



**UTPL**  
*La Universidad Católica de Loja*

Modalidad Abierta y a Distancia



# Gobernanza de Tecnologías de la Información

Guía didáctica

## Facultad de Ingenierías y Arquitectura

### Departamento de Ciencias de la Computación y Electrónica

---

## Gobernanza de Tecnologías de la Información

### Guía didáctica

Carrera	PAO Nivel
▪ <i>Tecnologías de la información</i>	IX

### Autoras:

Torres Aguilar Yadira Margarita  
Riofrío Pérez Blanca Cecilia



D S O F \_ 4 0 8 1

Asesoría virtual  
[www.utpl.edu.ec](http://www.utpl.edu.ec)

## **Universidad Técnica Particular de Loja**

### **Gobernanza de Tecnologías de la Información**

#### **Guía didáctica**

Torres Aguilar Yadira Margarita

Riofrío Pérez Blanca Cecilia

#### **Diagramación y diseño digital:**

Ediloja Cía. Ltda.

Telefax: 593-7-2611418.

San Cayetano Alto s/n.

[www.ediloja.com.ec](http://www.ediloja.com.ec)

[edilojacialtda@ediloja.com.ec](mailto:edilojacialtda@ediloja.com.ec)

Loja-Ecuador

ISBN digital - 978-9942-39-470-5



#### **Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0)**

Usted acepta y acuerda estar obligado por los términos y condiciones de esta Licencia, por lo que, si existe el incumplimiento de algunas de estas condiciones, no se autoriza el uso de ningún contenido.

Los contenidos de este trabajo están sujetos a una licencia internacional Creative Commons **Reconocimiento-NoComercial-CompartirIgual 4.0** (CC BY-NC-SA 4.0). Usted es libre de **Compartir – copiar y redistribuir el material en cualquier medio o formato. Adaptar – remezclar, transformar y construir a partir del material citando la fuente, bajo los siguientes términos: Reconocimiento- debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios.** Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciatario. **No Comercial-no puede hacer uso del material con propósitos comerciales. Compartir igual-Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la misma licencia del original.** No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia. <https://creativecommons.org/licenses/by-nc-sa/4.0/>

# Índice

<b>1. Datos de información.....</b>	<b>8</b>
1.1. Presentación de la asignatura .....	8
1.2. Competencias genéricas de la UTPL .....	8
1.3. Competencias específicas de la carrera.....	8
1.4. Problemática que aborda la asignatura.....	9
<b>2. Metodología de aprendizaje.....</b>	<b>9</b>
<b>3. Orientaciones didácticas por resultados de aprendizaje .....</b>	<b>10</b>
<b>Primer bimestre.....</b>	<b>10</b>
<b>Resultado de aprendizaje 1.....</b>	<b>10</b>
Contenidos, recursos y actividades de aprendizaje .....	10
<b>    Semana 1 .....</b>	<b>10</b>
<b>        Unidad 1. Conceptos fundamentales .....</b>	<b>10</b>
1.1. Gobernanza Corporativa .....	11
1.2. Gobernanza de TI .....	13
Actividades de aprendizaje recomendadas .....	15
<b>        Semana 2 .....</b>	<b>15</b>
Actividades de aprendizaje recomendadas .....	21
Autoevaluación 1.....	22
<b>        Semana 3 .....</b>	<b>25</b>
<b>        Unidad 2. Gobernanza empresarial y herramientas GRC.....</b>	<b>25</b>
2.1. Principios GRC.....	28
2.2. Gobernanza GRC .....	30
Actividades de aprendizaje recomendadas .....	33
<b>        Semana 4 .....</b>	<b>33</b>
2.3. Gestión de riesgos GRC .....	33
2.4. Cumplimiento GRC .....	36
2.5. Prácticas y principios GRC.....	38

Actividades de aprendizaje recomendadas .....	39
Autoevaluación 2.....	40
<b>Semana 5 .....</b>	<b>42</b>
<b>Unidad 3. Marcos de trabajo y Estándares .....</b>	<b>42</b>
3.1. COSO 2013.....	42
3.2. COBIT 2019.....	44
Actividades de aprendizaje recomendadas .....	49
3.3. ITIL (Information Technology Infrastructure Library).....	49
<b>Semana 6 .....</b>	<b>51</b>
3.4. Calder – Moir .....	51
3.5. Estándares ISO 9001, 27002 y 38500.....	53
Actividades de aprendizaje recomendadas .....	58
<b>Semana 7 .....</b>	<b>58</b>
3.6. Gestión de riesgos, COSO ERM y enfoque OCEG.....	58
Actividades de aprendizaje recomendadas .....	60
Autoevaluación 3.....	61
<b>Semana 8 .....</b>	<b>64</b>
Actividades finales del bimestre .....	64
<b>Segundo bimestre .....</b>	<b>65</b>
<b>Resultado de aprendizaje 2.....</b>	<b>65</b>
Contenidos, recursos y actividades de aprendizaje .....	65
<b>Semana 9 .....</b>	<b>65</b>
<b>Unidad 4. Gestionar la infraestructura de Gobierno de TI.....</b>	<b>65</b>
4.1. Cloud Computing.....	66
4.2. Virtualización.....	70
4.3. Mobility Computing .....	73
4.4. Seguridad TI.....	73
Actividades de aprendizaje recomendadas .....	77

<b>Semana 10 .....</b>	<b>77</b>
4.5. Plan de continuidad del negocio .....	78
4.6. Catálogos de servicios TI .....	80
Actividades de aprendizaje recomendadas .....	81
Autoevaluación 4.....	82
<b>Semana 11 .....</b>	<b>84</b>
<b>Unidad 5. Desarrollo, Configuración y Gestión de proyectos en el gobierno de TI .....</b>	<b>84</b>
5.1. Aplicaciones SOA.....	84
5.2. Implementación de sistemas y Gobierno de TI.....	85
Actividades de aprendizaje recomendadas .....	87
<b>Semana 12 .....</b>	<b>87</b>
5.3. Gestión de portafolios, proyectos y programas en el gobierno de TI	87
Actividades de aprendizaje recomendadas .....	91
Autoevaluación 5.....	92
<b>Semana 13 .....</b>	<b>95</b>
<b>Unidad 6. Monitoreo y medición del Gobierno de TI.....</b>	<b>95</b>
6.1. Gestión del contenido empresarial - ECM .....	95
Actividades de aprendizaje recomendadas .....	96
<b>Semana 14 .....</b>	<b>96</b>
6.2. Auditoria interna .....	97
Actividades de aprendizaje recomendadas .....	98
Autoevaluación 6.....	99
<b>Semana 15 .....</b>	<b>100</b>
<b>Unidad 7. Generalidades de empresa y el gobierno de TI .....</b>	<b>100</b>
7.1. Cultura organizacional .....	100
7.2. Redes sociales en el gobierno corporativo.....	103
7.3. Comité de auditoría.....	104
Actividades de aprendizaje recomendadas .....	106

Autoevaluación 7 .....	107
Semana 16 .....	109
Actividades finales del bimestre .....	109
<b>4. Solucionario .....</b>	<b>110</b>
<b>5. Referencias bibliográficas .....</b>	<b>118</b>
<b>6. Anexos .....</b>	<b>121</b>



---

## 1. Datos de información

---

### 1.1. Presentación de la asignatura



### 1.2. Competencias genéricas de la UTPL

Comunicación oral y escrita

### 1.3. Competencias específicas de la carrera

Administrar los servicios de tecnologías de información de la organización utilizando buenas prácticas de la industria asegurando la continuidad operacional del negocio.

Define y gestiona políticas, normas y procedimientos, mediante el uso de estándares y marcos de referencia para promover el alineamiento estratégico entre objetivos de negocio y objetivos de TI.

## **1.4. Problemática que aborda la asignatura**

Hoy en día, las organizaciones se enfrentan a un sinnúmero de retos que le generan complejidad como la competencia, las fluctuaciones del mercado, la innovación, los retos tecnológicos, entre otros. Gestionar la complejidad organizacional requiere diversos esfuerzos y aristas que provean una visión global de la organización. Se trata de establecer procedimientos y procesos que ayuden a supervisar la operación de la organización y los recursos TI de forma alineada. Es aquí donde la gobernanza TI juega un papel significativo, proponiéndose como un marco para permitir que la organización pueda gestionar adecuadamente sus recursos TI bajo diversos lineamientos empresariales, de modo que, la organización pueda cumplir con sus operaciones de forma controlada y cumplir con sus objetivos comerciales.



---

## **2. Metodología de aprendizaje**

---

Para lograr un aprendizaje consciente se utilizará el aprendizaje por análisis de estudio de caso que le permitirá al estudiante analizar situaciones problemáticas que viven las empresas y prepararlo para que proponga soluciones acordes a la necesidad planteada. Esto ayudará a que el alumno aplique conceptos teóricos, desarrolle habilidades de resolución y se motive por la rama profesional.



### 3. Orientaciones didácticas por resultados de aprendizaje



#### Primer bimestre

##### Resultado de aprendizaje 1

- Diseñar políticas y estrategias para Gobernanza de Tecnologías de la Información empleando marcos de referencia y estándares internacionales.

Para cumplir con el resultado de aprendizaje planteado, en el primer bimestre, vamos a estudiar 3 unidades fundamentales de gobernanza TI que son: conceptos fundamentales, gobernanza GRC, y marcos de trabajo y estándares. Estas unidades nos ayudarán a conocer los conceptos fundamentales para diseñar políticas y estrategias que permitan desarrollar y aplicar conceptos de gobernanza TI.

#### Contenidos, recursos y actividades de aprendizaje



##### Semana 1

Vamos a iniciar el estudio de la asignatura revisando los conceptos fundamentales de gobernanza TI, para ello, primero deducimos qué es gobernanza corporativa y qué es gobernanza TI: la definición, la importancia, la cobertura y los roles y responsabilidades que deben tomarse en cuenta.

#### Unidad 1. Conceptos fundamentales

Por favor, lea críticamente y estudie los contenidos propuestos en la presente unidad.

## 1.1. Gobernanza Corporativa

La gobernanza corporativa ha ido evolucionando a lo largo del tiempo, teniendo sus inicios en la crisis de Wall Street en 1929 en donde se buscaba transparentar y encontrar un medio por el cual los accionistas respondan por sus prácticas de negocio. En los 30 se definen los primeros roles que las corporaciones deben tener en su gobierno. Richard Eells, Andrei Shlifer y Robert W. Vishny fueron pioneros en utilizar el término y definir “gobierno de la buena empresa o gobierno corporativo”. Sin embargo, los años 90 fue el detonante ya que se produjeron varios escándalos corporativos; entre el más conocido se puede apreciar el caso de Enron la cual supuestamente facturaba más de 100.000 millones de dólares anuales; sin embargo, acabó en la banca rota por malos manejos contables y financieros y su reputación se vio afectada por falsos reportes de auditoría.

Con estos antecedentes de fraude y un pobre control de gobierno se creó un nuevo marco regulatorio llamada la Ley de Sarbanes- Oxley en Estados Unidos en el año 2002, la cual introdujo una serie de procesos para la auditoría externa y brindó nuevas responsabilidades de gobierno a los altos ejecutivos y miembros de la junta.

En la actualidad el gobierno corporativo se ha convertido en una herramienta para mitigar los continuos fraudes y fracasos empresariales. El gobierno corporativo de acuerdo a la (Banco de Desarrollo de Latinomérica CAF, 2010) la define como “el sistema por el cual una empresa es dirigida y controlada en el desarrollo de su negocio o actividad económica” (p.9), que involucra las prácticas formales o informales que establecen las relaciones entre la Junta Directiva, quienes definen las metas de la empresa; la Gerencia, los que la administran y operan día a día; y los accionistas, aquellos que invierten en ella.

Es decir, el gobierno corporativo abarca un conjunto de responsabilidades y prácticas implementadas por la dirección ejecutiva y el personal, con el objetivo de proveer dirección estratégica, asegurarse que los objetivos sean alcanzados, mitigar los riesgos y validar que los recursos de las empresas sean utilizados de forma responsable y correcta.

Las empresas en busca de mejorar sus procesos y transparentar sus operaciones deben considerar los siguientes aspectos de un buen gobierno corporativo de acuerdo a (Orellana, 2011).

1. Trato igualitario y protección a los intereses de los accionistas.
2. El reconocimiento de los interesados en la permanencia de la sociedad.
3. Emisión, revelación y transparencia de información
4. Aseguramiento de que existan guías estratégicas en la sociedad, monitores efectivos de la administración y responsabilidad fiduciaria del Directorio.
5. Identificación y control de riesgos a la que está sujeta la sociedad
6. La declaración de principios éticos y de responsabilidad social.
7. La prevención de operaciones ilícitas y conflictos de interés
8. La revelación de hechos indebidos y protección de informantes.
9. El cumplimiento de las regulaciones a que esté sujeta la sociedad.
10. La incertidumbre y confianza para los inversionistas y terceros interesados sobre la conducción honesta y responsable de los negocios de la sociedad. (p.9)

En el Ecuador, el 5 de septiembre del 2020 la Superintendencia de Compañías, el (Instituto Ecuatoriano de Gobernanza Corporativa y el BID Invest, 2020)emitió el primer grupo de normas para el gobierno corporativo en el país mediante la resolución SCVS-IND-DNCDN-2020-0013 denominado “[Normas Ecuatorianas para el Buen Gobierno Corporativo.](#)”

La cual se fundamenta en cuatro principios (Instituto Ecuatoriano de Gobernanza Corporativa y el BID Invest, 2020):

- **Igualdad:** Trato equitativo de los accionistas y demás personas interesadas.
- **Transparencia:** Obligación de comunicar y rendir cuentas de sus operaciones.
- **Responsabilidad:** Vigilar por la sustentabilidad de la empresa.
- **Voluntariedad:** Aplicación voluntaria de los principios, prácticas y lineamientos de las normas de gobierno. (p.8).

## 1.2. Gobernanza de TI

Como se revisó en el punto anterior la gobernanza corporativa es de obligatoriedad para mantener el control, dirección y seguimiento de todos componentes de una empresa. Así mismo, las TI llegan a ser parte integral de la gobernanza corporativa ya que se requiere un enfoque estructurado de gobierno y gestión que ayude a satisfacer las demandas internas y externas no solo del departamento de TI sino de la organización completa.

### 1.2.1. Definición

Existen varias definiciones, a continuación, se mencionarán algunas de ellas:

"El gobierno de TI es la responsabilidad del consejo de administración y la dirección ejecutiva. Es una parte integral de la gobernanza empresarial y consiste en el liderazgo, estructuras organizativas y procesos que aseguran que las TI de la organización sostiene y amplía las estrategias y objetivos de la organización." (IT Governance Institute, 2003) (p.10).

El Gobierno de TI es la capacidad organizacional que ejerce el Directorio, la gerencia ejecutiva y la gerencia de TI para controlar la formulación e implementación de la estrategia de TI y de esta manera asegurar la fusión de negocio y TI. (Grembergen, 2004) (p.5).

Como se pudo apreciar la gobernanza de TI es de igual responsabilidad de la junta y los ejecutivos y se encarga de liderar y administrar todos los procesos que aseguran que las TI se alinean a la estrategia y objetivos de la corporación.

Sin embargo, hay que saber diferenciar entre un gobierno corporativo y un gobierno de TI. En la siguiente tabla se puede apreciar preguntas que nos ayudan a entender el enfoque de cada una:

**Tabla 1.**

*Preguntas sobre gobierno corporativo y gobierno de TI*

Preguntas sobre gobierno corporativo	Preguntas sobre gobernanza de TI
¿Cómo consiguen los proveedores de finanzas que los gerentes les devuelvan parte de las ganancias?	¿Cómo consigue la alta dirección que su CIO y su organización de TI les devuelva algo de valor empresarial?

Preguntas sobre gobierno corporativo	Preguntas sobre gobernanza de TI
¿Cómo se aseguran los proveedores de finanzas de que los gerentes no roban el capital que suministran o lo invierten en malos proyectos?	¿Cómo se asegura la alta dirección de que sus organizaciones de TI y CIO no roben el capital que aportan o invierten en malos proyectos?
¿Cómo controlan los proveedores de finanzas a los gerentes?	¿Cómo controla la alta dirección a su CIO y su organización de TI?

Nota. Adaptado de Grembergen, W. V. (2004). En W. (Grupo Cavala, s.f.) V. Grembergen, *Strategies for Information Technology Governance* (pág. 6). Estados Unidos: Idea Group Publishing.

El gobierno de TI busca el apoyo y compromiso del directorio para la toma de decisiones en cuanto a TI, la definición de reglas, la forma en cómo se van a gestionar cada uno de los procesos de TI que son requeridos dentro de las distintas líneas de negocio que la comprende y así mismo de asegurarse que entregue valor a los interesados. Por otro lado, el gobierno corporativo vela por el futuro del negocio, en cómo brindar dirección a las inversiones que se realicen en ella y de brindar seguridad y transparencia a los interesados.

### 1.2.2. Importancia

De acuerdo al (*IT Governance Institute, 2003*)(p.13), el gobierno de TI se vuelve fundamental en una organización por los siguientes aspectos:

- Las Tecnologías de la Información se ha convertido en un componente de suma importancia para generar valor en las empresas y apoyar los distintos procesos de las líneas de negocio, para esto es necesario que se evalúe el nivel de dependencia que existe de TI en la organización y que tan crítica es la TI para la ejecución de las estrategias.
- En algunos directorios no se ha mostrado interés en las tecnologías de la información a pesar de que implique grandes riesgos en inversiones. En este tipo de empresas las TI aún siguen consideradas como una entidad separada del negocio o por qué se requiere de conocimientos más técnicos para entender cómo habilita a una empresa en la creación de nuevas oportunidades en el mercado.
- La expectativa y realidad de lo que espera el directorio de la gerencia difiere: la entrega de soluciones de TI dentro del cronograma y presupuesto definido, el retorno de valor de las TI y su uso para

aumentar la productividad y eficiencia mientras reduce y mitiga los riesgos al mismo tiempo.

- Muchas de las veces un mal gobierno de TI es el causante de problemas en el gobierno corporativo como: pérdidas financieras, reputación dañada, bajo cumplimiento de plazos establecidos, procesos de negocio afectados por la mala calidad de TI y fallas en los proyectos de TI para aportar innovación al negocio.



## Actividades de aprendizaje recomendadas

### Actividad 1

Estimado estudiante, lea el siguiente documento y elabore un mapa conceptual que enfatice los aspectos más importantes de la Ley de Sarbanes- Oxley. Éste le ayudará a entender su importancia en el gobierno corporativo. Recurso: [LA LEY SARBANES-OXLEY DE 2002](#)



### Semana 2

---

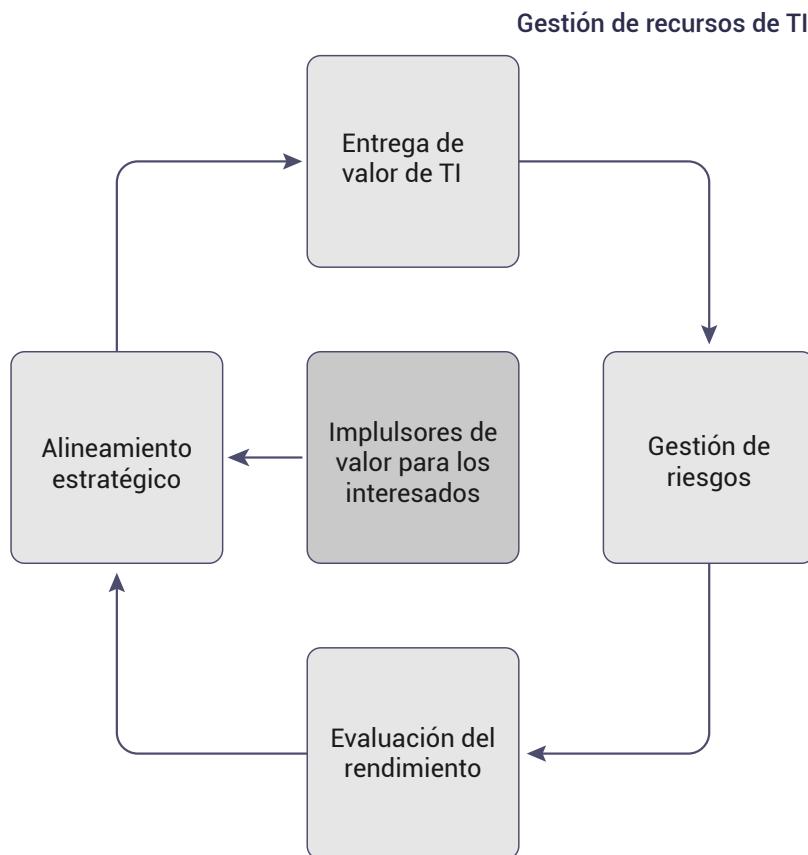
#### 1.2.3. Cobertura

En la presente sección se comprenderá a qué nivel empresarial encontramos involucrado al gobierno de TI. (*IT Governance Institute*, 2013,p.19), indica que el cuerpo de gobierno se preocupa por dos aspectos fundamentales:

- La entrega de valor de TI al negocio
- Mitigación de riesgos de TI.

La entrega de valor se encuentra influenciada por la alineación estratégica del negocio con TI y la mitigación de riesgos por incorporar la responsabilidad en la empresa. Esto conlleva a enfocarse en cinco áreas todas impulsadas por la entrega de valor al interesado:

**Figura 1.**  
Áreas de enfoque del Gobierno de TI



Nota. Adaptado de Focus Areas of IT Governance. [Fotografía], por IT Governance Institute, 2003.,Board Briefing on IT Governance

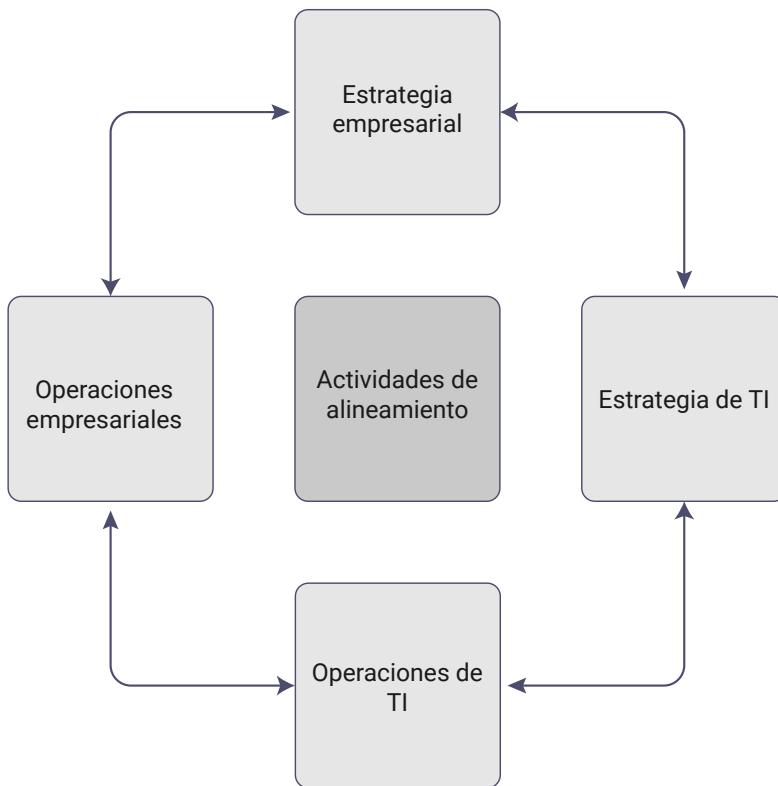
En la figura 1. Áreas de enfoque del Gobierno de TI se puede validar las siguientes áreas de cobertura o enfoque: alineamiento estratégico, entrega de valor de TI, gestión de riesgos y evaluación del rendimiento. A continuación, vamos a definir cada una de estas áreas.

- **Alineamiento estratégico**

Siempre hemos escuchado acerca de lo importante que es la alineación de la TI con el negocio; sin embargo, en la actualidad aún es complicado para muchas corporaciones lograr esta relación directa ya sea por la falta de apoyo del gobierno, la falta de comprensión acerca de lo que la empresa quiere lograr o por la no comprensión de aspectos técnicos que requiere la tecnología.

La alineación estratégica suele ser compleja y multifacética, pero debe ser abordada por el gobierno de tal forma que se garantice inversiones correctas. El gobierno de TI no se interesa únicamente por la alineación entre la organización de TI con el de la organización en general. De acuerdo a (IT Governance Institute, 2003), también se trata de si las operaciones de TI están alineadas con las operaciones empresariales actuales. (p.22), (Ver Figura 2. Alineación empresarial/IT)

**Figura 2.**  
*Alineación empresarial/IT*



Nota. Adaptado IT/Enterprise Alignment [Fotografía], por IT Governance Institute, 2003, Board Briefing on IT Governance

Así mismo es de vital importancia que al formular la estrategia de IT se consideren los objetivos de negocio y la competitividad empresarial, la capacidad de TI para el soporte de los actuales y nuevos servicios de negocio, el análisis de nuevas tecnologías y los costos, riesgos y beneficios que traerán a la corporación.

- **Entrega de valor**

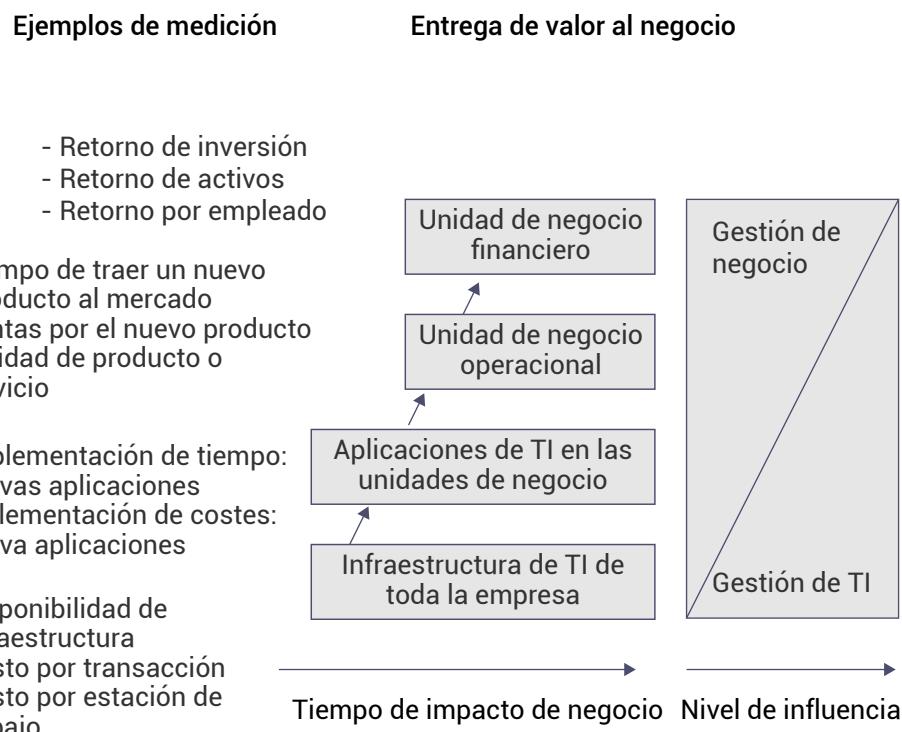
Se debe entender que significa la entrega de valor en las empresas. Pues esta denominación hace referencia a la obtención de beneficios reduciendo costos y riesgos.

