Fundación General UGR-Empresa

RESPONSIA Cumplimiento Legal

CURSO SUPERIOR EN CORPORATE COMPLIANCE. I EDICIÓN

Módulo IV. Control de riesgos en la empresa (I) -Modelos GRC-

Fundación General UGR-Empresa

PREVISIONES ESPECIALES

Ponente: David García Vega

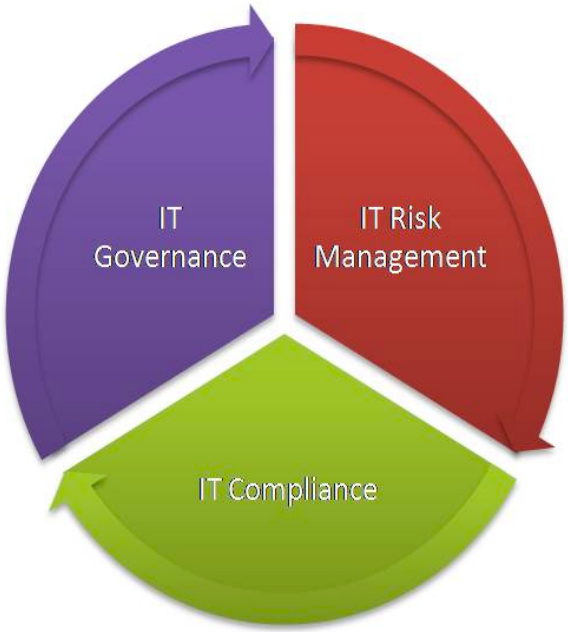
Economista-Auditor de Cuentas.
Miembro de Responsia Compliance, S.L.
Docente Master de Post-Grado Contabilidad y Auditoría de Cuentas UGR y UCA.

DEFINICIÓN

GRC se puede entender como una **rama de la gestión de las organizaciones** que permite **integrar las Tecnologías de la Información** junto con los marcos regulatorios y legisla vos, en la **estrategia corporativa.**

La filosofía de la gestión GRC permite realizar **un tratamiento integrado** sobre las áreas de Gobierno (Governance), Gestión de Riesgos (Risk-Management) y Gestión del Cumplimiento (Compliance).

estas tres áreas, dentro de la Organización, dejan de considerarse de forma separada para integrarse dentro de **una única visión de la gestión empresarial.**



OBJETIVOS

Gobierno

Responsabilidad de la Dirección en la gestión y transparencia en la organización, garantizando la implantación y adhesión a las polícas definidas **(LIDERAZGO).**

Gestión de Riesgos

Mecanismos de identificación, análisis y evaluación de las amenazas que impliquen riesgos para el logro de los obje vos de la organización, y planicación y seguimiento de las actividades o proyectos encaminados a la reducción del riesgo.

Gestión del Cumplimiento

Mecanismos de identificación de la legislación y regulación vigente aplicable y de verificación de su cumplimiento, considerando tanto **normas externas como internas.**

