

Unidad 1: GESTION DE TECNOLOGÍA DE INFORMACIÓN

Gobierno de TI: Alineamiento estratégico. Entrega de Valor. Administración de riesgos. Administración de Recursos. Medición de desempeño. Aseguramiento independiente.
Procesos de TI: Planeamiento y Organización. Adquisición e Implementación. Entrega y Soporte. Monitoreo y evaluación. **Organización de TI. Funciones.** Segregación de tareas. **Entrega y Soporte:** Servicios, niveles y asignación de costos **Desempeño de TI.** Métricas. Aspectos regulatorios. Monitoreo y seguimiento.

Objetivos específicos:

- Conocer los elementos clave del Gobierno eficiente de TI y sus áreas de enfoque
- Entender los beneficios y esencia del gobierno de TI y cuáles son sus áreas de responsabilidad.
- Cómo aplicar la Información y la tecnología asociada orientada a crear valor en los negocios

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México : Pearson Educación, 2012. . ISBN 978-607-32-0949-6. Nota de contenido: Cap 1. Los sistemas de información en los negocios globales contemporáneos – Cap 2. Comercio electrónico global y colaboración –Cap 3. Sistemas de información, organizaciones y estrategia.
- COBIT (Control Objectives for Information and Related Technology), Information Systems Audit and Control Fundation. Material actualizado al momento del dictado del módulo de Información Systems Audit and Control Association (ISACA) que es la organización líder en gobernabilidad en tecnologías de información, aseguramiento, seguridad y control www.isaca.org

Contenido

Unidad 1: GESTION DE TECNOLOGÍA DE INFORMACIÓN	1
INTRODUCCION	3
ISO / IEC 38500	3
MODELO	6
ASPECTOS CLAVE EN GOBIERNO DE TI	6
COBIT	8
ÁREAS DE ENFOQUE DEL GOBIERNO DE TI	9
SOPORTE A COSO	10
CUADRO DE RELACIÓN ÁREA DE ENFOQUE DEL GOBIERNO DE TI, DOMINIOS Y PROCESOS	12
PLANEAR Y ORGANIZAR	13
Definir un Plan Estratégico de TI	14
Definir la Arquitectura de la Información.	14
Definir los Procesos, Organización y Relaciones de TI.	14

Administrar la inversión de TI	15
Comunicar las Aspiraciones y la Dirección de la Gerencia	15
Administrar los Recursos Humanos de TI	16
Administrar la Calidad	16
Evaluar y Administrar los Riesgos de TI	16
Administrar Proyectos	17
ADQUIRIR E IMPLEMENTAR	17
Identificar Soluciones Automatizadas	18
Adquirir y Mantener Software Aplicativo	18
Adquirir y Mantener Infraestructura Tecnológica	18
Facilitar la Operación y el Uso	19
Adquirir Recursos de TI	19
ENTREGAR Y DAR SOPORTE	19
Definir y Administrar los Niveles de Servicio	20
Administrar los Servicios de Terceros	20
Garantizar la Continuidad del Servicio	20
Garantizar la Seguridad de los Sistemas	21
Identificar y Asignar Costos	21
Educar y Entrenar a los Usuarios	21
Administrar la Mesa de Servicio y los Incidentes	22
Administración de Datos	22
Administración de Operaciones	22
MONITOREAR Y EVALUAR	23
Monitorear y Evaluar el Desempeño de TI	23
Monitorear y Evaluar el Control Interno	23
Garantizar el Cumplimiento con Requerimientos Externos	24
Proporcionar Gobierno de TI	24
FUENTES DE CONSULTAS	24

INTRODUCCION

La administración efectiva de la información y de la Tecnología de Información (TI) relacionada se ha convertido en un elemento crítico para el éxito y la supervivencia de las organizaciones.