El valor de TI debe asegurarse de cumplir con las expectativas del negocio como: flexibilidad en adoptar nuevos requerimientos de negocio, que sea fácil de usar, adaptable y seguro y sobre todo que se aadecue al propósito y alcance de los objetivos estratégicos de la empresa.

El (IT Governance Institute, 2003) asegura que existen diferentes niveles de cómo los interesados perciben el valor de TI y se encuentran denotados en la siguiente Figura:

**Figura 3.**

*Vistas del valor de TI.*



Nota. Adaptado Views of IT Value (Weill and Broadbent) [Fotografía], por IT Governance Institute, 2003, Board Briefing on IT Governance

- **Gestión de riesgos**

La gestión de riesgos es una parte fundamental para asegurar un buen gobierno de TI ya que garantiza su correcto funcionamiento. De acuerdo a (IT Governance Institute, 2003) (p.27) la junta debe gestionar el riesgo mediante:

- Asegurarse de que haya transparencia sobre los riesgos importantes de la empresa y definir las políticas para la toma de riesgos y su prevención.
- Estar consciente de que la responsabilidad de los riesgos cae en la junta.
- Entender que un sistema de control interno para gestionar riesgos puede generar rentabilidad.
- Al gestionar los riesgos de forma proactiva tiene una ventaja competitiva hacia el entorno.
- Insistir en que la gestión de riesgos esté integrada en la operación de la empresa, responda rápidamente a los riesgos cambiantes e informe de inmediato a los niveles apropiados de gestión, con el apoyo de los principios acordados de escalamiento (qué informar, cuándo, dónde y cómo).

Una vez determinado el apetito por el riesgo y la exposición al riesgo identificada, se pueden establecer estrategias para administrar el riesgo y aclarar las responsabilidades. Según el tipo de riesgo y su importancia para el negocio, la gerencia y el directorio pueden optar por:

- Mitigar: implementar controles (p. ej., adquirir e implementar medidas de seguridad, tecnología para proteger la infraestructura de TI).
- Transferir: compartir el riesgo con los socios o transferir a la cobertura de seguro.
- Aceptar: reconocer formalmente que existe el riesgo y controlarlo.

#### ■ **Evaluación del rendimiento**

En el gobierno de TI la gestión, los cuadros de mandos integrales son una herramienta significativa para evaluar el rendimiento. Cada vista del mando está diseñado para responder una pregunta sobre la forma de hacer los negocios de la empresa (IT Governance Institute, 2003)(p.29):

- Perspectiva financiera—Para satisfacer a los accionistas, ¿qué objetivos debemos lograr?
- Perspectiva del cliente—Para lograr los objetivos financieros, ¿qué necesidades del cliente debemos atender?
- Perspectiva del proceso interno—Para satisfacer a los clientes y partes interesadas, ¿en qué procesos de negocio internos debemos sobresalir?
- Perspectiva de aprendizaje—Para alcanzar las metas, ¿cómo debe nuestra organización aprender e innovar?

Según (IT Governance Institute, 2003) (p.29), al usar el cuadro de mando integral, los gerentes confían en más que medidas financieras a corto plazo como indicadores del desempeño de la empresa. También tienen en cuenta elementos intangibles como el nivel de satisfacción del cliente, la racionalización de las funciones internas, la creación de eficiencias operativas y el desarrollo de las habilidades del personal. Esta visión única y más holística de las operaciones comerciales contribuye a vincular los objetivos estratégicos a largo plazo con las acciones a corto plazo.

#### ■ **Gestión del recurso:**

Hace referencia a la forma en la TI gestiona la inversión, el uso y asignación óptima de recursos (personas, aplicaciones, tecnología, instalación, datos) con el fin de satisfacer las necesidades empresariales. Por tal motivo, la junta debe abordar los recursos asegurando que (IT Governance Institute, 2003)(p.28):

- Las responsabilidades con respecto a la adquisición de sistemas y servicios de TI se entienden y aplican
- Existen métodos apropiados y habilidades adecuadas para administrar y respaldar proyectos y sistemas de TI.

- Reclutamiento y, más importante, retención de personal de TI calificado.
- Las necesidades de educación, capacitación y desarrollo de TI están completamente identificadas y abordadas para todo el personal.

De todos los activos indicados uno de los más complejos a administrar es el de los recursos humanos ya que se debe identificar y anticipar las competencias básicas requeridas en el ámbito laboral.

#### 1.2.4. Roles y Responsabilidades

Vamos a definir los roles y responsabilidades asociadas a la junta directiva, la gerencia ejecutiva y el comité de apoyo a los ejecutivos y al CIO, generalmente coordinados por la oficina de proyectos del CIO, el arquitecto jefe, el director de tecnología, etc. Estos roles se encuentran representados a continuación. De acuerdo a (IT Governance Institute, 2003)(pp.50-52) el gobierno de TI está compuesto los roles y responsabilidades mencionados anteriormente agrupados en las cinco áreas de cobertura.

#### Roles y responsabilidades para el gobierno de TI



#### Actividades de aprendizaje recomendadas

##### Actividad 1

Estimado estudiante, una vez revisado los contenidos de la Unidad 1, analice si es capaz de responder las siguientes preguntas:

- ¿Cuál es la diferencia entre gobierno corporativo y gobierno de TI?
- ¿Cuáles son las desventajas de no tener un gobierno de TI?
- ¿De qué se preocupa de solucionar un gobierno de TI?

Nota. Conteste las actividades en un cuaderno de apuntes o en un documento Word.

##### Actividad 2

Ha finalizado la Unidad 1, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 1

Llea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. Ley de Sarbanes- Oxley fue creada con el fin de:
  - a. Aumentar la confianza pública en la información de informes financieros.
  - b. Introducir una serie de procesos para la auditoría externa y brindar nuevas responsabilidades de gobierno a los altos ejecutivos y miembros de la junta.
  - c. Todas las anteriores.
2. ¿Qué no es el gobierno corporativo?
  - a. El sistema por el cual una empresa es dirigida y controlada en el desarrollo de su negocio o actividad económica.
  - b. Es la capacidad organizacional que ejerce el Directorio, la Gerencia Ejecutiva y la Gerencia de TI para controlar la formulación e implementación de la estrategia de TI y de esta manera asegurar la fusión de negocio y TI.
  - c. Involucra prácticas formales o informales que establecen las relaciones entre la Junta Directiva, quienes definen las metas de la empresa; la Gerencia, los que la administran y operan día a día; y los accionistas, aquellos que invierten en ella.

3. ¿Cuál de las siguientes preguntas corresponden al gobierno corporativo?
  - a. ¿Cómo controla la alta dirección a su CEO y su organización de TI?
  - b. ¿Cómo consigue la alta dirección que su CEO y su organización de TI les devuelva algo de valor empresarial?
  - c. ¿Cómo se aseguran los proveedores de finanzas de que los gerentes no roben el capital que suministran o lo inviertan en malos proyectos?
4. ¿A qué nivel empresarial encontramos involucrado al gobierno de TI?
  - a. La entrega de valor de TI al negocio.
  - b. Mitigación de riesgos de TI.
  - c. a y b.
5. En la entrega de valor del gobierno de TI, las aplicaciones de TI en las unidades de negocio se pueden medir por:
  - a. Implementación de costes de nueva aplicaciones.
  - b. Costo por estación de trabajo.
  - c. Costo por transacción.
6. ¿Cuál de las siguientes opciones demuestra la importancia de TI?
  - a. Generan valor en las empresas pero no buscan apoyar a los distintos procesos de las líneas de negocio.
  - b. Un mal gobierno de TI es el causante de problemas en el gobierno corporativo como: pérdidas financieras, reputación dañada, bajo cumplimiento de plazos establecidos, procesos de negocio afectados por la mala calidad de TI.
  - c. Trato igualitario y protección a los intereses de los accionistas.
7. Entre las responsabilidades del comité directivo de TI, encontramos:
  - a. Evalúa el ajuste estratégico de las propuestas.
  - b. Proporciona pautas de arquitectura.
  - c. Proporciona pautas tecnológicas.

8. En la gestión del riesgo el CEO:
  - a. Supervisa los riesgos de TI y acepta riesgos residuales de TI.
  - b. Se asegura que los roles sean bien definidos en la gestión de riesgos de TI.
  - c. Asegura que la arquitectura de TI refleje la necesidad de cumplimiento normativo.
9. La junta de revisión de arquitectura de TI gestiona el rendimiento mediante:
  - a. Cumplimiento de los estándares y pautas tecnológicas.
  - b. Supervisa y dirige los procesos claves de gobernanza de TI.
  - c. Verifica el cumplimiento de las pautas arquitectónicas.
10. ¿Cuál es la diferencia entre gobierno corporativo y gobierno de TI?
  - a. El gobierno de TI busca el compromiso del directorio para la toma de decisiones en cuanto a TI y el gobierno corporativo vela por el futuro del negocio.
  - b. La gobernanza de TI es de poca responsabilidad de la junta; mientras que el gobierno corporativo lidera y administra todos los procesos que aseguran que las TI se alinean a la estrategia.
  - c. a y b.

[Ir al solucionario](#)



## Semana 3

---

En esta semana vamos a estudiar el enfoque GRC, un marco de trabajo que permite administrar la gobernabilidad, gestionar los riesgos empresariales y el cumplimiento de las obligaciones regulatorias internas y externas de una organización. Para comprender este enfoque, iniciaremos deduciendo que significa y qué representa el acrónimo GRC. Luego, revisaremos los aspectos fundamentales que se deben tener en cuenta en cada uno de estos conceptos: gobernanza, riesgo y cumplimiento. Tenga en cuenta que, el enfoque GRC a pesar de que hace énfasis en la gobernabilidad TI, se amplía para abordar todo lo concerniente a prácticas y principios para administrar requisitos de gobernanza de toda la organización.

### **Unidad 2. Gobernanza empresarial y herramientas GRC**

---

Vamos a comenzar el estudio de la unidad 2, comprendiendo 3 aspectos fundamentales sobre gobernanza empresarial que se contextualizan en el acrónimo GRC. Sus siglas se definen como:

- G: Gobernanza
- R: Riesgo
- C: Cumplimiento

Recordemos estos 3 términos como una estrategia que emplean las organizaciones para llevar a cabo la administración de la gobernabilidad, la gestión de los riesgos empresariales y el cumplimiento de las obligaciones regulatorias. A continuación, vamos a analizar la importancia de cada uno de estos aspectos.

#### **Gobernanza**

##### **¿Por qué las organizaciones necesitan de gobernanza empresarial?**

La primera letra del acrónimo G, significa, no solo gobernanza de TI, sino gobernanza empresarial, es decir, gestionar los requisitos y las preocupaciones de toda la organización tomando en cuenta tanto aspectos TI como otros aspectos. Significa, ocuparse de los negocios, perseguir los objetivos empresariales, cumplir normas, reglamentos, y tomar decisiones internas y externas. También, significa, gestionar y alinear las expectativas

de las partes interesadas para que todos estén claros de cómo opera la organización. Recuerde que, todas las organizaciones y empresas tienen problemas y requisitos de gobernanza. La gobernanza es algo inherente y presente en cualquier organización.

Si bien, en el pasado, la gobernanza se traducía en establecer reglas y políticas para el cumplimiento interno del personal y estándares para la entrega de productos y servicios. A medida que, las organizaciones han crecido y se han digitalizado, las reglas y políticas se han adecuado o establecido mejor en las empresas pequeñas o unipersonales, pero, las necesidades y requisitos de gobernanza en empresas, organizaciones y corporaciones necesitan una base amplia de procesos de gobernabilidad para la entrega eficiente de productos y servicios. Los procesos de gobernanza deben garantizar que las operaciones se ejecutan para satisfacer los objetivos empresariales que la organización haya establecido.

Las organizaciones no pueden depender únicamente de las decisiones del liderazgo central (CEO, CIO...), ya que, existen conjuntos cada vez mayores de criterios de complejidad empresarial como el tamaño, la localización, las políticas, las reglas y las leyes que son emitidas por los gobiernos estatales, nacionales o internacionales, que impactan directamente en las decisiones de la organización, por ende, afectan sus productos y servicios. Actualmente, podemos ver cómo la pandemia del COVID y las leyes emitidas por el gobierno de Ecuador alrededor de ella, han afectado las operaciones de todas las organizaciones. Ahora, las organizaciones deben pensar en entregar eficientemente productos y servicios digitales para cumplir con las diversas normativas, lo que ha supuesto un reto de gobernanza.

Para adecuarse a estos cambios externos del entorno y a los requisitos internos, debe existir una base sólida de procesos de gobernanza para garantizar la adaptación, la respuesta y la sostenibilidad de la organización.

## Riesgo

La segunda letra del acrónimo R significa riesgo. Todos los aspectos involucrados en las operaciones comerciales generan algún factor de riesgo. En los negocios hay riesgos que deben asumirse porque pueden llegar a crear valor como la expansión estratégica de la empresa o agregar nuevos productos y servicios. También hay riesgos que deben gestionarse, como las nuevas políticas y normativas establecidas.

Las organizaciones deben cumplir con las políticas, las reglas y leyes estatales establecidas en toda una serie de niveles. Para ello, necesitan procesos sólidos que garanticen que las actividades están operando en conformidad con los criterios establecidos en estas normas. Además, aún con la adopción de las normas, las actividades deben seguir desarrollándose en cumplimiento de los objetivos empresariales.

Frente a todos estos aspectos y convenciones, existen un sinnúmero de riesgos asociados al asumir las diversas políticas tanto internas como externas que deben gestionarse. Sobre todo a nivel externo, porque las organizaciones podrían malinterpretar las leyes o violar alguna de ellas en el proceso de su adopción. También, hay riesgos de que las políticas estatales establecidas no logren los resultados comerciales deseados de la organización o que se susciten eventos externos más allá de su propio control, cómo recesiones económicas, guerras o pandemias que impactan directamente en el curso de sus operaciones. Este último ejemplo supone un riesgo actual de gobernanza que las organizaciones deben constantemente asumir. Por eso, es necesario comprender y gestionar adecuadamente todos estos riesgos empresariales.

## **Cumplimiento**

Finalmente, la última letra del acrónimo C, significa cumplimiento. Muchas normativas y leyes se aplican en varios aspectos de la organización, lo que significa que es importante establecer ciertos controles para garantizar que el cumplimiento está ocurriendo. Por ejemplo, se podría verificar que las importaciones se realizan de acuerdo a las reglas establecidas por aduana; que los costos respetan las regulaciones financieras; o qué las operaciones respetan las normativas establecidas. En la actual pandemia del COVID, las organizaciones deben cumplir criterios de sanidad, capacidad y soporte.

Para evitar las sanciones que pueden presentarse por falta de controles y para gestionar adecuadamente los riesgos, se habla de cumplimiento. De esta forma, bajo criterios internos y externos de cumplimiento, las organizaciones deben demostrar que todas sus operaciones se ejecutan acorde a los criterios empresariales y a las políticas y leyes estatales, nacionales e internacionales.

De este análisis, podemos deducir que, la gestión de una organización implica una gran responsabilidad. Se debe cumplir los objetivos empresariales, dando respuesta rápida a las incertidumbres de carácter

interno y externo y, además, garantizar que las operaciones se ejecutan siguiendo criterios de cumplimiento también internos y externos que estén siendo establecidos.

Al hablar de Gobernabilidad, Riesgo y Cumplimiento (GRC), estamos estableciendo un marco de referencia para la alineación de los objetivos empresariales, la gestión de los riesgos que se presenten y el cumplimiento de leyes y políticas. Tenga en cuenta a GRC como un paradigma que ayuda a las organizaciones a crecer de la mejor manera posible.

## 2.1. Principios GRC

Ya habíamos mencionado que GRC es un conjunto integral de 3 disciplinas: Gobernanza, Gestión de Riesgos y Cumplimiento. Ahora, es importante conocer que estas disciplinas integran, a su vez, 4 conceptos claves en el enfoque GRC que son: estrategia, procesos, personas y tecnología. Estos conceptos son inherentes al funcionamiento global de una organización, es decir, la operación de una organización viene dada por un conjunto de *estrategias* bien definidas, unos *procesos* que soportan la estrategia, diversas *personas* que ejecutan los procesos descritos y la *tecnología* que apalanca digitalmente toda la operación. Además, estos conceptos ayudan a generar los principios por los cuales se van a regir las diversas operaciones gestionadas y soportadas por conceptos GRC.

**Figura 4.**  
*Gobernanza GRC*



Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

Como podemos observar en la figura, los principios de gobernanza, gestión de riesgos y cumplimiento deben estar estrechamente vinculados para abordar los aspectos de estrategia, procesos, personas o tecnología que son necesarios para gestionar eficientemente las operaciones de la organización. En la Figura, también podemos observar que, los principios de gobernanza están influenciados directamente por las políticas internas, siendo estas, factores clave para respaldar diversas decisiones de gobernabilidad. Los principios de cumplimiento se generan a partir de las regulaciones externas. Y, los principios de riesgo nacen del llamado *risk appetite*, que significa la cantidad y el tipo de riesgo que una empresa está dispuesta a asumir, retener o perseguir. Finalmente, podemos analizar que, todo este enfoque y estas relaciones no serían posibles sin conceptos de comportamiento ético, eficiencia organizacional y mejora continua.

Los tres principios de GRC que respaldan el gobierno de TI deben pensarse en términos de un flujo continuo e interconectado de conceptos. Tanto gobernanza, como riesgo y cumplimiento tienen la misma importancia y deben ser vistos de manera integral.

Algunos beneficios resumidos del enfoque GRC son:

- Mejorar el proceso de toma de decisiones
- Alcanzar objetivos comerciales
- Alinear aspectos fundamentales de la empresa: estrategia, personas, procesos y tecnología
- Centralizar la información
- Tener convergencia
- Control interno
- Implementar procesos de auditoría
- Impactar en la cultura organizacional

## 2.2. Gobernanza GRC

Gobernanza GRC también conocida como gobernanza empresarial o corporativa se refiere a las normas, leyes, reglas o procesos que habilitan las operaciones de una organización, las mismas que, además, controlan y regulan el comportamiento de las operaciones. La gobernanza GRC considera aspectos internos y externos. Los aspectos internos tienen que ver con dichas normas, leyes o reglas que son establecidas por funcionarios internos, altos mandos, accionistas u otro ente directivo de la organización. Los aspectos externos son los que están establecidos por las leyes regulatorias estatales o gubernamentales o por los requisitos de clientes y consumidores de la organización.

Podemos definir a la gobernanza como:

- El conjunto de responsabilidades y prácticas ejercidas por la alta dirección de una organización para proporcionar dirección estratégica, asegurar que se cumplan los objetivos empresariales, verificar que se gestionen adecuadamente los riesgos y supervisar que los recursos se utilicen responsablemente.
- El proceso de establecer reglas, políticas y procedimientos en todos los niveles de la organización, comunicar las reglas a las partes interesadas, monitorear el desempeño del cumplimiento de las reglas y administrar recompensas y sanciones producto de las evaluaciones.

Tener un conjunto de principios bien definidos de gobernanza ayuda a tener una estructura sólida para administrar el comportamiento de una

organización, porque todos los involucrados deben adherirse a los principios éticos y a las mejores prácticas propuestas, así como a leyes, normas y estándares formales apropiados.

Algunas de las experiencias que han sufrido las organizaciones al no contar con un gobierno corporativo consisten en:

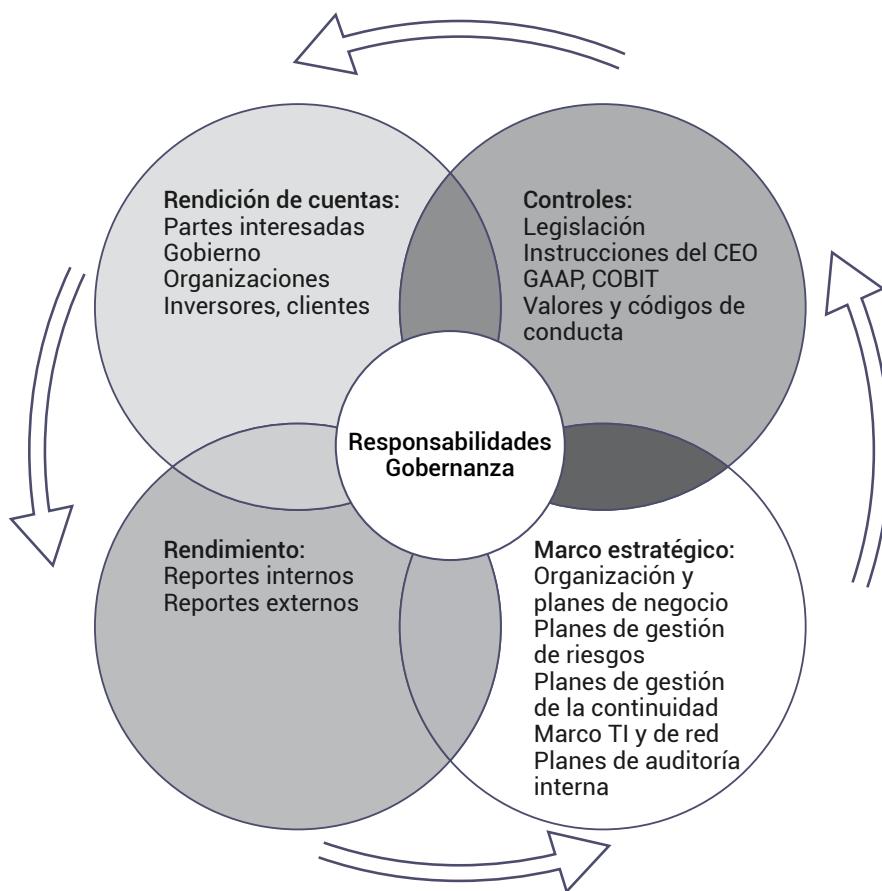
- Abusos de poder
- Errores de juicios financieros
- Actividades delictivas
- Falta o mal manejo de toma de decisiones
- Se reducen las capacidades de la organización para innovar
- No existe una buena cultura organizacional
- Disipaciones de poderes

Tomando en cuenta estas experiencias mencionadas, considere que, el gobierno corporativo también debe pensar en disposiciones civiles o penales para aquellas personas que realizan actos no éticos o ilegales que van en contra de los principios empresariales.

Los roles y responsabilidades del gobierno corporativo se encuentran representados en la Figura a continuación, en donde, podemos ver el grupo ejecutivo o los altos mandos y sus 4 perspectivas de responsabilidades interrelacionadas para establecer: controles, marcos estratégicos, características de rendimiento y rendición de cuentas.

**Figura 5.**

Responsabilidades de gobernanza GRC.



Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

En la Figura 5 se muestran algunos conceptos clave dentro de estas áreas de responsabilidad. Por ejemplo, el establecimiento de controles tiene que ver con la legislación, las instrucciones del CEO, la adopción de principios legales o promover valores y códigos de conducta. Para el marco estratégico, existen los elementos de planificación corporativa y actividades comerciales, gestión de riesgos, continuidad comercial, TI y auditoría interna. Para el rendimiento se debe considerar los reportes internos y los reportes externos. Finalmente, en la rendición de cuentas se deben establecer principios para las partes interesadas, el gobierno, los inversores y los clientes.



## Actividades de aprendizaje recomendadas

### Actividad 1

Llea el recurso propuesto para que pueda comprender cómo puede realizar la adopción de un enfoque GRC. En el recurso se presentan los pasos del estado actual GRC y los resultados de estado futuro deseado, para lo cual revise [Enfoque GRC](#)



### Semana 4

---

Una vez que hemos aprendido los conceptos clave del enfoque GRC y hemos revisado los principios concernientes a gobernanza y sus responsabilidades asociadas. En esta semana, vamos a analizar los principios de riesgos y cumplimiento. Para ello, primero analizamos un proceso de 4 pasos para gestionar adecuadamente los riesgos. Seguidamente, revisaremos cómo establecer un alcance para el cumplimiento y qué áreas deberíamos considerar.

### 2.3. Gestión de riesgos GRC

Tenga presente que, un programa eficaz de gestión de riesgos es un componente clave de los principios empresariales de GRC.

#### ¿Cómo se puede establecer este programa?

A través de 4 pasos o procesos interrelacionados que son:

1. Evaluación y planificación
2. Identificación y análisis
3. Explotación y desarrollo de estrategia en respuesta a los riesgos
4. Seguimiento

Estos pasos se describen y ejemplifican en el recurso a continuación.

[Gestión de Riesgos GRC - gobernanza, riesgo y cumplimiento.](#)

Revisemos más adelante detalladamente los temas para definir qué actividades involucran cada uno de estos pasos.

## Evaluación y planificación

Las organizaciones están constantemente sometidas a algún tipo de riesgo. Ya sea por regulaciones globales, nacionales o algún otro aspecto como el clima, la salud, etc. Considere también que, la globalización, la competencia, la crisis monetaria, la crisis sanitaria son factores que pueden ser fluctuantes, pero afectan el desempeño de la organización.

Tomando en cuenta estos aspectos, a pesar de que no se puede planificar o identificar cada tipo de riesgo que pueda afectar la operación de una organización, siempre se debe mantener un proceso de análisis continuo de los diversos riesgos potenciales que puede enfrentar la organización.