OBJETIVOS

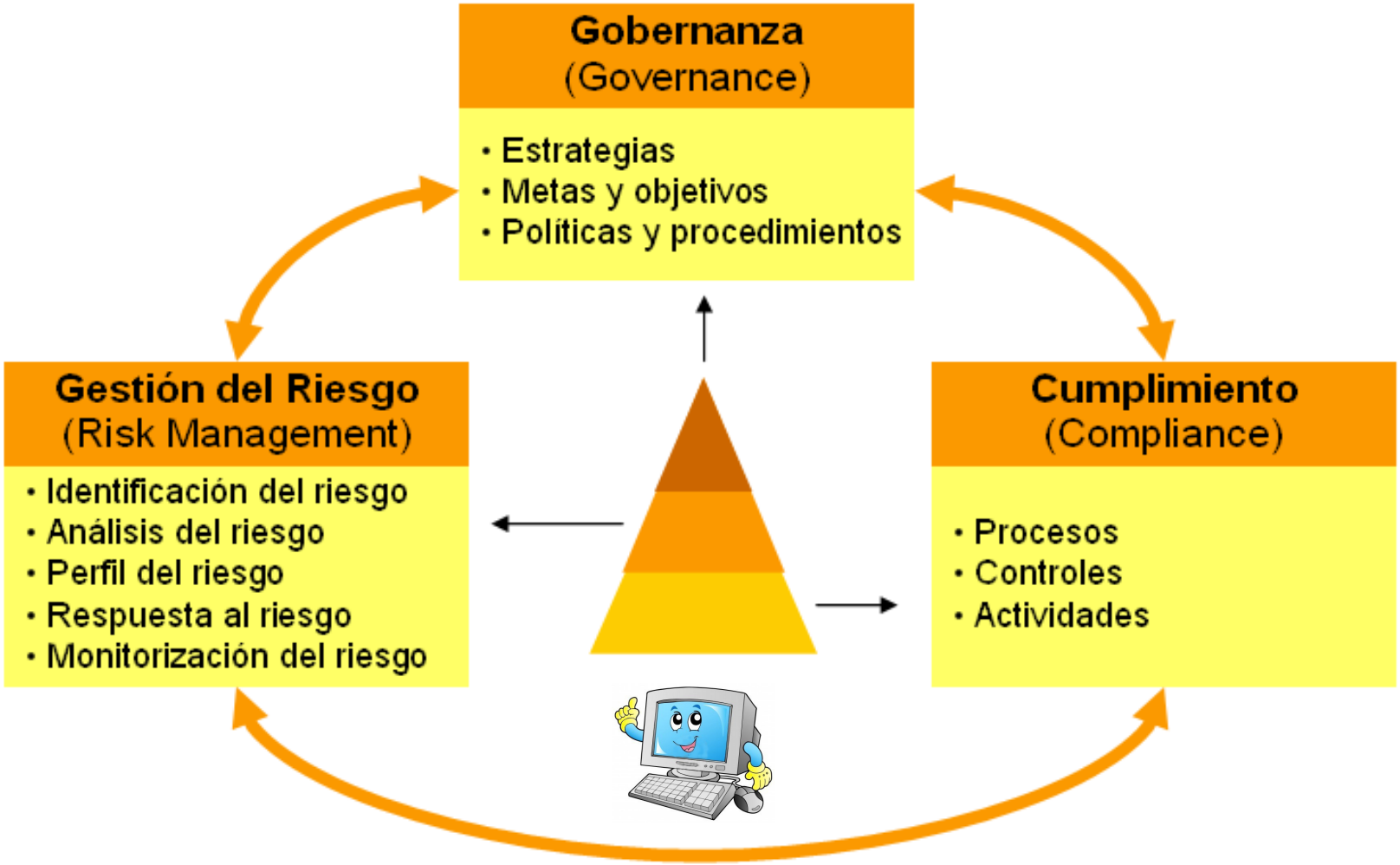
Control

Las políticas, procedimientos, prácticas y estructuras organizacionales para proporcionar seguridad razonable de que los objetivos organizacionales se alcanzarán y que los eventos no deseados se evitarán o detectarán y corregirán.

Objetivo de control

Una declaración de que el resultado o propósito deseado se alcanzará al implantar mecanismos de control en una actividad particular de tecnología de información

PROCESO


Gobernanza
(Governance)
• Estrategias
• Metas y objetivos
• Políticas y procedimientos
Gestión del Riesgo
(Risk Management)
• Identificación del riesgo
• Análisis del riesgo
• Perfil del riesgo
• Respuesta al riesgo
• Monitorización del riesgo
Cumplimiento
(Compliance)
• Procesos
• Controles
• Actividades

¿POR QUÉ IR A UNA FILOSOFÍA DEL GRC PARA ELABORAR COMPLIANCE?

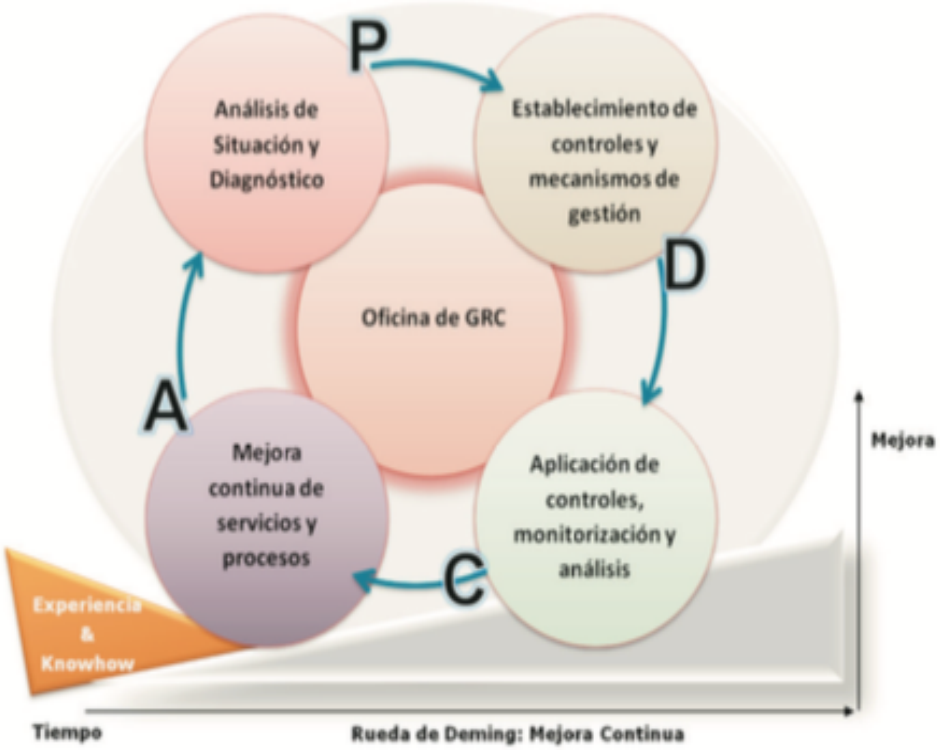
A medida que las organizaciones crecen en complejidad y tamaño, resulta más evidente la importancia de contar con una estructura adecuada en que cada nivel tome las decisiones para las que ha sido diseñado.

El buen gobierno permite controlar y mejorar los niveles de servicio, reducir los riesgos y mejorar los costes de los Servicios ofrecidos cumpliendo con el marco regulatorio y legal aplicable. Si el GRC está bien diseñado e implantado, se consigue una mayor calidad de servicios y gestión, facilitando el logro de los objetivos definidos y **optimizando los costes afrontados.**

¿CÓMO INTEGRAR EL GOBIERNO CORPORATIVO, LA GESTIÓN DE RIESGOS Y LA GESTIÓN DEL CUMPLIEMINTO?

