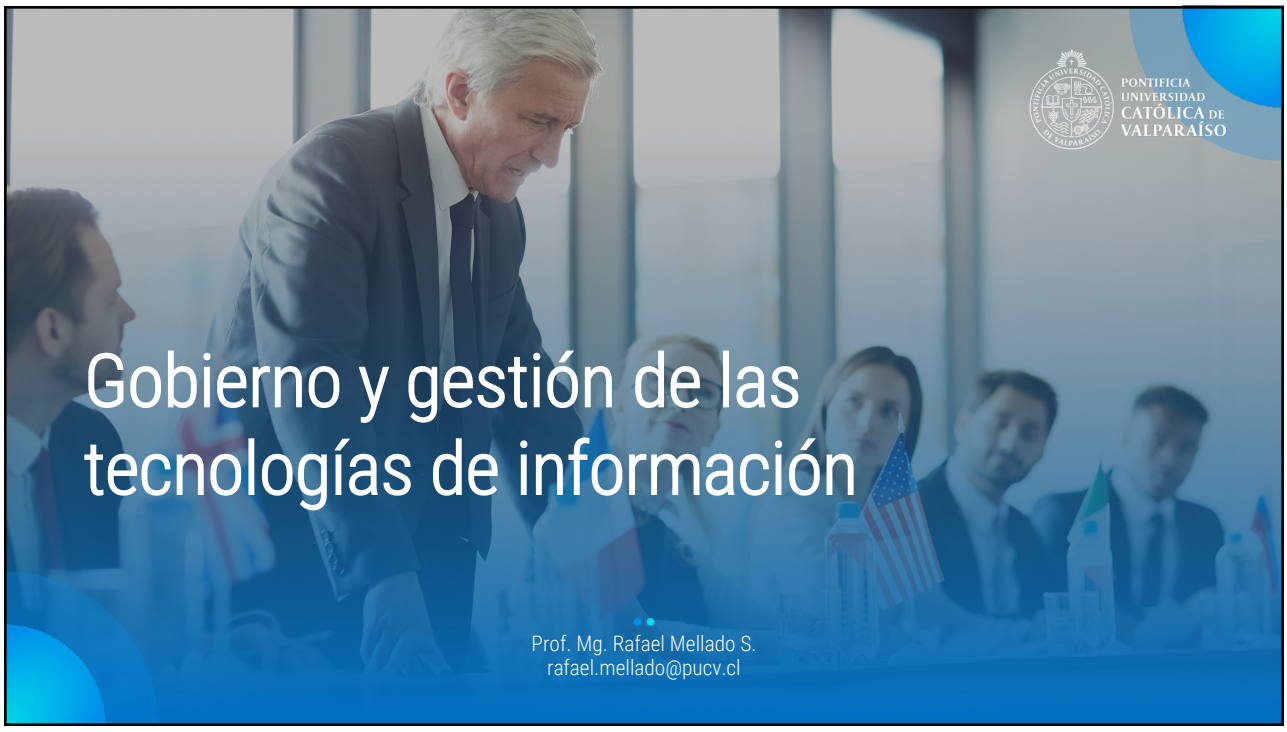


Gobierno y gestión de las tecnologías de información

Prof. Mg. Rafael Mellado S.
rafael.mellado@pucv.cl

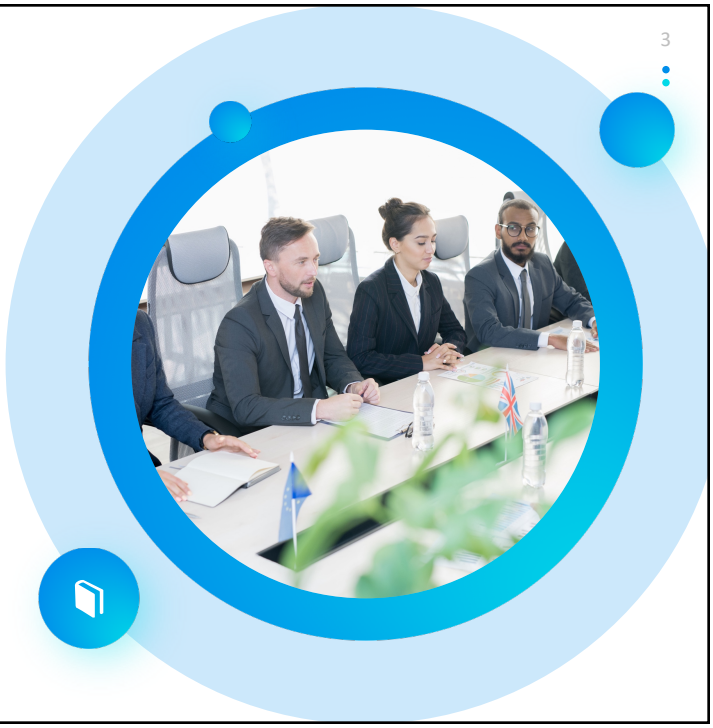
Resumen

Este módulo define los aspectos relevantes que un auditor debe considerar sobre gobierno y gestión de los recursos tecnológicos dentro de la empresa dentro del marco de la auditoría de sistemas de información.

3

1 Gobierno corporativo

Los aspectos éticos, la toma de decisiones y las prácticas en general dentro de una organización deben fomentarse por medio de prácticas de gobierno corporativo.



4

1 Gobierno corporativo

> Un gobierno corporativo es un conjunto de responsabilidades y prácticas usadas por la gerencia de una organización para proveer dirección estratégica, para garantizar, de ese modo, que las metas se puedan alcanzar, los riesgos sean manejados de manera adecuada y los recursos organizacionales sean utilizados apropiadamente.

5

2 Gobierno de TI en la empresa