En la sociedad de la información, donde esta última viaja a través del “ciberespacio” sin restricciones de tiempo, distancia y velocidad, esta criticidad surge de:

- Mayor dependencia en información y en sistemas que la proporcionan
- Mayor vulnerabilidad y amenazas, tales como las “ciberamenazas” y la guerra de información
- Escala y costo de las inversiones actuales y futuras en información y en tecnología de información
- Potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas empresas, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa.

Es más, en nuestro competitivo y cambiante ambiente actual, la gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI.

Por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega, al tiempo que demanda que esto se realice a un costo más bajo.

Muchas empresas reconocen los beneficios potenciales que la tecnología puede proporcionar. Las empresas exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología.

Por lo tanto, la administración debe tener un entendimiento básico de los riesgos y limitaciones del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

El Gobierno de TI es una disciplina relativa a la forma en la que la alta dirección de las empresas dirige la evolución y el uso de las tecnologías de la información. Se considera parte del "Gobierno Corporativo", centrada en el rendimiento, riesgos y control de las Tecnologías de la Información.

ISO / IEC 38500

Entre diversas definiciones de gobierno de TI, podemos citar la definición formal de la norma **ISO/IEC 38500** que trata el Gobierno Corporativo de Tecnologías de la Información.

ALCANCE, APLICACION Y OBJETIVOS

La norma se aplica al gobierno de los procesos de gestión de TI en todo tipo de empresas que utilicen (hoy todas) las tecnologías de la información, facilitando bases para la evaluación objetiva del gobierno de TI.

Dentro de los beneficios de un buen gobierno de TI estaría la conformidad de la empresa con:

- estándares de seguridad
- legislación de privacidad
- legislación sobre el spam
- legislación sobre prácticas comerciales
- derechos de propiedad intelectual, incluyendo acuerdos de licencia de software
- regulación medioambiental
- normativa de seguridad y salud laboral
- legislación sobre accesibilidad
- estándares de responsabilidad social

También la búsqueda de un buen rendimiento de la TI mediante:

- apropiada implementación y operación de los activos de TI
- clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización
- continuidad y sostenibilidad del negocio
- alineamiento de TI con las necesidades del negocio
- asignación eficiente de los recursos
- innovación en servicios, mercados y negocios
- buenas prácticas en las relaciones con los interesados (stakeholders)
- reducción de costes

- materialización efectiva de los beneficios esperados de cada inversión en TI

DEFINICIONES

La norma incluye 19 definiciones de términos, entre los que se pueden destacar los siguientes:

Gobierno corporativo de TI (corporate governance of IT): sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información

Gestión (management): sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la empresa. Está sujeta a la guía y monitorización establecida mediante el gobierno corporativo.

Interesado (stakeholder): Individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a ser afectado, por una decisión o una actividad.

Uso de TI (use of IT): Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de TI por unidades de negocio internas, unidades especializadas de TI, proveedores externos y "utility services" (como los que se proveen de software como servicio).

PRINCIPIOS

La norma define cinco principios de un buen gobierno corporativo de TI:

- **Responsabilidad**

Todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de TI. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.

- **Estrategia**

La estrategia de negocio de la empresa tiene en cuenta las capacidades actuales y futuras de las TI. Los planes estratégicos de TI satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.

- **Adquisición**

Las adquisiciones de TI se hacen por razones válidas, en base a un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.

- **Rendimiento**

La TI está dimensionada para dar soporte a la empresa, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.

- **Conformidad**

La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.

MODELO

La dirección ha de implementar un gobierno de TI mediante tres tareas principales:

- **Evaluar**

Examinar y juzgar el uso actual y futuro de las TI, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).

- **Dirigir**

Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto.

Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura.

Impulsar una cultura de buen gobierno de IT en la empresa.

- **Monitorizar**

Mediante sistemas de medición, vigilar el rendimiento de la TI, asegurando que se ajusta a lo planificado.

ASPECTOS CLAVE EN GOBIERNO DE TI

Los aspectos clave que la alta dirección de una empresa debe gestionar respecto a las Tecnologías de la Información, son:

- **Adecuación de la planificación de TI a la planificación general de la Organización**

La planificación de TI es un proceso fundamental de la gestión de TI, pero la alta dirección de las empresas debe asegurarse de que los planes de TI se integran adecuadamente con la planificación general.