No resulta sencillo implantar este modelo, como ocurre con cualquier mejora en el ámbito de la gestión corporativa.

Por ello, resulta recomendable definir **una unidad** que se encargue de implementar GRC a partir de la gestión multidisciplinar pero de manera centralizada. Es la **oficina GRC**, construida como un **centro de competencia** especializado.




GOBIERNO, RIESGO, CUMPLIMIENTO (GRC)
Líneas de Actividad
Resiliencia Organizacional
• Sistema de Gestión Integrado (SGI)
• Continuidad de Negocio (SGCN)
• Gestión del Riesgo
• Seguridad Física
• Protección de Infraestructuras Críticas (LPIC)
Cumplimiento Normativo
• Desarrollo del Marco Normativo
• Modelo Unificado de Controles (MUC)
• Adecuaciones y Auditorías regulatorias /estándares
• Payment Card Industry (PCI)
• Seguridad en la Nube
Inteligencia y Fraude
• Detección y Prevención del Fraude
• Vigilancia de Ciberamenazas
• Data Leak/Loss Prevention (DLP)
• Vigilancia de Reputación On-line
Formación y Concienciación
• Diseño de planes de Formación y Concienciación.
• Formación especializada (Seguridad de la Información, Contra Inteligencia, Reputación, etc..)

BASILEA

Los Acuerdos de Basilea se refieren a un conjunto de propuestas que forman el marco regulador internacional para bancos, siendo **Basilea III** la primera revisión de **Basilea II**, luego de la crisis financiera de 2008 debido al crecimiento excesivo de los valores presentados en los balances de los bancos.

Las decisiones de negocios deben hacerse con base en la gestión de riesgos:

- Riesgos de Mercado
- Riesgos de Crédito
- Riesgo de Contraparte
- Riesgos de liquidez
- Riesgos Operacionales
- Riesgos Legales
- Riesgos Tecnológicos

Fortalecer la regulación, supervisión y gestión de riesgos del sector bancario. Estas medidas persiguen:

- Mejorar la capacidad del sector bancario para afrontar perturbaciones ocasionadas por tensiones financieras o económicas de cualquier tipo
- Mejorar la gestión de riesgos y el buen gobierno en los bancos
- Reforzar la transparencia y la divulgación de información de los bancos.

TIPOS DE GOBIERNO

- Existen diferentes tipos de gobierno:
  - Gobierno Corporativo.
  - Gobierno de Proyectos.
  - Gobierno de Tecnologías de Información.
  - Gobierno Ambiental.
  - Gobierno Económico y Financiero.
- Cada tipo tiene una o más fuentes de orientación, cada uno con objetivos similares pero con frecuencia varían términos y las técnicas para su realización.

FORMA DE IMPLEMENTACIÓN

- La integración de la aplicación de las actividades de GRC dentro de una empresa requiere un enfoque sistémico para el eficaz logro de los objetivos empresariales de sus grupos de interés.
- Estos enfoques se basan normalmente en facilitadores de diversos tipos (por ejemplo, los principios, las políticas, modelos, marcos, estructuras organizacionales).

EJEMPLO MODELO DE GRC

8 COMPONENTES INTEGRADOS

8 RESULTADOS UNIVERSALES

- Lograr los objetivos del negocio
- Mejorar la cultura organizacional
- Aumentar la confianza de stakeholders
- Preparar y proteger a la entidad
- Evitar, detectar y reducir la adversidad
- Motivar e inspirar las conductas deseadas
- Mejorar la capacidad de respuesta y eficiencia
- Optimizar valor económico y social

GOBIERNO CORPORATIVO & TECNOLOGIA DE LA IFORMACIÓN

Alcance

Este estándar establece los principios rectores para directores de organizaciones (incluyendo propietarios, miembros del consejo, directores, socios, ejecutivos de alto nivel, o similar) sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI) dentro de sus organizaciones.

Esta norma se aplica a la gestión de los procesos de gestión **(toma de decisiones)** relativas a los servicios de información y comunicación utilizados por una organización. Estos procesos pueden ser controlados por especialistas en TI dentro de la organización o de los proveedores de servicios externos, o por unidades de negocio dentro de la organización.

GOBIERNO CORPORATIVO & TECNOLOGIA DE LA IFORMACIÓN

Principios

- Responsabilidad
- Estrategia
- Adquisición
- Desempeño
- Conformidad
- Comportamiento Humano

Modelo

Los administradores debe gobernar las TI a través de tres tareas principales:
a) Evaluar el uso actual y futuro de TI.
b) Preparación directa y la aplicación de planes y políticas para garantizar que el uso de las TI cumple con los objetivos de negocio.
c) Monitorear la conformidad de las políticas, y el desempeño contra los planes.

GOBIERNO CORPORATIVO & TECNOLOGIA DE LA IFORMACIÓN

Principios

- Responsabilidad
- Estrategia
- Adquisición
- Desempeño
- Conformidad
- Comportamiento Humano

Modelo

Los administradores debe gobernar las TI a través de tres tareas principales:
a) Evaluar el uso actual y futuro de TI.
b) Preparación directa y la aplicación de planes y políticas para garantizar que el uso de las TI cumple con los objetivos de negocio.
c) Monitorear la conformidad de las políticas, y el desempeño contra los planes.

