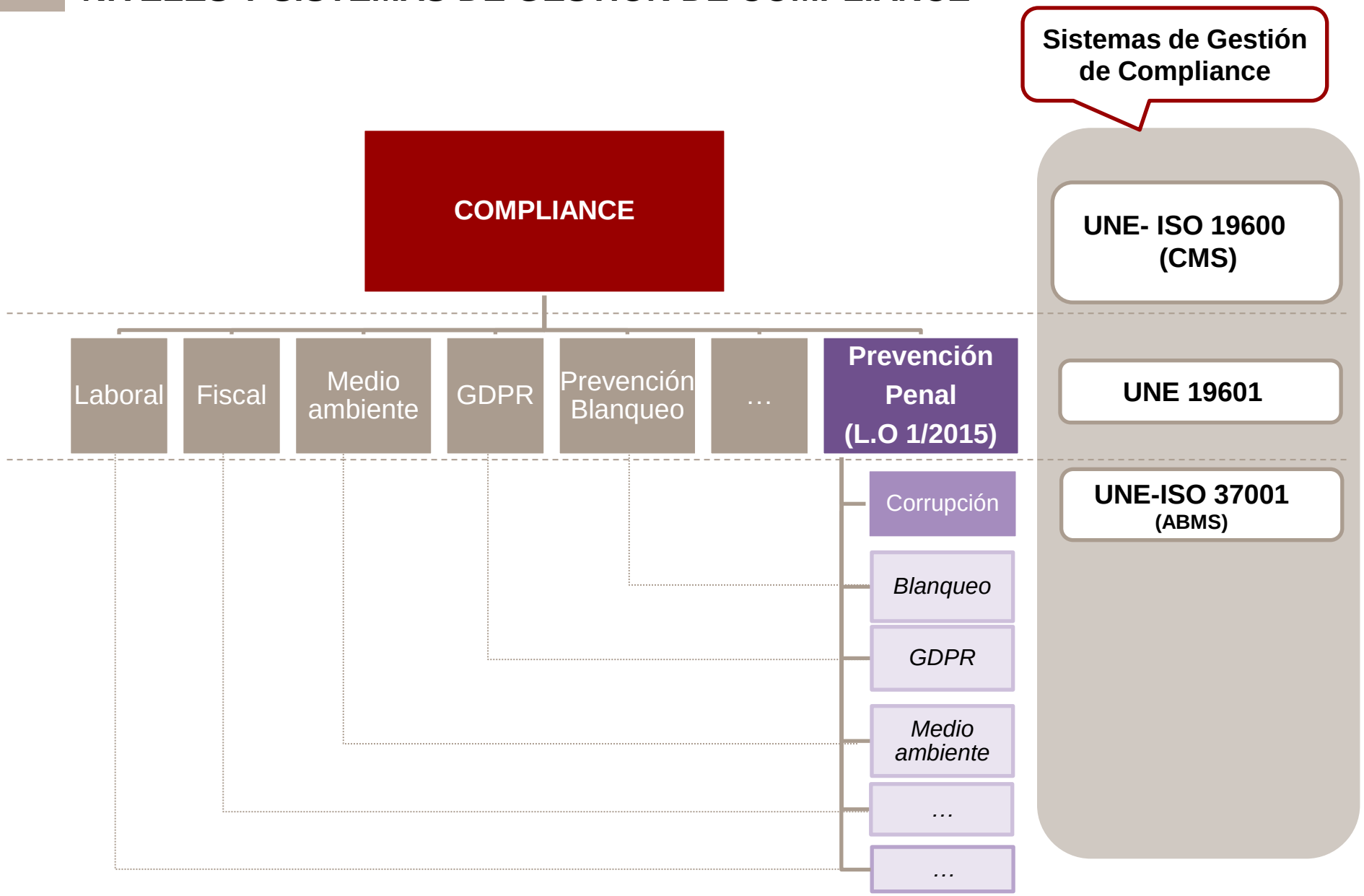


Riesgo de Compliance y Reputacional

Cumplimiento interno

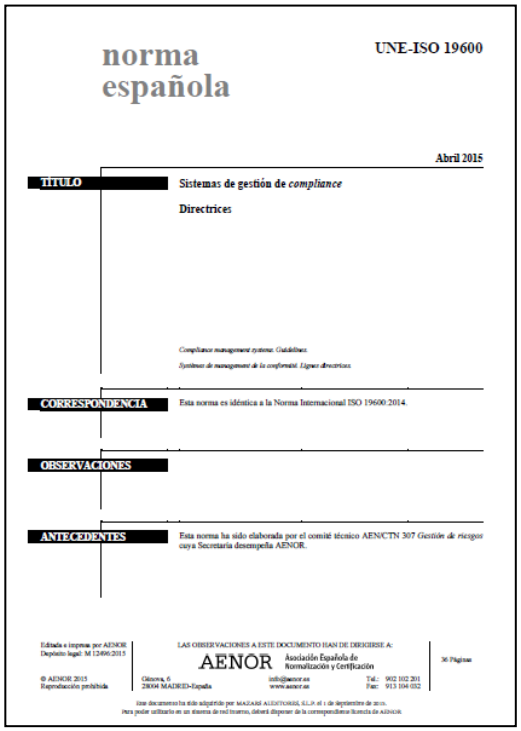
- Código de Ética / Conducta
- Códigos de buenas prácticas internacionales, locales o sectoriales
- Políticas internas: Manual de Funciones, Normas y Procedimientos
- Manual de Facultades y Poderes / Norma de Autorizaciones
- Niveles de autorización: Solicitud / aprobación / adjudicación / supervisión / registro / pago
- Normas Reguladoras internas: Función de Comité de Auditoría, Auditoría Interna, Risk Management, Compliance Officer,.....
- ....

