4.0

Objetivos de control

COBIT 4.0

CONTROLES DE PROCESOS DE TI

COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo común de referencia entendible para los responsables operacionales de las áreas de servicios informáticos. Para lograr un gobierno efectivo, los responsables de TI deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

REQUERIMIENTOS DE CONTROL GENÉRICOS

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Los objetivos de control detallados estan identificados por dos caracteres que respresentan el dominio más un número de proceso y un número de objetivo de control.

Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Propietario del proceso
Asignar un propietario para cada proceso COBIT de tal modo que la responsabilidad sea clara.

PC2 Repetibilidad
Definir cada proceso COBIT de tal forma que sea repetible.

PC3 Metas y objetivos
Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.

PC4 Roles y responsabilidades
Definir roles, actividades y responsabilidades claros para cada proceso COBIT para una ejecución eficiente.

PC5 Desempeño del proceso
Medir el desempeño de cada proceso COBIT en comparación con sus metas.

PC6 Políticas, planes y procedimientos
Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT.

CONTROLES GENERALES

Los controles generales son aquellos que están incrustados en los procesos y servicios de TI. Algunos ejemplos son:
• Desarrollo de sistemas
• Administración del cambio
• Seguridad
• Operació del computador

Los controles incluidos en las aplicaciones del proceso de negocios se conocen por lo general como controles de aplicación. Ejemplos:
• Integridad (Completitud)
• Precisión
• Validez
• Autorización
• Segregación de funciones

COBIT asume que el diseño e implementación de los controles de aplicaciones soportadas por TI son responsabilidad de las áreas de servicios informáticos, con base en los requerimientos de negocio definidos y usando los criterios de información de COBIT. Están cubiertos en el dominio de Adquirir e Implementar.
La responsabilidad operacional de administrar y monitorear los controles de cada aplicación soportada por TI es del

propietario del proceso de negocio, no del área de servicios informáticos, quien entrega y da soporte de servicios a las aplicaciones, a las bases de datos e infraestructura de soporte.

Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales sobre los procesos de TI, pero no a los controles de las aplicaciones, debido a que son responsabilidad de los propietarios de los procesos de negocio y, como se describió previamente, están integrados en los sistemas que sirven de apoyo a los procesos de negocio.

La siguiente lista ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados con ACn, que significa número de control aplicación (por sus siglas en inglés):

CONTROLES DE ORIGEN / AUTORIZACIÓN DE DATOS

AC1 Procedimientos de preparación de datos
Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de formas de entrada ayuda a asegurar que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades se detecten, reporten y corrijan.

AC2 Procedimientos de autorización de documentos fuente
El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de documentos fuente.

AC3 Recolección de datos de documentos fuente
Los procedimientos garantizan que todos los documentos fuente autorizados sean completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

AC4 Manejo de errores en documentos fuente
Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.

AC5 Retención de documentos fuente
Existen procedimientos para garantizar que los documentos fuente originales son retenidos o son reproducibles por la organización durante una cantidad de tiempo adecuada para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

CONTROLES DE ENTRADA DE DATOS

AC6 Procedimientos de autorización de captura de datos
Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.

AC7 Verificaciones de precisión, integridad y autorización
Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

AC8 Manejo de errores en la entrada de datos
Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

CONTROLES DE PROCESAMIENTO DE DATOS

AC9 Integridad de procesamiento de datos
Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.

AC10 Validación y edición del procesamiento de datos
Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de

inteligencia artificial.

AC11 Manejo de errores en el procesamiento de datos
Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

CONTROLES DE SALIDA DE DATOS

AC12 Manejo y retención de salidas
El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y toman en cuenta los requerimientos de privacidad y de seguridad.

AC13 Distribución de salidas
Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.

AC14 Cuadre y conciliación de salidas
Las salidas cuadran de forma rutinaria contra los totales de control correspondientes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.

AC15 Revisión de salidas y manejo de errores
Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.

AC16 Provisión de seguridad para reportes de salida
Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios.

CONTROLES DE LÍMITES

AC17 Autenticidad e integridad
Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

AC18 Protección de información sensitiva durante su transmisión y transporte
Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte.

COBIT 4.0

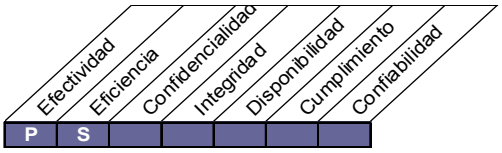
PLANEAR Y ORGANIZAR

PO1 Definir un plan estratégico de TI
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica
PO4 Definir los procesos, organización y relaciones de TI
PO5 Administrar la inversión en TI
PO6 Comunicar las metas y la dirección de la gerencia
PO7 Administrar recursos humanos de TI
PO8 Administrar la calidad
PO9 Evaluar y administrar los riesgos de TI
PO10 Administrar proyectos

Objetivo de control de alto nivel

PO1 Definir un plan estratégico para TI

Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia y las prioridades de negocio. La función de TI y los participantes del negocio son responsables de garantizar que se materialice el valor óptimo de los portafolios de proyectos y servicios. El plan estratégico debe mejorar el entendimiento de los participantes clave respecto a las oportunidades y limitaciones de TI, evaluar el desempeño actual y aclarar el nivel de inversión requerido. La estrategia de negocio y las prioridades se deben reflejar en el portafolios y deben ser ejecutadas por los planes tácticos de TI, los cuales establecen objetivos, planes y tareas específicas, entendidas y aceptadas tanto por el negocio como por TI.



Control sobre el proceso TI de

Definir un plan estratégico para TI

que satisface el requisito de negocio de TI para

sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos

enfocándose en

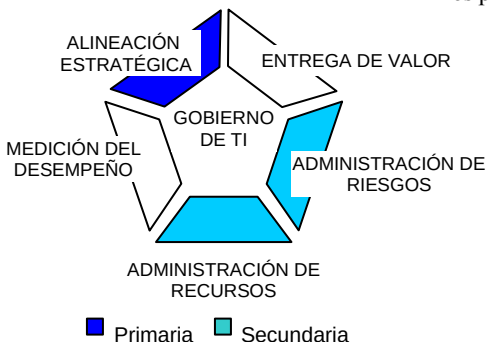
la incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para otorgar estos servicios de una forma transparente y rentable

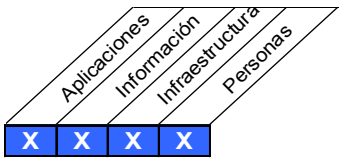
se logra con

- La intervención con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras
- El entendimiento de las capacidades actuales de TI
- La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio

y 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





Objetivos de control detallados

PO1.1 Administración del valor de TI
Trabajar con el negocio para garantizar que el portafolio de inversiones habilitadas por TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes de TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, calendario o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar basados en acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos debe ser claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

PO1.2 Alineación negocio - TI
Capacitar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado la TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, uniendo de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de la TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

PO1.3 Evaluación del desempeño actual
Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

PO1.4 Plan estratégico de TI
Crear un plan estratégico que defina, en cooperación con los participantes relevantes, cómo la TI contribuirá a los objetivos estratégicos de la organización (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los participantes. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

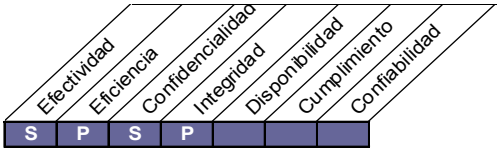
PO1.5 Planes tácticos-TI
Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán vigilados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.

PO1.6 Administración del portafolio-TI
Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y licenciar los proyectos requeridos al momento de lanzar el programa.