Las actividades a realizar en este proceso se pueden resumir y listar de la siguiente forma:

1. Identificar los factores de riesgo
2. Priorizar los factores de riesgo
3. Mapear las posibles oportunidades frente al riesgo

## Identificación y análisis

Cuando ya hemos realizado la evaluación de riesgos, debemos realizar un análisis detallado de la posibilidad que existe acerca de que estos riesgos lleguen a materializarse, además, debemos cuantificar un posible impacto en caso de que alguno de ellos ocurra y las medidas o estrategias que se podrían aplicar para mitigar el impacto. En las estrategias de mitigación se debe considerar el mejor camino de gestionar y si es posible eliminar el riesgo identificado. Un riesgo identificado será mucho más significativo si podemos detallar los costos totales para la organización si ocurre el riesgo identificado.

Las actividades a realizar en este proceso se pueden resumir y listar de la siguiente forma:

1. Cuantificar los impactos de los riesgos identificados
2. Mitigar los riesgos identificados
3. Considerar factores financieros

## **Explotación y desarrollo de estrategias en respuesta a los riesgos**

Se debe desarrollar planes y estrategias para volver a las operaciones normales y luego recuperarse de un evento de riesgo. Esto puede incluir un análisis de oportunidades relacionadas con el riesgo. Por ejemplo, relacionado a la pandemia del COVID, supuso una oportunidad que las organizaciones puedan ofrecer servicios y productos digitales, de esta forma, incrementaron el alcance de su mercado.

Las actividades a realizar en este proceso se pueden resumir y listar de la siguiente forma:

1. Analizar oportunidades
2. Desarrollar planes de gestión de riesgos
3. Implementar estrategias

## **Seguimiento de riesgos**

Es importante que la organización cuente con procesos y herramientas que le permitan monitorear los riesgos identificados y otros que puedan presentarse. Por ejemplo, desde decisiones de incluir tecnología para identificar riesgos de seguridad informática hasta instalar alarmas contra incendios para evitar riesgos de seguridad física.

Las actividades a realizar en este proceso se pueden resumir y listar de la siguiente forma:

1. Monitorear cambios
2. Establecer factores de riesgo
3. Monitoreo de la organización y el ambiente
4. Evaluar pasos previos

Como resumen de este proceso de 4 pasos, tenga presente que, la gestión de riesgos debe crear valor y ser una parte integral de los procesos organizacionales. Debe ser parte de los procesos de toma de decisiones y adaptarse de manera sistemática y estructurada para abordar explícitamente las incertidumbres que enfrenta una empresa en función de la mejor información disponible. Además, los procesos de gestión de riesgos deben ser dinámicos, iterativos y receptivos al cambio con la capacidad de innovación y mejoras continuas.

## 2.4. Cumplimiento GRC

El cumplimiento es el proceso de adherirse a las pautas o reglas establecidas por agencias gubernamentales, grupos de estándares o políticas corporativas internas. Cumplir con estos requisitos relacionados con el cumplimiento es un desafío para una empresa y sus partes interesadas relacionadas porque:

- Siempre existen nuevas leyes, normas o regulaciones por parte de las agencias gubernamentales o los gobiernos estatales o nacionales. Por ejemplo, actualmente siempre existen nuevas leyes relacionadas al comportamiento que debe llevarse a cabo frente a la crisis sanitaria en la actual pandemia del covid. Las organizaciones tienen el desafío de monitorear las nuevas políticas y determinar cómo abordarlas.
- Las nuevas leyes, normas o regulaciones siempre tienen un vacío que puede estar abierto a diversas interpretaciones. En Ecuador siempre sucede que las leyes que se emiten tienen su vacío que puede recaer en diversas interpretaciones. Además, se escriben adendas y mandatos anexos a las leyes que pueden ser difíciles de interpretar. El cumplimiento empresarial con este tipo de normas resulta altamente complicado.
- No hay consenso sobre mejores prácticas para el cumplimiento. No se han escrito estándares para mejores prácticas relacionadas al cumplimiento empresarial con respecto a las leyes nacionales.
- Pueden existir múltiples regulaciones. Por ejemplo, en la actual pandemia del COVID se establecen reglas de comportamiento empresarial tanto del COE nacional como de los COE provinciales y las instituciones pueden tener sus propios COE institucionales. Cada uno establece convenciones de comportamiento en donde el cumplimiento puede tener diversas aristas que causan múltiples interpretaciones.
- Las leyes, normas o regulaciones cambian constantemente. Por ejemplo, en la actual pandemia es imperativo que las organizaciones constantemente tengan que revisar las normas establecidas para poder planificar su operación. Los COE, en particular, a menudo cambian o reinterpretan constantemente sus propias reglas, lo que hace que el cumplimiento estricto sea un desafío.

El cumplimiento empresarial debe verse como un proceso continuo, no como un proyecto de una sola vez. Sin embargo, los requisitos de cumplimiento continúan impulsando las agendas comerciales, ya que las empresas son responsables de cumplir con la mirada de mandatos específicos de sus mercados o áreas de operación particulares. En la tabla a continuación, puede encontrar criterios para establecer un alcance adecuado para principios de cumplimiento.

**Tabla 2.**  
*Alcance para gobernanza GRC*

Área empresarial	Alcance
Estrategia	Se debe pensar en estrategias para la sostenibilidad de la organización. A medida que las organizaciones desarrollan sus planes estratégicos deben determinar qué regulaciones son más relevantes de acuerdo a su ámbito de aplicación.
Organización	Al momento de realizar el diseño organizacional se debe pensar en cómo la estructura puede tener estándares de cumplimiento. Para ello se pueden crear diversos comités, órganos o juntas para proponer criterios de diseño organizacional. Uno de ellos podría ser que las direcciones ejecutivas y el presidente o CEO sean dos personas diferentes.
Procesos	Los procesos clave o centrales de la organización deben estar documentados. Además, se debe garantizar que existen mecanismos que soportan o respaldan que la ejecución de estos procesos se da de acuerdo a los estándares de cumplimiento establecidos.
Aplicaciones y datos	Las aplicaciones deben diseñarse, desarrollarse y probarse garantizando criterios de cumplimiento. Uno de estos criterios tiene que ver con la integridad de los datos. Los datos deben ser debidamente tratados de acuerdo a las regulaciones.
Infraestructura	Las instalaciones deben estar dispuestas para cumplir diversas necesidades y garantizar la seguridad y disponibilidad del trabajo.

*Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

Con base en este alcance descrito, reflexione que la organización nunca debe ignorar estos estándares globales y resumidos de cumplimiento. Además, la organización podría incluir tecnología de soporte para garantizar el cumplimiento en cada una de estas áreas. La experiencia de las organizaciones que han incursionado con tecnología para el cumplimiento ha proporcionado los siguientes beneficios:

- **Flexibilidad:** la tecnología podría ayudar a que las respuestas frente a los cambios regulatorios se den con mayor facilidad. Esto podría incluir la generación de reportes o Dashboard de datos. A través de este tipo de iniciativas la organización puede adaptarse más rápidamente a los cambios.
- **Reducción de costos:** Con la tecnología y la centralización de la información se puede reducir costos. La inversión para crear una base de datos centralizada de información puede ser menor a la contratación de múltiples auditorías internas en diferentes períodos para obtener información. Además, este segundo paso puede traer consigo grandes pérdidas financieras en el proceso.
- **Ventaja competitiva:** Una arquitectura de cumplimiento amplia y coherente puede permitir que una empresa comprenda y controle mejor sus procesos comerciales, lo que le permite responder con mayor rapidez y precisión a las presiones de cumplimiento internas o externas.

Los procesos efectivos de cumplimiento de GRC ayudan a una empresa a transformar sus operaciones comerciales y obtener una visión más profunda de su información comercial a medida que aborda los requisitos normativos. Los impulsores comerciales clave aquí pueden incluir la capacidad de administrar mejor los activos de información, demostrar el cumplimiento de las obligaciones legales y reglamentarias, reducir el riesgo de litigios, reducir el costo de almacenamiento y descubrimiento, y demostrar la responsabilidad corporativa.

## 2.5. Prácticas y principios GRC

Una empresa necesita adoptar procesos sólidos de gobierno, riesgo y cumplimiento, con el objetivo de establecer un programa GRC eficaz. En el listado a continuación, le presentamos un resumen de prácticas y principios que se pueden realizar para la gobernanza GRC:

- Implementar sistemas integrados para gestionar el gobierno corporativo y para la gestión eficiente de TI.
- Establecer roles y responsabilidades claras para las personas que integran el gobierno corporativo.

- Crear planes de comunicación para comunicar a las partes interesadas y al personal en general los enfoques, principios y reglas de gobernanza que se han de llevar a cabo en diferentes niveles.
- Crear comités de auditoría interna.
- Gestionar los riesgos empresariales y crear una unidad dentro de la auditoría interna que supervise el rendimiento y la gestión de los riesgos, y los principales problemas de cumplimiento asociados.

En esta unidad hemos introducido algunos conceptos importantes de GRC empresarial de alto nivel, que son componentes fundamentales de los procesos efectivos de gobierno de TI.



## Actividades de aprendizaje recomendadas

### Actividad 1

Debido a la pandemia, en Ecuador, se han establecido una serie de normas y reglamentos que se deben cumplir dictados por el COE Nacional. Haga una línea de tiempo de los hitos más significativos que se han dado hasta la actualidad y añada observaciones que destaque como ha sido el comportamiento empresarial frente a estos cambios.

### Actividad 2

En Estados Unidos siempre ha resultado un desafío el cumplimiento empresarial debido al cambio constante de leyes y regulaciones. Un claro ejemplo es la ley de cuidado de salud a bajo precio llamada Obamacare o ley de Obama. Investigue en internet los vacíos legislativos relacionados a esta ley.

### Actividad 3

Ha finalizado la Unidad 2, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 2

Llea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. ¿Qué significan las siglas GRC?
  - a. Gestión, riesgo y cumplimiento.
  - b. Gobernanza, riesgo y cumplimiento.
  - c. Gobernanza, riesgo y control.
2. Gestionar los requisitos y las preocupaciones de toda la organización, tomando en cuenta aspectos TI y otros aspectos del negocio es una característica de:
  - a. Gobernanza.
  - b. Riesgo.
  - c. Cumplimiento.
3. Cuando hablamos de eventos que generan complejidad organizacional que deben asumirse o gestionarse, nos referimos a:
  - a. Gestión de riesgos.
  - b. Cumplimiento.
  - c. Gobernanza.
4. Establecer controles para garantizar que la empresa está operando de acuerdo a diversas normas, empresariales o gubernamentales es un aspecto que se considera en:
  - a. Riesgos.
  - b. Gobernanza.
  - c. Cumplimiento.
5. Los principios de gobernanza están directamente relacionados con:
  - a. Las políticas internas.
  - b. El cumplimiento.
  - c. Las regulaciones externas.

6. Los principios de cumplimiento están directamente relacionados con:
  - a. Las políticas internas.
  - b. Las regulaciones externas.
  - c. La estrategia.
7. La gobernanza GRC considera aspectos de la organización:
  - a. Internos como externos.
  - b. Internos.
  - c. Externos.
8. La identificación y análisis de los riesgos implica:
  - a. Cuantificar el impacto y eliminar los riesgos.
  - b. Cuantificar el impacto, mitigar los riesgos y considerar factores financieros.
  - c. Eliminar los riesgos y considerar factores financieros.
9. El cumplimiento debe considerar el siguiente alcance:
  - a. La estrategia, los procesos, las aplicaciones y datos, y la infraestructura de la organización.
  - b. La estrategia y la infraestructura de la organización.
  - c. Los procesos, las aplicaciones y datos, y la infraestructura de la organización.
10. Se considera una buena práctica GRC:
  - a. Implementar sistemas monolitos.
  - b. Implementar sistemas integrados.
  - c. Implementar sistemas móviles.

[Ir al solucionario](#)



## Unidad 3. Marcos de trabajo y Estándares

En esta sección se tratará marcos de trabajo y estándares que le ayudarán a entender cómo el gobierno de TI las utilizan para beneficiarse en varios aspectos de control.

Acorde a (Moeller, 2013)(p.49), la necesidad de tener controles internos fuertes y efectivos es un elemento clave para el gobierno de TI ya que los procedimientos de control son necesarios en todos los sistemas financieros, operativos y aquellos relacionados con el cumplimiento. Por ejemplo, se puede mencionar las puertas de seguridad que se colocan en el acceso al centro de datos se convierten en un tipo de control general para todos los equipos de cómputo que se encuentran en él. Uno de los marcos que ayuda con estos controles es COSO (*Committee of Sponsoring Organizations of the Tradeway Commission*)

### 3.1. COSO 2013

COSO (*Committee of Sponsoring Organizations of the Tradeway Commission*), según (QAEC, 2019) es una comisión voluntaria formada por representantes de cinco organizaciones del sector privado de los Estados Unidos que tratan: el control interno, la gestión del riesgo y la eliminación del fraude. Aquellas son:

- El Instituto Americano de Contadores Pùblicos Certificados (AICPA)
- La Asociación Americana de Contabilidad.
- Instituto de Contadores Administrativos AMI
- Ejecutivos de Finanzas Internacional (FEI), el Instituto de Auditores Internos (IIA).

Para COSO el control interno es un proceso que lo ejecuta la dirección y el resto del personal con el objetivo de proporcionar un grado de seguridad razonable en lo que refiere a la consecución de objetivos para: la eficiencia de las operaciones, confiabilidad en la información financiera y cumplimiento de leyes y reglas y normativas.

(Moeller, 2013) (p.29) indica que los gerentes de las empresas son los responsables de implementar y administrar los procesos de control interno, mientras que los auditores actúan como partes independientes con el fin de revisar y evaluar estos controles e informar a la gerencia y a otras partes si son los adecuados.

De acuerdo a (Schandl & Foster, 2019) (p.5), COSO 2013 es aplicable en cualquier modelo de negocio, tecnología y riesgos relacionados:

- Codifica los criterios que se pueden utilizar para desarrollar y evaluar la eficacia de los sistemas de control (17 principios).
- Expande los objetivos de informes para respaldar los informes internos, financieros y no financieros, y los objetivos operativos y de cumplimiento.

COSO 2013 se enfoca en cinco componentes integrales de control interno (Schandl & Foster, 2019)(p.5), los cuales se muestran en el siguiente recurso:

### [Componentes integrales de control interno.](#)

En la siguiente tabla se puede apreciar la relación de los 17 principios con sus 5 componentes.

**Tabla 3.**  
*5 Componentes y 17 principios del control interno*

5 Componentes	17 Principios
Control ambiental	1. Demuestra compromiso con la integridad y los valores éticos. 2. Ejerce la responsabilidad de fiscalización. 3. Establece estructura, autoridad y responsabilidad. 4. Demuestra compromiso con la competencia. 5. Hace cumplir la rendición de cuentas.
Evaluación del riesgo	6. Especifica objetivos adecuados 7. Identifica y analiza el riesgo 8. Evalúa el riesgo de fraude 9. Identifica y analiza cambios significativos.
Actividades de control	10. Selecciona y desarrolla actividades de control. 11. Selecciona y desarrolla controles generales sobre la tecnología. 12. Despliega actividades de control a través de políticas y procedimientos.

<b>5 Componentes</b>	<b>17 Principios</b>
Información y comunicación	13. Utiliza información relevante 14. Se comunica internamente 15. Se comunica externamente
Monitoreo de actividades	16. Realiza evaluaciones continuas y/o separadas. 17. Evalúa y comunica deficiencias.

Nota. Adaptado de Schandl, A., & Foster, P. (2019). *Coso Inter Control - Integrated Framework: An implementation guide for health care provider industry*.

Como se puede apreciar, el marco de control COSO ayuda a los altos ejecutivos a comprender cómo usar y gestionar los controles internos de la empresa y sobre todo aquellos relacionados con TI.

### 3.2. COBIT 2019

A través del tiempo se han desarrollado marcos y mejores prácticas para ayudar con el entendimiento y diseño de los gobiernos de información y tecnología. Uno de ellos es COBIT 2019, el cual lleva más de 25 años en este campo y es bien conocido por gran parte de los departamentos de TI.

De acuerdo a (ISACA, 2019)(p.15), COBIT es un marco de referencia para el gobierno y la gestión de información y la tecnología de la empresa. Está dirigido a los siguientes interesados:

**Tabla 4.**  
*Partes interesadas internas*

<b>Interesados Internos</b>	<b>Beneficios de COBIT</b>
Consejo de administración	Proporciona entendimiento sobre cómo obtener valor del uso de IT y explica las responsabilidades relevantes del consejo.
Dirección ejecutiva	Direcciones acerca de cómo organizar y monitorear el desempeño de IT.
Gerentes de negocio	Ayuda a entender cómo obtener las soluciones de IT que la organización requiere y cómo aprovechar las nuevas tecnologías como oportunidad estratégica.
Gerentes de TI	Direcciones acerca de la creación y estructura del departamento de IT, gestionar su desempeño, poner en funcionamiento la operación de IT, controlar costes y alinear la IT con el negocio, etc.

Interesados Internos	Beneficios de COBIT
Proveedores de aseguramiento	Ayuda a gestionar la dependencia con proveedores externos de servicios y asegurar la existencia de controles internos eficaces.
Gestión de riesgos	Ayuda con la identificación y gestión de los riesgos relacionados con IT.

Nota. Adaptado de ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg: ISACA.

**Tabla 5.**  
*Partes interesadas externas*

Interesados Externos	Beneficios de COBIT
Reguladores	Ayuda a garantizar que la empresa cumpla con las normas y reglamentos aplicables y cuente con el sistema de gobierno adecuado para administrar y mantener el cumplimiento.
Socios de negocio	Ayuda a garantizar que las operaciones de un socio comercial sean seguras, confiables y cumplan con las reglas y regulaciones aplicables.
Proveedores de IT	Ayuda a garantizar que las operaciones de un proveedor de TI sean seguras, confiables y cumplan con las reglas y regulaciones aplicables.

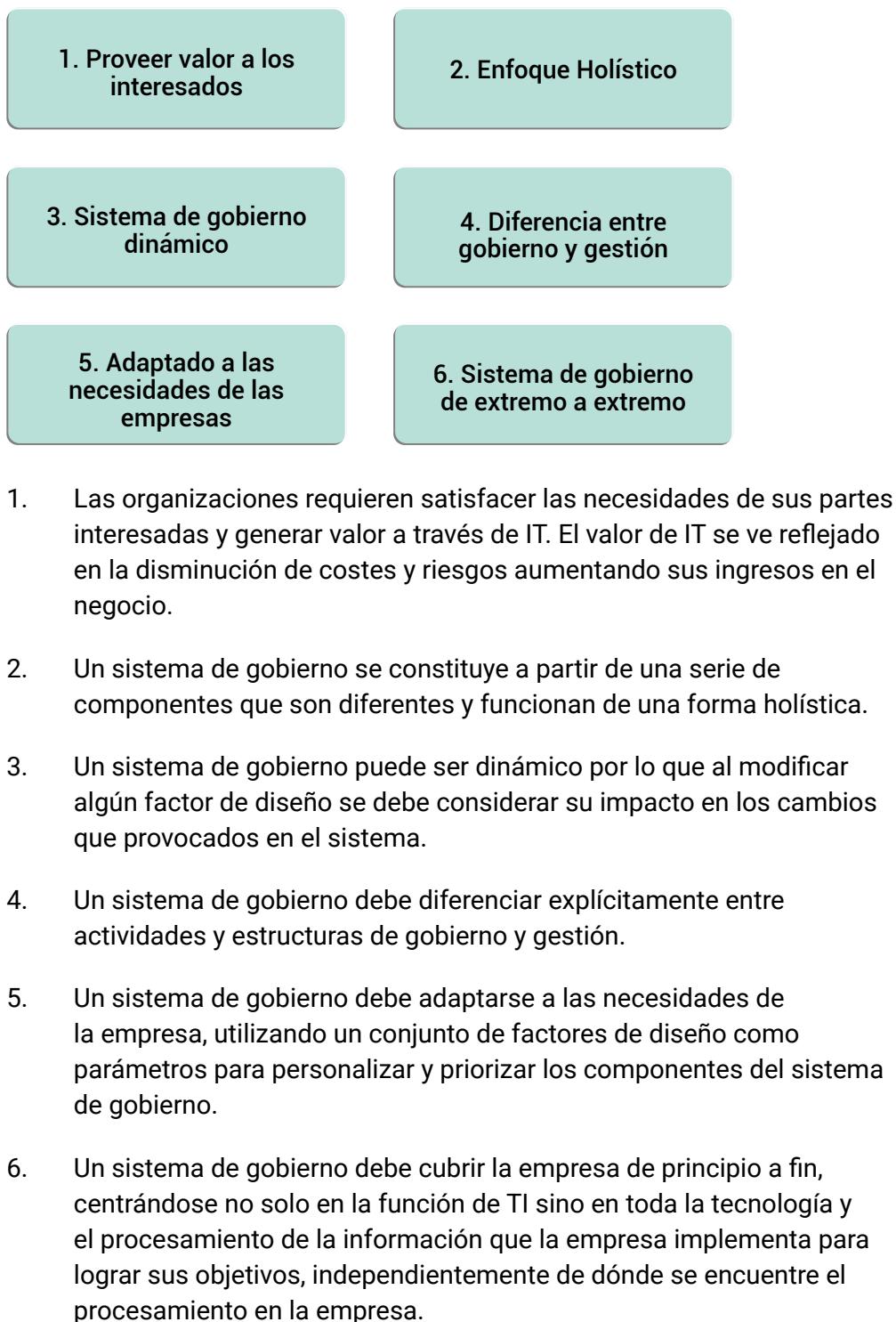
Nota. Adaptado de ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg: ISACA.

### 3.2.1. Principios de COBIT

COBIT se basa en seis principios para su sistema de gobierno (ISACA, 2019), (p.17):

**Figura 6.**

*Principios de COBIT.*



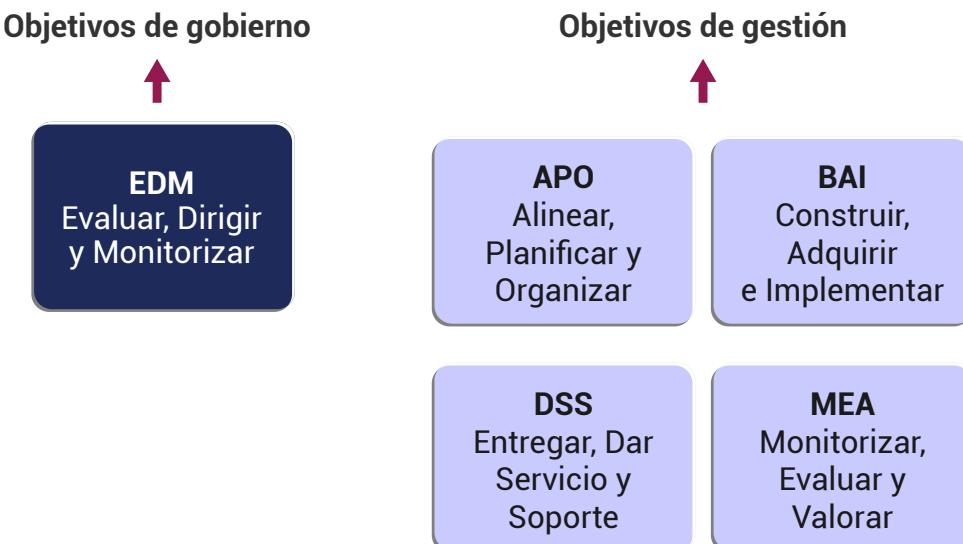
### 3.2.2. Objetivos de gobierno y gestión

(ISACA, 2019) (p.11), dicta que para que la información y tecnología contribuya a los objetivos de la empresa, deben lograrse una serie de objetivos de gobierno y gestión. Algunos de sus conceptos básicos incluyen:

- Un objetivo de gobierno o gestión siempre está relacionado con un proceso y una serie de componentes relacionados de otros tipos para contribuir a lograr el objetivo.
- Un objetivo de gobierno está relacionado con un proceso de gobierno, mientras que un objetivo de gestión está relacionado con un proceso de gestión.
- Los procesos de gobierno suelen ser responsabilidad de los consejos de administración y la dirección ejecutiva, mientras que los procesos de gestión pertenecen al dominio de la alta y media gerencia.

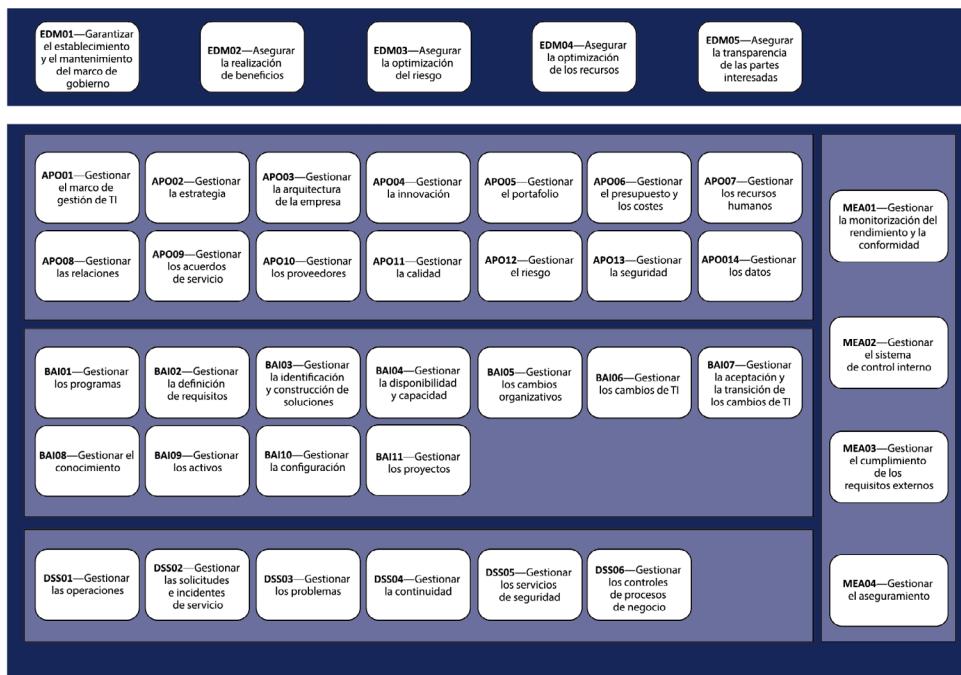
Estos objetivos están agrupados en cinco dominios indicados en la Figura 7. Estos son: EDM, APO, BAI, DSS Y MEA.