NIVELES Y SISTEMAS DE GESTIÓN DE COMPLIANCE



ISO 19600: 2015. SISTEMA DE GESTIÓN DE COMPLIANCE. DIRECTRICES

- **Primer estándar internacional** sobre Sistemas de Gestión de Cumplimiento
- Tiene su **origen en el estándar australiano 3806-2006** sobre Sistemas de Gestión de Compliance (CMS) de gran reconocimiento internacional
- **Estándar de alto nivel** que puede integrarse con estándares específicos (Soborno, Prevención penal)
- **No es certificable**
- **Fija principios** de actuación fundamentados en las **mejores prácticas internacionales** facilitando el diseño de sistemas de gestión de cumplimiento con un **alcance global**


norma española

UNE-ISO 19600

Abril 2015

TÍTULO

Sistemas de gestión de *compliance*

Directrices

Compliance management systems. Guidelines

Systèmes de management de la conformité. Lignes directrices

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO 19600:2014.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 307 *Gestión de riesgos* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 12496:2015

© AENOR 2015
Reproducción prohibida

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

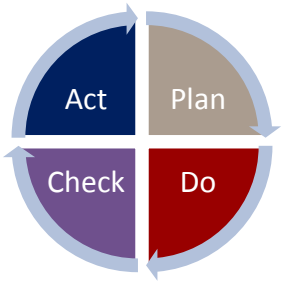
Tel.: 902 102 201
Fax: 913 104 032

36 Páginas

Este documento ha sido adquirido por MAZARS AUDITORES, S.L.P. el 1 de septiembre de 2015.
Para poder utilizarlo en un sistema de red interno, deberá disponer de la correspondiente licencia de AENOR.

- **No especifica requisitos,** proporciona orientación y prácticas recomendadas a utilizar
- **La cultura corporativa de cumplimiento es entendida como regla general**

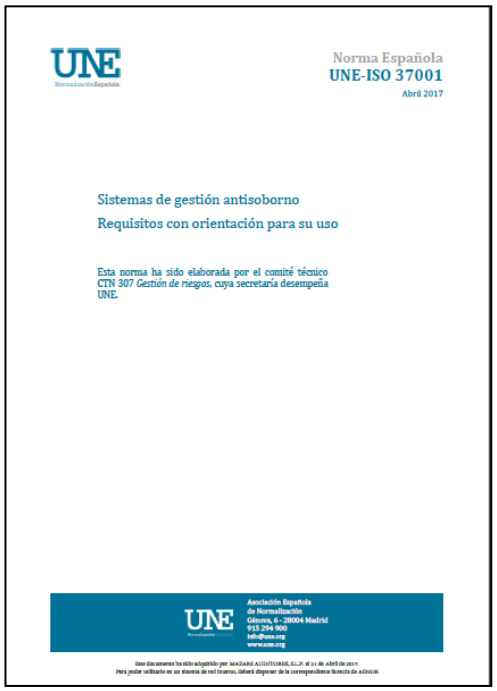
ISO 19600: 2015. SISTEMA DE GESTIÓN DE COMPLIANCE. DIRECTRICES



- **Coherente con otros Sistemas de Gestión** (ISO 9001, 14001,…)
- Basado en **el principio de mejora continua.** Modelo Planificar, Hacer, Verificar y Actual **(PDCA)** aplicable a los sistemas de gestión
- Sistema orientado a la **gestión de las distintas áreas de cumplimiento** que afectan a una organización ya sean sobre normas de obligado cumplimiento como voluntarias (**enfoque transversal**)
- **Enfoque basado en riesgos.** Identificación, evaluación y seguimiento.
- Aplicable a cualquier tipo de entidad, sector y tamaño **(principio de proporcionalidad),** resaltando:
  - La importancia del papel de la dirección, su compromiso y una adaptación adecuada del liderazgo.
  - Las responsabilidades, su designación y comprensión.
  - Identificación de las obligaciones del compliance.
  - El análisis y la adecuada gestión de los riesgos relacionados con el compliance.
  - La formación como base para mantener el sistema en el futuro.
  - La evaluación constante.

ISO 37001: 2016. SISTEMA DE GESTIÓN ANTISOBORNO

- **Primer estándar internacional** sobre Sistemas de Gestión de Cumplimiento
- Mejora normas y estándares nacionales anti-soborno (British Standards 10500 del año 2011)
- **Estándar de alto nivel** que puede integrarse en un sistema de gestión más amplio (ISO 19600) o implementarse de forma independiente
- **Es certificable**
- **Enfoque basado en riesgos**: Identificación, evaluación y seguimiento de los riesgos de soborno


UNE

Norma Española
UNE-ISO 37001
Abril 2017

Sistemas de gestión antisoborno
Requisitos con orientación para su uso

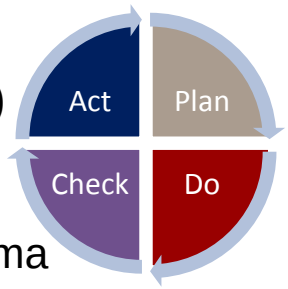
Esta norma ha sido elaborada por el comité técnico CTN 307 *Gestión de riesgos*, cuya secretaría desempeña UNE.