Objetivo de control de alto nivel

PO2 Definir la arquitectura de información

La definición de la función de los 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 mejorar la rendición de cuentas de la integridad y seguridad de los datos y para mejorar la efectividad y control de la compartición de datos a lo largo de las aplicaciones y de las entidades



Planear y organizar

Adquirir e implantar

Entrega y soporte

Monitorear y evaluar

Control sobre el proceso TI de

Definir la arquitectura de la información

que satisface el requisito de negocio de TI para

agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente y para integrar de forma transparente las aplicaciones a los procesos del negocio

enfocándose en

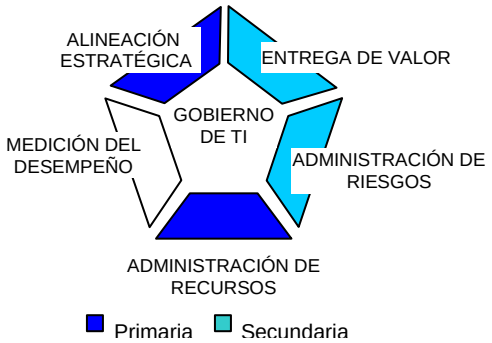
el establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos

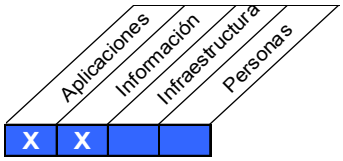
se logra con

- El aseguramiento de la precisión de la arquitectura de la información y del modelo de datos
- La asignación de propiedad de datos
- La clasificación de la información usando un esquema de clasificación acordado

y se mide con

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





Objetivos de control detallados

PO2.1 Modelo de arquitectura de información empresarial
Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, rentable oportuna segura y resistente al cambio.

PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos
Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita la compartición de elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.

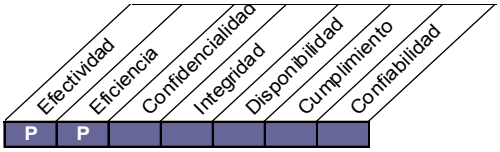
PO2.3 Esquema de clasificación de datos
Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y delicada es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y delicados son. Se usa como base para aplicar controles como el control de acceso, archivo y encriptación.

PO2.4 Administración de la integridad
Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

Objetivo de control de alto nivel

PO3 Determinar la dirección tecnológica

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un consejo de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para procuración de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.



Control sobre el proceso TI de

Determinar la dirección tecnológica

que satisface el requisito de negocio de TI para

contar con sistemas aplicativos estándar, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros

enfocándose en

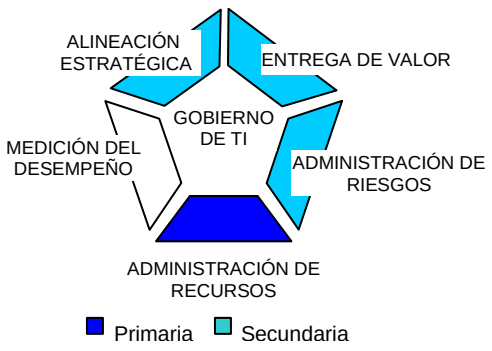
la definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas

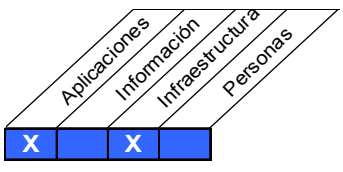
se logra con

- El establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento
- El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos
- La definición de estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información

y se mide con

- El número y tipo de desviaciones con respecto al plan de infraestructura tecnológica
- Frecuencia de las revisiones /actualizaciones del plan de infraestructura tecnológica
- Número de plataformas de tecnología por función a través de toda la empresa





Objetivos de control detallados

PO3.1 Planeación de la dirección tecnológica
Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

PO3.2 Plan de infraestructura tecnológica
Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye disposiciones de contingencia y orientación para la adquisición de recursos tecnológicos. También toma en cuenta las cambios en el ambiente competitivo, las economías de escala en la procuración de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

PO3.3 Monitoreo de tendencias y regulaciones futuras
Establecer un proceso para monitorear las tendencias ambientales del sector de la industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

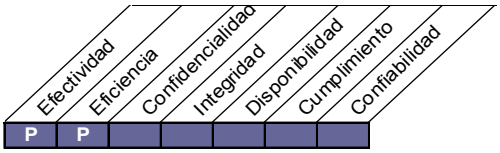
PO3.4 IT Estándares tecnológicos
Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su relevancia, y riesgo para el negocio y en el cumplimiento de requerimientos externos.

PO3.5 Consejo de arquitectura
Establecer un consejo de arquitectura de TI que proporcione directrices de arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Esto se relaciona con la arquitectura de la información

Objetivo de control de alto nivel

PO4 Definir los procesos, organización y relaciones de TI

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 estará incrustada en un marco de trabajo de procesos de TI que garantice la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la monitoreo del consejo directivo sobre la TI, y uno ó más comités administrativos, en los cuales participan tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas administrativas 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 tareas. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.



Control sobre el proceso TI de

Definir los procesos, organización y relaciones de TI

que satisface el requisito de negocio de TI para

agilizar la respuesta a las estrategias del negocio mientras al mismo tiempo cumple con los requerimientos de gobierno y se brindan puntos de contacto definidos y competentes

enfocándose en

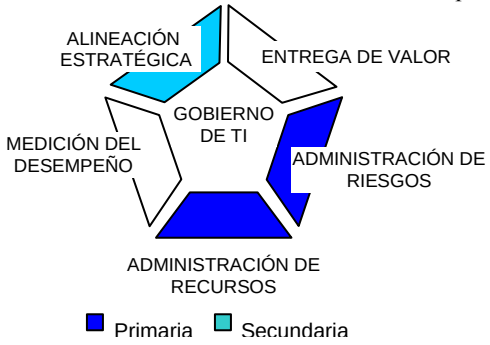
el establecimiento de estructuras organizacionales de TI transparentes, flexibles y sensibles, y en la definición e implantación de procesos de TI con los propietarios, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión

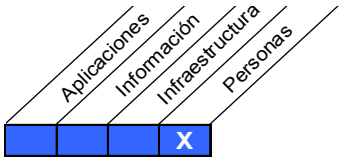
se logra con

- La definición de un marco de trabajo de procesos de TI
- El establecimiento de organismos y estructuras organizacionales apropiadas
- La definición de roles y responsabilidades

y se mide con

- El porcentaje de roles y 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 a 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





Objetivos de control detallados

PO4.1 Marco de trabajo del proceso
Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (esto es, administrar brechas y traslapes de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de TI, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.

PO4.2 Comité estratégico
Establecer un comité estratégico de TI a nivel del consejo directivo. Este comité garantiza que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo directivo completo.

PO4.3 Comité directivo
Establecer un comité directivo de TI (o su equivalente) compuesto de gerencia ejecutiva, del negocio y de TI para:
- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Rastrear el estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio

PO4.4 Ubicación organizacional de la función de TI
Ubicar a la función de TI dentro de la estructura general organizacional con un modelo de negocios supeditado a la importancia de TI dentro de la organización, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

PO4.5 Estructura organizacional
Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y de procuración para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

PO4.6 Roles y responsabilidades
Definir y difundir los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad.

PO4.7 Responsabilidad de aseguramiento de calidad de TI
Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad y proporcionar al grupo de aseguramiento los sistemas, los controles y la experiencia comunicativa necesaria. La ubicación organizacional y las responsabilidades y tamaño del grupo de aseguramiento de calidad satisfacen los requerimientos de la organización.

PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
Incluir la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel de responsabilidad apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad, seguridad física y cumplimiento de la información. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

PO4.9 Propiedad de datos y de sistemas
Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad de datos y de sistemas de información. Los propietarios toman decisiones sobre la clasificación de la información y los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

PO4.10 Supervisión
Implantar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores de desempeño clave.

PO4.11 Segregación de tareas
Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo corrompa un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

PO4.12 Procuración de personal
Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de personal competente de TI. La procuración de personal toma en cuenta la co-ubicación de personal de negocios / TI, el entrenamiento de funcionalidad recíproca, la rotación de puestos y las oportunidades de personal externo.

PO4.13 Personal clave de TI
Definir e identificar al personal clave de TI y minimizar la dependencia excesiva en ellos. Debe existir un plan para contactar al personal clave en caso de emergencia.

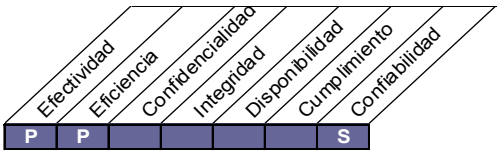
PO4.14 Políticas y procedimientos para personal sub-contratado
Definir e implantar políticas y procedimientos para controlar las actividades de los consultores y otro personal sub-contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales acordados.

PO4.15 Relaciones
Establecer y mantener una estructura óptima de unión, de comunicación y de coordinación, entre la función de TI y otras funciones dentro y fuera de la función de TI, tales como el consejo directivo, ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo corporativo de cumplimiento, los sub-contratistas y la gerencia fuera de sitio.