El gobierno de TI en la empresa (GEIT) implica un sistema en el cual todas las partes interesadas, incluyendo el Consejo, clientes y departamentos internos, tales como finanzas, proporcionan una entrada en el proceso de la toma de decisiones.

La implementación del marco de GEIT trata ciertos procesos, en los cuales se incluye:

- La gestión de los recursos de TI
- La medición del desempeño
- La gestión de cumplimiento de contratos y políticas

6

2.1 Mejores prácticas para el GEIT

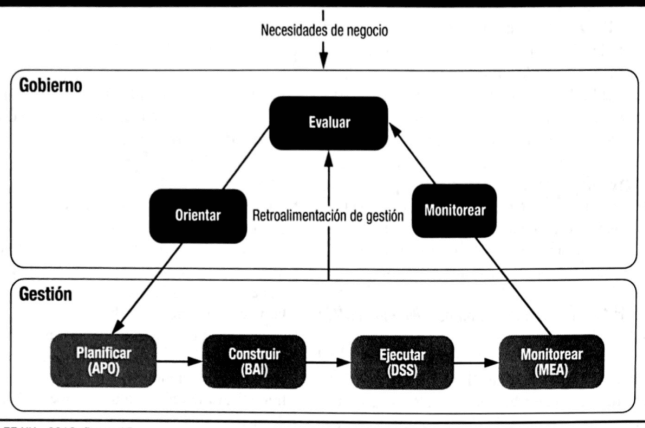
GEIT se ha vuelto significativo debido a numerosos factores:

- Exigencia de un mejor retorno de inversión en TI
- Creciente gasto en TI
- Cumplir con requerimientos regulatorios (Ley Sarbanes-Oxley USA)
- Selección de los proveedores de servicios y la gestión del servicio de externalización.
- Iniciativas del gobierno TI
- Optimización de costos
- Evaluación de desempeo

7

2.1 Mejores prácticas para el GEIT

Figura 2.3: Áreas clave de gestión y gobierno de COBIT 5.