UNE
Asociación Española de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

- Aplicable a cualquier tipo de entidad, sector y tamaño **(principio de proporcionalidad)**
- Requiere el **compromiso del más alto nivel** y obligación de una **política antisoborno**
- Exigencia de una **función de Compliance antisoborno** dotada de recursos

ISO 37001: 2016. SISTEMA DE GESTIÓN ANTISOBORNO

- Establecimiento de procedimientos de **diligencia debida** tanto en las personas de la **organización** como de las relaciones **externas**.
- Desarrollada sobre el **modelo Planificar, Hacer, Verificar y Actual (PDCA)** aplicable a los sistemas de gestión
- **Formación**, **divulgación** y **concienciación** son elementos claves del sistema
- **Actividades de control** en **:**



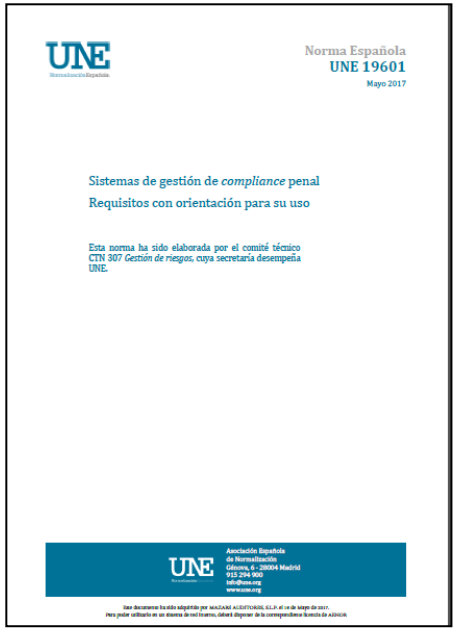
Entorno de Control	Risk assessment	Control actividades	Monitoring	Información y comunicacion
• "Tone at the top"	• Procedimientos de evaluación del riesgo	• Intermediación	• Línea de asesoramiento y canal de denuncias	• Formación
• Cultura Corporativa	• Comunicación de los resultados de la evaluación del riesgos	• Gifts / Hospitality	• Auditoría Interna	• Comunicación
• Código de conducta	• Seguimiento de las medidas de mitigación de riesgos	• Sponsoring	• Control interno	
• Programas anticorrupción		• Política de donaciones	• Gestión incidencias	
• Canal de denuncias		• M&A, JVs		
• Organización del Compliance		• Proveedores y otras partes relacionadas		
		• Viajes a clientes y funcionarios		
		• Costes de formación		
		• Conflictos de interés,		
		• …		

UNE 19601: 2017. SISTEMAS DE GESTIÓN DE COMPLIANCE PENAL

- **Esquema de requisitos para disponer de modelos de organización y gestión penal eficaces (art. 31 bis L.O. 1/2015 Código Penal):**

UNE 19601: 2017. SISTEMAS DE GESTIÓN DE COMPLIANCE PENAL

- **Primer estándar español** sobre Sistemas de Gestión de Compliance Penal
- **Estructura de alto nivel,** alineada a ISO 19600 e ISO 37001 de Compliance y adaptado al Código Penal L.O. 1/2015
- **Aplicación voluntaria**
- **Es certificable**
- Establece **requisitos** para establecer un modelo de prevención penal



PREVENCIÓN **DETECCIÓN** **REACCIÓN**

- *«esta norma **no da una garantía absoluta de eliminación del riesgo** de comisión de delitos que afronta una organización» y «**no asegura la exoneración o atenuación automática** de la responsabilidad penal de la persona jurídica»*

Posibles actuaciones del auditor en materia de compliance

NORMA ISAE (*) – 3000 ENCARGOS DE ASEGURAMIENTO NO AUDITORIA

ISAE 3000: establece los principios y procedimientos básicos para realizar **encargos de aseguramiento distintos de la auditoría** o la revisión de información financiera histórica.

- Aseguramiento de “seguridad razonable”
- Aseguramiento de “seguridad limitada”

En materia de compliance pueden ser utilizados, entre otros, los estándares ISO o UNE:

- Encargos sobre la verificación del cumplimiento normativo de uno o varios criterios de referencia
- Informes de sostenibilidad preparados por la entidad o un tercero
- Encargos destinados a la valoración monetaria de determinados activos u operaciones

(*) Internacional Standard on Assurance Engagements

UN EJEMPO: ESTÁNDAR ALEMAN IDW ASSA 980 (PS 980)

El **estándar IDW AssA 980 (PS 980)** regula en Alemania la auditoría de los modelos de compliance. Este estándar fue publicado en 2011 por el "*Instituto de Censores de Cuentas Alemán"* en relación con los "principios para el desarrollo de los **encargos sobre seguridad razonable en la evaluación de programas de Compliance Management Systems (CMS)**.