- **Posición de la Organización de TI en el organigrama general de la Empresa**

Sin que exista una regla general de cual debe ser la posición del CIO y de la organización de TI en el organigrama general, sí es cierto que una adecuada posición será crítica para el éxito. En los primeros años de la informática era frecuente que las TI dependieran de los departamentos de contabilidad y administración, dado que la introducción de las PC en las empresas y organismos públicos se inició para dar servicio a este tipo de funciones.

En la medida en que la tecnología va resultando cada vez mas esencial para todos los procesos de negocio, su impacto en la vida de la empresa ha ido creciendo. Esto generó que la organización de TI pasara a ser una parte importante de las áreas de medios.

En las empresas en que TI ha llegado a ser absolutamente esencial para el negocio, el área de TI ha adquirido un puesto de primer nivel, formando parte del comité de dirección o equipo de primer nivel de la gestión.

- **Criticidad de los servicios y el conocimiento de TI para el negocio. Fórmula óptima de aprovisionamiento de servicios de TI.**

Resulta vital evaluar la criticidad de los servicios que TI proporciona para el negocio y, especialmente, la relevancia del conocimiento del negocio incluido en los sistemas de información y en las personas que los construyen y mantienen. Este nivel de criticidad será un input esencial para decidir la fórmula óptima de aprovisionamiento de servicios de TI, que puede combinar en diferentes grados un equipo puramente interno, una combinación con servicios adquiridos externamente, e incluso una externalización total ("outsourcing").

Dentro de la fórmula de provisión externa, existe la opción de disponer de un cierto grado de control del proveedor, mediante la participación en su propiedad y gestión.

- **Nivel de inversión / gasto razonable en TI**

Es una de las decisiones más difíciles de adoptar por los órganos de gobierno de las empresas. Siempre se encuentran necesidades insatisfechas de las áreas de negocio y posibilidades tecnológicas propuestas por la gente de TI. En la mayor parte de las ocasiones es muy difícil hacer un análisis coste-beneficio riguroso, lo que obliga a

establecer un nivel de gasto e inversión considerado "razonable", normalmente en base anual.

En la práctica lo más habitual es regirse por comparaciones (benchmarking) con otras empresas similares del mismo sector, y ajustarlo según las pretensiones de avance tecnológico relativo.

- **Información periódica y puntual desde el CIO a la alta dirección. Métricas de rendimiento.**

La alta dirección debe disponer de una información periódica y consistente del rendimiento de los servicios, los proyectos, los procesos y la situación financiera de la TI. Para ello se deben establecer unas métricas que resulten significativas y estadísticamente rigurosas.

- **Participación de las áreas de negocio y otras áreas de soporte en la planificación y la gestión de la demanda**

En determinados procesos de la gestión de TI, especialmente en la planificación y gestión de la demanda, deben participar las áreas de negocio y otras áreas de soporte (por ejemplo: RRHH), manteniendo una colaboración armoniosa.

- **Imputación de los costes de TI a las áreas de negocio y sus productos, procesos o clientes**

La alta dirección debe decidir cuales han de ser los criterios de imputación de los costes de TI al resto de las áreas. En muchas ocasiones no es algo pacífico, puesto que puede tratarse de costes que impacten de forma relevante en las cuentas de resultados de las áreas de negocio.

- **Requisitos de seguridad de la información y los procesos**

El nivel de exigencia en cuanto a requisitos de seguridad tiene un fuerte impacto en los costes y la gestión diaria de la TI. Por lo tanto, será importante establecer el nivel óptimo que equilibre los costes y los riesgos globales. Muchas veces una seguridad excesiva supone un derroche, pero en otras, una seguridad laxa pone en riesgo la supervivencia de la empresa.