Fuente: ISACA, COBIT 5, EE.UU., 2012, figura 15

8

2.2 Comités de gobierno de TI

Figura 2.4—Análisis de las responsabilidades del Comité directivo

Nivel	Comité de Estrategia de TI	Comité de Dirección de TI
Responsabilidad	• Proporciona información detallada y asesoría al consejo de dirección sobre temas como: – La relevancia de los desarrollos de TI desde la perspectiva de negocios – La alineación de TI con la dirección del negocio – El logro de los objetivos estratégicos de TI – La disponibilidad de los recursos, destrezas e infraestructura de TI apropiados para satisfacer los objetivos estratégicos – Optimización de los costos de TI, incluyendo el rol y la entrega de valor de la contratación externa de servicios de TI – Riesgo, retorno y aspectos competitivos de las inversiones de TI – Progreso en los proyectos mayores de TI – La contribución de TI al negocio (por ejemplo, entrega del valor de negocios prometido) – Exposición a riesgos de TI, incluyendo riesgos de cumplimiento – Contención de los riesgos de TI – Dirección a la gerencia respecto a la estrategia de TI – Impulsores y catalizadores de TI para el consejo de dirección	• Decide el nivel global del gasto de TI y la distribución de los costos • Alinea y aprueba la arquitectura de TI de la empresa • Aprueba los planes y presupuestos de proyectos, establece prioridades y objetivos parciales • Obtiene y asigna los recursos apropiados • Garantiza que los proyectos cumplan de manera continua con los requerimientos del negocio, incluyendo la reevaluación del caso de negocios • Monitorea los planes de proyectos para verificar la entrega de valor esperado y resultados deseados, a tiempo y dentro del presupuesto • Monitorea el conflicto de recursos y prioridades entre divisiones de la empresa y la función de TI, así como entre proyectos • Hace recomendaciones y solicitudes para cambios a los planes estratégicos (prioridades, financiamiento, tecnología, enfoques y recursos etc.) • Comunica las metas estratégicas a los equipos de proyectos • Es un contribuyente importante para las prácticas y responsabilidades de gobierno de TI de la gerencia

9

2.2 Comités de gobierno de TI

Autoridad	• Asesora al consejo de dirección y a la gerencia sobre estrategia de TI • Por delegación del consejo de dirección, proporciona información de entrada para la estrategia y prepara su aprobación • Se concentra en problemas estratégicos de TI presentes y futuros	• Asiste a los ejecutivos en la preparación de la estrategia de TI • Supervisa el gerenciamiento en el día a día de la prestación del servicio de TI y de los proyectos de TI • Se concentra en la implementación
Membresía	• Miembros del consejo de dirección y especialistas no miembros del consejo de dirección	• Ejecutivo patrocinante • Ejecutivo de negocios (usuarios clave) • CIO • Asesores clave según se requiera (TI, auditoría, legal, finanzas)

10

2.3 Gobierno de la seguridad de la información

Hay que poner mucha atención en el comité de seguridad. Los esfuerzos deben estar focalizados en:

- Mantener información de alta calidad → Toma de decisiones
- Usar TI para alcanzar metas estratégicas y obtener beneficios económicos.
- Mantener el riesgo TI en un nivel aceptable
- Lograr excelencia operativa.
- Optimizar costos TI
- Cumplir con leyes y regulaciones.

11

3 Modelos de madurez y mejoramiento de procesos

La implementación de un gobierno TI requiere de una medición de desempeño constante de los recursos de una organización que contribuyan a la ejecución de procesos que prestan servicios de TI al negocio.

12

3.1 Modelo de evaluación de procesos PAM™ de COBIT®

El **Process Assessment Model** de COBIT ha sido desarrollado para mejorar el rigor y la confiabilidad de las revisiones de procesos de TI.

Este modelo sirve como documento de referencia para llevar a cabo las evaluaciones de capacidad de los procesos de TI actuales.

Se alinea con ISO/IEC 15504-2 y utiliza la capacidad de procesos y los indicadores del desempeño de proceso para determinar si se han alcanzado los atributos del proceso.

06. Process Assessment Model COBIT 5.pdf

13

3.2 Modelo IDEAL™

El modelo IDEAL está centrado en el mejoramiento de procesos de software. Fue desarrollado por el Software Engineering Institute.