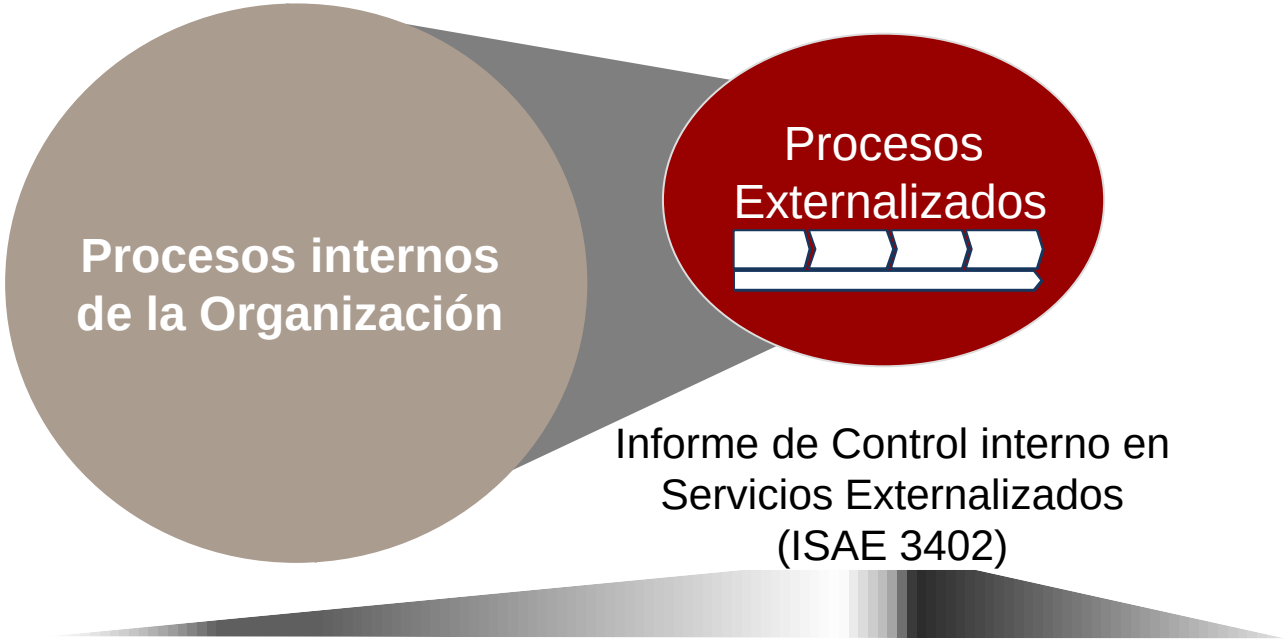
Alcances en la auditoría de los CMS

1. Evaluación del **diseño** del modelo
2. Evaluación del **diseño** + **implementación** del modelo
3. Evaluación del **diseño** + **implementación** + **eficacia** del modelo

Tipos de informes en la auditoría de los CMS

1. **Informe Completo**
2. **Informe Abreviado**

ISAE 3402 ASEGURAMIENTO SOBRE LOS CONTROLES EN LAS ORGANIZACIONES DE SERVICIOS



- **Tecnología**
  - Infraestructura de TI.
  - Desarrollo de sistemas.
  - Soporte tecnológico.
- **Recursos Humanos**
  - Nóminas
- **Contabilidad**
  - Cuentas a cobrar
  - Cuentas a pagar
  - Estados financieros
- **Atención a Clientes**

Informe de Tipo 1

- **Descripción de los controles relevantes** en un momento específico.
- **Opinión** sobre si los **controles** fueron adecuadamente implantados para lograr sus objetivos.
- Ofrece un **"assurance" menor**. Generalmente es utilizado como una etapa anterior de otro informe

Informe de Tipo 2

Tipo 1

+

- **Descripción** de las **pruebas ejecutadas** sobre los controles y resultados obtenidos.
- Mínimo de 6 meses de operación de los controles.

OTRAS POSIBLES ACTUACIONES DEL AUDITOR

- NORMA ISRS (*) – 4400 ENCARGOS DE PROCEDIMIENTOS ACORDADOS

ISRS 4400: **Encargo de procedimientos acordados** en el que se contrata a un auditor para que éste aplique los **procedimientos de auditoría que haya acordado con el cliente** y, en su caso, con terceros interesados, **informando sobre los hechos concretos detectados**.

No se emite opinión profesional al respecto.

- INFORMES PERICIALES

(*) Internacional Standard on Related Services

Principales retos en los modelos de compliance

PRINCIPALES RETOS DE LOS MODELOS DE COMPLIANCE

PRINCIPALES RETOS

1. IMPLEMENTAR UNA CULTURA DE CUMPLIMIENTO Y CONTROL

*"El **objeto** de **los modelos de organización y gestión** no es solo evitar la sanción penal de la empresa sino **promover una verdadera cultura ética corporativa".***

*"Cualquier **programa eficaz** depende del inequívoco **compromiso y apoyo de la alta dirección** para trasladar una **cultura de cumplimiento** al resto de la compañía".*