APLICACIÓN DEL CUMPLIMIENTO

GRC

Aspectos legales y económicos

RIESGOS DE CUMPLIMIENTO

GRC

RIESGOS

- Definir tipos de riesgos
- Identificar riesgos asociados
- Establecer parámetros de medición
- Elegir una metodología de tratamiento
- Analizar y evaluar riesgos
- Crear un Plan de Mitigación

NEGOCIO

- Identificar procesos
- Analizar entorno regulatorio
- Analizar cultura interna
- Analizar madurez operativa
- Analizar entorno documental

MATRIZ DE RIESGO

DIRECTORIO

ISACA®
Trust in, and value from, information systems

COBIT®

Control

OBjectives

for **I**nformation**a**nd Related **T**echnology

(Objetivos de Control para Tecnología de Información y Tecnologías relacionadas)

Fuente: Control Objectives for Information and Related Technology (CObIT)

Definición

Es un marco de control interno de TI. Parte de la premisa de que la TI requiere proporcionar información para lograr los objetivos de la organización.
Promueve el enfoque y la propiedad de los procesos.

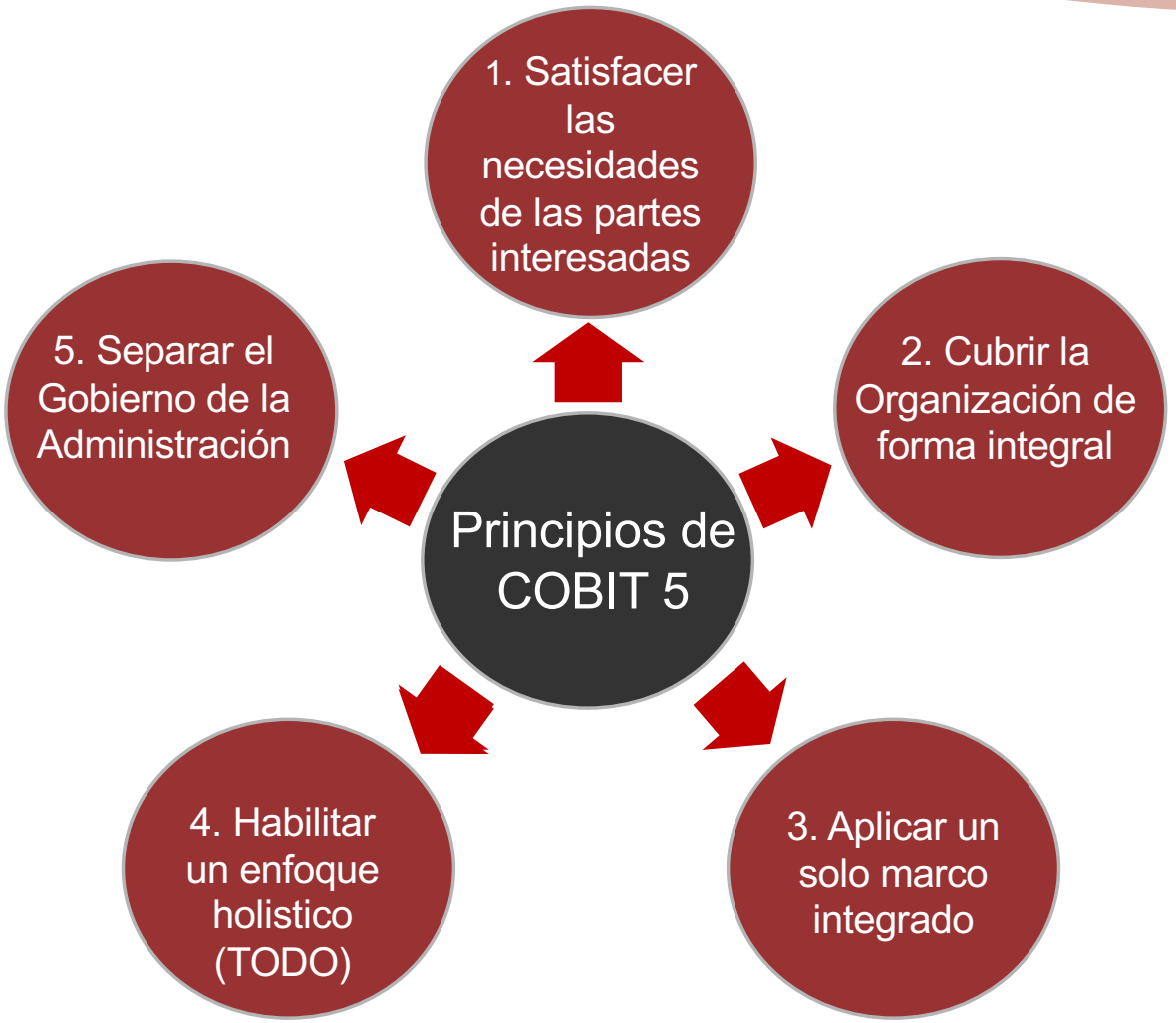
Apoya a la organización al proveer un marco que asegura que:

- La Tecnología de Información (TI) esté alineada con la misión y visión.
- LA TI capacite y maximice los beneficios.
- Los recursos de TI sean usados responsablemente.
- Los riesgos de TI sean manejados apropiadamente

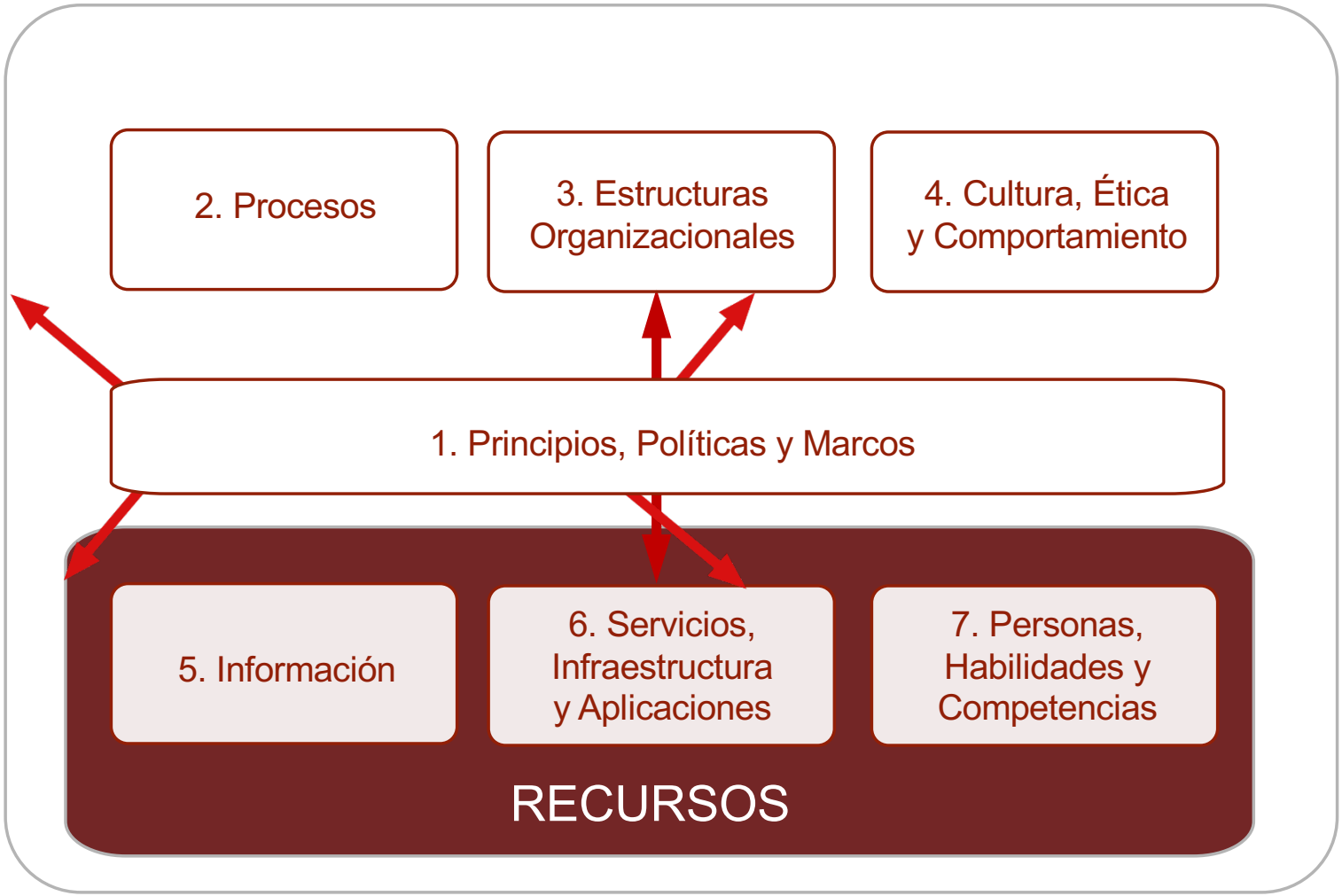
COBIT 5 reúne a los **cinco principios** que permiten a la empresa de construir una **gobernabilidad** efectiva y un marco de **gestión** basado en un conjunto holístico de **siete facilitadores** que optimiza la **información** y la inversión en **tecnología** y el uso para el beneficio de las partes interesadas.

COBIT 5 ayuda a las empresas a crear valor óptimo de TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos.
COBIT 5 permite que la información y la tecnología relacionada para ser gobernado y administrado de manera integral para el conjunto de la empresa, teniendo en el pleno de extremo a extremo del negocio y áreas funcionales de responsabilidad, teniendo en cuenta los intereses relacionados con la TI de grupos de interés internos y externos.
Los **principios** y los **facilitadores** de COBIT 5 son de carácter genérico y útil para las empresas de todos los tamaños, ya sea comercial, sin fines de lucro o en el sector público.