**Figura 7.**  
*Objetivos de gobierno y gestión*



A continuación se encuentra el detalle del framework propuesto por COBIT.

**Figura 8.**  
*Modelo base de COBIT*



Nota. Adaptado de COBIT Core Model [Fotografía], por ISACA, 2019, *COBIT 2019 Framework: Introduction and Methodology*.

### 3.2.3. Componentes de sistema de gobierno

(ISACA, 2019) (p.21) menciona que, para cumplir con los objetivos de gobierno y gestión, las empresas deben establecer y adaptar un sistema de gobierno a partir de componentes. Estos componentes interactúan entre sí proporcionando un sistema holístico y que de forma individual y colectiva contribuyen al buen funcionamiento del gobierno de la empresa en cuanto a IT.

A continuación se presenta cada uno de los componentes del sistema de gobierno.

#### Componentes de sistema de gobierno.

Implementar COBIT aborda una fortaleza que se ve reflejada en su amplio uso para gestionar y evaluar los procesos generales de gobernanza en un entorno netamente orientado a las IT.



## Actividades de aprendizaje recomendadas

### Actividad 1

Estimado estudiante, cree una cuenta y descargue la información [COBIT 2019: Objetivos de gobierno y gestión](#), seleccione dos procesos del modelo base de cobit y analice en qué tipos de escenarios de TI podría ayudarle a controlar o evaluar.

### 3.3. ITIL (Information Technology Infrastructure Library)

ITIL (Information Technology Infrastructure Library) es un framework detallado de las mejores prácticas de TI, con listas de verificación, tareas, procedimientos y responsabilidades integrales adaptables a cualquier departamento de IT. Este marco es de gran ayuda para el gobierno ya que proporciona controles internos importantes para la infraestructura, desarrollo y operaciones de TI y cómo gestionarlas hacia la mejora de calidad del servicio.

ITIL 4 considera que la entrega de servicios y la creación de valor debe considerarse en cuatro dimensiones como:

- Organización y Personas
- Información y Tecnología
- Socios y proveedores
- Cadena de valor y procesos

El sistema de valor de ITIL consiste en (Tec Management, 2019):

- Principios: Son recomendaciones que pueden guiar a una empresa en cualquier evento independientemente de los cambios que surjan. Entre los principios encontramos: enfocados en el valor, empieza desde dónde estás, progresá iterativamente con retroalimentación, colabora y promueve la visibilidad piensa y trabaja holísticamente, manténlo simple y práctico y optimiza y automatiza.
- Gobernanza: Medio por el cual la empresa es dirigida y controlada

- Cadena de valor del servicio: Son todas las actividades que realiza una empresa para entregar un servicio o producto a sus consumidores agregando valor.
- Prácticas: Conjunto de actividades para lograr un objetivo.
- Mejora continua: Garantiza que el desempeño de una organización cumpla continuamente con las expectativas de sus interesados.

Entre las prácticas que ITIL trata encontramos las siguientes:

**Tabla 6.**  
*Prácticas de ITIL*

Prácticas Gestión General	Prácticas Gestión del servicio	Prácticas Gestión Técnicas
Gestión de arquitectura	Gestión de la disponibilidad	Gestión de implementación
Mejora continua	Análisis de negocio	Gestión de infraestructura y plataformas
Gestión de seguridad de la información	Gestión de la capacidad y desempeño	Desarrollo y gestión de software
Gestión del conocimiento	Control de cambios	
Medición y reporte	Gestión de incidentes	
Gestión del cambio organizacional	Gestión de activos de TI	
Gestión del portafolio	Gestión de eventos y monitoreo	
Gestión de proyectos	Gestión de problemas	
Gestión de relaciones	Gestión de liberación	
Gestión de riesgos	Gestión de catálogo de servicio	
Gestión financiera del servicio	Gestión de configuración del servicio	
Gestión de la estrategia	Gestión de continuidad del servicio	
Gestión de proveedores	Diseño de servicio	
Gestión del personal y talento	Service Desk	
	Gestión de niveles de servicios	
	Gestión de solicitudes de servicio	
	Validación y pruebas del servicio	

Como se pudo evaluar en la tabla anterior, ITIL ofrece una gran cantidad de prácticas que sirven a la infraestructura de IT para brindar sus servicios de manera eficiente. Sin embargo, de acuerdo a (Moeller, 2013) (p.93) dentro de la gestión financiera de servicio es una práctica que la gerencia

financiera y la gerencia de IT tiende a ignorar ya que para ambos tiende a ser un tema difícil de tratar por desconocer de temas financieros en el caso de IT y conceptos técnicos en el caso de las personas financieras. A pesar de aquello, las organizaciones deben tener un control interno importante e ITIL les ayuda a ejecutarla. El objetivo que tiene el control de gestión financiera es sugerir una guía para la administración rentable de los recursos utilizados en la prestación de servicios de IT. El área de tecnología debe poder contabilizar plenamente sus gastos en servicios y atribuir estos costos prestados a los clientes.

Otra práctica importante que (Moeller, 2013) (p.95) indica se debe considerar en todo gobierno, es la gestión de la capacidad de prestación de servicios; ya que gracias a ITIL asegura que la capacidad de infraestructura se alinee a las necesidades del negocio para mantener un nivel de servicio adecuado a un costo rentable la cual tiene algunas entradas como: Incumplimiento de SLAS, planes y estrategias comerciales, horarios operativos, problemas de desarrollo de aplicaciones, incidentes y problemas de IT, presupuesto y planes financieros que deben ser considerados por la gerencia de IT cuando se estén revisando los procesos de gobernanza de IT.



#### Semana 6

---

### 3.4. Calder – Moir

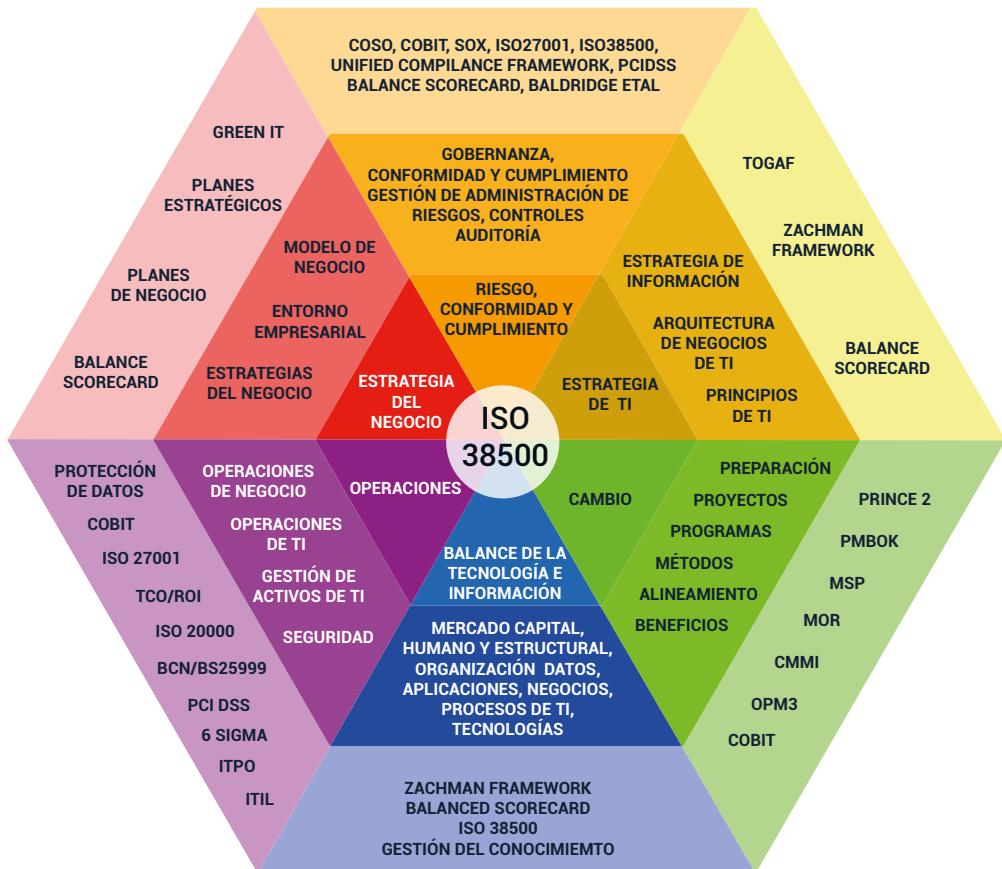
El marco de Calder-Moir es un metamodelo para coordinar modelos y organizar el gobierno de IT proveyendo guía estructural al enfocar el gobierno de IT. Al utilizar este modelo, la organización puede obtener el máximo beneficio de todos los otros marcos de trabajo y estándares. Es una herramienta sencilla para ayudar a las organizaciones a implementar la norma ISO / IEC 38500 para el gobierno de TI en el mundo real. (Muñoz & Ulloa, 2011) (p.41).

Está compuesta por seis elementos divididos en 3 capas de extremo a extremo empezando con la definición de la estrategia hasta el soporte operacional. La capa interna representa la Junta quienes son los encargados de "dirigir, evaluar, y supervisar" el soporte de las TI en el negocio. La parte intermedia representa la gestión ejecutiva, quienes son los responsables de administrar las actividades que llevan el proceso de extremo a extremo.

Finalmente, la capa más externa representa a todos los profesionales de IT, quienes usan herramientas y metodologías comprobadas (COSO, ISO, TOGAF, COBIT) para planificar, diseñar. Evaluar, controlar y brindar el soporte requerido al negocio.

**Figura 9.**

Calder – Moir.



Nota. Adaptado de IT Governance Framework [Fotografía], por IT Governance Europe, 2022, *The Calder- Moir IT Governance Framework*

Calder-Moir se basa en los principios de la ISO 38500, para la evaluación de riesgos usa el marco de riesgos IT RISK y en cuanto a seguridad informática implementa ISO 17799/ISO 27002 entre otros marcos de referentes que ayudan a mantener las buenas prácticas de gobierno de IT.

### **3.5. Estándares ISO 9001, 27002 y 38500**

Las normas ISO (Organización Internacional de Estándares), es considerada una autoridad mundial en el establecimiento de estándares con sede en Ginebra, Suiza. Estas normas son de alto reconocimiento y de cumplimiento a nivel empresarial ya que permite que todas las empresas hablen un mismo idioma para afirmar que tienen algún sistema implementado como la gestión de riesgos ISO 3001. El cumplimiento de las normas ISO es evaluado por un auditor externo certificado en el estándar requerido.

(Moeller, 2013) (p. 109) acota que los estándares ISO deben ser de conocimiento para cualquier alto ejecutivo de tal forma que pueda adoptar el adecuado para su negocio. En la presente sección se tratará tres de ellos. La ISO 9001 que ayuda con prácticas de calidad para procesos comerciales y de fabricación, la 27002 y 38500 que ayuda a definir las características de los procesos para la gestión de servicios, esenciales para un servicio de alta calidad.

#### **3.5.1. Estándares de gestión de calidad ISO 9000**

Las normas de la serie ISO 9000 se crearon con el fin de precisar los requisitos que debería tener un sistema de gestión de calidad. Su origen se da en Japón en las décadas de 1950 y 1960, cuando su proceso de fabricación de automóviles fue reconocida de mejor calidad que la de los Estados Unidos.

Actualmente, la ISO 9000 está compuesta por 3 normas:

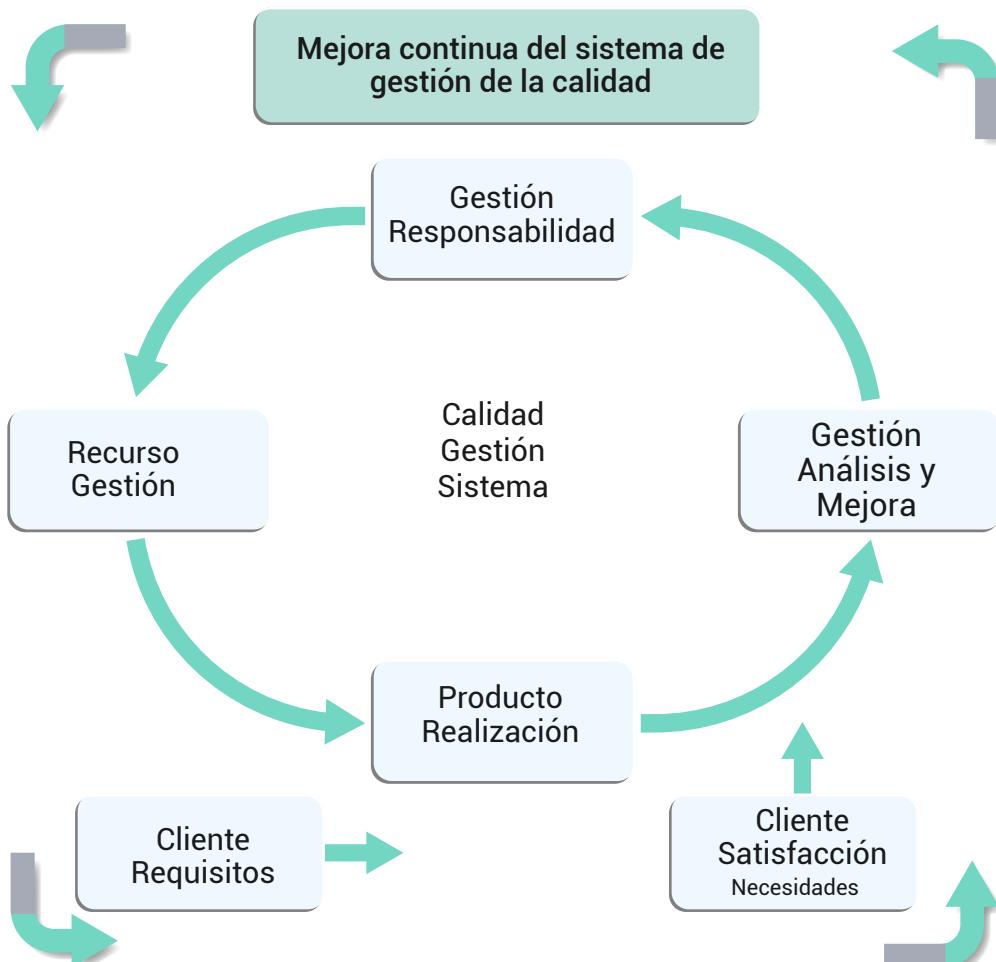
- ISO 9000: 2005 "Sistemas de gestión de calidad. Principios y vocabulario."
- ISO 9001: 2008 "Sistemas de gestión de la calidad. Requisitos"
- ISO 9004: 2009 "Gestión para el éxito sostenido de una organización. Enfoque de gestión de la calidad"

Estas normas contienen requisitos para aspectos como: Mantener registros adecuados de los procesos comerciales, comprobación de los resultados de producción en busca de defectos con las acciones correctivas, monitoreo de los procesos para asegurar que sean efectivos, etc.

De las 3 normas indicadas, la que contiene los requisitos para cumplir con un sistema de gestión de calidad y su certificación es la ISO 9001: 2008.

En la siguiente figura, se muestra un modelo de gestión de calidad basado en procesos que está impulsado por procedimientos internos para mejoras continuas, así como las solicitudes de los clientes. De acuerdo a (Moeller, 2013) (p.113) el proceso de mejora continua no es nuevo para los altos mandos. Los profesionales de desarrollo de sistemas también han utilizado el mismo conjunto de procesos generales de los inicios del desarrollo de software con el llamado ciclo de vida de software.

**Figura 10.**  
*Sistema de gestión de calidad por procesos.*



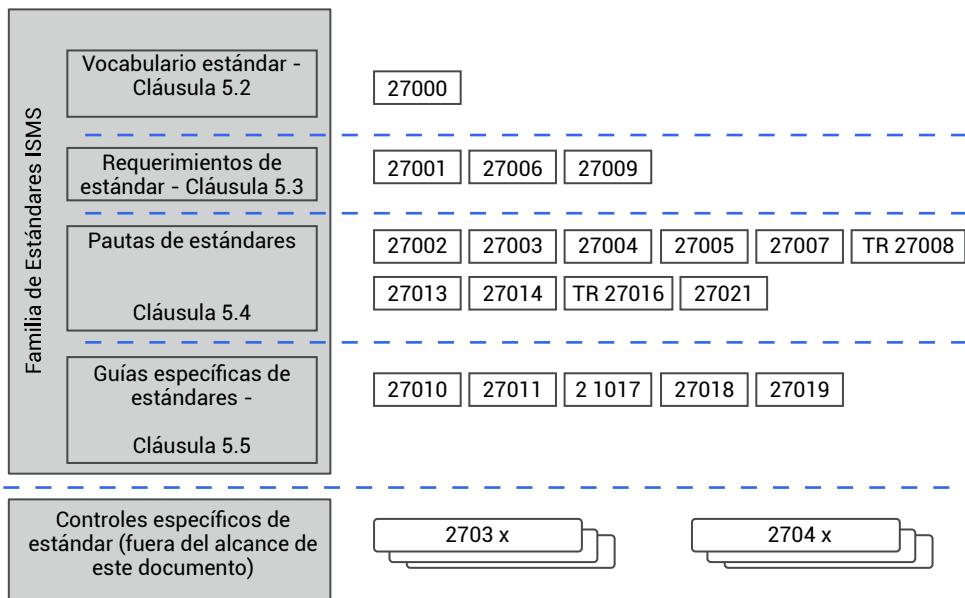
Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

### 3.5.2. Normas de seguridad de TI: ISO 27001 y 27002

Las normas ISO 27001 y 27002 forman parte de la familia ISO 27000:2018 y ayudan a establecer un sistema de seguridad de la información o SGSI con políticas, procedimientos, recursos y demás actividades necesarias para que la organización proteja su información generada de distintos activos.

**Figura 11.**

*Relaciones de la familia de normas ISMS.*



Nota. Adaptado de ISM Family Standards relationships [Fotografía], por ISO/IEC, 2018, ISO/IEC 27000

Según (Moeller, 2013) (p.112) el primer paso que las empresas deben realizar si desean implementar la ISO 27002, es identificar sus propias necesidades y requisitos de seguridad de la información. Esto requiere hacer una evaluación de riesgos de seguridad de la información de acuerdo con los procesos de riesgos empresariales del comité de organizaciones patrocinadoras (COSO). Dentro del esquema de esta norma se puede encontrar:

1. Alcance
2. Términos y definiciones
3. Necesidad de una política de seguridad de alto nivel
4. Requisitos
  - Infraestructura de seguridad de la información
  - Políticas de seguridad y accesos de terceros
  - Consideraciones de subcontratación
5. Normas de control y clasificación de activo
  - 5.1. Responsabilidad por activos
  - 5.2. Clasificaciones de información
6. Seguridad personal
  - 6.1. Consideraciones de seguridad en las estaciones de trabajo
  - 6.2. Formación de usuarios para la seguridad personal
  - 6.3. Estándares para responder a incidentes de seguridad y mal funcionamiento
7. Seguridad física y ambiental:
  - 7.1. Áreas seguras
  - 7.2. Seguridades de equipo
  - 7.3. Controles generales
8. Gestión de comunicaciones
9. Control de accesos
10. Estándares de desarrollo y mantenimiento de sistemas
11. Normas de gestión de continuidad empresarial
12. Estándares de seguridad que cubren cuestiones de cumplimiento

El cumplimiento de esta norma asegura un mayor nivel de confianza entre todos los socios ya que cuentan con una mejor protección de los datos confidenciales y mejores prácticas de cumplimiento de leyes y privacidad.

El ISO 27001 explica cómo aplicar el ISO 27002 mediante la medición, monitoreo y control de la gestión de seguridad de información. Este estándar define la implementación en seis partes (Moeller, 2013) (p.117-118):

1. Definir la política de seguridad
2. Definir el alcance del sistema de gestión de seguridad de TI
3. Evaluación de riesgos
4. Gestión del riesgo
5. Selección de objetivos de control y los controles que se implementarán
6. Declaración previa de aplicabilidad

### **3.5.3. ISO 38500**

El ISO 38500 proporciona un marco de seis principios para que las empresas evalúen, dirijan y monitorean el uso de las TI. A continuación se detallan (Moeller, 2013) (p.120):

#### **Principio 1: Responsabilidad**

El personal y grupos de la organización deben comprender y aceptar las responsabilidades asignadas con respecto a la oferta y demanda de TI.

#### **Principio 2: Estrategia**

La estrategia de la empresa debe tener en cuenta las capacidades actuales y futuras de las TI. Los planes estratégicos de TI (PETI) tienen que basarse en la estrategia de negocio de la empresa.

#### **Principio 3: Adquisición**

Las adquisiciones de TI deben basarse en las necesidades detectadas tras un análisis pertinente. Este debe tener un equilibrio entre los beneficios, oportunidades, costes y riesgos.

#### **Principio 4: Rendimiento**

Las TI deben apoyar a la organización y a la prestación de los servicios para que alcance los objetivos empresariales actuales y futuros.

#### **Principio 5: Cumplimiento**

Es mandatorio cumplir con todas las leyes y reglamentos obligatorios tanto internos y externos.

#### **Principio 6: Factor Humano:**

Políticas, prácticas y decisiones de TI deben considerar el comportamiento humano, incluyendo sus necesidades actuales y futuras de todas las personas involucradas.



## Actividades de aprendizaje recomendadas

### Actividad 1

Estimado estudiante, refuerce sus conocimientos con el siguiente recurso y analice todos los ámbitos que le permite controlar y evaluar la normativa [ISO/IEC 27002:2013](#)



Semana 7

---

### 3.6. Gestión de riesgos, COSO ERM y enfoque OCEG

La gerencia debe poner empeño en identificar todos los riesgos que puedan poner en riesgo la operación del negocio.

(*UN Office for Disaster Risk Reduction, s.f.*) menciona que la gestión de riesgos es el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se producen por algún desastre. De igual forma, identifica acciones preventivas, correctivas y reductivas que deben realizarse.

De acuerdo a (Moeller, 2013) (p.126) la gestión de riesgos debe considerarse como un proceso de cuatro pasos:

1. Identificación de riesgos: Las organizaciones necesitan identificar los problemas y circunstancias que puedan convertirse en riesgos significativos para sus actividades.
2. Evaluaciones cuantitativas o cualitativas de los riesgos documentados: Al haber identificado los riesgos, el siguiente paso es utilizar herramientas para estimar el impacto si ocurre alguno de ellos
3. Priorización de riesgos y planificación de la respuesta: los riesgos deben ser priorizados y se desarrollan planes de respuesta en el caso de que estos ocurran.

4. Seguimiento de los riesgos: Se debe implementar procesos continuos para evaluar el estado actual de los riesgos detectados, y en el caso de que ocurran evaluar el progreso de las acciones correctivas.

En el mundo de los negocios existen varias prácticas que permiten a una empresa gestionar sus riesgos, una de ellas es COSO ERM.

COSO ERM es un marco que ayuda a las empresas a tener una definición lógica de lo que se entiende por riesgo a nivel empresarial. La versión 2017 es la última actualización y pretende, según (Deloitte, 2017) (p.20):

- Una mayor comprensión del valor de la gestión del riesgo para ejecutar y definir la estrategia.
- Acondiciona de mejor manera las expectativas de gobierno y supervisión.
- Mayor transparencia para los stakeholders.
- Interpreta la evolución de la tecnología y la difusión del análisis de datos que soporta para la toma de decisiones.

Además, aclara la importancia de los riesgos empresariales en la planificación estratégica y la integra en toda la empresa. De acuerdo al marco, la gestión de riesgos comparativos está conformada por 5 componentes y 20 principios, los cuales se describe a continuación (Deloitte, 2017)(p.23):

- Gobierno y Cultura: El gobierno es el encargado de reforzar la importancia de la gestión de riesgos y establecer responsabilidades de supervisión. La cultura se refiere a los valores éticos y la comprensión de riesgos dentro de la organización.
- Estrategia y objetivos: La estrategia, objetivos y la gestión de riesgos empresariales trabajan de la mano en el proceso de la planeación estratégica ya que los objetivos de negocio ponen la estrategia en acción mientras sirve para identificar, evaluar y responder los riesgos.
- Desempeño: Todos los riesgos que afecten a la estrategia y objetivos de negocio pueden ser identificados y evaluados. Los riesgos son priorizados de acuerdo a su impacto. La empresa crea las respuestas a los riesgos y toma el riesgo que ha asumido.
- Revisión: Para revisar el desempeño de la entidad, una organización puede considerar qué tan bien funcionan los componentes de gestión

de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y qué revisiones se necesitan.

- Información, comunicación y reporte: La gestión de riesgos requiere de un proceso continuo para obtener y compartir información necesaria que fluya a través de toda la organización.

Los principios son (Deloitte, 2017) (p.24)

Seguidamente se muestran los componentes de COSO ERM.

### Componentes de COSO ERM.

La OCEG es una organización sin fines de lucro que ayuda a las empresas a mejorar su gobierno, gestión de riesgos y cumplimiento. El "libro rojo", libro publicado por la OCEG muestra su desarrollo de un modelo de capacidad de GRC. Este modelo de capacidad tiene varios conceptos similares a COSO ERM y otros de GRC e incluyen los siguientes objetivos: (Moeller, 2013) (p.153-154)

- Mejora los objetivos de negocio generales
- Mejora la cultura de la organización
- Incrementa la confianza de las partes interesadas
- Prepara y protege a la empresa
- Previene, detecta y reduce la adversidad
- Motiva e inspira la conducta deseada
- Optimiza el valor económico y social



### Actividades de aprendizaje recomendadas

#### Actividad 1

Estimado estudiante, observe el siguiente video y realice un infograma con los elementos más importantes del Modelo [COSO ERM 2017](#)

Ha finalizado la Unidad 3, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 3

Llea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. ¿Cuál de los siguientes estándares y marcos de trabajo son utilizados en el gobierno de TI?
  - a. ITL, COSO 2013, COBIT 2019.
  - b. ISO 27001, ISO 27002, NIFF.
  - c. Calder-Mor, Ley de Sarbanes- Oxley, Método Cuantitativo.
2. ¿Cuáles son los cinco componentes integrales de control interno?
  - a. Control ambiental, evaluación de riesgos, actividades de control, información, monitoreo de actividades.
  - b. EDM (evaluar , dirigir, monitorear), APO (alinear, planificar y organizar), BAI (construir, adquirir e implementar), BAI (construir, adquirir e implementar), DSS (entregar, dar servicio y soporte), MEA (monitorizar, evaluar y valorar).
  - c. Procesos, estructura organizativas, flujos y elementos de información, personas, políticas.
3. COBIT se basa en 6 principios básicos:
  - a. BAI01 – Gestionar programa, DSS01 – Gestionar las operaciones, EDM03 - Asegurar la optimización del riesgo, AP002 - Gestionar la estrategia.
  - b. AP012 – Gestionar el riesgo, MEA02 - Gestionar el sistema de control interno.
  - c. Proveer valor a los interesados, enfoque holístico, gobierno dinámico, diferencia entre gobierno y gestión, adaptable, sistema de extremo a extremo.