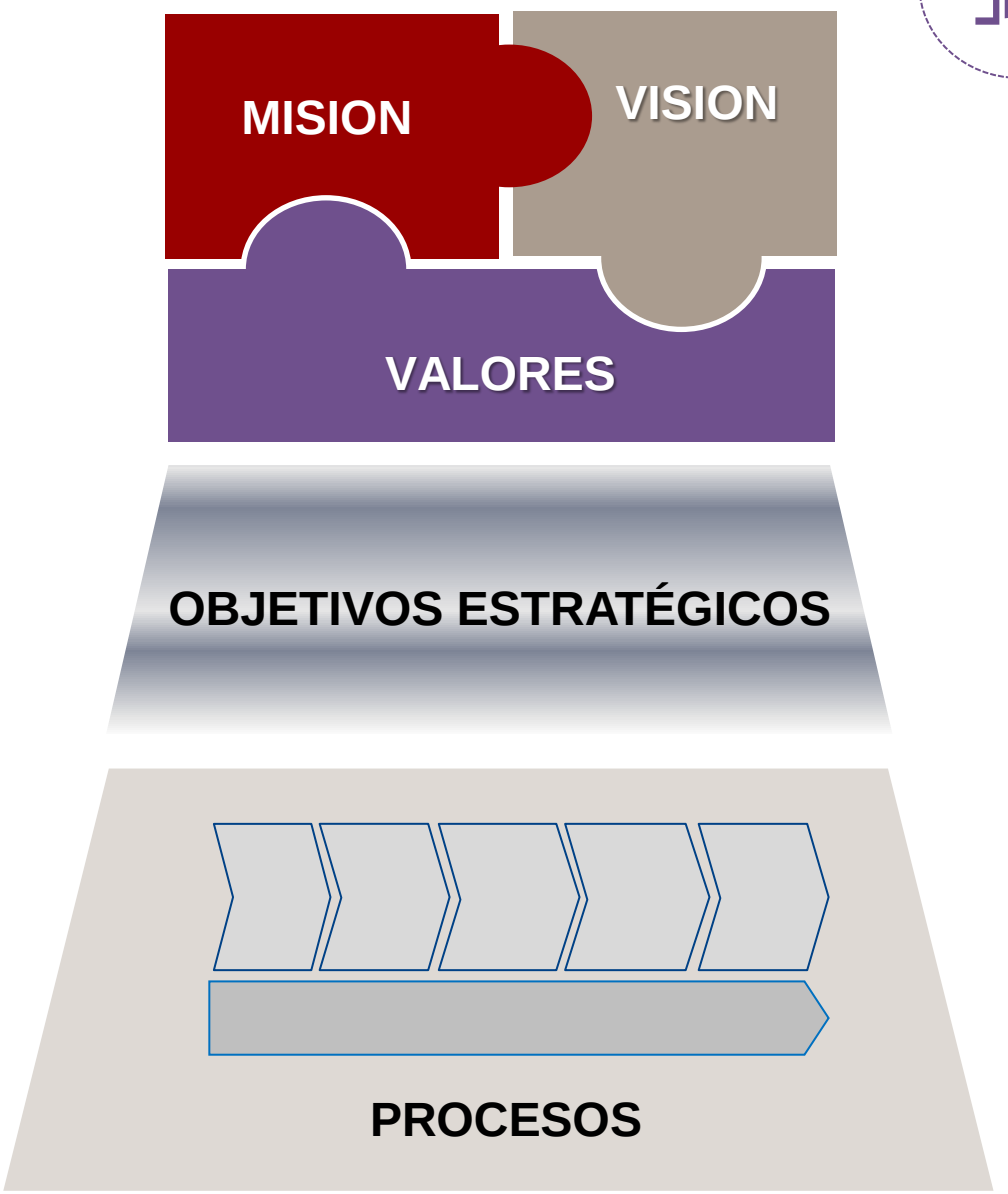
*"…la **elaboración y el cumplimiento de las normas de autorregulación** de las empresas o compliance guide, solo **son relevantes** en la medida en que **traduzcan una conducta**.*

1. IMPLEMENTAR UNA CULTURA DE CUMPLIMIENTO Y CONTROL

Tone from the top

Tone at the middle

Tone at the bottom



1. IMPLEMENTAR UNA CULTURA DE CUMPLIMIENTO Y CONTROL

La **seguridad de la información** se articula sobre **tres dimensiones**, que son los pilares sobre los que aplicar las medidas de protección de la información:

Disponibilidad

Información accesible cuando sea necesaria (denegación de servicio: correos electrónicos,…)

Información correcta y libre de errores (alteración de ficheros en los S.I. intencionado o por existir vulnerabilidad)

Información accesible solo por **personal autorizado** (falta de confidencialidad, accesos sin permisos, divulgación no autorizada, …)

Integridad

Confidencialidad

Inversión en formación en seguridad a los empleados IT

- Seguridad en los sistemas operativos y aplicaciones: políticas de seguridad, gestión vulnerabilidades,...
- Gestión y administración de elementos de seguridad perimetral: cortafuegos, antivirus,…
- Copias de seguridad
- Sistemas de seguridad de los equipos informáticos a nivel de usuario
- Gestión y resolución de incidencias
- Políticas de seguridad sobre soportes extraíbles
- Autentificación, gestión de contraseñas,…
- …

1. IMPLEMENTAR UNA CULTURA DE CUMPLIMIENTO Y CONTROL

Establecer políticas, normas y procedimientos de seguridad

- Manual de Funciones y Obligaciones de los Usuarios de los S.I.