Objetivo de control de alto nivel

PO5 Administrar la inversión en TI

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Trabajar con los participantes 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. El proceso fomenta la sociedad entre TI y los participantes del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y rendición de cuentas dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.



Control sobre el proceso TI de

Administrar la inversión en TI

que satisface el requisito de negocio de TI para

mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrales y estándar que satisfagan las expectativas del usuario

enfocándose en

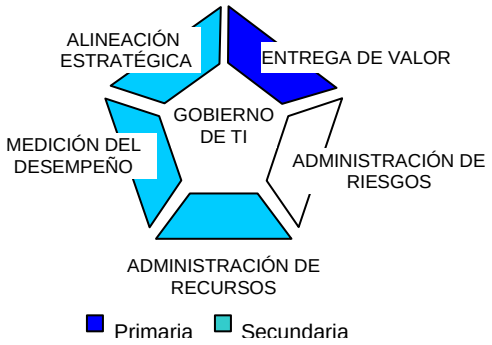
decisiones de portafolio e inversión en TI efectivas y eficientes, y por medio del establecimiento y rastreo de presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión

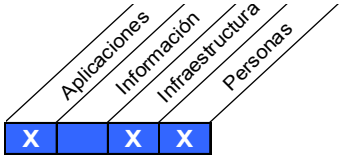
se logra con

- El pronóstico y la asignación de presupuestos
- La definición de criterios formales de inversión (ROI, periodo de restitución, NPV)
- La medición y evaluación del valor del negocio en comparación con el pronóstico

y 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
- % de gasto de TI expresado en impulsores de valor del negocio (esto es, mejora en ventas / servicios debidos a la mejora en conectividad





Objetivos de control detallados

PO5.1 Marco de trabajo para la administración financiera
Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos. Dar mantenimiento a los portafolios de los programas de inversión de TI, de servicios y de activos de TI, los cuales forman la base para el presupuesto corriente de TI. Brindar información de entrada hacia los casos de negocio de nuevas inversiones, tomando en cuenta los portafolios actuales de activos y servicios de TI. Las nuevas inversiones y el mantenimiento a los portafolios de servicios y de activos influenciarán el futuro presupuesto de TI. Comunicar los aspectos de costo y beneficio de estos portafolios a los procesos de prioridad de presupuestos, administración de costos y administración.

PO5.2 Prioridades dentro del presupuesto de TI
Implantar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

PO5.3 Proceso presupuestal
Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y los presupuestos de programas individuales.

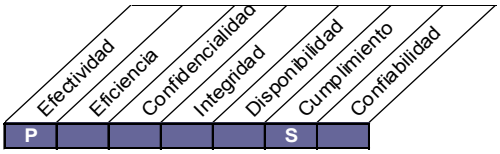
PO5.4 IT Administración de costos
Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, estas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

PO5.5 Administración de beneficios
Implantar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar. Los reportes se deben revisar y, donde existan oportunidades para mejorar la contribución de TI, se deben definir y tomar las medidas apropiadas. Siempre que los cambios en la contribución de TI tengan impacto en el programa, o cuando los cambios a otros proyectos relacionados impacten al programa, el caso de negocio deberá ser actualizado.

Objetivo de control de alto nivel

PO6 Comunicar las metas y la dirección de la gerencia

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 implantar 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 conciencia el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.



Control sobre el proceso TI de

Comunicar las metas y la dirección de la gerencia

que satisface el requisito de negocio de TI para

una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades

enfocándose en

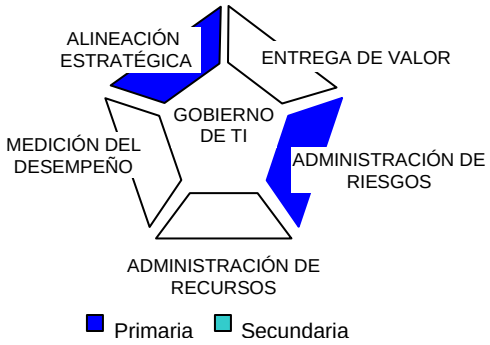
la procuración de políticas, procedimientos, directrices y otra documentación, de forma precisa, a los participantes

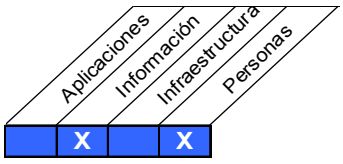
se logra con

- La definición de un marco de trabajo de control para TI
- La elaboración e implantación de políticas para TI
- La implantación de políticas de TI

y se mide con

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





Objetivos de control detallados

PO6.1 Ambiente de políticas y de control
Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras que al mismo tiempo administra riesgos significativos, fomenta la colaboración inter-divisional y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI. El marco de trabajo debe estar integrado por el marco de procesos de TI y el sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio.

PO6.3 Administración de políticas para TI
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular.

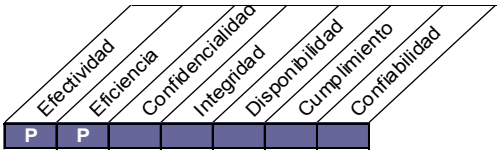
PO6.4 Implantación de políticas de TI
Asegurarse de que las políticas de TI se implantan y se difunden a todo el personal relevante, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. Los métodos de implantación deben resolver necesidades e implicaciones de recursos y concientización.

PO6.5 Comunicación de metas y dirección de TI
Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización. La información comunicada debe abarcar una misión claramente articulada, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código de ética y conducta, políticas y procedimientos, etc., y se deben incluir dentro de un programa de comunicación continua, apoyado por la alta dirección con acciones y palabras. La dirección debe dar especial atención a comunicar la conciencia sobre la seguridad de TI y el mensaje de que la seguridad de TI es responsabilidad de todos.

Objetivo de control de alto nivel

PO7 Administrar los recursos humanos de TI

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.



Control sobre el proceso TI de

Administrar los recursos humanos de TI

que satisface el requisito de negocio de TI para

personas competentes y motivadas para crear y entregar servicios de TI

enfocándose en

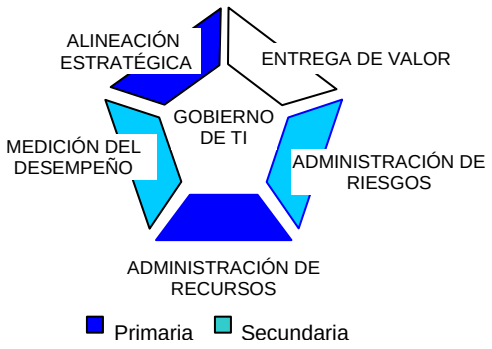
la contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos

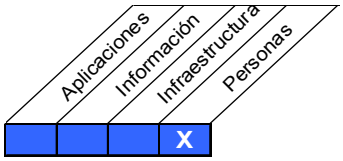
se logra con

- La revisión del desempeño del personal
- La contratación y entrenamiento de personal de TI para apoyar los planes tácticos de TI
- La mitigación del riesgo de sobre-dependencia en recursos clave

y se mide con

- El nivel de satisfacción de los participantes 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





Objetivos de control detallados

PO7.1 Ambiente de políticas y de control
Asegurarse de que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (esto es, contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

PO7.2 Habilidades del personal
Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

PO7.3 Procuración de personal para roles
Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. Los términos y condiciones de empleo deben enfatizar la responsabilidad del empleado respecto a la seguridad de la información, al control interno y al cumplimiento regulatorio. El nivel de supervisión debe estar de acuerdo con a la sensibilidad del puesto y el grado de responsabilidades asignadas.

PO7.4 Entrenamiento del personal de TI
Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

PO7.5 Dependencia sobre los individuos
Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

PO7.6 Investigación del personal
Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

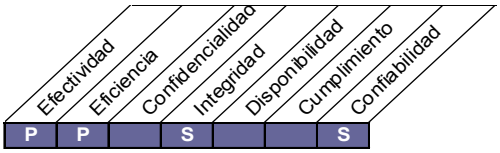
PO7.7 Evaluación del desempeño del empleado
Es necesario que las evaluaciones de desempeño se realicen de manera periódica, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

PO7.8 Modificaciones al puesto y terminaciones
Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

Objetivo de control de alto nivel

PO8 Administrar la calidad

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 de la constante monitoreo, corrección de desviaciones, y la comunicación de los resultados a los participantes. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los participantes.