4. Gestión de proyectos, gestión de portafolio, gestión de seguridad de la información pertenecen al grupo de prácticas de ITIL.
  - a. General.
  - b. Servicio.
  - c. Técnicas.
5. El ISO 38500 proporciona:
  - a. Como aplicar el ISO 27002 mediante la medición, monitoreo y control de la gestión de seguridad de información.
  - b. Un marco de seis principios para que las empresas evalúen, dirijan y monitorean el uso de las TI.
  - c. Ayuda a entender cómo obtener las soluciones de IT que la organización requiere y cómo aprovechar las nuevas tecnologías como oportunidad estratégica.
6. ¿A qué principio de la ISO 38500 hace referencia el siguiente enunciado?, “Las TI deben apoyar a la organización y a la prestación de los servicios, para que alcance los objetivos empresariales actuales y futuros.”
  - a. Adquisición.
  - b. Factor humano.
  - c. Rendimiento.
7. El proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se producen por algún desastre es:
  - a. Gestión de portafolio.
  - b. Gestión de riesgos.
  - c. Gestión de servicios.

8. Es una herramienta sencilla para ayudar a las organizaciones a implementar la norma ISO/IEC 38500 para el gobierno de TI en el mundo real.
  - a. Calder – Moir.
  - b. Zachman.
  - c. PCI DSS.
9. Permite que todas las empresas hablen un mismo idioma para afirmar que tienen algún sistema implementado.
  - a. COSO.
  - b. ISO.
  - c. PETI.
10. Ayuda a definir las características de los procesos para la gestión de servicios, esenciales para un servicio de alta calidad.
  - a. ISO 27002 y 38500.
  - b. ISO 9001 Y 27001.
  - c. ISO 38500 Y 17799.

[Ir al solucionario](#)



### Actividades finales del bimestre

Hemos culminado con el estudio del primer bimestre. Por ello, le invitamos a prepararse para rendir la evaluación presencial correspondiente al primer bimestre. Le sugerimos algunos lineamientos que pueden ayudarle:

- Revise las unidades estudiadas a lo largo del primer bimestre
- Refuerce cada uno de los contenidos, realizando lecturas rápidas y tomando nota de los ítems importantes mostrados en cada semana
- Realice las autoevaluaciones sugeridas en cada unidad
- Comuníquese con su tutor en caso de presentar dudas
- Finalmente, tenga presente las fechas para rendir la evaluación presencial del primer bimestre

¡Muchos éxitos!



## Segundo bimestre

### Resultado de aprendizaje 2

- Analizar y proponer soluciones de Gobernanza de Tecnologías de la Información

Para cumplir con el resultado de aprendizaje planteado, en el segundo bimestre, vamos a estudiar cómo se puede gestionar la infraestructura de gobierno de TI mostrando aspectos a considerar en diferentes tipos de tecnologías, entre ellas cloud computing y virtualización. También, revisaremos diversas estrategias para el desarrollo, configuración y gestión de proyectos en el gobierno de TI. Revisaremos, además, cómo podemos monitorear el gobierno TI, a través de un marco para la gestión del contenido empresarial y analizando el rol que debe cumplir la auditoría interna. Finalmente, examinaremos cómo se relaciona la organización con el gobierno TI. Todos estos contenidos mencionados forman la base para analizar y proponer soluciones de gobernanza de TI.

### Contenidos, recursos y actividades de aprendizaje



#### Semana 9

¡Iniciamos con los contenidos del segundo bimestre!

Para iniciar el estudio, en esta semana vamos a analizar algunas tecnologías que nos permiten gestionar la infraestructura de gobierno de TI: la computación en la nube, la virtualización y la computación móvil. Además, revisaremos cuáles son los problemas de gobierno asociados a estos temas.

#### Unidad 4. Gestionar la infraestructura de Gobierno de TI

Sabemos que, la tecnología está en constante evolución y asimismo está revolucionando continua y aceleradamente la forma en cómo las organizaciones soportan los procesos de negocio y gestionan los servicios TI. Pero, asociada a esta digitalización y revolución tecnológica también

existen muchos retos. Por ello, en esta unidad vamos a analizar 3 tipos de tecnología que son más comunes en la gestión de TI y los problemas de gobierno que estas tecnologías traen consigo.

#### 4.1. Cloud Computing

Los recursos TI se ofrecen cada vez a través de este concepto de Cloud Computing o Computación en la nube. Tenga presente que, las organizaciones cada vez están utilizando la computación en la nube para construir, administrar y utilizar sistemas TI. Revisemos la siguiente definición:

“Cloud computing o computación en la nube es la disponibilidad bajo demanda de recursos de computación como servicios a través de Internet. Esta tecnología evita que las empresas tengan que encargarse de aprovisionar, configurar o gestionar los recursos y permite que paguen únicamente por los servicios que usen” (Google, 2022).

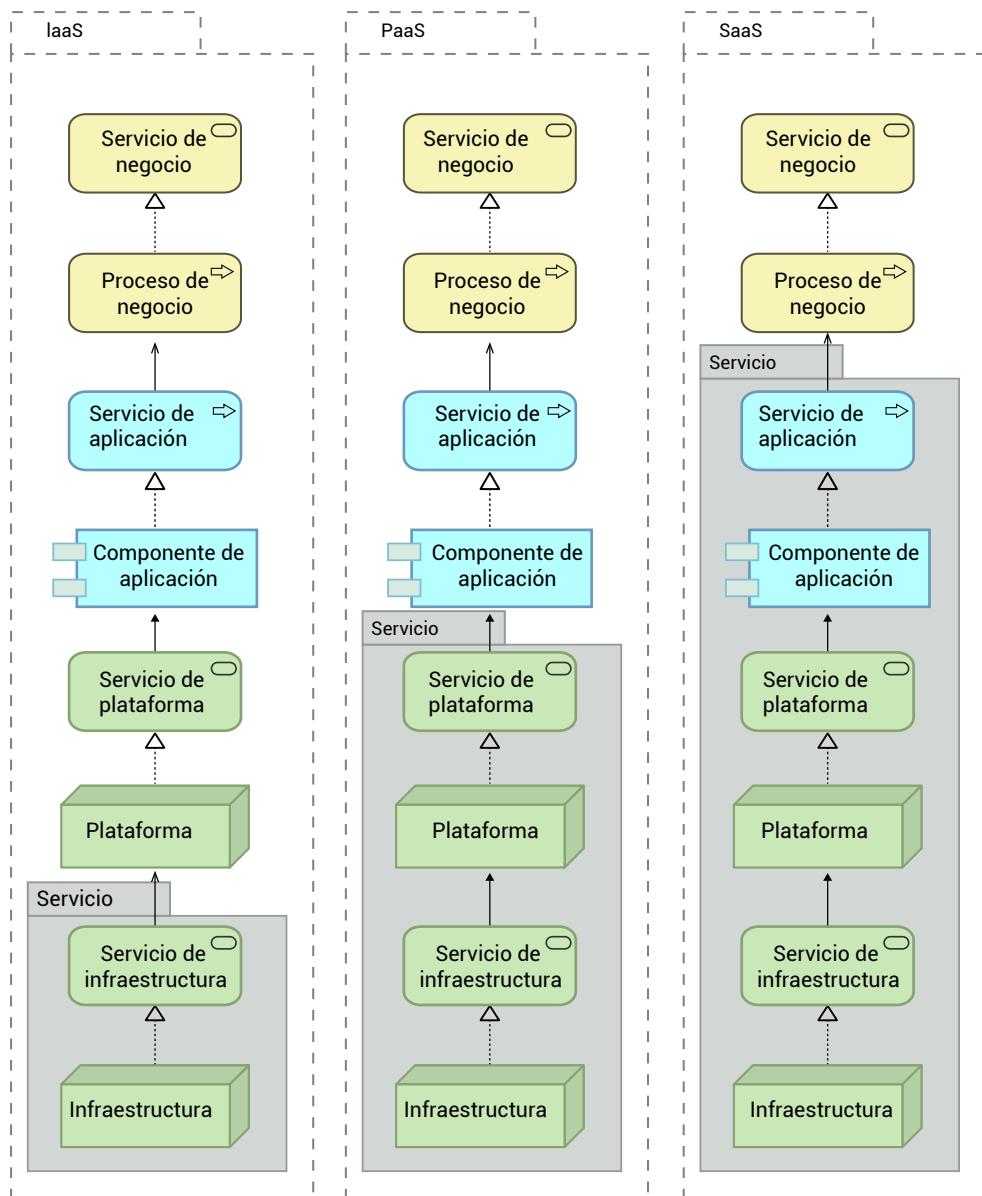
Como puede observar en la definición, la metáfora de la nube se usa para denotar que la infraestructura TI o las instalaciones TI son responsabilidad de proveedores externos y que el cliente o la organización quien utiliza y hace uso de este servicio no gestiona o da soporte a esta infraestructura TI. Esto quiere decir que, las organizaciones hacen uso de servicios que los proveedores de computación en la nube ofrecen. Hay tres tipos de modelos de servicio:

1. **Infraestructura como servicio (IaaS):** ofrece servicios de computación y almacenamiento.
2. **Plataforma como servicio (PaaS):** proporciona un entorno de desarrollo y despliegue para crear aplicaciones en la nube.
3. **Software como servicio (SaaS):** facilita aplicaciones como servicios.

El alcance de cada uno de los modelos de servicio está representado en la imagen a continuación:

**Figura 12.**

Tipos de modelos de servicio de nube.



La imagen ha sido realizada en la herramienta Archimate, el color amarillo define el dominio de negocio de una organización, el azul el dominio de aplicación y el verde el dominio de infraestructura. Y la etiqueta en plomo “servicio” define el concepto que se asocia en cada uno de los tipos de modelos de servicio de computación en la nube.

Los beneficios de estos tipos de modelos de servicio son:

- Costos reducidos de infraestructura
- Escalabilidad de la infraestructura
- Rendimiento consistente
- Recuperación frente a fallos

Al implementar un gobierno TI se debe tener en cuenta todas las bondades y enfoques de la computación en la nube, tener presente la seguridad, los modelos de servicio y los controles internos que hay que tener con las aplicaciones. Queremos decir que, el hecho de que una aplicación funcione en un entorno SOA no significa que desaparezca la necesidad de evaluar y comprender los controles internos. La aplicación basada en SOA debe seguir teniendo los mismos registros de auditoría, procedimientos de verificación de errores y otras buenas prácticas que se encontrarían en cualquier aplicación de TI bien controlada. Como resumen, comprenda que, aunque existe un nivel implícito de confianza en estos servicios y la organización tenga aplicaciones ejecutadas bajo un proveedor de la nube importante como Google o AWS, los líderes y auditores TI, deben asegurarse de que estas aplicaciones basadas en la nube estén bien controladas.

Algunos de los problemas clave de seguridad y gobierno de TI de la computación en la nube son:

- **Transparencia:** Los proveedores deben demostrar que existen controles adecuados que permitan garantizar la seguridad de la información. Siendo un tema sensible para la organización, ya que debe salvaguardar los datos proveyendo integridad a los clientes sobre la información que está siendo recopilada. Por ello, es necesario que los proveedores de la nube puedan dar respuesta a varias interrogantes: ¿Qué tipos de empleados tienen acceso a la información? ¿Qué controles existen para prevenir, detectar y reaccionar ante cualquier brecha de seguridad?
- **Privacidad:** Los proveedores deben garantizar que existen controles de privacidad que puedan prevenir, detectar y reaccionar de manera oportuna frente a cualquier riesgo existente.
- **Cumplimiento:** Los proveedores deben garantizar que cumplen con las normas y reglamentos para el almacenamiento y tratamiento de los datos de la organización. Por ejemplo, en el caso de que

las autoridades soliciten datos de la organización que se puedan proporcionar sin comprometer otra información.

- **Flujos de información transfronterizos:** Dado que la información generada en la nube se almacena potencialmente en cualquier lugar de la nube, la ubicación física de la información puede convertirse en un problema. La ubicación física dicta jurisdicción y obligación legal.
- **Certificación:** Los proveedores de servicios de computación en la nube deben garantizar a sus clientes que están haciendo las cosas "correctas".

Aunque no existen estándares o reglamentos sobre lo que los proveedores deben dar como garantía a las organizaciones para ofrecer sus servicios en la nube, al menos, la organización debería asegurarse que se le pueda dar respuestas efectivas en los siguientes 3 aspectos:

- **Eventos:** Que se pueda documentar y comunicar cambios y otros factores que hayan afectado la disponibilidad de los servicios.
- **Registros:** Que se pueda proveer información sobre los servicios y su entorno en tiempo de ejecución.
- **Seguimiento:** Que se realice seguimientos oportunos.

Además de considerar estos aspectos, los líderes y auditores TI deberían asegurar que el proveedor de servicios de la nube abarque las siete áreas descritas a continuación:

- **Acceso de usuario privilegiado:** Garantiza que los datos tengan un correcto tratamiento solo por usuarios privilegiados que mantengan controles sobre el acceso a dicha información.
- **Cumplimiento normativo:** A pesar de que la infraestructura no se gestione por parte de la organización, los datos siguen siendo responsabilidad de la misma. Por ello, debemos asegurarnos que los proveedores mantengan políticas de gobierno sobre seguridad y resultados informados de auditorías externas y certificaciones de seguridad recientes.
- **Ubicación de los datos:** Debido a las leyes de propiedad de datos, los proveedores de servicios en la nube deben identificar las jurisdicciones específicas donde almacenarán y procesarán los datos de la organización. Pero, también debe comprometerse contractualmente

a obedecer los requisitos locales de privacidad en nombre de sus clientes.

- **Segregación de los datos:** Los datos en la nube suelen estar en un entorno compartido junto con los datos de otros clientes. El proveedor de la nube debe proporcionar información detallada sobre lo que se está haciendo para separar los datos en reposo y también debe proporcionar evidencia de que sus esquemas de encriptación fueron diseñados y probados por especialistas experimentados.
- **Recuperación:** Incluso si la organización no conoce la ubicación de sus datos almacenados en la nube, el proveedor de la nube debe documentar lo que sucederá con los datos y servicios de una empresa en caso de un desastre. El proveedor de servicios debe proporcionar evidencia, incluidos los resultados de las pruebas, de que sus métodos de recuperación replicarán la infraestructura de datos y aplicaciones en múltiples sitios. El servicio debe afirmar si tiene la capacidad de realizar una restauración completa y cuánto tiempo llevará.
- **Apoyo investigativo:** El proveedor de servicios debe proporcionar un compromiso contractual para apoyar formas específicas de investigación.
- **Viabilidad a largo plazo:** El proveedor debe garantizar que su empresa no fracasará ni será fusionada. Pero, se debería dar garantías por si estos eventos suceden.

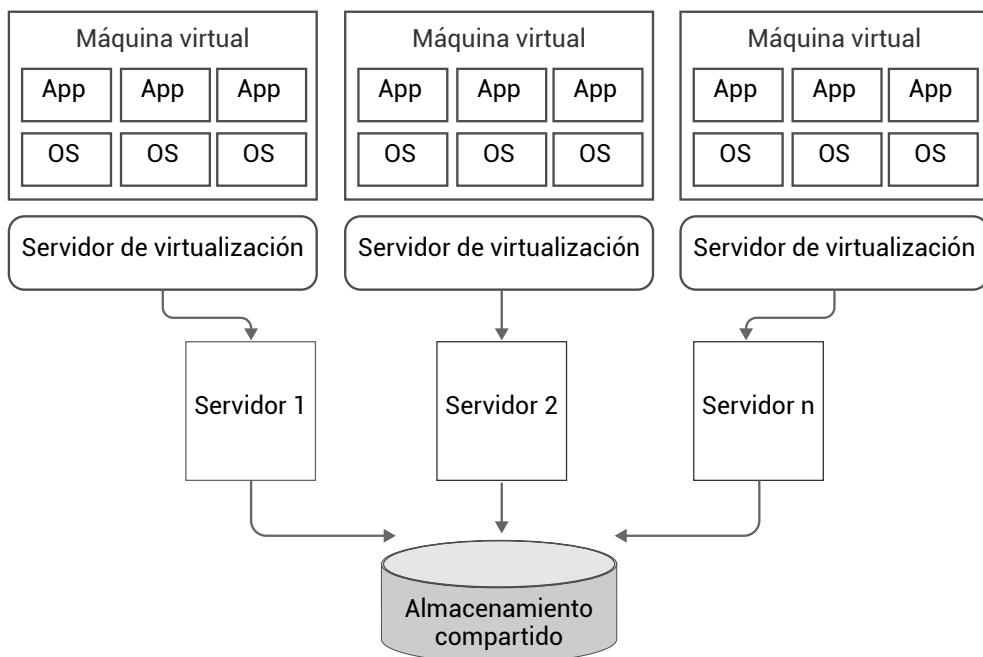
Cómo puede analizar, la computación en la nube se ha vuelto casi un estándar para la gobernanza de TI. Por ello, las organizaciones deben comprender todas las oportunidades y problemas de gobierno que pueden enfrentar al tener este tipo de modelos de servicios para sus sistemas y aplicaciones.

## 4.2. Virtualización

La virtualización es un esquema en donde se imitan las características del hardware para crear sistemas informáticos virtualizados. Esto permite que las organizaciones ejecuten múltiples sistemas virtuales y múltiples sistemas operativos y aplicaciones en un solo servidor. En la imagen a continuación, se encuentra representado el esquema de virtualización:

**Figura 13.**

Esquema de virtualización.



Existen diferentes tipos de esquemas de virtualización:

- **Almacenamiento:** múltiples dispositivos de almacenamiento en red en lo que parece ser una sola unidad de almacenamiento.
- **Servidores o plataforma:** Partición de un servidor físico en múltiples servidores virtuales más pequeños.
- **Sistemas operativos:** Este es un tipo de tecnología de virtualización de servidores que funciona con sistemas operativos complejos con capas de software.
- **Redes:** Una única red física puede convertirse en virtual mediante la segmentación lógica de los recursos de la red.
- **Aplicaciones:** Son aplicaciones que aparentemente se ejecutan en entornos locales como aplicaciones remotas o el streaming de aplicaciones.
- **Datos:** Integrar datos de fuentes dispersas, en distintas localizaciones y formatos, sin replicar los datos.

Debemos tomar en cuenta que la virtualización ha permitido que las organizaciones no se preocupen por la gestión de la infraestructura de almacenamiento. Por ejemplo, para que una organización pueda adquirir un nuevo servidor para un centro de datos debe tener varios recursos como personas, procesos y procedimientos específicos para dicho fin. Sin embargo, con la virtualización se pueden crear nuevas máquinas virtuales con un solo clic, lo que permite que se pueda eludir toda esta cantidad de recursos (personas, procesos, procedimientos).

Al hablar de virtualización se debería garantizar los siguientes aspectos:

- **Gestión de la identidad:** Dado el dinamismo de las máquinas virtuales se necesitará algún nivel de gestión de archivos y recursos. Los líderes y auditores TI deberían evaluar los procesos para garantizar que existen políticas de gestión de identidad que se aplican correctamente.
- **Control de movilidad:** Las máquinas virtuales están diseñadas para ser móviles y se mueven fácilmente de un host a otro en respuesta a los procesos automatizados de equilibrio de carga o la eliminación manual. Sin embargo, la movilidad puede ser un arma de doble filo, ya que no todas las máquinas virtuales deben ser móviles. Es posible que se requieran políticas sobre dónde se debe y no se debe permitir que se ejecuten máquinas virtuales específicas, así como cuánto tiempo duran las máquinas virtuales.
- **Aprovisionamiento:** Los procesos tradicionales de aprovisionamiento de servidores se pueden eludir fácilmente en el espacio virtual, por lo que es necesario establecer nuevos procesos que controlen tanto lo que se aprovisiona como quién tiene la autoridad para autorizar nuevos servidores.
- **Separación de datos:** Es importante tener en cuenta cómo harán cumplir esto en el lado virtual, no solo cuando se aprovisiona la máquina virtual sino también para protegerla de ataques inesperados.
- **Recuperación:** Garantizar que las máquinas virtuales redundantes o no utilizadas se eliminen de manera oportuna es otra área que requiere políticas y objetivos específicos.

Los aspectos mencionados anteriormente se deberían analizar al elaborar un plan de gobernanza considerando aspectos de virtualización. Para el

buen funcionamiento de las operaciones TI y los procesos de GRC que hemos mencionado, la administración de TI debería determinar que se mantengan estándares de control interno adecuado para los entornos virtualizados.

### 4.3. Mobility Computing

Nos referiremos al término Mobility Computing para hablar de la computación móvil: celulares, tablets, dispositivos de almacenamiento USB u otros. Hoy en día, el uso de este tipo de dispositivos en los lugares de trabajo es muy común, es decir, este tipo de dispositivos de uso personal se utilizan también para fines laborales dentro de una organización y esta práctica sin lugar a duda genera problemas de gobierno. Por ejemplo, sabemos que un celular o una Tablet tienen incorporadas cámaras que se podrían usar para tomar fotos de información confidencial de la organización. O acceder a repositorios o servidores de la organización a través de este tipo de dispositivos podría tener problemas de seguridad. Por ello, la administración y los equipos de seguridad deberían diseñar planes corporativos para el uso eficiente de dispositivos móviles y es un aspecto que se debe tener en cuenta al hablar de gobernanza TI.

### 4.4. Seguridad TI

Hoy en día, la seguridad TI es un área crítica de gobernanza empresarial. Es común escuchar noticias de robo de información en diversas organizaciones tanto gubernamentales como empresariales a pesar de que tengan controles internos y auditorías que se desarrollen de forma continua para gestionar la seguridad TI. Es importante comprender que, existen muchos riesgos asociados a la seguridad TI siendo la divulgación de datos uno de los más preocupantes.

Las preocupaciones con respecto a la seguridad de TI se encuentran entre los principales problemas que afectan tanto a la gestión general como a la de TI en una organización. Para asegurarse de tener una seguridad de TI eficaz, la organización necesita establecer y construir un entorno de seguridad de TI sólido y bien administrado. Esta tarea es responsabilidad de las operaciones de TI y la gestión empresarial en todos los niveles. La administración de TI puede ayudar en este proceso implementando

controles internos efectivos y políticas y procedimientos de seguridad sólidos, y trabajando con todos los niveles de la empresa para establecer un entorno de seguridad efectivo.

#### 4.4.1. Principios

Vamos a analizar los principios de seguridad del estándar GASSP (Generally Accepted System Security Principles o principios de seguridad de sistemas generalmente aceptados en español), conocidos como las mejores prácticas para desarrollar procesos y estándares de seguridad de TI efectivos.

GASSP es un conjunto consensuado de principios, estándares, convenciones y mecanismos relacionados con la seguridad de TI que los profesionales de la seguridad de TI deben emplear, que los productos de procesamiento de información deben proporcionar, y que los propietarios de la información deben reconocer para garantizar la seguridad de su información y sistemas de TI. El GASSP se relaciona con la seguridad de la información física, técnica y administrativa y abarca la seguridad integral, amplia, funcional y detallada.

GASSP se basa en ocho principios de alto nivel que la administración y los especialistas en seguridad de TI pueden usar como ancla sobre la cual construir sus programas de seguridad de TI. Cada uno de los ocho principios GASSP se explica a continuación:

- 1. La seguridad de TI debe respaldar la misión de la empresa.** Se debe proteger los activos de la organización como la información, el hardware y el software y por consecuencia los controles internos aplicados en estos activos ayudan a cumplir la misión empresarial, ya que, salvaguardan los recursos físicos y financieros, la reputación, la posición, los clientes y empleados, y otros activos tangibles e intangibles de la organización.
- 2. La seguridad de TI debe ser rentable.** Se debe tener un costo beneficio en términos de seguridad TI, es decir, los controles internos aplicados a los recursos deben proporcionar los resultados esperados. La seguridad debe ser adecuada y proporcional al valor y grado de confianza en los sistemas de TI y a la gravedad, probabilidad y alcance del daño potencial. La seguridad de TI debe verse como una práctica comercial inteligente y, al invertir adecuadamente en medidas de

seguridad, una empresa puede reducir la frecuencia y la gravedad de las pérdidas relacionadas con la seguridad.

3. **La seguridad de TI es un elemento integral de las buenas prácticas de gestión.** Los sistemas TI son activos de valor de una organización que no están exentos a riesgos, a pesar de que se ejecuten con controles internos adecuados. Por ello, se debe considerar el nivel de riesgo que está dispuesto a aceptar la organización, teniendo en cuenta el costo de los controles de seguridad.
4. **Los propietarios de los sistemas tienen responsabilidades de seguridad fuera de su propia organización.** Si un sistema tiene usuarios externos, sus propietarios tienen la responsabilidad de compartir el conocimiento adecuado sobre la existencia y el alcance general de las medidas de seguridad para que otros usuarios puedan confiar en que su sistema es adecuadamente seguro.
5. **La responsabilidad de seguridad de TI y la rendición de cuentas debe ser explícita.** La responsabilidad relacionada con la seguridad y la rendición de cuentas de los propietarios, proveedores y los usuarios de los sistemas de TI y otras partes interesadas en la seguridad de los sistemas de TI debe ser explícita.
6. **La seguridad de TI requiere un enfoque integral e integrado.** Se debe considerar una variedad de áreas dentro y fuera del campo de la seguridad TI que se extienden a lo largo de todo el ciclo de vida de los sistemas de información. A menudo, los controles de seguridad requieren el correcto funcionamiento de otros controles.
7. **La seguridad de TI debe reevaluarse periódicamente.** Los sistemas de TI y los entornos en los que operan son dinámicos y cambian constantemente. Estos cambios afectan la seguridad. Muchos tipos de cambios afectan la seguridad del por lo que es necesario reevaluar periódicamente la seguridad de los sistemas de TI.
8. **La seguridad de TI está limitada por factores sociales.** La capacidad de la seguridad de TI para respaldar la misión de una empresa puede verse limitada por factores tales como problemas sociales donde la seguridad y la privacidad en el lugar de trabajo pueden estar en conflicto.