Supervisar el cumplimiento de las buenas prácticas en seguridad

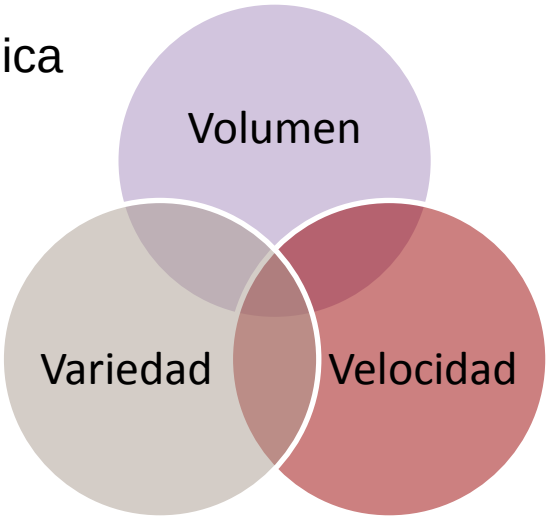
Acciones de divulgación/concienciación en seguridad de usuarios

- Uso de redes wifi
- Uso del correo electrónico
- Prácticas de navegación
- Identificación de virus y malware
- Gestión de contraseñas
- Clasificación de la información
- Borrado de la información
- Uso de dispositivos USB
- Seguridad en dispositivos móviles
- Uso de programas de mensajería instantánea
- Riesgos de las redes sociales
- …

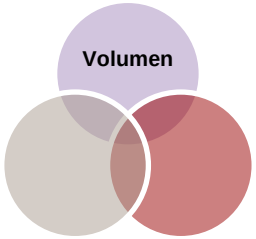
2. HIPERREGULACIÓN: UN *BIG DATA* REGULATORIO

El **entorno regulatorio** para las empresas y sus negocios es en la actualidad excepcionalmente **complejo** y asimila las características de los 3 elementos que definen el **BIG DATA** (3 V's)

- **Volumen** significativo de nuevas normas y adaptaciones de obligado cumplimiento
- Gran **Variedad** de normas y con alta complejidad técnica
- Que evolucionan a una gran **Velocidad**

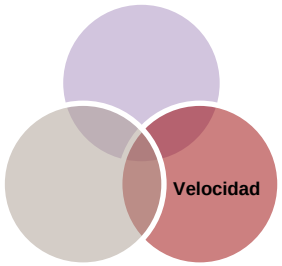


2. HIPERREGULACIÓN: UN *BIG DATA* REGULATORIO

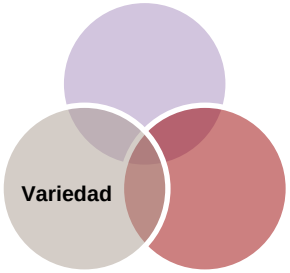


+ 110.000 Número de **normas** (directivas, reglamentos, sentencias, estándares, …) en la **Unión Europa** (*)

+ 40.000 Número de **normas estatales** en España en el período de 1970 – 2017 (*)



+ 1.900 **Actos legislativos por la Unión Europea**(*) en 2017 (reglamentos, directivas y decisiones)



- **Geográfica:** Internacional, Nacional, Local,…
- **Sectorial:** Financiero, Seguros, Farmacéutico, Energético, Químico, …
- **Específica:** Blanqueo, Prevención Riesgos Laborales, GDPR, Privacidad, Competencia, Fiscal, Penal Transparencia, …

(*) CEOE: Estudio Producción normativa 2017

2. AUTORREGULACIÓN EN LOS MODELOS DE COMPLIANCE

Los actuales modelos de compliance inciden en la **autorregulación** y la **responsabilidad proactiva en las empresas**, obligando a éstas a revisar sus procesos, gestionar sus riesgos, establecer normas y procedimientos adaptados a su organización, divulgando e implantando sistemas que evidencien su vigilancia y cumplimiento.

La **autorregulación** en los modelos de compliance requiere un **cambio** en la cultura corporativa en muchas **empresas acostumbradas a normativas legales intervencionistas.**

3. AUMENTO DE RESPONSABILIDAD Y SANCIONES

El alcance e importe de las multas y sanciones, junto con el aumento de las responsabilidades y contingencias de ámbito personal, especialmente a consejeros y también a directivos, seguirán aumentando (Ley Sociedades de Capital, LO 1/2015, GDPR,…)

Ejemplo

ANTIGUA NORMATIVA LOPD

La **función sancionadora** de la **AEPD** era ejercida en función de:

Tipos de Infracciones	Tipos de Sanciones
Leves	900 € a 40.000 €
Graves	40.001 € a 300.000 €
Muy Graves	300.001 € a 600.000 €

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RGPD / GDPR

Elevado aumento de multas dependiendo del incumplimiento:

Tipos de Infracciones	Tipos de Sanciones
Nivel I	10 Millones como máximo o 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Siempre optándose por la mayor cuantía.
Nivel II	20 Millones como máximo o 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Siempre optándose por la mayor cuantía.

4. UN ENFOQUE BASADO EN LA GESTIÓN DE RIESGOS INTEGRAL

- Los modelos de Compliance ponen en énfasis en la evaluación de los riesgos relacionados, implementando los controles necesarios a todos los niveles (Entity Level Controls / Process Level Control).

- Una acción coordinada de la Governanza, Gestión de Riesgos y Cumplimiento (GRC) es necesaria para garantizar, sobre los fundamentos de buenas prácticas, el desarrollo de los negocios.

4. UN ENFOQUE BASADO EN LA GESTIÓN DE RIESGOS INTEGRAL

El modelo de las **Tres Líneas de Defensa** (*) distingue tres tipos de funciones que participan en una efectiva gestión de riesgos integral:

(*) Fuente: Institutes of Internal Auditors

5. EVALUACIÓN DE TERCEROS O "SOCIOS DE NEGOCIO"

- La empresa debe **implantar procesos de revisión de diligencia debida sobre terceros** con los que tiene o prevé tener, algún tipo de relación de negocios

- El **nivel** de diligencias debe de ser **adaptado al perfil de riesgo** del tercero en cuestión.