Los Principios de COBIT 5



HABILITADORES DEL COBIT



USUARIOS COBIT

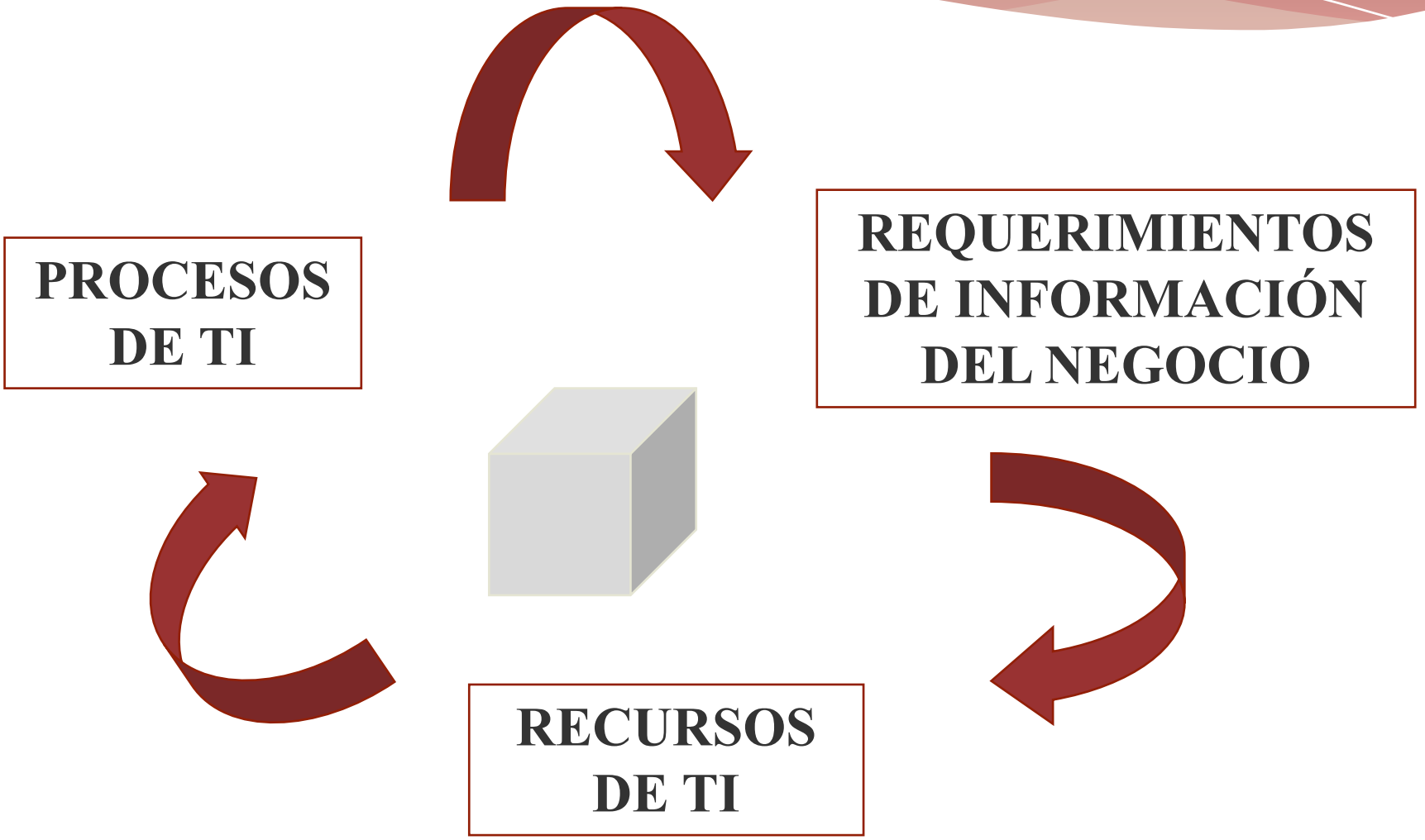
Gerencia: Apoyar decisiones de inversión en TI y control sobre su rendimiento, así como analizar el costo-beneficio del control.

Usuarios Finales: Garantizar seguridad y control de los productos que adquieren interna y externamente

Auditores : Apoyar sus opiniones sobre los controles de los proyectos de TI , su impacto en la organización y el control mínimo requerido.

Responsables de TI: Identificar los controles que requieren.

PRINCIPIOS DEL COBIT



ESTRUCTURA COBIT

EVENTOS

Objetivos de negocio
Oportunidades de negocio
Requerimientos externos
Regulación
Riesgos

INFORMACIÓN

Efectividad
Eficiencia
Confidencialidad
Integridad
Disponibilidad
Cumplimiento
Confiabilidad

Cobit - Estructura

Procesos del Negocio

Lo que usted Obtiene

Lo que Usted Necesita

Información

Criterios

Efectividad
Eficiencia
Confidencialidad
Integridad
Disponibilidad
Cumplimiento
Confiabilidad