Estos principios generales abordan las propiedades de la confidencialidad, integridad y disponibilidad de la información de seguridad de TI. Proporcionan una guía de gobierno general para establecer y mantener la seguridad de la información.

#### 4.4.2. Estrategias

Adoptar e implementar un conjunto de principios de seguridad amplios, como GASSP, puede tener un valor considerable, pero una empresa también debe implementar una estrategia general de seguridad de TI. En esta era de la digitalización, la seguridad hoy en día implica desarrollar arquitecturas y utilizar tecnologías emergentes y en constante evolución.

Para asegurarse que la organización use niveles apropiados de seguridad TI se puede considerar el uso de modelos de seguridad con enfoques "de arriba hacia abajo". Esto permite que los líderes TI puedan comprender mejor la gravedad de los problemas de seguridad TI y luego iniciar procesos adecuados para comunicar cómo debería operar el personal de la organización. Este enfoque se diferencia del enfoque de "abajo hacia arriba" en donde el personal operativo de la organización encuentra los hallazgos y los comunica a los líderes TI. Este enfoque se encuentra representado en la imagen a continuación:

**Figura 14.**  
*Estrategia de arriba hacia abajo sobre seguridad TI.*



Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

A continuación, vamos a describir el detalle de cada uno de estos conceptos:

- **Políticas de seguridad:** Los líderes TI deben comprender la dimensión y la capacidad de la organización, sus recursos, su cultura y los aspectos clave, y crear políticas de seguridad efectivas que puedan ejecutarse en todos los niveles de la organización. Por ejemplo, aplicar los principios de la norma ISO o COBIT.
- **Estrategias de seguridad:** Se debe diseñar estrategias detalladas que estén respaldadas por estándares para cubrir todos los detalles relacionados con aspectos TI, por ejemplo, implementar cortafuegos, monitorear sistemas, entre otros.
- **Políticas y estándares:** Las normas deben especificar los pasos a seguir para ejecutar cada una de las actividades relacionadas a la seguridad TI, por ejemplo, procesos para aprobaciones y cumplimiento.



### Actividades de aprendizaje recomendadas

#### Actividad 1

Para profundizar el aprendizaje sobre seguridad TI, le invitamos a leer el recurso a continuación, que habla sobre seguridad informática. Lea las páginas 21 a la 35 de [Fundamentos de la Seguridad de la Información](#)



#### Semana 10

---

En esta semana, vamos a revisar los conceptos relacionados al plan de continuidad del negocio, que es un documento que define cómo la organización puede recuperar sus sistemas TI y sus procesos de negocio frente a eventos que puedan suscitarse. También, vamos a estudiar cómo diseñar efectivamente un catálogo de servicios TI.

#### 4.5. Plan de continuidad del negocio

El plan de continuidad del negocio (BCP – Business Continuum Plan) es un documento que abarca los procesos necesarios que deben ejecutarse para la recuperación de los sistemas TI y los procesos de negocio centrales de la organización, frente a eventos que puedan suscitarse, sean estos, físicos, sociales o climáticos que generan la interrupción de las operaciones. Para establecer gobernanza empresarial, cualquier organización debería contar con un BCP, sin importar el tamaño de las operaciones centrales o la criticidad de los recursos TI. El BCP debería hacer énfasis en las personas, las instalaciones físicas y otros recursos de la organización, ya que un BCP efectivo se extiende más allá de TI e implica la recuperación, reanudación y mantenimiento de todas las operaciones comerciales.

Para crear un BCP se debería realizar las actividades a continuación:

- Priorizar los objetivos comerciales.
- Priorizar las operaciones centrales que son críticas para la organización.
- Desarrollar procesos BCP a corto y largo plazo, que consideren las operaciones centrales críticas, las unidades de negocio, el departamento y los recursos TI que deberán responder frente a eventos como interrupciones. Para con ello, establecer cuáles serán las soluciones de recuperación que deben implementarse.
- Realizar actualizaciones periódicas de los procesos BCP en función de los cambios en los procesos de negocio centrales, las recomendaciones de auditoría y las lecciones aprendidas.

Tenga presente que, el plan BCP ayudará a la organización a reanudar los servicios de manera eficiente y el mejor tiempo posible. Para la organización, los procesos orientados al cliente son críticos, por ello, el BCP debe demostrar las alternativas que la organización podría tomar frente a interrupciones.

Pero, ¿cómo podemos mapear las áreas que han de tomarse en cuenta para el desarrollo de este plan? Para ello, se debe articular un conjunto de criterios que deben considerar los aspectos y dominios de la organización que mencionamos a continuación.

- **Personas:** Se deberá identificar las estrategias apropiadas para mantener las habilidades y conocimientos básicos de las personas en la empresa. Esto incluye describir la estructura organizacional, los roles y funciones de la organización, planificaciones de sucesos, entre otros.
- **Lugar de trabajo:** La organización debe idear una estrategia para reducir el impacto de la indisponibilidad de los lugares normales de trabajo. Tenga en cuenta que, en la actual pandemia del COVID, las organizaciones que mejor se han adaptado son las que han podido trabajar de forma coordinada a través del teletrabajo.
- **Tecnología:** Se deben considerar planes BCP que involucren a la tecnología. Para ello, es importante comprender y describir sus actividades basadas en tecnología para poder desarrollar estrategias.
- **Información física y virtual:** Cualquier información requerida para entregar actividades críticas debe tener controles apropiados de confidencialidad, integridad, disponibilidad y encriptación.
- **Equipos y suministros:** La organización debe identificar y mantener un inventario de los suministros y equipos básicos que respaldan las actividades críticas. Las estrategias basadas en actividades pueden incluir el almacenamiento de suministros en ubicaciones alternativas, arreglos con terceros para la entrega de suministros, mantener ciertos materiales de suministro en almacenes separados o la identificación de fuentes de suministro alternativas.
- **Partes interesadas, socios y contratistas:** La organización debe desarrollar estrategias adecuadas para gestionar las relaciones con las partes interesadas clave, los socios comerciales o de servicios y los contratistas.

Como puede observarse, desarrollar un BCP significa considerar las amenazas de continuidad en relación con los vínculos e interconexiones de todas las principales actividades empresariales.

## 4.6. Catálogos de servicios TI

El catálogo de servicios TI es una guía que describe y orienta a la organización sobre los recursos TI disponibles. Sirve para alinear mejor los servicios con las necesidades de negocio, mejorar la satisfacción del cliente interno e implementar procesos estandarizados para lograr una mayor eficiencia operativa. Un catálogo de servicios de TI es un componente importante en la necesidad de mejorar el servicio al cliente. Como ejemplo, ITIL es un marco y una buena práctica que se basa en estos conceptos de servicio de TI y atención al cliente, el catálogo TI, sería el núcleo de estos conceptos fundamentales.

Para crear un catálogo de servicios TI se necesita determinar qué servicios se van a publicar a través del levantamiento de necesidades y requerimientos del cliente, luego se debería incorporar y desplegar esta solución. Para garantizar una iniciativa de servicios de TI exitosa y centrada en el cliente, las organizaciones deben seguir tres pautas para crear y desarrollar un catálogo de servicios de TI:

- 1. El catálogo de servicios de TI debe mapear las necesidades del cliente.** Se debe crear un catálogo de servicios con un enfoque inquebrantable en las necesidades internas del cliente. El error más común que cometan las organizaciones es poner demasiado énfasis en articular sus servicios desde una perspectiva de TI. Los clientes por lo general no quieren revisar las descripciones detalladas de los servicios en lenguaje técnico; quieren ver los servicios descritos en términos que puedan entender, escritos en terminología no técnica y que abordan inquietudes o necesidades inmediatas. Por ello, los catálogos de servicios exitosos se definen desde el cliente hacia adentro, en lugar de desde la infraestructura hacia afuera.
- 2. El catálogo de servicios de TI debe ser accionable.** Un catálogo debe incorporar vistas para el cliente con procesos de solicitudes de servicios, carrito de compras, entre otros. Asimismo, vistas para los ejecutivos TI que brinde una mayor transparencia en los elementos detallados del presupuesto de TI, los impulsores de consumo, los niveles de servicio y el impacto comercial de cada servicio. Finalmente, vistas para los empleados que les permita obtener servicios de soporte, por ejemplo, mantenimiento de equipos, creación de correos, entre otros.

- 3. El catálogo de servicios de TI debería ser un sistema de registro.** Un catálogo de servicios de TI procesable debe servir como un “sistema de registro” que permita administrar una organización de servicios de TI como un negocio dentro de un negocio. El catálogo de servicios de TI puede proporcionar el vehículo para administrar la demanda de los clientes, mapear los procesos de cumplimiento para cada servicio, garantizar el cumplimiento del nivel de servicio, impulsar la eficiencia de los procesos y realizar un seguimiento de los costos.

Un catálogo de servicios de TI puede ser la piedra angular del éxito en muchas iniciativas de TI centradas en el cliente. Al definir y publicar una cartera estándar de ofertas de servicios relevantes para el negocio, una función de TI puede comercializar su valor de manera más efectiva y establecer un marco para la comunicación con el negocio. Y al hacer que el catálogo de servicios sea operativo y transaccional, las operaciones de TI pueden ayudar a estandarizar los procesos de cumplimiento de servicios, administrar el consumo e impulsar la mejora continua.



### Actividades de aprendizaje recomendadas

#### Actividad 1

El video a continuación, proporciona una guía con estrategias de [Cómo elaborar un plan de continuidad del negocio](#)

#### Actividad 2

Ha finalizado la Unidad 4, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 4

Llea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. En la computación en la nube los recursos se ofrecen en Internet a través de:
  - a. Servicios.
  - b. Aplicaciones.
  - c. Infraestructura.
  
2. El concepto de computación en la nube evita que la organización deba:
  - a. Aprovisionar recursos TI.
  - b. Gestionar recursos TI.
  - c. Ambas respuestas son correctas.
  
3. Son los tipos de modelos de servicios en la nube:
  - a. IaaS, PaaS y SaaS.
  - b. IaaS, virtualización y computación móvil.
  - c. Computación en la nube, virtualización y computación móvil.
  
4. No es considerado un beneficio de la computación en la nube:
  - a. Escalabilidad.
  - b. Rendimiento.
  - c. BCP.
  
5. Proporciona un entorno de desarrollo y despliegue para crear aplicaciones en la nube:
  - a. BCP.
  - b. SaaS.
  - c. PaaS.

6. La virtualización es un esquema en donde:
  - a. Se expone, como servicios virtuales, los recursos TI en diferentes modelos.
  - b. Se imita características del *hardware* para crear sistemas virtuales.
  - c. Se aprovisiona los recursos TI de forma virtual.
7. Al hablar de computación móvil nos referimos al uso de:
  - a. Celulares o *tablets*.
  - b. Servicios.
  - c. Esquemas virtuales.
8. GASSP hace referencia a:
  - a. Conjunto de principios y prácticas para seguridad TI.
  - b. Tipos de modelos de servicios para la seguridad TI.
  - c. Conjunto de principios y modelos para la gestión de contenido empresarial.
9. El plan de continuidad del negocio BCP debe considerar:
  - a. Sistemas TI.
  - b. Procesos de negocio.
  - c. Sistemas TI y procesos de negocio.
10. El catálogo de servicios TI orienta a la organización sobre:
  - a. Los riesgos de seguridad TI.
  - b. Los principios de servicios TI.
  - c. Los recursos TI disponibles.

[Ir al solucionario](#)



## Unidad 5. Desarrollo, Configuración y Gestión de proyectos en el gobierno de TI

### 5.1. Aplicaciones SOA

La arquitectura orientada a servicios (SOA) permite crear aplicaciones comerciales como un conjunto de elementos acoplados y orquestados para brindar un buen nivel de servicio mediante su vinculación con los procesos de negocio.

Entre algunas características de SOA tenemos las siguientes (Hurwitz, Bloor, Kaufman, & Halper, 2009):

- SOA es para crear aplicaciones comerciales: En el ámbito tecnológico existe un sin número de arquitecturas de software y SOA no está destinado para todo tipo de aplicaciones. Está explícitamente dirigido a construir aplicaciones comerciales.
- Los componentes de SOA están débilmente acoplados: El término débil hace referencia a cómo los componentes interactúan dentro de SOA. Un componente pasa datos a otro componente y realiza una solicitud. El segundo componente lleva a cabo la solicitud y si es necesario devuelve los datos primero. El énfasis está en la simplicidad y autonomía. Cada componente es capaz de ofrecer una pequeña gama de servicios simples a otros componentes.

Un conjunto de componentes débilmente acoplados hace las mismas tareas que se realizan dentro de aplicaciones robustas y estructuradas, pero los componentes pueden combinarse y recombinarse de innumerables formas. Esto hace que la infraestructura de TI sea más flexible.

- Los componentes de SOA están orquestados para vincularse entre sí a través de procesos de negocio para brindar un nivel de servicio bien definido. SOA crea un arreglo que pueden, en conjunto, brindar

un servicio comercial muy complejo. Al mismo tiempo, SOA debe proporcionar niveles de servicio aceptables.

A continuación el siguiente recurso, le permitirá profundizar su aprendizaje, referente a las [Aplicaciones SOA y Gestión de la configuración de TI](#).

## 5.2. Implementación de sistemas y Gobierno de TI

En la gobernanza es de vital importancia poseer sólidos procesos sobre sus procesos de desarrollo de software.

Existen algunas metodologías para el desarrollo de software, entre ellas la “Metodología en Cascada”, es una de más antiguas y consta de una técnica lineal y consta de algunas fases que hay que ir completando para avanzar a la siguiente. Estás fases se detallan a continuación (Intelequia, 28):

1. Planificación: Antes de iniciar con el desarrollo de un proyecto de software se debe establecer varios estudios como: ámbito del proyecto, viabilidad, riesgos, costes y recursos de tal forma de evitar contratiempos en la ejecución del mismo.
2. Análisis: Esta fase se enfoca en hacer un levantamiento de requerimientos enfocándose en las necesidades de los stakeholders para definir cada una de sus funciones requeridas.
3. Diseño: Se define la estructura de desarrollo del sistema. Esta fase es compleja y debe realizarse de forma iterativa
4. Implementación: Una vez entendido las necesidades y el diseño del aplicativo, se procede a seleccionar las herramientas, entornos de desarrollo y el lenguaje de programación adecuado.
5. Pruebas: Se evalúa si el software cumple con la calidad necesaria para satisfacer al cliente. La fase de pruebas busca cualquier error para ser corregido antes del despliegue.
6. Instalación/Despliegue: En dicha fase el software entra en funcionamiento tomando en cuenta su planificación oportuna del entorno en que va a ser ejecutado: equipos, redes, sistemas operativos, seguridades, etc.

7. Uso y mantenimiento: A lo largo del tiempo el software requiere de mantenimiento como eliminar los defectos encontrados en su uso, adaptarlo a nuevas necesidades y funcionalidades.

Existe una gran variedad de metodologías para el ciclo de vida de software, entre ella la más tradicional denominada “Cascada”, y otras propuestas en el mercado actual como las metodologías ágiles: “Scrum”, “Kanban”, “Extreme Programming XP”, etc.

Las últimas surgieron al ver que el método tradicional no cumplía con las realidades que se vive en el día a día del desarrollo de software, entre algunas podemos mencionar el retraso en la toma de decisiones y poca planificación adaptativa.

A continuación, se expone una tabla comparativa para evaluar sus principales diferencias:

**Tabla 7.**  
*Comparación Metodología tradicional vs. ágiles*

Metodologías Tradicionales	Metodologías Ágiles
Cierta resistencia a los cambios	Preparados para cambios en el proyecto
El cliente interactúa con el equipo de desarrollo en las reuniones	El cliente es parte del equipo de desarrollo
Varios artefactos	Pocos artefactos
Pocos ciclos de entrega	Varios ciclos de entrega
Procesos controlados con varias políticas	Procesos con menos controles y principios

Nota. Adaptado de Orjuela Duarte, A., & Rojas C., M. (2 de junio de 2008). Las Metodologías de Desarrollo Ágil como una Oportunidad para la Ingeniería del Software Educativo. Medellín, Colombia

En el desarrollo de software, el gobierno de TI debe conocer el rol de los auditores de TI que participan en este tipo de proyectos. El tener un auditor ayuda a validar las siguientes actividades:

- Identifican riesgos
- Verifican que exista cumplimiento de aplicación de estándares, políticas, procedimientos y regulaciones
- Estudia el sistema de seguridad y evalúa los métodos de accesos permitidos.

Adicional a ello, para satisfacer los estándares de cumplimiento los gerentes de proyectos pueden utilizar buenas prácticas que le sirvan de guías de monitoreo y control; entre algunas podemos mencionar: PMBOK, CMMI, ISO 10006:2007, ISO IEC 12207:2008 y COBIT 2019.



## Actividades de aprendizaje recomendadas

### Actividad 1

Estimado estudiante, es importante que conozca qué es y cómo se desarrolla un [plan de TI](#). Ya que esta es una herramienta importante para restablecer los servicios que impactan directamente en las empresas.

### Actividad 2

Revise el siguiente ejemplo que le ayuda a comprender cómo se estructura un [plan de continuidad de servicios de TI](#)

### Actividad 3

Estimado estudiante, revise el presente video el cual presentará prácticas, mecanismos de control, procesos, estructuras de gobierno necesario para el éxito de implementación de SOA, por ello le invito a visitar [Análisis SOA](#)



## Semana 12

---

### 5.3. Gestión de portafolios, proyectos y programas en el gobierno de TI

En la presente sección se demostrará la importancia de implementar un estándar reconocido para la gestión de proyectos y programas.

#### Gobernanza y PMBOK

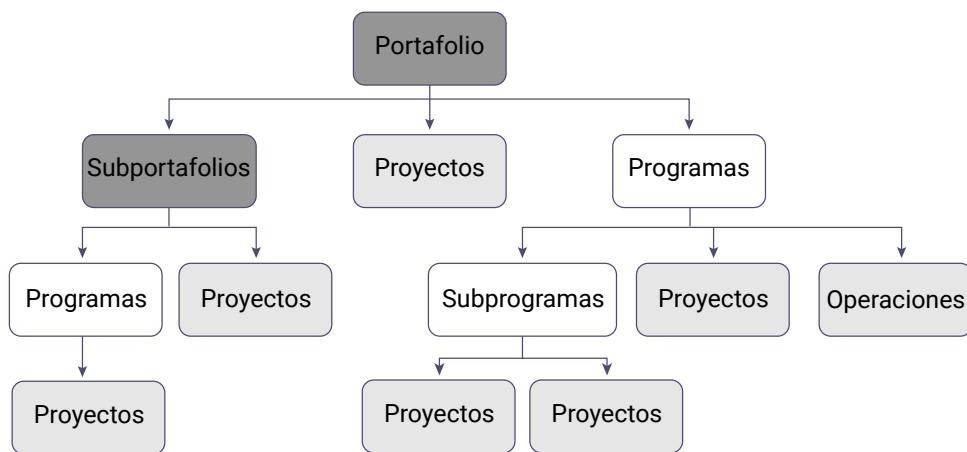
PMBOK proporciona conceptos, lineamientos, ciclo de vida de la dirección de proyectos y del proyecto y todos los procesos relacionados. Este documento estándar proporciona un vocabulario común para los interesados en la gestión de proyectos y programas.

Para (Project Management Institute., 2017), un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. Este resultado puede ser tanto tangible o intangible. Se puede considerar como proyecto el desarrollo de un nuevo sistema, producto, migración de plataformas, cambio organizacional, compra de un nuevo hardware, etc.

De acuerdo a (Project Management Institute, 2008) existen portafolios, proyectos y programas. La gestión de portafolios es aquella gestión coordinada de los componentes del portafolio para lograr los objetivos organizacionales definidos (p.2). Dicha gestión crea una oportunidad para que el cuerpo de gobierno tome decisiones que controlen o influyan en la dirección de un grupo de componentes (subportafolio, programa, proyectos) a medida que trabajan para lograr resultados definidos. El objetivo de la gestión de portafolio es garantizar que la organización esté haciendo el trabajo correcto.

**Figura 15.**

*Portafolio, programas y proyectos – Vista de alto nivel*



Nota. Adaptado de Portfolios, Programs, and Projects – High Level View [Fotografía], por Project Management Institute ,2008, The Standard For Portfolio Management – Third Edition

A continuación se presenta la comparativa de portafolios, proyectos y programas para mejor entendimiento.

**Comparativa entre proyectos, programas y portafolios.**

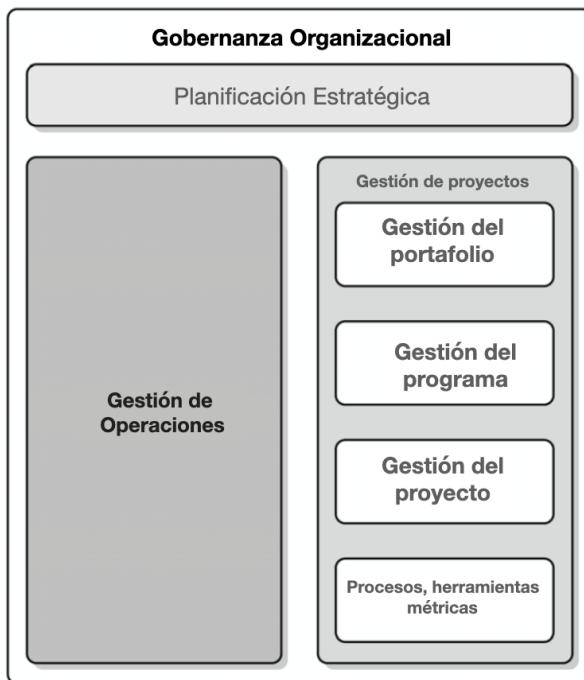
De acuerdo al (*Project Management Institute, 2008*), las organizaciones tienen Frameworks de gobierno para guiar cada una de las actividades de las organizaciones. El gobierno del portafolio de proyectos es un conjunto de procesos organizacionales interrelacionados mediante los cuales una organización prioriza, selecciona y asigna recursos internos limitados para lograr mejor los objetivos organizacionales (p.5).

La gestión de portafolios es una disciplina dentro del gobierno organizacional. Las organizaciones que no vinculan la gestión del portafolio con la gobernanza aumentan el riesgo de que las iniciativas desalineadas o de baja prioridad consuman recursos críticos. Por lo tanto, la aplicación de las técnicas de gestión de portafolios en el contexto del gobierno de la organización proporciona una seguridad razonable de que se puede lograr la estrategia de la organización.

La siguiente imagen ilustra las relaciones entre el gobierno organizacional, la gestión operativa y la gestión de proyectos que componen el portafolio. Los principios de gobierno aseguran la alineación entre las actividades resultantes y la estrategia organizacional.

**Figura 16.**

*Relación entre gobierno, operaciones y gestión del portafolio*



Nota. Adaptado de Relationships among organizational governance, operations, and portfolio management [Fotografía], por Project Management Institute ,2008, The Standard For Portfolio Management – Second Edition

### 5.3.1. Gobernanza y PMO

En lo que refiere a proyectos, la dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas, técnicas a las actividades del proyecto para cumplir con los requerimientos o alcance que viene direccionado por los objetivos del programa o portafolio.

Entre sus principales actividades encontramos (Moeller, 2013)(p.285):

- Asesoramiento y guía interna: Con el afán de proveer una buena gestión de proyectos, la PMO asesora a los colaboradores con las mejores prácticas del PMBOK.
- Herramientas de software para la gestión de proyectos: Selecciona aquellas herramientas que serán de uso para los participantes de los proyectos.

- Gestión de portafolio: Ayuda una guía para gestionar múltiples proyectos relacionados.
- Aborda todas las necesidades, exceptivas de los stakeholders en la planificación y ejecución del proyecto.
- Mantiene comunicaciones activas entre todos los interesados

Para PMBOK, la oficina de gestión de proyectos (PMO) es una estructura que estandariza los procesos de gobierno relacionados con el proyecto. Su responsabilidad es de gestión y apoyo. Constituye, además, un vínculo natural entre los portafolios, programas y proyectos de la organización y tiene la autoridad de actuar como un interesado integral y tomar decisiones importantes a lo largo del ciclo de vida del proyecto.

Existen los siguientes tipos de PMOS que se detallan a continuación:

**Tabla 8.**

*Tipos de PMO*

Tipo de PMO	Rol	Función	Grado de control
De apoyo	Consultivo (Repositorio de proyectos).	Recomiendan mejores prácticas, capacitaciones y lecciones aprendidas.	Reducido
De control	Apoyo, supervisión y control	Imponen la adopción de estándares, Frameworks, metodologías.	Moderado
Directiva	Dirección	Asumen la dirección integral.	Elevado



### Actividades de aprendizaje recomendadas

#### Actividad 1

Ha finalizado la Unidad 5, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 5

Lea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. Es la arquitectura que permite crear aplicaciones comerciales como un conjunto de elementos acoplados y orquestados para brindar un buen nivel de servicio, mediante su vinculación con los procesos de negocio.
  - a. Arquitectura por capas.
  - b. Arquitectura orientada a servicios.
  - c. Arquitectura cliente-servidor.
2. ¿Cuál es el motivo por el cual las gerencias implementan SOA?
  - a. Permite saber qué tareas ejecuta un servicio y qué políticas lo rodean.
  - b. Aumento de costos.
  - c. Fácil de implementar.
3. El gobierno de SOA trata los siguientes aspectos:
  - a. Visión, objetivos, casos de negocio, y modelo funcional, arquitecturas de referencia, políticas, estándares y formatos.
  - b. Portafolio de aplicaciones, portafolios de arquitectura, portafolios de proyectos.
  - c. Detectar nuevos CI y agregarlos a los CMS.
4. ¿Qué framework permite gestionar la configuración de TI?
  - a. PMBOK.
  - b. TOGAF.
  - c. ITIL 2019.