- Los **procesos de revisión de diligencia debida** deben estar **documentados** y permitir:
  - identificar a los beneficiarios finales,
  - los riesgos en materia de imagen y de reputación,
  - los posibles litigios o casos en los que se les pueda pedir responsabilidades a las empresas y
  - elaborar un mapa de terceros y sus relaciones de negocio para identificar posibles conflictos de intereses.

5. EVALUACIÓN DE TERCEROS O "SOCIOS DE NEGOCIO"

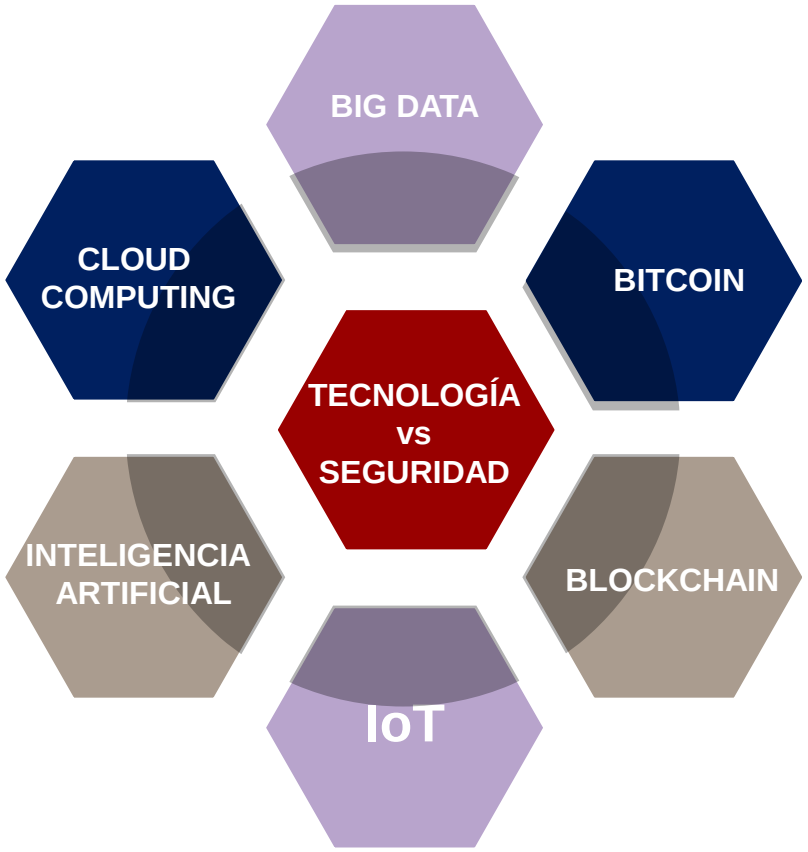
- A modo de ejemplo, el establecimiento de una relación de **externalización de servicios IT** exigiría que con la contratación se asegure la correcta prestación del servicio y de una perfecta coordinación. El contrato debería recoger los siguientes aspectos:
  - Descripción de los productos a recibir, niveles de cumplimiento y niveles de servicio a mantener y penalizaciones si no se alcanzan.
  - Responsabilidades y elementos de relación para gestionar el proceso.
  - Procedimientos para someter a continua revisión el contenido y alcance de las actividades objeto del contrato.
  - Mecanismos que aseguren la continuidad del servicio en caso de rescisión.

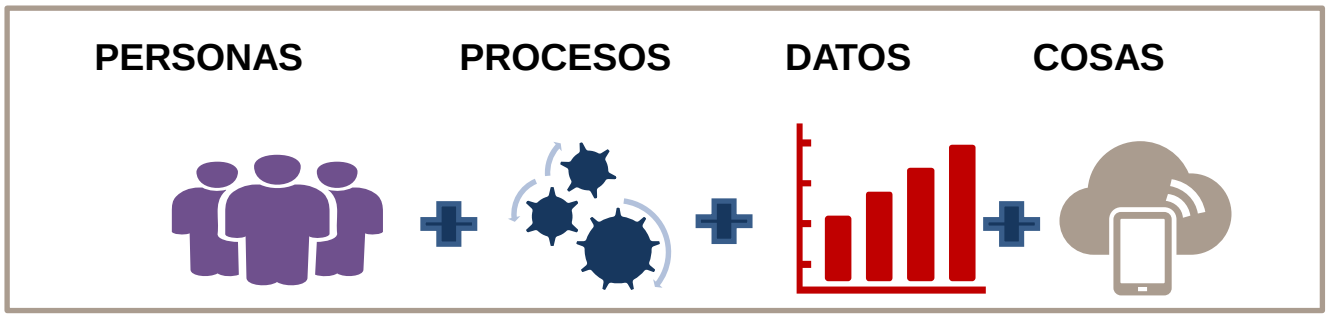
6. EL COMPLIANCE COMO VENTAJA COMPETITIVA

- La disposición y, en mayor medida, la certificación de modelos de compliance eficaces en las organizaciones, previsiblemente, serán en el futuro un elemento fundamental para el desarrollo de los negocios.