Control sobre el proceso TI de

Administrar la calidad

que satisface el requisito de negocio de TI para

la mejora continua y medible de la calidad de los servicios de TI prestados

enfocándose en

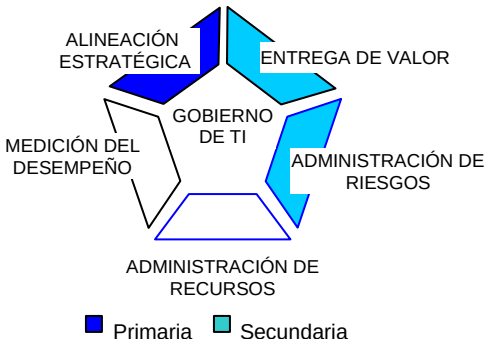
la definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), la monitoreo continua del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI

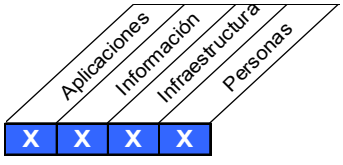
se logra con

- La definición de estándares y prácticas de calidad
- La monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas
- Mejorar el QMS de manera continua

y se mide con

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





Objetivos de control detallados

PO8.1 Sistema de administración de calidad
Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.

PO8.2 Estándares y prácticas de calidad
Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

PO8.3 Estándares de desarrollo y de adquisición
Adoptar y mantener estándares para todo el desarrollo y adquisición que siguen el ciclo de vida de hasta el último entregable e incluyen la aprobación en puntos clave con base en criterios de aprobación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter-operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

PO8.4 IT Enfoque hacia el cliente
Garantiza que la administración de calidad se enfoque en los clientes, al determinar sus requerimientos y alinearlos con los estándares y prácticas de TI. Se definen los roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

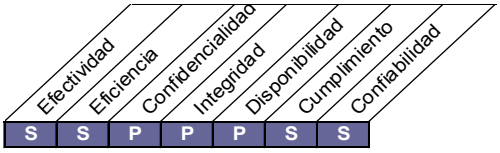
PO8.5 Mejora continua
Se elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.

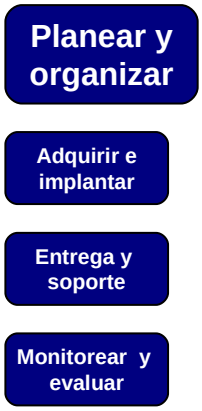
PO8.6 Medición, monitoreo y revisión de calidad
Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, la monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

Objetivo de control de alto nivel

PO9 Evaluar y administrar los riesgos de TI

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 acordados. 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 participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.





Control sobre el proceso TI de

Evaluar y administrar los riesgos de TI

que satisface el requisito de negocio de TI para

analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio

enfocándose en

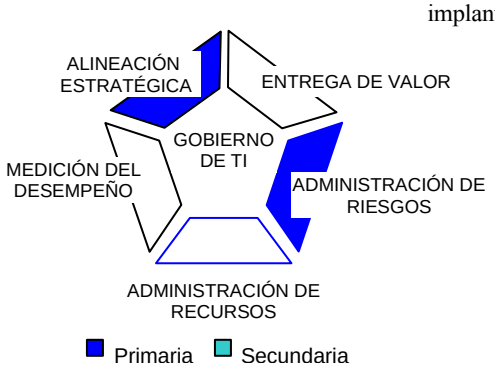
la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y difusión de riesgos residuales

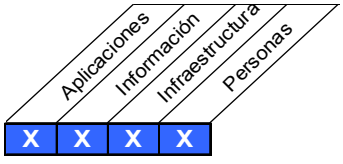
se logra con

- La garantía de que la administración de riesgos está completamente incluida en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente
- La realización de evaluaciones de riesgo
- Recomendar y comunicar planes de acciones correctivas de riesgos

y 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





Objetivos de control detallados

PO9 Evaluar y administrar riesgos de TI

PO9.1 Alineación de la administración de riesgos de TI y del negocio
Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con la aceptación del riesgo y con el nivel de tolerancia al riesgo de la organización

PO9.2 Establecimiento del contexto del riesgo
Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos
Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

PO9.4 IT Evaluación de riesgos
Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

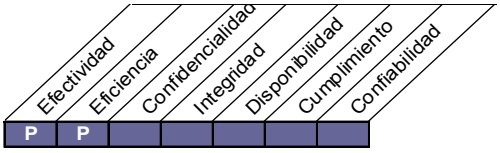
PO9.5 Respuesta a los riesgos
Identificar a los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos
Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes, y reportar cualquier desviación a la alta dirección..

Objetivo de control de alto nivel

P010 Administrar proyectos

Establecer un programa y un marco de control administrativo de proyectos para la administración de todos los proyectos de TI. 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 revisión post-implantación después de la implantación 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 su contribución a los programas de inversión en TI.



Control sobre el proceso TI de

Administrar proyectos

que satisface el requisito de negocio de TI para

la entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados

enfocándose en

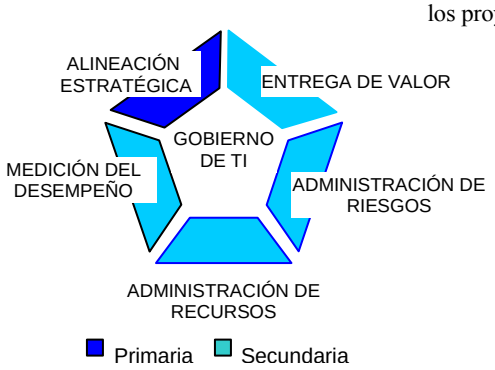
un programa y un enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los participantes y la monitoreo de los riesgos y los avances de los proyectos

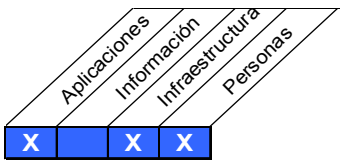
se logra con

- La definición e implantación de marcos y enfoques de programas y de proyectos
- La emisión de directrices administrativas para proyectos
- La planeación de proyectos para todos los proyectos incluidos en el portafolio de proyectos

y se mide con

- Porcentaje de proyectos que satisfacen las expectativas de los participantes (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 los estándares y las prácticas administrativas de los proyectos





Objetivos de control detallados

P010 Administrar los proyectos

P010.1 Marco de trabajo para la administración de programas
Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los programas apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

P010.2 Marco de trabajo para la administración de proyectos
Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas.

P010.3 Enfoque de administración de proyectos
Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

P010.4 Compromiso de los participantes
Obtener el compromiso y la participación de los participantes afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.

P010.5 Estatuto de alcance del proyecto
Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los participantes, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversión en TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de arrancar el proyecto.

P010.6 Inicio de las fases del proyecto
Asegurarse que el arranque de las etapas importantes del proyecto se apruebe de manera formal y se comunique a todos los participantes. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión mayor del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto.

P010.7 Plan integrado del proyecto
Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

P010.8 Recursos del proyecto
Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros apropiados del equipo y/o a los contratistas al proyecto. La procuración de productos y servicios requeridos para cada proyecto se deben planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de procuración de la organización.

P010.9 Administración de riesgos del proyecto
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

PO10.10 Plan de calidad del proyecto
Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.

PO10.11 Control de cambios del proyecto
Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (esto es, costos, calendario, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

PO10.12 Planeación de métodos de aseguramiento para el proyecto
Identificar las tares de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

PO10.13 Medición del desempeño, reportes y monitoreo del proyecto
Medir el desempeño del proyecto contra los criterios clave del proyecto (esto es, alcance, calendario, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los participantes clave; y recomendar, implantar y monitorear las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

PO10.14 Cierre del proyecto
Solicitar que al finalizar cada proyecto, los participantes del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad sobresaliente requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas

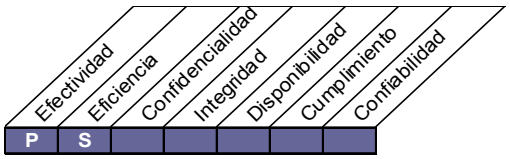
ADQUIRIR E IMPLEMENTAR

AI1 Identificar soluciones automatizadas
AI2 Adquirir y mantener software aplicativo
AI3 Adquirir y mantener infraestructura tecnológica
AI4 Facilitar operación y uso
AI5 Procurar recursos de TI
AI6 Administrar cambios
AI7 Instalar y acreditar soluciones y cambios

Objetivo de control de alto nivel

AI1 Identificar soluciones automatizadas

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 implantar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.