5. A nivel de gestión de configuración de TI, ¿cuáles son los conceptos por los cuales las empresas suelen mostrar interés?
  - a. Control de activos, gestión de incidencia, acuerdos en los niveles de servicio.
  - b. Arquitectura actual, futura y transición.
  - c. Ciclo de vida del desarrollo, arquitectura de sistemas, patrones de desarrollo.
6. Usted, en posición de jefe de desarrollo del departamento de TI, ¿qué tipo de metodología de desarrollo recomendaría implementar si desea que su equipo esté preparado para cambios en el proyecto y deba realizar varios ciclos de entrega?
  - a. Metodología en cascada.
  - b. COBIT 2019.
  - c. Metodología ágil.
7. En el desarrollo de software, uno de los roles del gobierno de TI es:
  - a. Control de calidad.
  - b. Auditores de TI.
  - c. Líder de proyecto.
8. La gestión del portafolio es una disciplina dentro del:
  - a. Gobierno organizacional.
  - b. Gobierno de TI.
  - c. Gobierno de riesgos y controles.
9. ¿Cuáles son los tipos de PMO que existen?
  - a. Portafolio, programa y proyecto.
  - b. Directivo, control y apoyo.
  - c. Planificación, cambio y monitoreo.

10. La oficina de PMO se encarga de:

- a. Sistemas e infraestructura física de administración de software como: administración de redes, almacenamiento en nube, seguridades.
- b. Los gastos que abarca el desarrollo de innovaciones tecnológicas para la empresa.
- c. Estandarizar los procesos de gobierno relacionados con el proyecto. Su responsabilidad es de gestión y apoyo.

[Ir al solucionario](#)



En esta semana vamos a revisar qué es la gestión del contenido empresarial ECM, las características, los procesos y la creación de este documento que nos permite monitorear los flujos de información clave de la organización. También, estudiaremos la importancia de la auditoría interna en la gobernanza empresarial.

## **Unidad 6. Monitoreo y medición del Gobierno de TI**

---

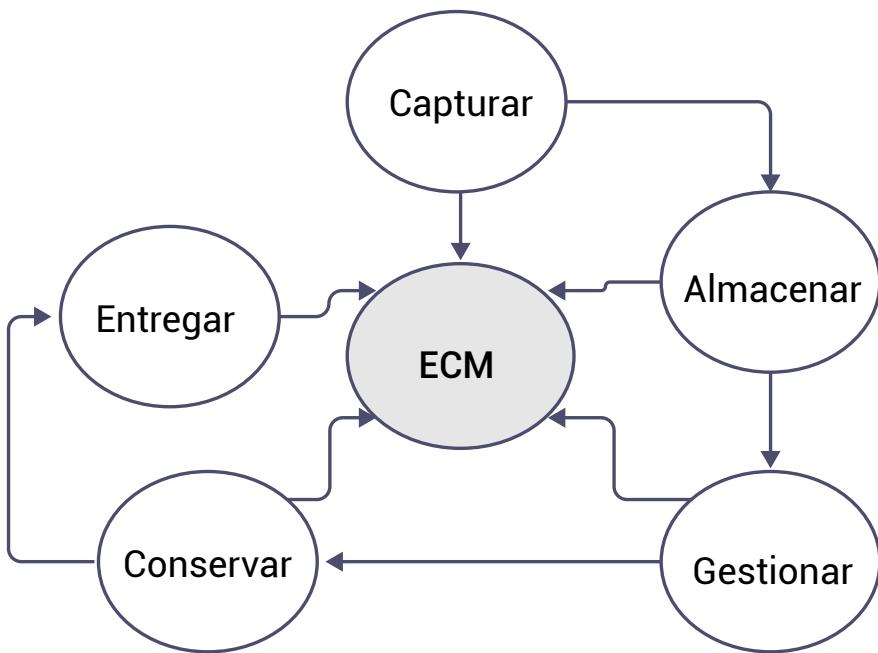
En la presente unidad vamos a revisar dos temas clave que permiten monitorear y medir el gobierno TI y además agregan valor empresarial.

### **6.1. Gestión del contenido empresarial - ECM**

La gestión del contenido empresarial (ECM – Enterprise Content Management) describe las estrategias, los métodos y las herramientas utilizadas para capturar, almacenar, gestionar, conservar y entregar el contenido y los documentos relacionados a los procesos de negocio de la organización. ECM es un sistema de organización y recopilación de información estratégica.

ECM se utiliza para describir el flujo de la información de la organización, sea que este flujo incorpore documentación, aplicaciones, bases de datos, correos electrónicos, entre otros. Es decir, todo el ciclo de vida de la información empresarial independientemente de dónde se encuentre almacenada. En la imagen a continuación, podrá observar los objetivos de ECM: capturar, almacenar, gestionar, conservar y entregar información.

**Figura 17.**  
*ECM insumos y proceso.*



En el siguiente recurso, podrá apreciar la descripción de los procesos ECM.

[Procesos de la arquitectura ECM.](#)



### Actividades de aprendizaje recomendadas

#### Actividad 1

Revise en internet software ECM existente y haga una lista priorizada de las soluciones más utilizadas para gestionar el contenido empresarial y cuáles son las ventajas.



Semana 14

En esta semana vamos a revisar cómo la auditoría interna hace parte en la gobernanza de TI a través de sus procesos de revisión y evaluación.

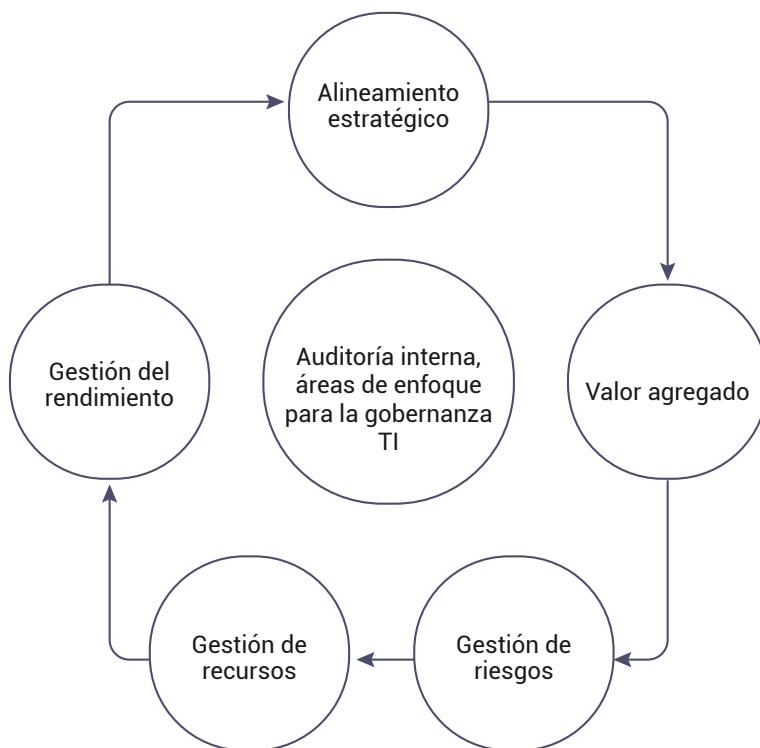
## 6.2. Auditoría interna

Uno de los objetivos de la auditoría interna respecto a TI es el de evaluar si el gobierno de TI persigue y respalda las estrategias y los objetivos de la organización, es decir, se trata de analizar si la infraestructura de TI de una organización alinea y sostiene los procesos comerciales para administrar adecuadamente los objetivos a largo plazo.

Recordemos que los principales objetivos del gobierno TI son asegurar que los recursos TI generen valor y mitigar los riesgos inherentes a estos recursos. Las actividades de auditoría interna pueden abonar a la gobernanza TI a través de revisiones y evaluaciones en cinco áreas generales: entrega de valor, gestión de riesgos, gestión de recursos, gestión del rendimiento y alineación estratégica.

**Figura 18.**

*Rol de la auditoría interna en la gobernanza de TI.*



Nota. Adaptado de Quality Management System Process [Fotografía], por Moeller, R., 2013, *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*

En la imagen podemos observar la participación de la auditoría interna con respecto a la gobernanza de TI. A continuación, vamos a definir qué implica esta participación en cada una de estas áreas:

- **Alineamiento estratégico:** Revisar y evaluar cómo TI se alinea con la misión, visión, valores, objetivos y estrategias de la organización. Debe haber un enfoque integrado entre negocio y la estrategia TI, con corresponsabilidades entre ambos.
- **Entrega de valor:** El auditor interno debería revisar y evaluar la entrega de valor de TI. Los recursos TI deberían seguir abordando las estrategias establecidas
- **Gestión de riesgos:** El auditor interno debería revisar y evaluar los riesgos que pueden afectar negativamente al entorno TI.
- **Gestión de recursos:** El auditor interno debería revisar y evaluar la eficacia de los recursos de TI.
- **Gestión del rendimiento:** El auditor interno debería revisar y evaluar la eficacia de los procesos de gestión del rendimiento. Revisar si la función TI tiene una declaración clara sobre el desempeño esperado por el negocio (efectividad y eficiencia) y evaluar su logro. También, revisar y evaluar el cumplimiento de los requisitos legales, ambientales y de calidad.



## Actividades de aprendizaje recomendadas

### Actividad 1

Ha finalizado la Unidad 6, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 6

Lea detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. ¿Qué significan las siglas ECM?
  - a. Gestión del contenido empresarial.
  - b. Gestión de riesgos.
  - c. Gobernanza, riesgo, cumplimiento.
  
2. ECM es un sistema de organización y recopilación de:
  - a. Seguridad de información.
  - b. Auditoria interna.
  - c. Información estratégica.
  
3. No es un objetivo de ECM:
  - a. Capturar información.
  - b. Destruir información.
  - c. Almacenar información.
  
4. En ECM se considera la información que es almacenada de forma:
  - a. Virtual.
  - b. Física y virtual.
  - c. Física.
  
5. Uno de los objetivos de la auditoría interna es evaluar si el gobierno TI está alineado a:
  - a. La estrategia empresarial.
  - b. La infraestructura.
  - c. Los recursos TI.

[Ir al solucionario](#)



## Unidad 7. Generalidades de empresa y el gobierno de TI

### 7.1. Cultura organizacional

Para el gobierno en general, no solo de TI es importante establecer una cultura organizacional con misión, visión y valores que ayuden al gobierno a guiar la toma de decisiones y comportamiento ético tanto para ellos como para todos los que conforman la organización. Al tener una cultura organizacional sólida, la empresa podrá prevenir cualquier conflicto que impacte los intereses de la misma.

La misión declara el propósito de existir de la organización. Como ejemplo de misión podemos indicar a de Microsoft:

*"Nuestra misión es empoderar a todas las personas y organizaciones del planeta para que puedan lograr más"*

La visión está enfocada en el futuro e indica lo que quiere lograr a posterior. A continuación, le mostramos un ejemplo:

*"Brindar mayor poder a la gente a través de un excelente software– en cualquier momento, en cualquier lugar y en cualquier dispositivo"*

Los valores: Define los principios éticos, morales y empresariales de una organización. Entre ellos encontramos el respeto, integridad, responsabilidad, etc.

La cultura organizacional es beneficiosa ya que actúa en dos frentes: interno y externo. El interno abarca toda la relación de la empresa con sus trabajadores, clima laboral, bienestar, etc.; mientras que el externo abarca su actitud social con el ambiente que le rodea como imagen corporativa, filosofía ecológica, temas gubernamentales entre otros.

Otro aspecto importante a considerar dentro de la cultura organizacional es el código de conducta empresarial. De acuerdo a (Grupo Cavala, s.f.), un código de conducta es un instrumento de gestión que da los lineamientos

para perfilar las prácticas y comportamientos que deben promocionarse o prohibirse en una organización basados en valores, principios y creencias. Este debe ser cumplido desde la alta gerencia hasta los colaboradores operativos que conforman la empresa.

De acuerdo a (Moeller, 2013) (p.341) La alta gerencia de la empresa debe reunir un equipo de gerentes financieros y de operaciones de la unidad, representantes de auditoría interna y aseguramiento de la calidad, comunicaciones corporativas, recursos humanos y, ciertamente, el área legal corporativa para construir o reconstruir un código de conducta efectivo que promueva prácticas comerciales éticas en toda la empresa.

Según (Ramirez, 2020), un código de ética debe contener algunos de los siguientes aspectos:

- Cumplimiento a la legislación vigente de cada país: Se debe respetar lo establecido en las organizaciones legislativas a nivel laboral y constitucional en general.
- Respeto por las personas e igualdad de trato: No debe existir violencia, acoso sexual, ni discriminación por religión, raza, edad, sexo en el trato de las personas que colaboran en la institución. Cualquier tipo de infracción en este aspecto la empresa debe alentar a su denuncia.
- Respeto por los derechos humanos: Es importante que se incluya este aspecto ya que se debe evitar el trabajo forzoso, esclavitud o trabajo infantil.
- Conflictos de interés: Ayuda a dejar en claro cómo tratar estos conflictos, por lo general las empresas exigen a los empleados que cualquier decisión que tomen debe hacerse en interés de la empresa delante del personal.
- Transparencia: La transparencia siempre debe usarse en la toma de decisiones y en las actividades diarias de la empresa. Esta debe ser usada por todos los empleados incluidos los de la alta dirección.
- Seguridad y Medioambiente: Son las directrices que se deben cumplir para la seguridad del medioambiente.

- Protección de seguridad de la información: Es importante declarar normas que eviten la fuga de información de la compañía a terceros ajenos a la empresa.
- Imagen corporativa: Declara su reputación, valores y principios por lo que es necesario especificarla en el código de conducta ya que es la portada con la que se presenta la empresa al exterior.
- Responsabilidad social corporativa: Declara su responsabilidad destacando su compromiso con esta área.

Este código debe estar respaldado por acciones y respuestas hacia las violaciones de cada uno de los parámetros. Por lo general su manejo puede gestionarse mediante el departamento de recursos humanos que conllevaría a alguna sanción verbal, escrita o despido dependiendo al nivel de gravedad de la falta realizada. Si alguna falta violenta derechos civiles puede ser denunciado a autoridades externas.

Para (Moeller, 2013) (pp.352-353) las organizaciones deben tener un programa de ética ya que mejorará las prácticas de gobierno corporativo para toda la empresa en lugar de solo para las personas en la oficina ejecutiva. De acuerdo a su libro, indica que se debe considerar las siguientes cinco acciones para el lanzamiento eficaz de estos programas:

1. Política corporativa: Los altos mandos deben promover en la empresa la necesidad de llevar todas sus preocupaciones sobre aspectos financieros a la dirección sin tomar represalias sobre ellos.
2. Programa de preocupaciones de los empleados: Todas las inquietudes presentadas por los empleados deben ser confidenciales o anónimas. Estas deben ser investigadas y controladas por el personal pertinente.
3. Formación de supervisores: Se debe incentivar una buena comunicación entre los supervisores y sus colaboradores para que exista la confianza y seguridad de que sus preocupaciones van a ser atendidas sin afectar su trabajo en la institución.
4. Orientación a contratistas: Debe existir una cláusula que proteja a sus empleados en los contratos con proveedores externos.

5. Encuestas a los empleados: Mediante la retroalimentación de estas encuestas se podrá evaluar la cultura organizativa y si los mismos sienten la libertad de expresar sus preocupaciones.

## 7.2. Redes sociales en el gobierno corporativo

Las redes sociales son plataformas digitales que permiten a las personas interactuar entre sí a través del internet. Si bien es cierto, en la actualidad existe un sin número de redes como Facebook, Twitter, Instagram, TikTok, etc. Pero ¿cómo estás pueden llegar a impactar las organizaciones y por qué el gobierno corporativo debe preocuparse por su uso?

Las empresas al no tener una política que controle la utilización de las redes de sus empleados corre muchos riesgos entre ellos la pérdida de clientes, pérdida de reputación, virus y software espía incluso problemas legales simplemente con la publicación de un comentario, foto o video que no debería circular por el internet. Estos riesgos están netamente atados al comportamiento de los individuos que están fuera de los límites de la infraestructura de la empresa o los sistemas de TI.

Por tal motivo, el objetivo de la política es establecer que los colaboradores las usen con el criterio adecuado y que cualquiera de sus publicaciones a nivel personal o corporativo no comprometan a la organización en la que se encuentran.

A continuación, se detalla algunas pautas a considerar en la política de redes sociales (Acsendo, 2013):

- Sentido común: Los colaboradores deben ser conscientes de su forma de actuar y responder en las redes sociales. Se debe evitar el uso de palabras ofensivas.
- Separar perfiles: El colaborador debe declarar en alguna publicación que es su opinión personal y no la de la empresa. Para ello si existe alguna inconformidad dentro del trabajo debe ser tratada de forma interna y no públicamente.
- Información reservada: Se debe evitar la fuga de información por estos medios para evitar que información confidencial o sensible que pueda llegar a afectar a la empresa.

- Derechos de autor: Siempre se debe de citar las fuentes utilizadas en cualquier publicación para evitar conflictos. Adicionalmente, se debe verificar que dicha fuente es verídica y comprobada.
- Valores: Los valores siempre deben prevalecer en el uso de las redes. Por lo tanto, se debe prohibir insultos, falsas expectativas, discusiones, controversias en los medios que podrían dañar la imagen corporativa.
- Manejo de crisis: Debe existir procedimientos para controlar y solventar el uso inadecuado de las redes.
- Sanciones: Se debe dar a conocer al personal que cada acción realizada en las redes sociales y que atente con el bienestar de la empresa tendrá su sanción. Esta puede ir desde una amonestación en sueldo o incluso el despido.

### 7.3. Comité de auditoría

Para finalizar los contenidos de esta materia, es de vital importancia que conozca el rol del comité de auditoría y su relación con el gobierno de TI.

Las empresas están administradas por juntas directivas que son elegidas por los accionistas y roles de las principales actividades de gestión; estos miembros pueden ser pertenecientes a los miembros de administración (internos) o totalmente independiente de las actividades de las empresas (externos).

El comité de auditoría es un director importante para las juntas directivas ya que tienen la responsabilidad de evaluar los controles internos y la supervisión de datos financieros. De acuerdo a (Flores), “la existencia y buen funcionamiento del comité de auditoría son sinónimos del grado en que las prácticas de gobierno corporativo realmente se aplican. Su efectividad e independencia de actuación generan gran confianza entre socios, inversionistas y acreedores, e incluso de clientes y entidades gubernamentales de supervisión, fiscalización y control”.

De acuerdo a (Ley Sarbanes-Oxley, 2002) “Es un comité (o cuerpo equivalente) establecido por y dentro de una junta de directores de un emisor, con la finalidad de supervisar los procesos de reportaje de

contabilidad y financiero del emisor, y auditorías de los estados financieros del emisor”.

Entre sus principales funciones se pueden detallar (Flores):

- Son los encargados de la selección, designación, compensación, supervisión de auditores internos y externos.
- Aseguran la independencia de criterio de actividad de auditoría externa e interna.
- Ayudan a reforzar los procesos de supervisión de la organización
- Evalúan los riesgos, oportunidades y retos de la empresa
- Informan a la junta directiva y a la junta general de accionistas
- Evalúan la efectividad del control interno, cumplimiento de disposiciones, criterios y prácticas contables correctas, la auditoría interna.

El comité de auditoría también está a cargo de la auditoría de TI, que conjuntamente con la auditoría interna juegan un rol importante para la evaluación de controles internos sobre informes financieros y procesos de TI. Estos evalúan también los riesgos relacionados con la seguridad informática y problemas de gobierno de TI. (Moeller, 2013) (373)

Adicional, (Moeller, 2013) (p. 375) comenta que algunos de los gerentes de nivel superior que sirven en comités de auditoría, suelen desconocer los problemas y preocupaciones de gobernanza de TI. Los ejecutivos a nivel de comité de auditoría a menudo se han familiarizado con un número limitado de problemas de gobernanza relacionados con TI, tales como los planes adecuados de continuidad de TI, posibles problemas legales con el uso de las redes sociales o los ataques de virus/malware en la organización. Sin embargo, este autor, recomienda que la alta dirección y las auditorías de TI traten temas más técnicos con el comité de auditoría a pesar de que su comunicación sea un poco compleja ya que por lo general estos comités tratan asuntos netamente financieros y de riesgos no enfocados directamente con TI.

Por tal razón, (Moeller, 2013)(p.375) indica que para algunas empresas ha sido de gran utilidad implementar una sesión informativa trimestral con el

comité de auditoría sobre los riesgos de gobierno de TI empresarial y los problemas en evolución. Este tipo de sesiones ayudará a asesorar a los miembros del comité sobre el gobierno de IT y cualquier problema de riesgo y se puede realizar entre los integrantes de la auditoría de TI, el CIO y el director ejecutivo de auditoría.



## Actividades de aprendizaje recomendadas

### Actividad 1

Lea el recurso propuesto para que pueda comprender de mejor manera el [comité de auditoría](#). En el recurso se presentan definiciones principios, características.

### Actividad 2

Estimado estudiante, revise el presente video sobre la cultura organizacional que le ayudará a entender cómo el departamento de recursos humanos la gestiona en todas sus aristas, por ello le invito a revisar [Activación de la cultura organizacional](#)

### Actividad 3

Estimado estudiante, revise el presente video con ejemplos que le indicarán el [impacto real del uso de las redes sociales en las empresas](#).

### Actividad 4

Ha finalizado la Unidad 7, por lo que es necesario que evalúe sus conocimientos para ir reforzando aquellos temas no comprendidos. Las respuestas se encuentran al final del texto guía para su retroalimentación.



## Autoevaluación 7

Ley detenidamente cada una de las preguntas y seleccione la alternativa correcta según corresponda.

1. Dentro de la cultura organizacional se deben considerar:
  - a. Misión, visión, valores.
  - b. Planificación, presupuestos, riesgos.
  - c. Personas, información y tecnología.
2. Para construir o reconstruir un código de conducta efectivo la alta gerencia debe reunir un equipo con los siguientes cargos:
  - a. Gerentes de posventa, ventas y recursos humanos.
  - b. Accionistas y gerente general.
  - c. Gerentes financieros y de operaciones, representante de la auditoría interna, aseguramiento de calidad, área legal corporativa.
3. ¿Cuál de los siguientes motivos es de preocupación para el gobierno corporativo, en lo que refiere al uso de redes sociales?
  - a. Pérdida de clientes, pérdida de reputación, virus y software espía, problemas legales.
  - b. El uso de redes sociales no es motivo de preocupación.
  - c. Únicamente el área de *marketing* es quién realiza las publicaciones redes sociales.
4. ¿Qué pautas se debe considerar para crear una política de uso de redes sociales?
  - a. Recompensas por su mal uso.
  - b. Red social, fecha de publicación, autor de publicación.
  - c. Separación de perfiles, evitar fuga de información, derechos de autor.

5. ¿Cuáles son las funciones del comité de auditoría?
- a. Selección, designación, compensación, supervisión de auditores internos y externos; ayudan a reforzar los procesos de supervisión de la organización.
  - b. Selecciona aquellas herramientas que serán de uso para los participantes de los proyectos.
  - c. Aborda todas las necesidades exceptivas de los *stakeholders* en la planificación y ejecución del proyecto.

[Ir al solucionario](#)



## Actividades finales del bimestre

Estimados estudiantes culminamos con el estudio del segundo bimestre. Por ello, le invitamos a prepararse para rendir la evaluación presencial correspondiente al segundo bimestre. Le sugerimos algunos lineamientos que pueden ayudarle:

- Revise las unidades estudiadas a lo largo del segundo bimestre.
- Refuerce cada uno de los contenidos, realizando lecturas rápidas y tomando nota de los ítems importantes mostrados en cada semana.
- Realice las autoevaluaciones sugeridas en cada unidad.
- Comuníquese con su tutor en caso de presentar dudas.
- Finalmente, tenga presente las fechas para rendir la evaluación presencial del segundo bimestre.

¡Muchos éxitos!



## 4. Solucionario

Autoevaluación 1		
Pregunta	Respuesta	Retroalimentación
1	c	La ley de Sarbanes – Oxley se creó con el fin de transparentar las actividades que se realizan en la operación del negocio e introducir nuevas responsabilidades al gobierno corporativo.
2	a	El gobierno corporativo es el encargado de dirigir, evaluar y monitorear las actividades del negocio, para asegurarse que este realizando de forma ética y en base a buenas prácticas.
3	c	¿Cómo se aseguran los proveedores de finanzas de que los gerentes no roban el capital que suministran o lo invierten en malos proyectos?
4	c	El gobierno de TI es el encargado de dirigir las operaciones de TI, con el fin de proporcionar valor al negocio y reducir los riesgos.
5	a	Costo por estación de trabajo y por transacción están orientados a la infraestructura tecnológica.
6	b	Se debe tomar en cuenta que el gobierno de TI permite evaluar de forma holística cada componente que involucra tecnología en la organización; por tal motivo, ayuda a prevenir pérdidas financieras, procesos de negocios afectados y el bajo cumplimiento, ya que el personal del gobierno debe asegurarse de tomar las mejores decisiones que permitan apoyar y evolucionar el estado de sus tecnologías.
7	a	Proporcionar pautas de arquitectura es responsabilidad de la Junta de revisión de arquitectura de TI, mientras que las pautas tecnológicas hacen referencia al Consejo Tecnológico.
8	b	La supervisión de los riesgos de TI y aceptar riesgos residuales de TI es actividad del CEO; mientras que el asegurar que la arquitectura de TI refleje la necesidad de cumplimiento normativo es actividades de la Junta de revisión de arquitectura de TI.
9	c	El cumplimiento de los estándares y pautas tecnológicas es actividad del Consejo Tecnológico; la supervisión y dirección de los procesos claves de gobernanza de TI es del Comité directivo de TI.

## Autoevaluación 1

Pregunta	Respuesta	Retroalimentación
10	a	La gobernanza de TI dirige las decisiones en el ambiente tecnológico y el gobierno corporativo dirige decisiones de toda la empresa.