Busca orientar a las empresas en la planificación y aplicación de un programa efectivo de mejoramiento de procesos de software de manera eficaz.

07. IDEAL - A User's Guide for Software Process Improvement.pdf

14

3.3 CMMI ®

Basado en la ISO/IEC 15504 es un enfoque para el mejoramiento de procesos que proporciona a las empresas los elementos esenciales de procesos efectivos.

Pensado en mejorar la calidad en procesos de software para empresas que consideran la factoría de sistemas de información.

Nunca olvidar: Software a la media es distinto que software empaquetado.

08. CMMI-DEV V1.3.pdf

15

4 Políticas y procedimientos

Se debe considerar:

- Política de seguridad de la información.
- Política de clasificación de los datos.
- Política de uso aceptable.
- Política informática para el usuario final.
- Políticas de control de acceso.

16

4 Políticas y procedimientos

Se debe considerar:

- Política de seguridad de la información.
- Política de clasificación de los datos.
- Política de uso aceptable.
- Política informática para el usuario final.
- Políticas de control de acceso.

17

5 Gestión de recursos humanos

Para la gestión del recurso humano en la empresa se debe contemplar:

- Contratación → Es bueno externalizar?
- Manual del empleado
- Políticas de promoción
- Capacitación
- Cronogramas y reportes de tiempo.
- Evaluaciones del desempeño de los empleados
- Vacaciones legales
- Políticas de finalización de contrato

18

5.1 Políticas de finalización de contrato

Al finalizar un contrato se deben aplicar los siguientes procedimientos de control:

- Devolución de todas las claves de acceso, tarjetas y distintivos de identificación.
- Eliminación/revocación de la identificación.
- Notificación
- Arreglo de las rutinas de pago final.
- Realización de la entrevista final.

5.2 Prácticas de outsourcing

La entrega de funciones de SI pueden incluir:

- Funciones internas
- Externalizadas
- Híbrido

Lugares o fuentes de prestación del servicio:

- En el sitio
- Fuera del sitio
- En el extranjero.

5.2 Prácticas de outsourcing

Figura 2.8—Ventajas, desventajas y riesgos del negocio, y opciones de reducción de riesgos relacionadas con la externalización

Posibles ventajas	Posibles desventajas y riesgos del negocio	Opciones de reducción de riesgos
• Las compañías de externalización (outsourcing) pueden lograr economías de escala por medio de la implementación de software de componentes reutilizables. • Los proveedores de servicios externos tienen la posibilidad de dedicar más tiempo y concentrarse con mayor efectividad y eficiencia en un proyecto dado que el personal interno. • Los proveedores de servicios externos tienen probablemente más experiencia con un conjunto más amplio de problemas, aspectos y técnicas que el personal interno. • El acto de desarrollar especificaciones y acuerdos contractuales empleando servicios externos probablemente tenga como resultado mejores especificaciones que si fueran desarrollados únicamente por el personal interno. • Dado que los proveedores son altamente sensibles a las variaciones y los cambios que consumen tiempo, es mucho menos probable que haya un exceso de funcionalidades con los proveedores de servicios externos.	• Costos que excedan las expectativas del cliente • Pérdida de la experiencia interna de SI • Pérdida del control sobre SI • Incumplimiento del proveedor (preocupación constante) • Acceso limitado al producto • Dificultad para revertir o cambiar los contratos de servicios externos • Deficiente cumplimiento de los requerimientos legales y regulatorios • Incumplimiento de los términos del contrato • Falta de lealtad del personal del contratista para con el cliente • Clientes/empleados insatisfechos como consecuencia del acuerdo de contratación de servicios externos • Que los costos del servicio no sean competitivos durante el período total del contrato • Obsolescencia de los sistemas de TI del proveedor • Que ninguna de las dos compañías reciba los beneficios anticipados del acuerdo de externalización • Daño a la reputación de una de las compañías, o de ambas, debido a fallas del proyecto • Litigios prolongados y costosos • Pérdida o fuga de información o procesos	• Establecer metas y recompensas compartidas, mensurables, como parte de la sociedad • Usar múltiples proveedores o retener una parte del negocio como incentivo • Realizar revisiones periódicas competitivas y establecer un estándar de análisis comparativo/de tendencias • Implementar contratos a corto plazo • Formar un equipo interfuncional de administración de contratos • Incluir provisiones contractuales para considerar tantas contingencias como puedan anticiparse razonablemente