Recursos de TI

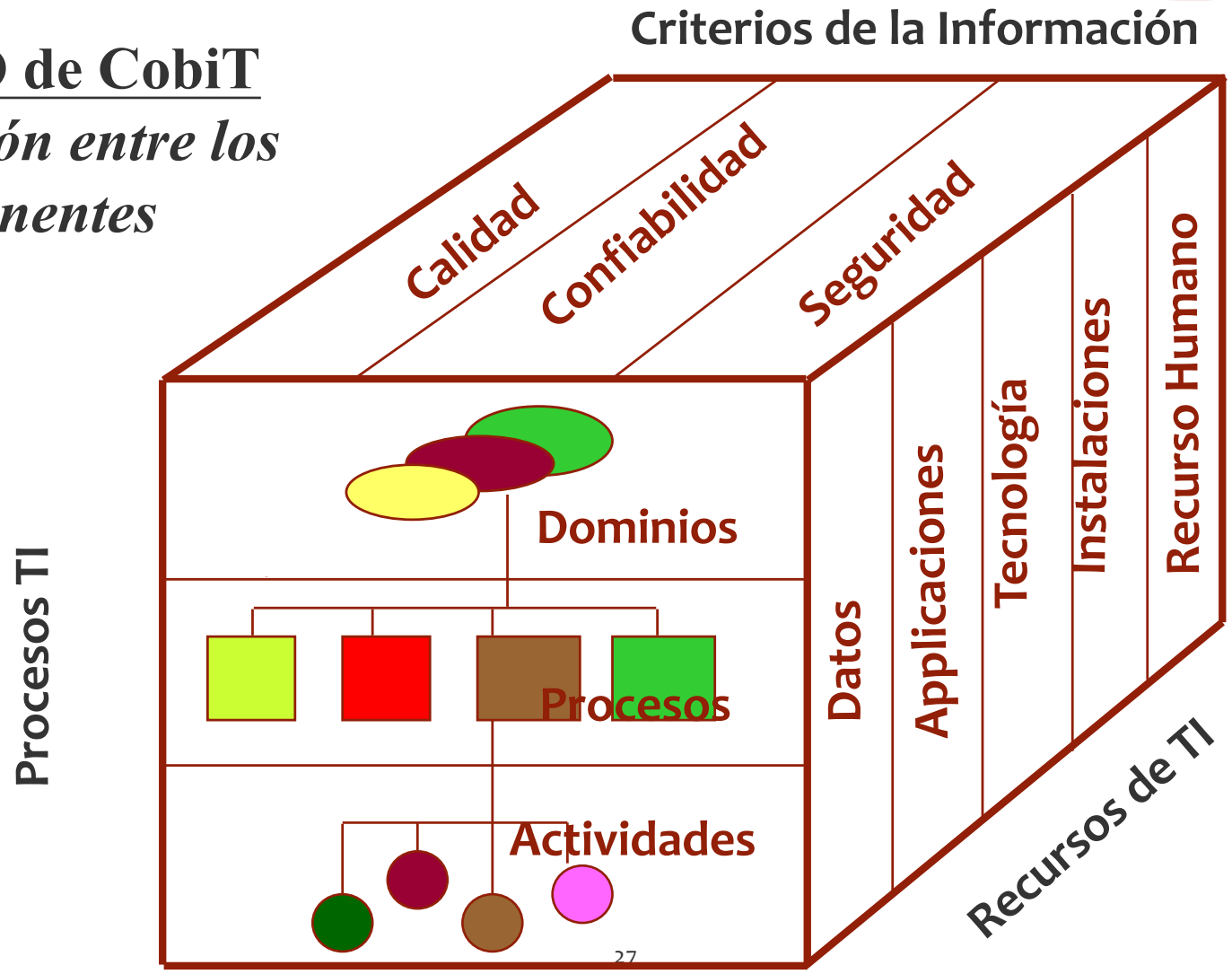
Datos
Aplicaciones
Tecnología
Instalaciones
Recurso Humano

Concuerdan ?