[Ir a la  
autoevaluación](#)

Autoevaluación 2		
Pregunta	Respuesta	Retroalimentación
1	b	Las siglas GRC significan gobernanza, riesgo y cumplimiento.
2	a	La gobernanza persigue gestionar los requisitos de toda la organización, incluyendo los requisitos TI.
3	a	La gestión de riesgos implica gestionar diversos eventos. Esta gestión tiene que ver con asumir o mitigar los riesgos empresariales.
4	c	En el cumplimiento se debe establecer controles para garantizar que la organización opera de acuerdo a diversas normas.
5	a	Los principios de gobernanza están directamente relacionados con las políticas internas.
6	b	Los principios de cumplimiento están directamente relacionados con las regulaciones externas.
7	a	En la gobernanza GRC se consideran aspectos internos y externos.
8	b	La identificación y análisis de los riesgos implica: cuantificar el impacto, mitigar los riesgos y considerar factores financieros.
9	a	El cumplimiento debe considerar el siguiente alcance de la estrategia, los procesos, las aplicaciones y datos, y la infraestructura de la organización.
10	b	Implementar sistemas integrados es una práctica GRC.

[Ir a la autoevaluación](#)

Autoevaluación 3		
Pregunta	Respuesta	Retroalimentación
1	a	Las NIFF y método cuantitativo no son marcos o estándares utilizados en la implementación de un gobierno de TI.
2	a	EDM (evaluar, dirigir, monitorear), APO (alinear, planificar y organizar), BAI (construir, adquirir e implementar), BAI (construir, adquirir e implementar), DSS (entregar, dar servicio y soporte), MEA (monitorizar, evaluar y valorar) son parte de COBIT 2019.
3	c	Proveer valor a los interesados, enfoque holístico, gobierno dinámico, diferencia entre gobierno y gestión, adaptable, sistema de extremo a extremo son los principios básicos de COBIT, sirven como pautas para la gestión del día a día de los sistemas de información.
4	a	En prácticas de servicio encontramos a gestión de disponibilidad, control de cambios, gestión de incidentes, etc. Prácticas técnicas abarca desarrollo de software, gestión de plataformas, entre otras.
5	b	El ISO 38500 proporciona un marco de seis principios que ayudan a asegurar el cumplimiento normativo y la correcta implementación de los recursos de TI.
6	c	El principio de "Adquisición" se basa en las necesidades detectadas tras un análisis pertinente. El principio de "Factor Humano" refiere a políticas prácticas y las decisiones de TI deben considerar el comportamiento humano.
7	b	La gestión de riesgos permite identificar, en una fase temprana, cualquier vulnerabilidad que afectar a la operación del negocio.
8	a	Zachman es un framework que ayuda a la arquitectura empresarial más no a la ISO 38500.
9	b	Las normas ISO son conocidas por garantizar que las empresas cumplan con los más altos estándares para brindar calidad, seguridad y eficiencia en sus productos.
10	a	La ISO 9001 se enfoca en productos y servicios de calidad; mientras que 27001 en la seguridad de la información. El ISO 17799 es una norma que describe el código de buenas prácticas para la gestión de seguridad y el 38500 se enfoca en el gobierno de TI.

**Ir a la  
autoevaluación**

Autoevaluación 4		
Pregunta	Respuesta	Retroalimentación
1	a	En la computación en la nube los recursos se ofrecen en Internet a través de servicios.
2	c	Cuando se aplica computación en la nube se evita que la organización aprovisione y gestione la infraestructura de recursos TI.
3	a	Los tipos de modelos de servicios en la nube son IaaS, PaaS y SaaS.
4	c	El BCP es el plan de continuidad del negocio y no tiene que ver con los conceptos en relación a la computación en la nube.
5	c	El modelo PaaS es un modelo de desarrollo y despliegue para crear aplicaciones.
6	b	La virtualización es un esquema en donde se imita características del hardware para crear sistemas virtuales.
7	a	Al hablar de computación móvil nos referimos al uso de celulares o tablets.
8	a	GASSP hace referencia a un conjunto de principios y prácticas para seguridad TI.
9	c	El plan de continuidad del negocio BCP debe considerar a los sistemas TI y procesos de negocio.
10	c	El catálogo de servicios TI orienta a la organización sobre los recursos TI disponibles.

Ir a la  
autoevaluación

Autoevaluación 5		
Pregunta	Respuesta	Retroalimentación
1	b	La arquitectura cliente-servidor y por capas no permite, son poco escalables y no tienen buena tolerancia a fallos.
2	a	SOA es una arquitectura compleja y costosa; sin embargo, para el gobierno es útil, ya que conocen las tareas que ejecuta cada servicio.
3	a	Detectar nuevos CI y agregarlos a los CMS es parte de la gestión de configuración de ITIL no SOA.
4	c	PMBOK trata la gestión de proyectos y TOGAF es un framework de arquitectura empresarial.
5	a	Al hablar de arquitectura actual, futura y transición nos referimos a la arquitectura empresarial. Ciclo de vida del desarrollo, arquitectura de sistemas, patrones de desarrollo es parte del desarrollo de aplicaciones.
6	c	Las metodologías ágiles son las más utilizadas en la actualidad, debido a que permiten realizar varias entregas de los productos sin tener que seguir un ciclo en cascada.
7	b	El líder del proyecto se encarga de la dirección y coordinación de los recursos a utilizar en un proyecto. Control de calidad asegura que el producto cumpla con las expectativas del cliente.
8	a	La gestión de portafolio es una disciplina dentro del gobierno organizacional, ya que abarca varios programas que no son únicamente de TI.
9	b	Los distintos tipos de PMO crean una supervisión eficaz de los proyectos, reduciendo sus fallas y maximizando su éxito.
10	c	La oficina PMO es la encargada de dirigir y controlar la cartera de proyectos de una unidad de negocio.

[Ir a la autoevaluación](#)

Autoevaluación 6		
Pregunta	Respuesta	Retroalimentación
1	a	ECM significa gestión del contenido empresarial.
2	c	ECM es un sistema de organización y recopilación de información estratégica.
3	b	Destruir información no es un objetivo ECM, lo que se persigue es conservar información.
4	b	En ECM se considera la información de forma física y virtual.
5	a	Uno de los objetivos de la auditoría interna es evaluar si el gobierno TI está alineado a la estrategia empresarial.

[Ir a la autoevaluación](#)

Autoevaluación 7		
Pregunta	Respuesta	Retroalimentación
1	a	La misión, visión y valores facilitan al gobierno corporativo la toma de decisiones.
2	c	Los gerentes financieros y de operaciones, representante de la auditoría interna, aseguramiento de calidad y área legal corporativa deben asegurarse de que el código de conducta tenga lineamientos que promocionen la transparencia, respeto por los derechos humanos, imagen corporativa, etc.
3	a	El uso de las redes sociales debe ser un motivo de preocupación no solo para el área de <i>marketing</i> sino para el gobierno y toda la corporación, ya que puede causar impactos negativos que dañen su reputación .
4	c	Las políticas de redes sociales no deben considerar fecha de publicación ni recompensas por el mal uso. Estas deben ser explícitas referente a la prevención de fuga de información, perfiles y derechos de autor.
5	a	La selección de herramientas para el uso de participantes de los proyectos y el manejo de las necesidades de los <i>stakeholders</i> son actividades de la PMO.

[Ir a la autoevaluación](#)



## 5. Referencias bibliográficas

- Orellana, C. M. (octubre de 2011). *Buen gobierno corporativo = competitividad. Lo que todo empresario debe saber.* Obtenido de Espae: <http://www.espae.espol.edu.ec/wp-content/uploads/2011/12/buengobiernocorporativo.pdf>
- Banco de Desarrollo de Latinoamérica CAF. (2010). *Gobierno Corporativo.* Obtenido de CAF: [https://scioteca.caf.com/bitstream/handle/123456789/842/GC\\_todoEmpresario.pdf?sequence=1](https://scioteca.caf.com/bitstream/handle/123456789/842/GC_todoEmpresario.pdf?sequence=1)
- IT Governance Institute. (2003). *Board Briefing on IT Governance .* Rolling Meadows, Estados Unidos. Obtenido de Board Briefing of IT Governance.
- ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology.* Schaumburg: ISACA.
- Schandl, A., & Foster, P. (2019). *Coso Inter Control - Integrated Framework: An implementation guide for health care provider industry.*
- Muñoz, I., & Ulloa, G. (2011). *Gobierno de TI – Estado del arte.* Cali, Colombia.
- Torres, Y., & Cabrera, A. (2018). *Texto-Guía: Gestión de Tecnologías de la Información.* Universidad Técnica Particular de Loja, Departamento de Ciencias de la Computación y Electrónica. Loja: EDILOJA.
- ISO/IEC. (2018). *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.* Ginebra, Suiza.
- Deloitte. (2017). Obtenido de COSO ERM 2017 y la Generación de Valor: [https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Presentación%20COSO%20ERM%202017%20\(Oct%2024\).pdf](https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Presentación%20COSO%20ERM%202017%20(Oct%2024).pdf)
- Hurwitz, J., Bloor, R., Kaufman, M., & Halper, F. (2009). *Service Oriented Architecture for Dummies.* Indianapolis: Wiley Publishing, Inc.

- Josuttis, N. (2007). *SOA in practice*. California: O'Reilly Media, Inc.
- Project Management Institute. (2008). Obtenido de Organizational Project Management Maturity Model (OPM3).
- Project Management Institute. (2008). *The standard for portfolio management*. Pennsylvania: Project Management Institute, Inc.
- Acsendo. (15 de Noviembre de 2013). Obtenido de Política de manejo de redes sociales.
- Flores, A. (s.f.). Obtenido de El Comité de Auditoría: [https://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/quipukamayoc/2008\\_1/a04.pdf](https://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/quipukamayoc/2008_1/a04.pdf)
- Ley Sarbanes-Oxley. (2002). SAS 90: Comunicaciones con el comité de auditoria emitida por Instituto Americano de Contadores Públicos Certificados (AICPA).
- Project Management Institute. (2017). A Guide to the Project Management Body of Knowledge (PMBOK® Guide).
- Project Management Institute. (2013). Guía de los fundamentos para la dirección de proyectos – guía del PMBOK.
- Grupo Cavala. (s.f.). *Responsabilidad Social Corporativa*. Obtenido de <https://responsabilidad-social-corporativa.com/contacto/>
- Ramirez, H. (agosto de 2020). ¿Qué es el Código de conducta de una empresa? ¿Cómo hacerlo? Obtenido de <https://protecciondatos-lopd.com/empresas/codigo-de-conducta/>
- Moeller, R. (2013). *Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL*. (I. John Wiley & Sons, Ed.) New Jersey: John Wiley & Sons.
- Calder. (2008). *The Calder-Moir IT Governance Framework*. Obtenido de <http://www.itgovernance.co.uk/>
- IT Governance Europe. (2022). *The Calder-Moir IT Governance Framework*. Obtenido de <https://www.itgovernance.eu/es-es/calder-moir-es>
- Project Management Institute. (2008). THE STANDARD FOR PORTFOLIO MANAGEMENT SECOND EDITION. Atlanta, Estados Unidos.

Instituto Ecuatoriano de Gobernanza Corporativa y el BID Invest. (2020).

*Normas Ecuatorianas para el buen gobierno corporativo.* Obtenido de [https://portal.supercias.gob.ec/wps/wcm/connect/bcb89c88-f97d-46f7-9285-f27ed48ab401/CODIGO\\_DE\\_GOBERNANZA.pdf?MOD=AJPERES&CACHEID=bcb89c88-f97d-46f7-9285-f27ed48ab401](https://portal.supercias.gob.ec/wps/wcm/connect/bcb89c88-f97d-46f7-9285-f27ed48ab401/CODIGO_DE_GOBERNANZA.pdf?MOD=AJPERES&CACHEID=bcb89c88-f97d-46f7-9285-f27ed48ab401)

Grembergen, W. V. (2004). En W. V. Grembergen, *Strategies for Information Technology Governance* (pág. 6). Estados Unidos: Idea Group Publishing.

QAEC. (2019). COSO. Obtenido de <https://www.aec.es/web/guest/centro-conocimiento/coso>

ISACA. (2019). *Governance and Management Objectives*.

Tec Management. (19 de mayo de 2019). *Gestión de Servicios*. Obtenido de ITIL 4 y el Sistema de Cadena de Valor: <https://tecmanagement.org/itil-4-y-el-sistema-de-valor-del-servicio/>

UN Office for Disaster Risk Reduction. (s.f.). Obtenido de Gestión del riesgo: [https://www.eird.org/cd/toolkit08/material/proteccion-infraestructura/gestion\\_de\\_riesgo\\_de\\_amenaza/8\\_gestion\\_de\\_riesgo.pdf](https://www.eird.org/cd/toolkit08/material/proteccion-infraestructura/gestion_de_riesgo_de_amenaza/8_gestion_de_riesgo.pdf)

Interpolados. (20 de septiembre de 2020). *INGENIERÍA Y SERVICIOS IT*. Obtenido de ITIL 4: PRÁCTICAS DE GESTIÓN DE ITIL: GESTIÓN DE LA CONFIGURACIÓN DEL SERVICIO: <https://interpolados.wordpress.com/tag/itil-v4/page/2/>

Intelequia. (2020 de noviembre de 28). *CICLO DE VIDA DEL SOFTWARE: TODO LO QUE NECESITAS SABER*. Obtenido de Qué es el ciclo de vida del software: <https://intelequia.com/blog/post/2083/ciclo-de-vida-del-software-todo-lo-que-necesitas-saber>

Orjuela Duarte, A., & Rojas C., M. (2 de junio de 2008). Las Metodologías de Desarrollo Ágil como una Oportunidad para la Ingeniería del Software Educativo. Medellín, Colombia.



## 6. Anexos

### Anexo 1. Roles y responsabilidades para el gobierno de TI

#### Junta Directiva

Tabla 9.

*Roles y Responsabilidades para el Gobierno de TI de la Junta directiva*

Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
Junta directiva	Asegurar que la gerencia haya implementado un proceso de planificación estratégica eficaz	Asegurar que las inversiones de TI presenten un balance entre riesgo y beneficio Existan procesos de gestión y prácticas	Monitorear como la gerencia determina los recursos de TI para satisfacer la estrategia de la empresa Garantizar un equilibrio en las inversiones de TI para garantizar la rentabilidad de la empresa	Ser consciente de los riesgos de TI y sus consecuencias Evaluar la efectividad del monitoreo de TI por parte de la gerencia de riesgos	Evaluar el desempeño de la alta dirección en la operación de estrategias de TI. Trabajar con el ejecutivo para definir y monitorear el alto rendimiento de TI

Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
Comité de Estrategia de IT	Proveer dirección estratégica y alineación de TI con el negocio	Confirmar que la arquitectura TI/ Negocio está diseñada para brindar el máximo valor posible.	Proveer una dirección de alto nivel para el abastecimiento y el uso de recursos de TI.	Asegurarse que la gerencia cuente con los recursos para garantizar la gestión adecuada de riesgos de TI.	Verificar el cumplimiento de la estrategia, la alineación de TI con el negocio. Evaluar la medición de desempeño entre TI y su entrega de valor al negocio (promedio del valor de negocio).

Nota. Adaptado de IT Governance Institute. (2003). Board Briefing on IT Governance . Rolling Meadows, Estados Unidos. Obtenido de Board Briefing of IT Governance.



## Gerencia Ejecutiva

**Tabla 10.**

*Roles y Responsabilidades para el Gobierno de TI de la Gerencia Ejecutiva*

Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
CEO	<p>Alinea e integra la estrategia de TI con los objetivos de negocio. Alinea las operaciones de TI con las operaciones financieras de negocio. Mediar entre el negocio y la tecnología</p> <p>Alinea e integra la estrategia de TI con los objetivos de negocio. Alinea las operaciones de TI con las operaciones financieras de negocio. Mediar entre el negocio y la tecnología</p> <p>Se asegura que el presupuesto de TI y el plan de inversiones es realista y se integra en el plan financiero de la empresa. Se asegura de que los informes financieros tengan una contabilidad exacta de TI.</p>	<p>Dirige la optimización de costes de TI. Se asegura que el presupuesto de TI y el plan de inversiones es realista y se integra en el plan financiero de la empresa. Se asegura de que los informes financieros tengan una contabilidad exacta de TI.</p>	<p>Establece prioridades comerciales y asigna recursos para permitir un efectivo desempeño de TI. Establece estructuras organizativas y responsabilidades que faciliten la implementación de la estrategia de TI.</p>	<p>Adopta un marco de riesgo, control y gobernanza. Supervisa los riesgos de TI y acepta riesgos residuales de TI. Incorpora responsabilidades para la gestión de riesgos.</p>	<p>Trabaja conjuntamente con el CIO para desarrollar el balance scorecard de IT asegurándose de que estén correctamente alineados con el negocio.</p>
Ejecutivos de negocio	<p>Comprender la organización, su infraestructura y las capacidades de TI de la empresa. Impulsa la definición de los requisitos de negocio y adueñarse de ellos. Actúa como patrocinador de importantes proyectos de TI.</p> <p>Actuar como cliente de los servicios disponibles de TI. Identifique y adquiere nuevos servicios de TI.</p>	<p>Aprobar y controlar los niveles de servicio</p>	<p>Asignar los recursos de negocio requeridos para asegurar un efecto gobierno de IT frente a los proyectos y operaciones</p>	<p>Proporciona evaluaciones de impacto negocio a la gestión de riesgos de la empresa</p>	<p>Aprueba el cuadro de mando integral</p> <p>Supervisa los niveles de servicio</p> <p>Proporciona prioridades para abordar los problemas de rendimiento de TI y acciones correctivas.</p>



Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
CIO	<p>Impulsa el desarrollo de la estrategia de TI y la ejecuta, asegurando que el valor medible se entregue a tiempo y dentro del presupuesto, en la actualidad y en futuro</p> <p>Implementa estándares y políticas de TI</p>	<p>Clarifica y demuestra el valor de TI.</p> <p>Busca de forma proactiva aumentar la entrega de valor de TI.</p> <p>Vincula los presupuestos de TI a estrategias y objetivos de negocio.</p> <p>Establece una disciplina sólida de gestión de proyectos de TI.</p>	<p>Provee de infraestructura de TI que facilite la creación y compartición de información de negocio a un costo rentable.</p> <p>Asegura la disponibilidad de los recursos de TI, habilidades e infraestructura para alcanzar los objetivos estratégicos.</p> <p>Estandariza arquitecturas y tecnología.</p>	<p>Evaluá riesgos, los mitiga efectivamente y hace que los riesgos sean transparentes para los interesados.</p> <p>Implementa un framework de control</p> <p>Se asegura que los roles sean bien definidos en la gestión de riesgos de TI.</p>	<p>Asegura la gestión del día a día y verifica los procesos y controles de TI.</p> <p>Implementa un cuadro de mando integral de TI con pocas pero precisas medidas que reflejen el desempeño y su vinculación con la estrategia de la empresa</p>

Nota. Adaptado de T Governance Institute. (2003). Board Briefing on IT Governance . Rolling Meadows, Estados Unidos. Obtenido de Board Briefing of IT Governance.



**Comité de apoyo a los ejecutivos y al CIO, generalmente coordinados por la oficina de proyectos del CIO, el arquitecto jefe, el director de tecnología, etc.**

**Tabla 11.**

*Roles y Responsabilidades para el Gobierno de TI del Comité de Apoyo de los Ejecutivos.*

Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
Comité directivo de TI	Define las prioridades de proyectos Evalúa el ajuste estratégico de las propuestas Realiza revisiones del portafolio para mantener la relevancia estratégica	Revisa, aprueba y financia las iniciativas, evalúa cómo han mejorado los procesos de negocio. Asegura la identificación de todos los costos y el cumplimiento de análisis de costo/beneficio. Realiza revisiones del portafolio para optimizar costos.	Equilibra las inversiones entre el soporte y crecimiento de la empresa	Se asegura que en todos los proyectos exista un componente de gestión de riesgos. Actúa como patrocinador del control, riesgos y framework de gobernanza Toma decisiones claves sobre el gobierno de TI.	Define medidas de éxito del proyecto Da seguimiento al progreso de los principales proyectos de TI. Supervisa y dirige los procesos claves de gobernanza de TI
Consejo Tecnológico	Proporciona pautas tecnológicas Monitorea la relevancia de los últimos desarrollos de TI desde una perspectiva comercial.	Consultar / asesorar sobre la selección de tecnología dentro de los estándares. Ayuda con la revisión de variaciones	Asesoría sobre productos de infraestructura. Direcciona estándares y prácticas tecnológicas.	Asegura que se realicen evaluaciones acerca de las nuevas tecnologías.	Verifica el cumplimiento de los estándares y pautas tecnológicas.

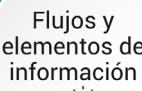
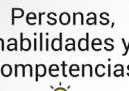
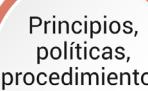


Rol	Responsabilidad Alineación estratégica	Entrega de Valor	Gestión de los recursos de IT	Gestión del riesgo	Gestión del rendimiento
Junta de revisión de arquitectura de TI	Proporcionan pautas de arquitectura	Consulta / asesora en la aplicación de arquitectura.	Dirige el diseño de arquitectura	Asegura que la arquitectura de TI refleja la necesidad de cumplimiento normativo y legislativo, el uso ético de información y la continuidad de negocio.	Verifica el cumplimiento de las pautas arquitectónicas

Nota. Adaptado de IT Governance Institute. (2003). Board Briefing on IT Governance . Rolling Meadows, Estados Unidos. Obtenido de Board Briefing of IT Governance.



## Anexo 2. Componentes de sistema de gobierno

Componente	Descripción
 <b>Procesos</b>	<p>Describen una serie de actividades organizadas cuya serie de resultados contribuyen a la consecución de los objetivos relacionados con IT.</p> 
 <b>Estructuras organizativas</b>	<p>Entidades claves que toman decisiones en una empresa. Como buenas prácticas de una estructura organizacional encontramos: Principios operativos, nivel de autoridad, delegación de responsabilidad y procedimientos de escalamiento.</p>
 <b>Flujos y elementos de información</b>	<p>COBIT se enfoca en la información necesaria para el funcionamiento eficaz del sistema de gobierno.</p>
 <b>Personas, habilidades y competencias</b>	<p>Son habilitantes para la toma de buenas decisiones, ejecutar acciones correctivas y llevar a cabo las actividades.</p>
 <b>Principios, políticas, procedimientos</b>	<p>Ayudan a convertir el comportamiento deseado en una guía para su práctica diaria. Los principios expresan los valores de la empresa; mientras que las políticas son directrices detalladas de cómo ejecutar los principios.</p>

Componente	Descripción
 Cultura, ética y comportamiento	Son considerados un factor de éxito en las actividades de gobierno y gestión.
 Servicios, infraestructura y aplicaciones	Componentes utilizados para el procesamiento de la IT. COBIT 2019 indica los siguientes principios para este componente: Reutilización, comprar frente a construir, simplicidad, agilidad y apertura.

### Anexo 3. Componentes COSO ERM

Gobierno y Cultura	Estrategia y objetivos	Desempeño	Revisión	Información, comunicación y reporte
<ul style="list-style-type: none"> <li>La junta directiva establece estructuras operativas para definir la cultura deseada que demuestra compromiso con los valores éticos.</li> <li>Atrae, desarrolla y retiene individuos competentes.</li> </ul>	<ul style="list-style-type: none"> <li>Analiza el contexto empresarial para definir el apetito del riesgo.</li> <li>Evalúa estrategias alternativas para formular los objetivos empresariales.</li> </ul>	<ul style="list-style-type: none"> <li>Identifica riesgos.</li> <li>Evalúa la severidad de los riesgos.</li> <li>Prioriza los riesgos.</li> <li>Implementa la respuesta al riesgo.</li> <li>Desarrolla un portafolio de riesgos.</li> </ul>	<ul style="list-style-type: none"> <li>Evalúa los cambios sustanciales en los riesgos y el desempeño.</li> <li>Revisa los riesgos y el desempeño.</li> <li>Propone mejoras en la gestión de riesgos empresariales.</li> </ul>	<ul style="list-style-type: none"> <li>Aprovecha la información y la tecnología para comunicar los riesgos de información.</li> <li>Comunica los riesgos, cultura y desempeño.</li> <li>Informe sobre riesgos, cultura y desempeño.</li> </ul>

Nota. Adaptado de Deloitte. (2017). Obtenido de COSO ERM 2017 y la Generación de Valor: <https://www2.deloitte.com/content/dam/Deloitte/>

## Anexo 4. Comparativa entre proyectos, programas y portafolios

	<b>Proyectos</b>	<b>Programas</b>	<b>Portafolios</b>
Alcance	Tienen definido objetivos. El alcance es elaborado progresivamente a través del ciclo de vida del proyecto.	Los programas tienen un gran alcance y generan mayores beneficios.	Tiene un alcance de negocio que cambia con la estrategia de la organización.
Cambio	Los líderes de proyectos esperan cambios y lo mantienen controlado	El líder del programa debe esperar el cambio a nivel interno y externo el programa y este debe estar preparado para manejarlo	El líder del portafolio monitorea el cambio continuo del entorno.
Planificación	Los líderes de proyectos elaboran continuamente información de alto nivel en planes detallados a través del ciclo de vida del proyecto.	El líder del programa desarrolla toda la planificación del programa y crea planes para guiar la planificación detallada.	El líder del portafolio crea y mantiene los procesos necesarios y la comunicación para el portafolio.
Gestión	Gestionan el proyecto y los recursos para alcanzar las metas del proyecto.	Gestionan el equipo del programa y los líderes de proyectos. Proveen visión y liderazgo	Podrían gestionar y coordinar al equipo de programas.
Éxito	Su éxito es medido por la calidad del proyecto y producto, servicio y la satisfacción del cliente	Es medido por el grado a la cual los programas satisfacen las necesidades y beneficios para lo cual fueron establecidos.	Medido en término de desempeño de los componentes del portafolio
Monitoreo	Los líderes de proyecto monitorean y controlan el trabajo de producir productos, servicios o resultados que el proyecto debe generar.	Monitorean el progreso de los componentes del programa para asegurar el cumplimiento de metas, presupuesto y calendario.	Monitorea el rendimiento agregado y los indicadores de valor.

Nota. Adaptado de Project Management Institute. (2008). The standard for portfolio management. Pennsylvania: Project Management Institute, Inc