Control sobre el proceso TI de

Identificar soluciones de automatización

que satisface el requisito de negocio de TI para

traducir los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas

enfocándose en

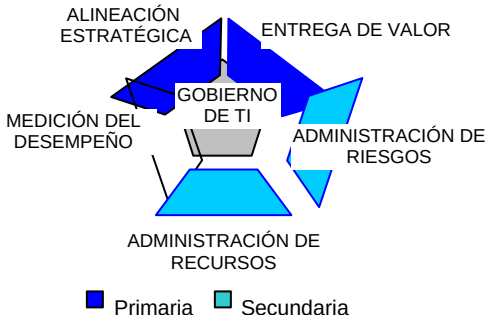
la identificación de soluciones técnicamente factibles y rentables

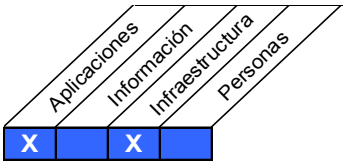
se logra con

- La definición de los requerimientos técnicos y de negocio
- Realizar estudios de factibilidad como se define en los estándares de desarrollo
- Aprobar (o rechazar) los requerimientos y los resultados de los estudios de factibilidad

y se mide con

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





Objetivos de control detallados

AI1 Identificar las soluciones automatizadas

AI1.1 Definición y mantenimiento de los requerimientos de negocio funcionales y técnicos
Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI. Definir los criterios de aceptación de los requerimientos. Estas iniciativas deben incluir todos los cambios requeridos dada la naturaleza del negocio, de los procesos, de las aptitudes y habilidades del personal, su estructura organizacional y la tecnología de apoyo.

Los requerimientos toman en cuenta las necesidades funcionales, la dirección tecnológica, el desempeño, el costo, la confiabilidad, la compatibilidad, la auditoría, la seguridad, la disponibilidad y continuidad, la ergonomía, la funcionalidad, la seguridad y la legislación de la empresa. Establecer procesos para garantizar y administrar la integridad, precisión y la validez de los requerimientos del negocio, como base para el control de la adquisición y el desarrollo continuo de sistemas. Estos requerimientos deben ser propiedad del patrocinador del negocio.

AI1.2 Reporte de análisis de riesgos
Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos. Los riesgos incluyen las amenazas a la integridad, seguridad, disponibilidad y privacía de los datos, así como el cumplimiento de las leyes y reglamentos.

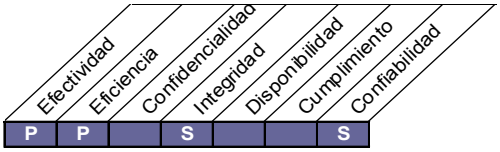
AI1.3 Estudio de factibilidad y formulación de cursos de acción alternativos
Desarrollar un estudio de factibilidad que examine la posibilidad de implantar los requerimientos. Debe identificar los cursos alternativos de acción para el software, hardware, servicios y habilidades que satisfagan los requerimientos establecidos, tanto funcionales como técnicos, y evaluar la factibilidad tecnológica y económica (costo potencial y análisis de beneficios) de cada uno de los cursos de acción identificados en el contexto de inversión en TI. Es posible que existan varias iteraciones en el desarrollo del estudio de factibilidad, a medida que factores tales como los cambios a los procesos del negocio, la tecnología y las habilidades son evaluados. La administración del negocio, apoyada por la función de TI, debe evaluar la factibilidad y los cursos alternativos de acción y realizar recomendaciones al patrocinador del negocio.

AI1.4 Requerimientos, decisión de factibilidad y aprobación.
El patrocinador del negocio aprueba y autoriza los requisitos de negocio, tanto funcionales como técnicos, y los reportes del estudio de factibilidad en las etapas clave predeterminadas. Cada autorización va después de la terminación de las revisiones de calidad. El patrocinador del negocio tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.

Objetivo de control de alto nivel

AI2 Adquirir y mantener software aplicativo

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.



Control sobre el proceso TI de

Adquirir y dar mantenimiento a software aplicativo

que satisface el requisito de negocio de TI para

haciendo que las aplicaciones estén de acuerdo con los requerimientos del negocio, y haciéndolo a tiempo y a un costo razonable

enfocándose en

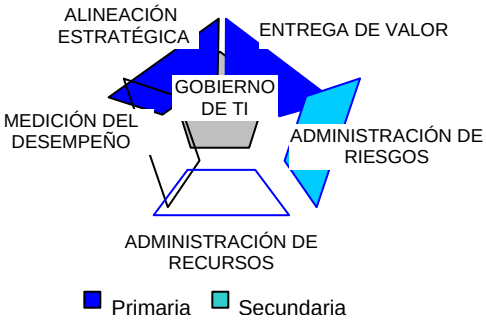
garantizar que exista un proceso de desarrollo oportuno y confiable

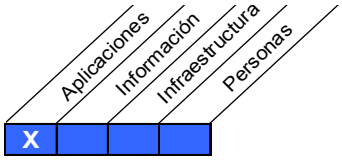
se logra con

- La traducción de requerimientos de negocio a especificaciones de diseño
- La adhesión a los estándares de desarrollo para todas las modificaciones
- La separación de las actividades de desarrollo, de pruebas y operativas

y se mide con

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





Objetivos de control detallados

AI2 Adquirir y mantener software aplicativo

AI2.1 Diseño de alto nivel
Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta los dominios tecnológicos y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.

AI2.2 Diseño detallado
Preparar el diseño detallado y los requerimientos de aplicación del software técnico. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Los conceptos a considerar incluyen, pero no se limitan a, definir y documentar los requerimientos de entrada de datos, definir la interfase, la interfase de usuario, el diseño para la recopilación de datos fuente, la especificación de programa, definir y documentar los requerimientos de archivo, requerimientos de procesamiento, definir los requerimientos de salida, control y auditoría, seguridad y disponibilidad, y pruebas. Realizar una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.

AI2.3 Control de aplicación y auditoria
Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable. Los asuntos que se consideran de forma especial son: mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

AI2.4 Seguridad y disponibilidad aplicativas.
Abordar la seguridad aplicativa y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo. Los asuntos a considerar incluyen derechos de acceso y administración de privilegios, protección de información delicada en todas las etapas, integridad de autentificación y transacción, y recuperación automática.

.
AI2.5 Configuración e implantación de software aplicativo adquirido
Personalizar e implantar la funcionalidad automatizada de adquisición con el uso de procedimientos de configuración, aceptación y prueba. Los asuntos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

AI2.6 Ampliaciones importantes a sistemas existentes
Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales. Los asuntos a considerar incluyen análisis, justificación costo/beneficio y administración de requerimientos.

AI2.7 Desarrollo de software aplicativo
Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad. Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación de revisiones de funcionalidad, desempeño y calidad. Los asuntos a considerar incluyen aprobar las especificaciones de diseño que satisfacen los requerimientos de negocio, funcionales y técnicos; aprobar las solicitudes de modificación; y confirmación de que el software aplicativo es compatible con la producción y está listo para su migración. Además, garantizar que se identifican y dirigen todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.

AI2.8 Aseguramiento de la Calidad del Software
Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen especificar el criterio de calidad y procesos de validación y verificación, incluyendo inspección, chequeos superficiales de programas y pruebas.

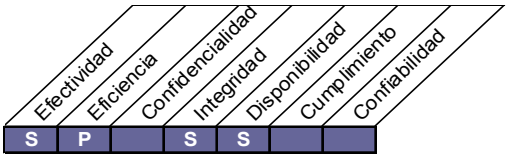
AI2.9 Administración de los requerimientos de aplicaciones
Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

AI2.10 Mantenimiento de software aplicativo
Desarrollar una estrategia y plan para el mantenimiento y liberación de aplicaciones de software. Los asuntos a considerar incluyen liberación de planeación y control, planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de mejoramiento, condiciones contractuales tales como publicaciones de apoyo y mejoras, revisión periódica de acuerdo a las necesidades del negocio, riegos y requerimientos de seguridad.