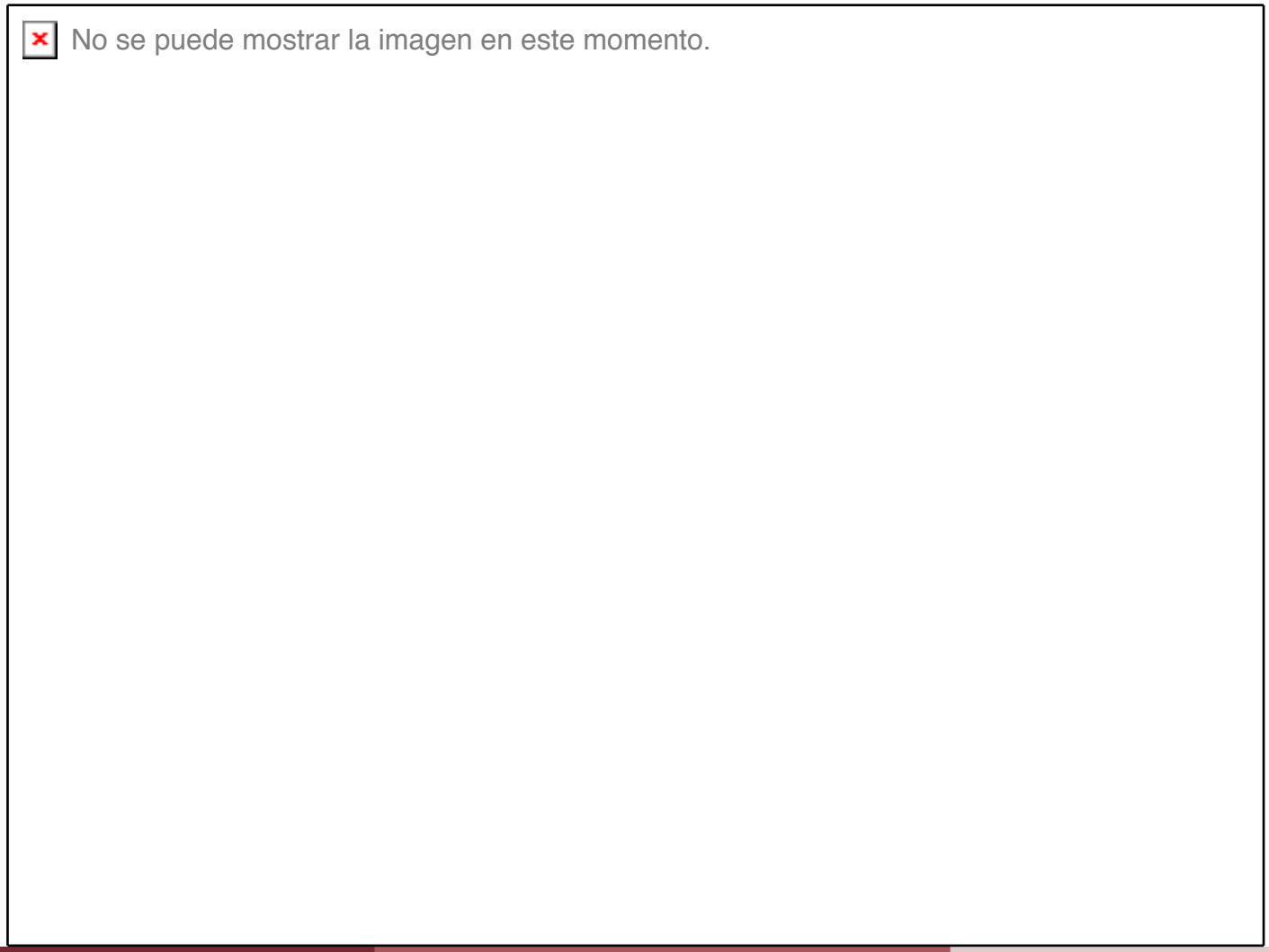
RESPONSIA
Cumplimiento Legal

CUBO de CobiT

Relación entre los componentes




No se puede mostrar la imagen en este momento.


No se puede mostrar la imagen en este momento.

Cobit - Requerimientos de la Información del Negocio

- **Efectividad:** Información relevante y pertinente, proporcionada en forma oportuna, correcta, consistente y utilizable
- **Eficiencia:** Empleo óptimo de los recursos.
- **Confidencialidad:** Protección de la información sensitiva contra divulgación no autorizada
- **Integridad:** Información exacta y completa, así como válida de acuerdo con las expectativas de la organización.

Cobit - Requerimientos de la Información del Negocio

- **Disponibilidad**: accesibilidad a la información y la salvaguarda de los recursos y sus capacidades.
- **Cumplimiento:** Leyes, regulaciones y compromisos contractuales.
- **Confiabilidad:** Apropiada para la toma de decisiones adecuadas y el cumplimiento normativo.

Recursos de TI

- **Datos**: Todos los objetos de información interna y externa, estructurada o no, gráficas, sonidos, etc.
- **Aplicaciones**: Sistemas de información, que integran procedimientos manuales y sistematizados.
- **Tecnología**: Hardware y software básico, sistemas operativos, de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- **Instalaciones**: Recursos necesarios para alojar y dar soporte a los sistemas.
- **Recurso Humano** :Habilidad, actitud y productividad del personal.


No se puede mostrar la imagen en este momento.

Planeación y Organización

- Definición de un plan estratégico
- Definición de la arquitectura de información
- Determinación de la dirección tecnológica
- Definición de organización y relaciones
- Administración de la inversión
- Comunicación de las políticas
- Administración de los recursos humanos
- Asegurar el cumplimiento con los requerimientos Externos
- Evaluación de riesgos
- Administración de proyectos
- Administración de la calidad

Adquisición e Implantación

- Identificación de soluciones automatizadas
- Adquisición y mantenimiento del software aplicativo
- Adquisición y mantenimiento de la infraestructura tecnológica
- Desarrollo y mantenimiento de procedimientos
- Instalación y aceptación de los sistemas
- Administración de los cambios

Servicios y Soporte

- Definición de los niveles de servicios
- Administración de los servicios de terceros
- Administración de la capacidad y rendimientos
- Aseguramiento del servicio continuo
- Aseguramiento de la seguridad de los sistemas
- Entrenamiento a los usuarios
- Identificación y asignación de los costos
- Asistencia y soporte a los clientes
- Administración de la configuración
- Administración de los problemas
- Administración de los datos
- Administración de las instalaciones
- Administración de la operación

Seguimiento

- Seguimiento de los procesos
- Evaluación del control Interno
- Contratación de un aseguramiento independiente

RESUMEN

- El marco COBIT 5 incluye la orientación necesaria para apoyar los objetivos de GRC de la empresa y actividades de apoyo:
  - Actividades de gobierno relacionadas a GEIT (5 procesos)
  - Procesos de gestión de riesgos y apoyo para la gestión de riesgos a través del espacio GEIT
  - Cumplimiento: un enfoque específico en las actividades de cumplimiento en el marco y cómo encajan dentro de la imagen completa de la empresa
- La inclusión de los acuerdos de GRC en el marco de negocio para GEIT ayuda a las empresas a evitar el problema principal con soluciones GRC -silos de actividad!

MUCHAS GRACIAS POR SU ATENCION

David García Vega
Economista Auditor
David.garcia@responsia.es