COBIT

COBIT es un documento aceptado internacionalmente para la gestión de TI, su sigla significa Objetivos de Control para la Información y la Tecnología Relacionada – Control Objectives for Information and Related Technology, desarrollado por Information Systems

Audit and Control Association (ISACA). COBIT, en su última versión 4.1, hace hincapié en que el valor, el riesgo y el control son la esencia del gobierno de TI.

Gobierno de TI

Según COBIT, “el gobierno de TI integra e institucionaliza buenas prácticas para garantizar que TI soporte los objetivos del negocio. De esta manera, facilita que la empresa aproveche al máximo su información, maximizando beneficios, capitalizando oportunidades y ganando ventajas competitivas”

COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

COBIT ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona “prácticas sanas” a través de un **Marco Referencial** de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las prácticas sanas de COBIT representan el consenso de los expertos, ayudan a optimizar la inversión en información.

COBIT da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. La medición del desempeño es esencial para el gobierno de TI.

Un gobierno de TI efectivo ayuda a:

- Garantizar que TI soporte las metas de negocio
- Optimizar la inversión del negocio en TI
- Administrar de forma adecuada los riesgos y oportunidades asociadas a TI

El soporte que proporciona COBIT al Gobierno de TI se puede observar desde las cinco áreas de enfoque que define al efecto:

ÁREAS DE ENFOQUE DEL GOBIERNO DE TI



Alineación Estratégica

Se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de Valor

Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI

Administración de Riesgos

Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Administración de Recursos

Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI; aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Medición del Desempeño

Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

En esta unidad se desarrollarán:

Alineación Estratégica

Se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de Valor

Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI

Medición del Desempeño

Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

SOPORTE A COSO

COBIT constituye un marco de referencia para controlar la TI que sirve como soporte a COSO (Committee Of Sponsoring Organisations Of The Treadway Commission) Marco de Referencia Integrado – Control Interno, el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos.

Las empresas deben satisfacer calidad, requerimientos de seguridad de su información, así como de todos sus activos. Deben optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas.

Para lograr estos objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos. Presenta las actividades en una estructura manejable y lógica.

Las buenas prácticas de COBIT están enfocadas fuertemente en el control más que en la ejecución. Lo que permite optimizar las inversiones habilitadas por TI, asegurar la entrega del servicio y brindar una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

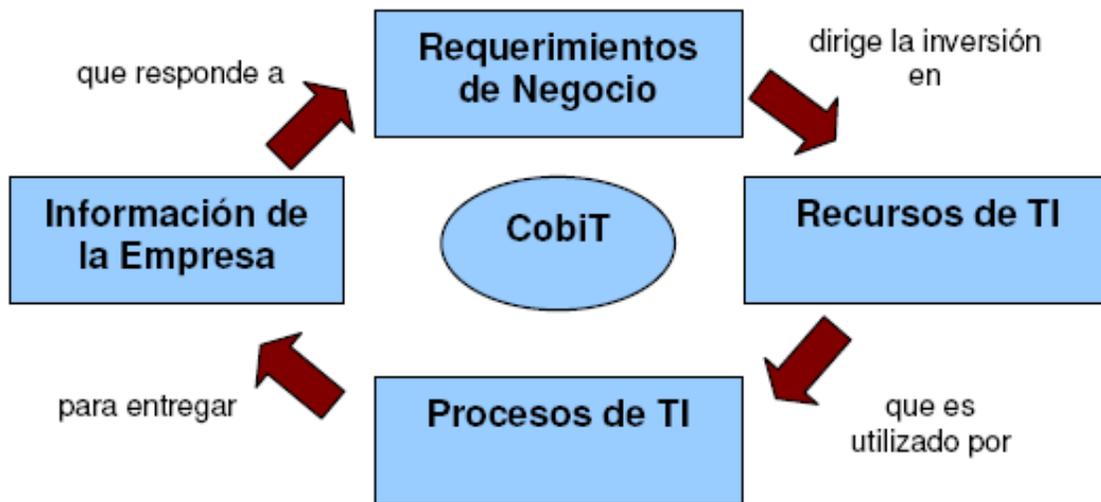
- Establece un vínculo con los requerimientos del negocio
- Organiza las actividades de TI en un modelo de procesos generalmente aceptado
- Identifica los principales recursos de TI a ser utilizados
- Define los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT consiste en subdividir los procesos de TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