21

5.3 Externalización de activos de información y procesos

En este caso se puede encontrar:

- Computación en la nube
- Externalización e informes de auditoría de terceros
- Gobierno en externalización
- Capacidad y planificación de crecimiento

22

6 Cloud computing

Figura 2.9—Modelos de servicio de la computación en la nube

Modelo de servicio	Definición	Lo que se debe considerar
Infraestructura como un servicio (IaaS)	Capacidad para configurar procesamiento, almacenamiento, redes y otros recursos de computación fundamentales, ofreciendo al cliente la posibilidad de implementar y ejecutar software arbitrario, el cual puede incluir sistemas operativos y aplicaciones. IaaS coloca estas operaciones de TI en las manos de un tercero.	Opciones de minimizar el impacto si el proveedor de la nube experimenta una interrupción del servicio
Plataforma como un servicio (PaaS)	Capacidad para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el cliente que se hayan creado utilizando lenguajes y herramientas de programación que estén respaldados por el proveedor	• Disponibilidad • Confidencialidad • La privacidad y la responsabilidad legal en caso de una violación de la seguridad (ya que las bases de datos que contienen información sensitiva ahora estarán hospedadas fuera de la sede) • Propiedad de los datos • Preocupaciones acerca del e-discovery
Software como un servicio (SaaS)	Capacidad para utilizar las aplicaciones del proveedor que se ejecutan en la infraestructura de la nube. Se puede acceder a las aplicaciones desde diferentes dispositivos cliente a través de una interfaz de cliente ligero (thin client), como un explorador web (por ejemplo, correo electrónico basado en la web).	• ¿Quién es el dueño de las aplicaciones? • ¿Dónde residen las aplicaciones?

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, EE. UU., 2009, imagen 1, página 5, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

23

6 Cloud computing

Figura 2.10—Modelos de implementación de la computación en la nube

Modelo de implementación	Descripción de la infraestructura de la nube	Lo que se debe considerar
Nube privada	• Operada únicamente para una organización • Puede ser manejada por la organización o un tercero • Puede existir dentro o fuera de las instalaciones	• Servicios en la nube con riesgo mínimo • Es posible que no proporcione la escalabilidad y agilidad de los servicios de la nube pública
Nube comunitaria	• Compartida por varias organizaciones • Respalda una comunidad específica que haya compartido su misión o interés • Puede ser manejada por las organizaciones o un tercero • Puede residir dentro o fuera de las instalaciones	• Igual que la nube privada, pero adicionalmente: • Los datos pueden estar almacenados con los datos de los competidores
Nube pública	• Esta disponible para el público en general o un grupo industrial grande • Pertenece a una organización que vende servicios en la nube	• Igual que la nube comunitaria, pero adicionalmente: • Los datos pueden estar almacenados en ubicaciones desconocidas y pudieran no ser fáciles de recuperar
Nube híbrida	Una composición de dos o más nubes (privada, comunitaria o pública) que continúan siendo entidades únicas, pero que están unidas mediante tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones (por ejemplo, ampliación de la nube [cloud bursting] para equilibrar la carga entre las nubes)	• El riesgo agregado de combinar dos modelos de implementación diferentes • La clasificación y el etiquetado de datos ayudará al gerente de seguridad a garantizar que los datos se asignen al tipo de nube correcto

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, EE. UU., 2009, imagen 2, página 5, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