Objetivo de control de alto nivel

AI3 Adquirir y mantener infraestructura tecnológica

Las organizaciones deben contar con procesos para adquirir, implantar y mejorar 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 para desarrollar y realizar pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.



Control sobre el proceso TI de

Adquirir y dar mantenimiento a infraestructura tecnológica

que satisface el requisito de negocio de TI para

adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI

enfocándose en

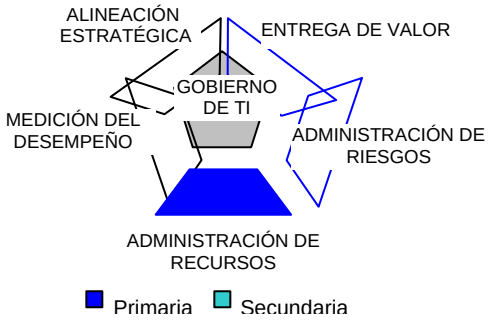
proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología

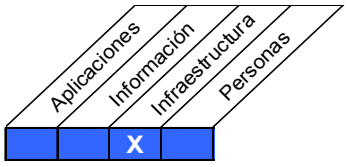
se logra con

- La producción de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica
- La planeación de mantenimiento de la infraestructura
- La implantación de medidas de control interno, seguridad y auditoría

y 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)
- El número de componentes de infraestructura que ya no se pueden soportar (o que ya no se podrán en el futuro cercano)





Objetivos de control detallados

AI3 Adquirir y mantener infraestructura tecnológica

AI3.1 Plan de adquisición de infraestructura tecnológica
Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con el rumbo tecnológico de la organización. El plan debe considerar extensiones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para ampliaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir capacidad técnica nueva.

AI3.2 Protección y disponibilidad del recurso de infraestructura
Implantar medidas de control interno, seguridad y auditoría durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura delicados por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

AI3.3 Mantenimiento de la Infraestructura
Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan las modificaciones, de acuerdo con el procedimiento de administración de modificaciones de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de programas de ajuste y estrategias de mejoramiento, riesgos, evaluación de vulnerabilidad y requerimientos de seguridad.

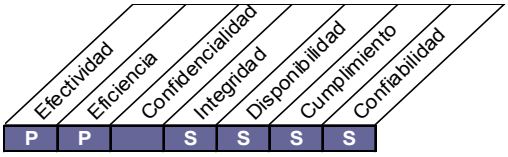
AI3.4 Ambiente de prueba de factibilidad
Establecer el ambiente de desarrollo y pruebas para respaldar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versión, datos y herramientas de prueba, y seguridad.

.

Objetivo de control de alto nivel

AI4 Facilitar la operación y el uso

El conocimiento de los nuevos sistemas debe ser accesible. 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.



Control sobre el proceso TI de

Facilitar la operación y el uso

que satisface el requisito de negocio de TI para

garantizar la satisfacción de los usuarios finales mediante ofrecimientos y niveles de servicio, y de forma transparente integrar las soluciones de aplicación y tecnología dentro de los procesos del negocio.

enfocándose en

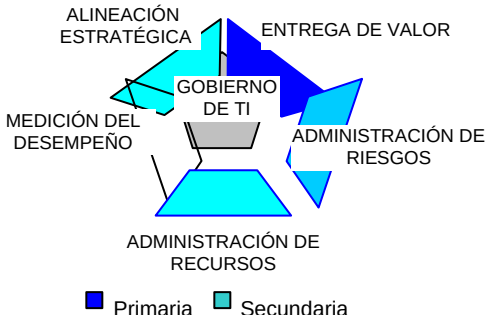
proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema.

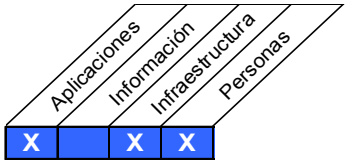
se logra con

- El desarrollo y la disponibilidad de documentación para transferir el conocimiento
- Comunicación y entrenamiento a usuarios y a la gerencia del negocio, al personal de apoyo y al personal de operación
- La generación de materiales de entrenamiento

y 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 propietarios 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





Objetivo de control detallados

AI4 Facilitar la operación y el uso

AI4.1 Plan para soluciones de operación
Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los participantes puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o mejora de sistemas automatizados o de infraestructura.

AI4.2 Transferencia de conocimiento a la gerencia del negocio
Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, diferenciación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.

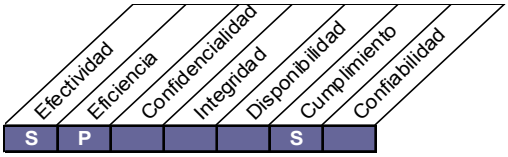
AI4.3 Transferencia de conocimiento a usuarios finales
Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de la aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave, y evaluación.

AI4.4 Transferencia de conocimiento al personal de operaciones y apoyo
Transferir el conocimiento y habilidades para permitir al personal de apoyo técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.
.

Objetivo de control de alto nivel

AI5 Adquirir recursos de TI

Se necesitan adquirir los 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. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.



Control sobre el proceso TI de

Adquirir recursos de TI

que satisface el requisito de negocio de TI para

mejorar la rentabilidad de TI y su contribución a la utilidad del negocio.

enfocándose en

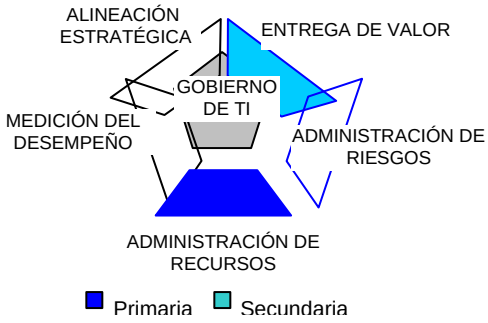
adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI

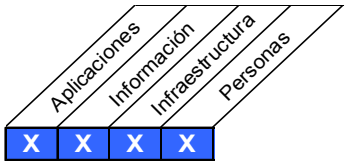
se logra con

- La obtención de asesoría profesional legal y contractual
- La definición de procedimientos y estándares de adquisición
- La adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos

y se mide con

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





Objetivo de control detallados

AI5 Adquirir recursos de TI

AI5.1 Control de adquisición
Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.

AI5.2 Administración de contratos con proveedores
Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores. El procedimiento debe cubrir, al mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión (que incluya cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

AI5.3 Selección de proveedores
Seleccionar proveedores mediante una práctica justa y formal para garantizar el mejor ajuste viable que se base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).

AI5.4 Adquisición de software
Garantizar que se protegen los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir e implantar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software. Estos derechos y obligaciones pueden incluir la propiedad y licencia de propiedad intelectual, mantenimiento, garantías, procedimientos de arbitraje, términos de ampliación, y conveniencia de propósitos incluyendo seguridad, derechos de custodia y acceso.

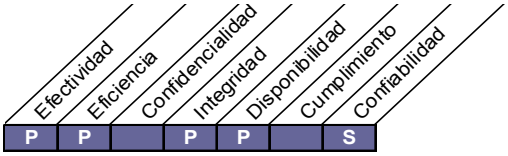
AI5.5 Adquisición de recursos de desarrollo
Garantizar la protección de los intereses de la organización en todos los acuerdos de adquisición contractuales. Incluir e implantar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo. Estos derechos y obligaciones pueden incluir la propiedad y licencia de propiedad intelectual, aptitud para el propósito, incluyendo metodologías de desarrollo, lenguajes, pruebas, procesos de administración de calidad que comprenden los criterios de desempeño requeridos, revisión de desempeño, términos de pago, garantías, procedimientos de arbitraje, administración de recursos humanos y cumplimiento con las políticas de la organización.

AI5.6 Adquisición de infraestructura, instalaciones y servicios relacionados
Incluir e implantar los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados. Estos derechos y obligaciones pueden abarcar los niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, revisión de desempeño, términos de pago y procedimientos de arbitraje.

Objetivo de control de alto nivel

AI6 Administrar cambios

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, en relación con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y en manera controlada. Los cambios (incluyendo procedimientos, procesos, parámetros de sistema y servicio) se deben poner en bitácora, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados posteriores a la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.