Para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

PRINCIPIO BASICO DE COBIT



Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

CUADRO DE RELACIÓN ÁREA DE ENFOQUE DEL GOBIERNO DE TI, DOMINIOS Y PROCESOS

Área Enfoque Gobierno TI	Dominio COBIT	Proceso COBIT
Alineación Estratégica	Planear y Organizar	Definir un plan estratégico de TI
Alineación Estratégica	Planear y Organizar	Definir arquitectura de la información
Alineación Estratégica	Planear y Organizar	Comunicar las aspiraciones y la Dirección de la Gerencia
Alineación Estratégica	Planear y Organizar	Administrar Recursos Humanos de TI
Alineación Estratégica	Planear y Organizar	Administrar la Calidad
Alineación Estratégica	Planear y Organizar	Evaluar y Administrar Riesgos de TI
Alineación Estratégica	Planear y Organizar	Administrar Proyectos
Alineación Estratégica	Monitorear y Evaluar	Garantizar Cumplimiento con Requerimientos Externos
Alineación Estratégica / Entrega de Valor / Medición de Desempeño	Monitorear y Evaluar	Proporcionar Gobierno de TI
Alineación Estratégica / Entrega de Valor	Adquirir e Implementar	Identificar Soluciones Automatizadas
Entrega de Valor /	Adquirir e Implementar	Adquirir y Mantener Software

Área Enfoque Gobierno TI	Dominio COBIT	Proceso COBIT
Alineación Estratégica		Aplicativo
Entrega de Valor	Planear y Organizar	Administrar la inversión en TI
Entrega de Valor	Adquirir e Implementar	Facilitar la Operación y el Uso
Entrega de Valor	Adquirir e Implementar	Instalar y Acreditar Soluciones y Cambios
Entrega de Valor / Alineación Estratégica / Medición de Desempeño	Entregar y Dar Soporte	Definir y Administrar Niveles de Servicio
Entrega de Valor	Entregar y Dar Soporte	Administrar Servicios de Tercero
Entrega de Valor	Entregar y Dar Soporte	Garantizar la Continuidad del Servicio
Entrega de Valor	Entregar y Dar Soporte	Educar y Entrenar a los Usuarios
Entrega de Valor	Entregar y Dar Soporte	Administrar la Mesa de Servicios y los Incidentes
Entrega de Valor	Entregar y Dar Soporte	Administrar la Configuración
Entrega de Valor	Entregar y Dar Soporte	Administrar Problemas
Entrega de Valor	Entregar y Dar Soporte	Administrar Datos
Entrega de Valor	Monitorear y Evaluar	Monitorear y Evaluar Control Interno
Medición de Desempeño	Monitorear y Evaluar	Monitorear y Evaluar Desempeño de TI

A continuación se transcriben dominios y procesos vinculados a las áreas de enfoque de gobierno de TI desde COBIT:

PLANEAR Y ORGANIZAR

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

Procesos asociados

Definir un Plan Estratégico de TI.

Definición

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.

Medición

Se mide con

- El porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio
- El porcentaje de proyectos TI en el portafolio de proyectos que se pueden rastrear hacia el plan táctico de TI
- El retraso entre las actualizaciones del plan estratégico de TI y las actualizaciones de los planes tácticos de TI

Definir la Arquitectura de la Información.

Definición

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.

Medición

Se mide con:

- El porcentaje de elementos de datos redundantes / duplicados
- El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la empresa
- La frecuencia de actividades de validación de datos

Definir los Procesos, Organización y Relaciones de TI.

Definición

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.