24

6 Cloud computing

Figura 2.11—Características fundamentales de la computación en la nube

Característica	Definición
Autoservicio a solicitud	El proveedor de la nube debe poder suministrar automáticamente capacidades de computación, tales como el almacenamiento en servidores y redes, según sea necesario sin requerir interacción humana con cada proveedor de servicios.
Acceso a redes de banda ancha	De acuerdo con el NIST, debe ser posible acceder a la red en la nube desde cualquier lugar y por medio de casi cualquier dispositivo (por ejemplo, teléfono inteligente, laptop, dispositivos móviles, PDA).
Agrupación de recursos	Los recursos informáticos del proveedor se agrupan para prestar servicios a diversos clientes utilizando un modelo de múltiples usuarios, con diferentes recursos físicos y virtuales asignados y reasignados de manera dinámica según la demanda. Existe un sentido de independencia geográfica. Generalmente, el cliente no tiene control o conocimiento de la ubicación exacta de los recursos proporcionados. Sin embargo, puede ser capaz de especificar una ubicación en un nivel de abstracción mayor (por ejemplo, país, región o centro de datos). Los ejemplos de recursos incluyen almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales.
Elasticidad rápida	Las capacidades se pueden suministrar de manera rápida y elástica, en muchos casos automáticamente, para una rápida expansión y liberar rápidamente para una rápida contracción. Para el cliente, las capacidades disponibles para suministro, con frecuencia, parecen ser ilimitadas, además, se puede adquirir cualquier cantidad de capacidades en cualquier momento.
Servicio medido	Los sistemas en la nube controlan y optimizan el uso de recursos de manera automática utilizando una capacidad de medición (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de los recursos se puede monitorear, controlar y notificar, lo que proporciona transparencia tanto para el proveedor como para el cliente que utiliza el servicio.

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, EE. UU., 2009, imagen 3, página 6, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

25

6.1 Amazon Web Services – Elastic Compute Cloud

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de Amazon Web Services (AWS). El uso de Amazon EC2 elimina la necesidad de invertir inicialmente en hardware, de manera que puede desarrollar e implementar aplicaciones en menos tiempo. Puede usar Amazon EC2 para lanzar tantos servidores virtuales como necesite, configurar la seguridad y las redes y administrar el almacenamiento. Amazon EC2 le permite escalar hacia arriba o hacia abajo para controlar cambios en los requisitos o picos de popularidad, con lo que se reduce la necesidad de prever el tráfico.

26

6.1 Amazon Web Services – Elastic Compute Cloud

- Entornos informáticos virtuales, conocidos como instancias
- Varias configuraciones de CPU, memoria, almacenamiento y capacidad de red de las instancias, conocidos como tipos de instancias
- Información de inicio de sesión segura para las instancias con pares de claves (AWS almacena la clave pública y usted guarda la clave privada en un lugar seguro)
- Volúmenes de almacenamiento para datos temporales que se eliminan cuando detiene o termina la instancia, conocidos como volúmenes de almacén de instancias
- Varias ubicaciones físicas para los recursos, como las instancias y los volúmenes de Amazon EBS, conocidas como regiones y zonas de disponibilidad

27

6.1 Amazon Web Services – Elastic Compute Cloud

- Un firewall que permite especificar los protocolos, los puertos y los rangos de direcciones IP que pueden alcanzar las instancias mediante el uso de grupos de seguridad
- Metadatos, conocidos como etiquetas, que se pueden crear y asignar a los recursos de Amazon EC2
- Redes virtuales que puede crear que están aisladas lógicamente del resto de la nube de AWS y que, opcionalmente, puede conectar a su propia red, conocidas como nubes privadas virtuales (VPC)

28

7 Gestión de la seguridad de la información

Las herramientas que consideran aspectos de seguridad son:

- Six Sigma (ver: 09. Principios de six sigma.pdf)
- Cuadro de mando integral
- Indicadores de desempeño (KPI's)
- Estudio de mercado comparativo
- Reingeniería de procesos
- Análisis de causa raíz
- Análisis de costo-beneficio del ciclo de vida.

29

7 Estructura organizativa y responsabilidades

Considerar:

- Usuario final
- Gestión de soporte al usuario final
- Gestión de datos
- Gestión de aseguramiento de la calidad (QA)
- Gestión de la seguridad de la información.

30

7 Estructura organizativa y responsabilidades