- Todo ello conlleva el reto de integrar en las organizaciones una verdadera cultura ética corporativa que busque la excelencia en las relaciones **(enfoque proactivo),** más allá de un formal cumplimiento normativo **(enfoque reactivo)**.

7. TECNOLOGÍA Y SEGURIDAD





7. TECNOLOGÍA Y SEGURIDAD

CIBERSEGURIDAD vs SEGURIDAD DE IT

Los **ciberataques** se han **incrementado de forma muy significativa** en los últimos años, siendo cada día más complejos de prevenir y detectar, y requieren:

- promover la cultura de la seguridad
- mayores medidas de seguridad en los sistemas de información,
- incrementar la prevención en medidas de ciberseguridad y resilencia,
- aumentar los esfuerzos en la gestión de sus riesgos

+ 140 % **en dos años**(*)

2017

120.000

2014

18.000

número incidentes registrados (INCIBE)(*)

77 % **de las empresas no tiene un plan de respuesta ante ciberataques, según un estudio de IBM**

(*) Datos INCIBE 2017 ataques por internet en España

7. TECNOLOGÍA Y SEGURIDAD

CIBERSEGURIDAD vs SEGURIDAD DE IT

CIBERSEGURIDAD

ENFOQUE PREVENTIVO

- Desarrollo de una **estrategia global de seguridad**
- **Monitorización** y **vigilancia** de la **seguridad**
- **Gestión** de las amenazas de manera **proactiva**
- **Coordinación** e intercambio de **información**
- **Personal** dedicado y **experto**
- **Formación** y **concienciación de personal**

SEGURIDAD IT

- **Controles centrados** en el **cumplimiento normativo**
- **Compliance técnico** con auditorías y estándares
- **Escaso análisis de amenazas externas**. Foco casi exclusivo en el personal interno
- **Análisis** de logs y **eventos** de **seguridad**, únicamente **tras sufrir incidentes** o ataques relevantes

ENFOQUE REACTIVO

Fuente: Instituto de Auditores Internos de España. Ciberseguridad. Una guía de supervisión

7. TECNOLOGÍA Y SEGURIDAD

CIBERSEGURIDAD vs SEGURIDAD DE IT

- Las organizaciones son cada vez más conscientes del **riesgo creciente de brechas de seguridad en sus redes**:
  - **Múltiples puntos de entrada.**
  - Crecimiento de **redes compleja** y su administración cada vez más **complicada**.
  - Las herramientas de **hacking** se han **automatizado** y requieren de menos conocimientos para su uso (aumento de hackers, más ataques y más dañinos).
  - El **número de vulnerabilidades** que pueden ser explotadas está en **aumento**.
  - La **reducción de los ciclos de vida** de **desarrollo de software** han resultado en productos de baja calidad: expone a los usuarios a mayores riesgos y vulnerabilidades ocultas.

Para ello deben considerar proyectos de **análisis de vulnerabilidades** (puertos abiertos, parches de seguridad, etc.) y aplicar, en su caso, test de intrusión

7. TECNOLOGÍA Y SEGURIDAD

BUENAS PRÁCTICAS EN CIBERSEGURIDAD Y SEGURIDAD

- **Normas ISO relacionadas**
  - ISO 27302 . Estándar de ciberseguridad
  - ISO 27014 “Gobierno de la seguridad de la información”
  - Conjunto ISO 27000, entre las que destacan entre otras:
    - ISO 27001 “Estándar para la seguridad de la información”.
    - ISO 27002 “Código de buenas prácticas para la gestión de seguridad de la información”
    - ISO 27003 “Directrices para la implantación de un SGSI”
    - ISO 27004 “Métricas para la gestión de la seguridad de la información”
    - ISO 27005 “Gestión de riesgos en seguridad de la información”.
- **Nacional Institute of Standards and Technology - NIST 02-2014. Marco para mejorar la ciberseguridad**

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
• Gestión de activos • Entorno de negocio • Gobierno • Análisis de riesgos • Estrategia de gestión	• Control de acceso • Formación y concienciación • Seguridad de los datos • Protección de la información • Mantenimiento • Tecnologías de protección	• Anomalías y eventos • Monitorización continua • Procesos de detección	• Plan de respuesta • Comunicaciones • Mitigación	• Plan de recuperación • Análisis • Mejoras

8. INTEGRACIÓN CON OTRAS ÁREAS DEL COMPLAINCE OFFICER

- Es esencial **promover la cultura corporativa** de compliance en las áreas de gestión operativa por parte del Compliance Officer requiriendo competencias muy diversas que requieren, en muchos casos, de **soporte externo**

- La función de cumplimiento normativo debe tener una conocimiento del negocio y transversal con:
  - Visión estratégica
  - Enfoque de riesgos
  - Liderazgo
  - Integridad y actuación ética
  - Independencia

CONCLUSIÓN

La función de compliance debe integrarse de forma transversal y ayudar a implementar una cultura ética empresarial en todos los niveles organizativos, incluyendo los servicios externalizados

Se seguirán ampliando las exigencias en responsabilidad para las organizaciones, sus responsables de gobierno y dirección, con una mayor exposición al riesgo de sanciones

Implementar enfoques proactivos en compliance resulta imprescindible para minimizar los riesgos en seguridad ante la actual "revolución" tecnológica

El aumento de la regulación y su complejidad, requerirán esfuerzos importantes de formación y divulgación, especialmente, en el entorno de la seguridad

MUCHAS GRACIAS