Medición

Se mide con:

- El porcentaje de roles con descripciones de puestos y autoridad documentados
- El número de unidades/procesos de negocio que no reciben soporte de TI y que deberían recibirlo, de acuerdo con la estrategia
- Número de actividades clave de TI fuera de la organización de TI que no son aprobadas y que no están sujetas a los estándares organizacionales de TI

Administrar la inversión de TI.

Definición

Establecer y mantener un marco de trabajo para administrar programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias.

Medición

Se mide con:

- El porcentaje de reducción en el costo unitario del servicio de TI
- Porcentaje del valor de la desviación respecto al presupuesto en comparación con el presupuesto total
- Porcentaje de gasto de TI expresado en impulsores de valor del negocio (Ej. Incremento en ventas / servicios debidos a la mejora en conectividad)

Comunicar las Aspiraciones y la Dirección de la Gerencia.

Definición

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.

Medición

Se mide con:

- El número de interrupciones en el negocio debidas a interrupciones en el servicio de TI
- Porcentaje de interesados que entienden el marco de trabajo de control de TI de la empresa
- Porcentaje de interesados que no cumple las políticas

Administrar los Recursos Humanos de TI.

Definición

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.

Medición

Se mide con:

- El nivel de satisfacción de los interesados respecto a la experiencia y habilidades del personal
- La rotación de personal de TI
- Porcentaje de personal de TI certificado de acuerdo a las necesidades del negocio

Administrar la Calidad

Definición

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.

Medición

Se mide con:

- Porcentaje de Interesados (Stakeholders) satisfechos con la calidad (ponderado por importancia)
- Porcentaje de procesos de TI revisados de manera formal por aseguramiento de calidad de modo periódico que satisfaga las metas y objetivos de calidad
- Porcentaje de procesos que reciben revisiones de aseguramiento de calidad (QA)

Evaluar y Administrar los Riesgos de TI.

Definición

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la

organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

Medición

Se mide con:

- Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos
- Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados
- Porcentaje de planes de acción de administración de riesgos aprobados para su implantación

Administrar Proyectos

Definición

Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. El marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y post-implantación después de la instalación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. Este enfoque reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza la contribución a los programas de inversión facilitados por TI.

Medición

Se mide con:

- Porcentaje de proyectos que satisfacen las expectativas de los interesados (a tiempo, dentro del presupuesto, y con satisfacción de los requerimientos – ponderados por importancia)
- Porcentaje de proyectos con revisión post-implantación
- Porcentaje de proyectos que siguen estándares y prácticas de administración de proyectos

ADQUIRIR E IMPLEMENTAR

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?

- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

Procesos asociados

Identificar Soluciones Automatizadas

Definición

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”. Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.

Medición

Se mide con:

- Número de proyectos donde los beneficios establecidos no se lograron debido a suposiciones de factibilidad incorrectas
- Porcentaje de estudios de factibilidad autorizados por el dueño del proceso
- Porcentaje de usuarios satisfechos con la funcionalidad entregada

Adquirir y Mantener Software Aplicativo

Definición

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas

Medición

Se mide con:

- Número de problemas en producción por aplicación, que causan tiempo perdido significativo
- Porcentaje de usuarios satisfechos con la funcionalidad entregada

Adquirir y Mantener Infraestructura Tecnológica

Definición

Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.

Medición

Se mide con:

- El porcentaje de plataformas que no se alinean con la arquitectura de TI definida y los estándares de tecnología
- El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será)

Facilitar la Operación y el Uso

Definición

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la Infraestructura.

Medición

Se mide con:

- El número de aplicaciones en que los procedimientos de TI se integran en forma transparente dentro de los procesos de negocio
- El porcentaje de dueños de negocios satisfechos con el entrenamiento De aplicación y los materiales de apoyo.
- El número de aplicaciones que cuentan con un adecuado entrenamiento de apoyo al usuario y a la operación

Adquirir Recursos de TI

Definición

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí.