Control sobre el proceso TI de

Administrar cambios

que satisface el requisito de negocio de TI para

responder a los requerimientos del negocio de acuerdo con la estrategia de negocio, mientras que se reducen los defectos y re-trabajo en la prestación del servicio y la solución.

enfocándose en

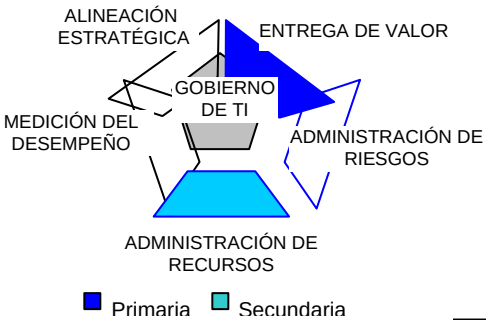
controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados

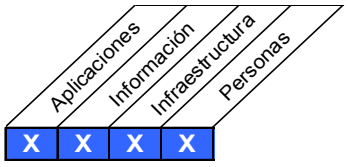
se logra con

- La definición y comunicación de los procedimientos de cambio, que comprenden cambios de emergencia
- La evaluación, la asignación de prioridad y autorización de cambios
- Rastreo del estatus y reporte de cambios

y se mide con

- El número de interrupciones o errores de datos provocados por especificaciones inexactas o una evaluación de impacto incompleta
- La aplicación de revisión de trabajo en infraestructura debida a especificaciones de cambio inadecuadas
- El porcentaje de cambios que siguen procesos de control de cambio formales





Objetivo de control detallados

AI6 Administrar cambios

AI6.1 Estándares y procedimientos para cambios
Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y programas de servicio o parches) para cambios de aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

AI6.2 Evaluación de impacto, asignación de prioridades y autorización
Garantizar que todas las solicitudes de cambio se evalúan en forma estructurada en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y prioridades de los cambios. Previo a la migración hacia la producción, los participantes correspondientes autorizan los cambios.

AI6.3 Cambios de emergencia
Establecer un proceso para definir, plantear, evaluar y autorizar cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

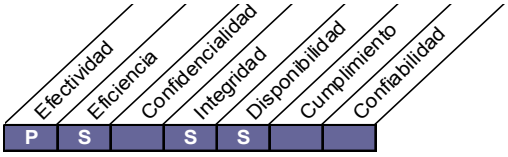
AI6.4 Rastreo y reporte del estatus de cambio
Establecer un sistema de rastreo y reporte para mantener actualizados a los solicitantes de cambio y a los participantes relevantes, acerca del estatus de cambio a las aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y plataformas fundamentales.

AI6.5 Cierre y documentación del cambio
Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

Objetivo de control de alto nivel

AI7 Instalar y acreditar soluciones y cambios

Los nuevos sistemas necesitan ser funcionales una vez que su desarrollo se completa. Esto requiere de pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas de operación estén en línea con las expectativas convenidas y los resultados.



Control sobre el proceso TI de

Instalar y acreditar soluciones y cambios

que satisface el requisito de negocio de TI para

contar con sistemas nuevos o modificados que trabajen sin problemas mayores después de la instalación

enfocándose en

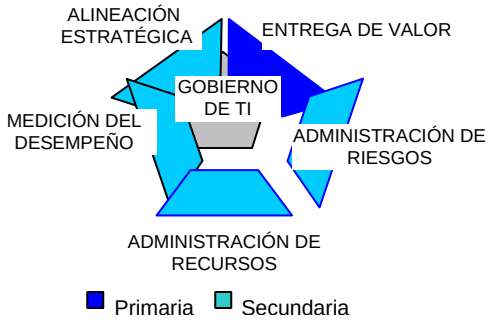
probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libre de errores, y planear las liberaciones a producción

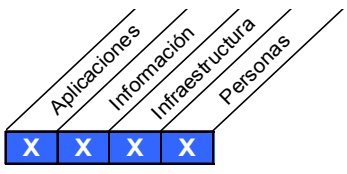
se logra con

- El establecimiento de una metodología de prueba
- Realizar la planeación de la liberación
- Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio
- Ejecutar revisiones posteriores a la implantación

y se mide con

- Tiempo perdido de aplicación o problemas de datos provocados por pruebas inadecuadas
- Porcentaje de sistemas que satisfacen los beneficios esperados, medidos en el proceso posterior a la implantación
- Porcentaje de proyectos con plan de prueba documentado y aprobado





Objetivos de control detallados

AI7 Instalar y acreditar soluciones y cambios

AI7.1 Entrenamiento
Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.

AI7.2 Plan de prueba
Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito. El plan considera la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo de errores y corrección, y aprobación formal. Con base a la evaluación de riesgos de fallas en el sistema y en la implantación, el plan deberá incluir los requerimientos de prueba de desempeño, de tensión, de usabilidad, piloto y de seguridad.

AI7.3 Plan de implantación
Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de liberación, construcción de paquetes de liberación, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la liberación y documentación de cambios. El plan deberá también incluir medidas de respaldo/retroceso.

AI7.4 Ambiente de prueba
Establecer un ambiente de prueba separado para pruebas. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas. Se deben tener presentes los procedimientos para garantizar que los datos utilizados en el ambiente de prueba sean representativos de los datos (se limpian si es necesario) que se utilizarán eventualmente en el ambiente de operación. Proporcionar medidas adecuadas para prevenir la divulgación de datos delicados. Los resultados documentados de prueba se deben retener.

AI7.5 Conversión de sistema y datos
Garantizar que los métodos de desarrollo de la organización, contemplen para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfases con otros sistemas, procedimientos, documentación de sistema, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se desarrolla y mantiene una pista de auditoría de los resultados previos y posteriores a la conversión. Se ejecuta una verificación detallada del proceso inicial del nuevo sistema por parte de los propietarios del sistema para confirmar una transición exitosa.

AI7.6 Prueba de cambios
Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular. Las pruebas paralelas o piloto se consideran parte del plan. Los controles de seguridad se prueban y evalúan antes del posicionamiento, de manera que se pueda certificar la efectividad de la seguridad. Los planes de respaldo/retroceso se deben desarrollar y probar antes de transferir el cambio a producción.

AI7.7 Prueba final de aceptación
Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramiento de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las prueba deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba se deben salvar para propósitos de pistas de auditoría y para pruebas futuras.

AI7.8 Transferencia a producción
Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de

pruebas, de acuerdo con el plan de implantación. La gerencia debe requerir que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año.

AI7.9 Liberación de software
Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.

AI7.10 Distribución del sistema

Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración. Esto implica controles de integridad; separación de tareas entre los que construyen, prueban y operan; y pistas adecuadas de rastreo de todas las actividades.

AI7.11 Registro y rastreo de cambios
Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.

AI7.12 Revisión posterior a la implantación
Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información de operación para evaluar y reportar si es que el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados de la forma más rentable.

COBIT 4.0

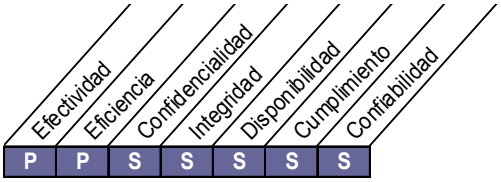
ENTREGA Y SOPORTE

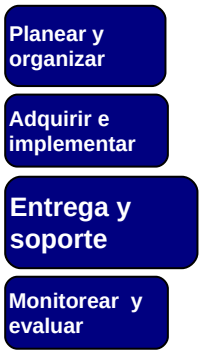
DS1 Definir y administrar los niveles de servicio
DS2 Administrar los servicios de terceros
DS3 Administrar el desempeño y la capacidad
DS4 Garantizar la continuidad de los servicios
DS5 Garantizar la seguridad de los sistemas
DS6 Identificar y asignar costos
DS7 Educar y entrenar a los usuarios
DS8 Administrar la atención a usuarios y los incidentes
DS9 Administrar la configuración
DS10 Administrar los problemas
DS11 Administrar los datos
DS12 Administrar el ambiente físico
DS13 Administrar las operaciones

Objetivo de control de alto nivel

DS1 Definir y administrar niveles de servicio

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 participantes sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.