Medición

Se mide con:

- El número de controversias en relación con los contratos de adquisición
- La reducción del costo de compra
- El porcentaje de interesados clave satisfechos con los proveedores

ENTREGAR Y DAR SOPORTE

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.

Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?

- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

Procesos asociados

Definir y Administrar los Niveles de Servicio

Definición

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.

Medición

Se mide con:

- El porcentaje de Interesados satisfechos de que la entrega del servicio cumple con los niveles previamente acordados.
- El número de servicios entregados que no están en el catálogo
- El número de reuniones formales de revisión del Acuerdo de Niveles de Servicio (SLA) con las personas de negocio por año

Administrar los Servicios de Terceros

Definición

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

Medición

Se mide con:

- El número de quejas de los usuarios debidas a los servicios contratados
- El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio
- El porcentaje de los principales proveedores sujetos a monitoreo

Garantizar la Continuidad del Servicio

Definición

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

Medición

Se mide con:

- Número de horas perdidas por usuario por mes, debidas a interrupciones no planeadas
- Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad

Garantizar la Seguridad de los Sistemas

Definición

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

Medición

Se mide con:

- El número de incidentes que dañan la reputación con el público.
- El número de sistemas donde no se cumplen los requerimientos de seguridad.

Identificar y Asignar Costos

Definición

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios.

Medición

Se mide con:

- Porcentaje de facturas de servicios de TI aceptadas/pagadas por la gerencia del negocio.
- Porcentaje de variación entre los presupuestos, pronósticos y costos actuales.
- Porcentaje de costos totales de TI que son distribuidos de acuerdo con los modelos acordados

Educar y Entrenar a los Usuarios

Definición

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.

Medición

Se mide con:

- Número de llamadas de soporte debido a problemas de entrenamiento

- Porcentaje de satisfacción de los Interesados con el entrenamiento recibido
- Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo

Administrar la Mesa de Servicio y los Incidentes.

Definición

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.

Medición

Se mide con:

- Satisfacción del usuario con el soporte de primera línea
- Porcentaje de incidentes resueltos dentro de un lapso de tiempo aceptable / acordado.
- Índice de abandono de llamadas

Administración de Datos

Definición

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios

Medición

Se mide con:

- Satisfacción del usuario con la disponibilidad de los datos.
- Porcentaje de restauraciones exitosas de datos.
- Número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados

Administración de Operaciones

Definición

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware.

Medición

Se mide con:

- Número de niveles de servicio afectados a causa de incidentes en la operación.
- Horas no planeadas de tiempo sin servicio a causa de incidentes en la operación.

- Porcentaje de activos de hardware incluidos en los programas de mantenimiento

MONITOREAR Y EVALUAR

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

Procesos asociados

Monitorear y Evaluar el Desempeño de TI

Definición

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas

Medición

Se mide con:

- Satisfacción de la gerencia y de la entidad de gobierno con los reportes de desempeño
- Número de acciones de mejoramiento impulsadas por las actividades de monitoreo
- Porcentaje de procesos críticos monitoreados

Monitorear y Evaluar el Control Interno

Definición

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

Medición

Se mide con:

- Número de brechas importantes del control interno
- Número de iniciativas para la mejora del control
- Número y cubrimiento de auto evaluaciones de control

Garantizar el Cumplimiento con Requerimientos Externos

Definición

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.

Medición

Se mide con:

- El costo del no cumplimiento de TI, incluyendo arreglos y multas
- Tiempo promedio de demora entre la identificación de los problemas externos de cumplimiento y su resolución
- Frecuencia de revisiones de cumplimiento

Proporcionar Gobierno de TI

Definición

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.

Medición

Se mide con:

- La frecuencia de informes del consejo directivo sobre TI a los interesados (incluyendo el nivel de madurez)
- La frecuencia de los reportes de TI hacia el consejo directivo (incluyendo el nivel de madurez)
- Frecuencia de revisiones independientes del cumplimiento de TI

FUENTES DE CONSULTAS

COBIT 4.1

ISO / IEC 38500

www.adacsi.org.ar