Control sobre el proceso TI de

Definir y manejar niveles de servicio

que satisface el requisito de negocio de TI para

Asegurar la alineación de los servicios claves de TI con la estrategia del negocio

enfocándose en

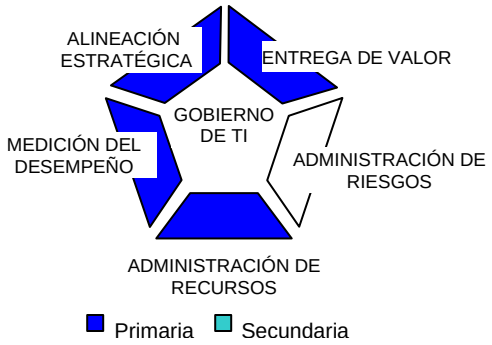
la identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio

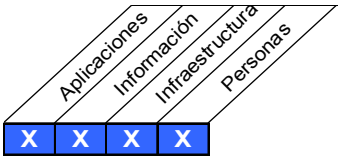
se logra con

- La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega
- La notificación del cumplimiento de los niveles de servicio (reportes y reuniones)
- La identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica.

y se mide con

- El porcentaje de participantes 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





Objetivos de control detallados

DS1 Definir y administrar los niveles de servicio

DS1.1 Marco de trabajo de administración de los niveles de servicio
Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, convenios de niveles de servicio (SLAs), convenio de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.

DS1.2 Definición de servicios
Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

DS1.3 Convenios de niveles de servicio
Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los involucrados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y supervisión de demanda.

DS1.4 Convenios de niveles de operación
Asegurar que los convenios de niveles de operación expliquen como serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.

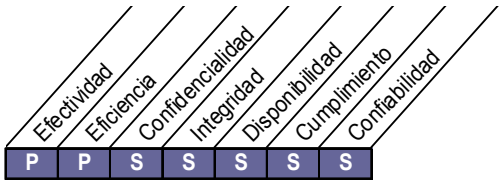
DS1.5 Monitoreo y notificación del cumplimento de los niveles de servicio
Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los participantes. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

DS1.6 Revisión de los convenios de niveles de servicio y de los contratos
Revisar regularmente con los proveedores internos y externos los convenios de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

Objetivo de control de alto nivel

DS2 Administrar los servicios de terceros

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 convenios de los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos convenios. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.



Control sobre el proceso TI de

Administrar servicios de terceros

que satisface el requisito de negocio de TI para

Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos

enfocándose en

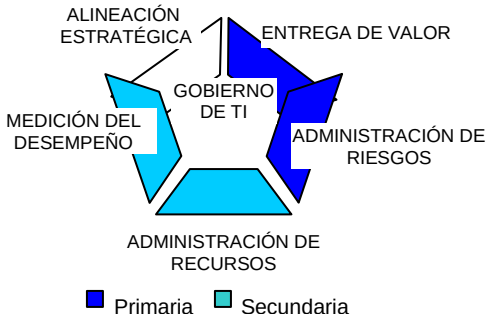
el establecimiento de relaciones y responsabilidades bilaterales con proveedores calificados de servicios en tercería y el monitoreo de la prestación del servicio para verificar y asegurar el apego a los convenios.

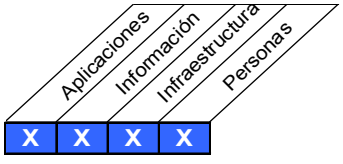
se logra con

- La identificación y categorización de los servicios del proveedor
- La identificación y mitigación de riesgos del proveedor
- El monitoreo y la medición del desempeño del proveedor

y 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





Objetivos de control detallados

DS2 Administrar los servicios de terceros

DS2.1 Identificación de las relaciones con todos los proveedores
Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

DS2.2 Administración de las relaciones con los proveedores
Formalizar el proceso de administración de relaciones con proveedores por cada proveedor. Los responsables de las relaciones deben coordinar a los proveedores y los clientes y asegurar la calidad de las relaciones con base en la confianza y la transparencia (por ejemplo, a través de convenios de niveles de servicio).

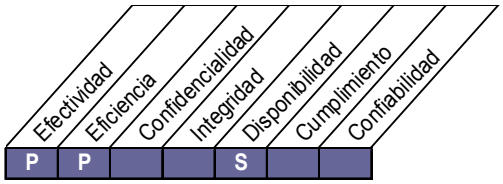
DS2.3 Administración de riesgos del proveedor
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, continuidad de la viabilidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

DS2.4 Monitoreo del desempeño del proveedor
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

Objetivo de control de alto nivel

DS3 Administrar el desempeño y la capacidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.



Control sobre el proceso TI de

Administrar el desempeño y la capacidad

que satisface el requisito de negocio de TI para

Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio.

enfocándose en

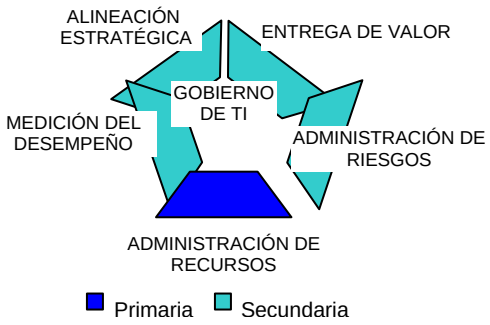
cumplir con los requerimientos de tiempo de respuesta de los convenios de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.

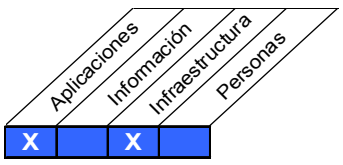
se logra con

- La planeación y la procuración de capacidad y disponibilidad del sistema
- Monitoreando y reportando el desempeño del sistema
- Modelando y pronosticando el desempeño del sistema.

y se mide con

- Número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad
- Porcentaje de picos donde se excede la meta de utilización
- Porcentaje de SLAs de tiempo de respuesta que no se satisfacen





Objetivos de control detallados

DS3 Administrar el desempeño y la capacidad

DS3.1 Planeación del desempeño y de la capacidad
Establecer un proceso de planeación para la revisión del desempeño y de la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado.

DS3.2 Capacidad y desempeño actual
Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

DS3.3 Capacidad y desempeño futuros
Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

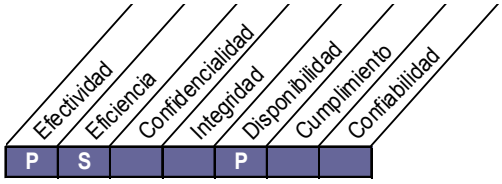
DS3.4 Disponibilidad de recursos de TI
Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas, y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

DS3.5 Monitoreo y reporte
Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:
• Mantener y poner a punto el desempeño actual dentro de TI y atender temas como resiliencia, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
• Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs. Acompañar todos los reportes de excepción con recomendaciones para llevar acabo acciones correctivas.

Objetivo de control de alto nivel

DS4 Garantizar la continuidad de los servicios

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 capacitar 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.



Control sobre el proceso TI de

Garantizar la continuidad de los servicios

que satisface el requisito de negocio de TI para

asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI.

enfocándose en

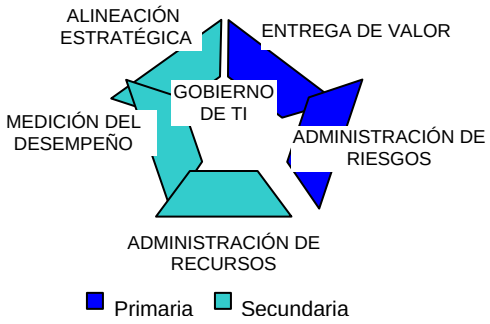
el desarrollo de resistencia en las soluciones automatizadas y el desarrollo, manteniendo y prueba de los planes de continuidad de TI
.

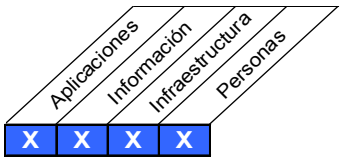
se logra

- Desarrollando y manteniendo (mejorando) los planes de contingencia de TI
- Con capacitación y pruebas de los planes de contingencia de TI
- Guardando copias de los planes de contingencia y de los datos fuera de las instalaciones.

y 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.





Objetivos de control detallados

DS4 Garantizar la continuidad de los servicios

DS4.1 IT Marco de trabajo de continuidad
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicio internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 Planes de continuidad de TI
Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 Recursos críticos de TI
Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 Mantenimiento del plan de continuidad de TI
Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 Pruebas del plan de continuidad de TI
Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considere el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 Capacitación del plan de continuidad de TI
Asegurarse de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar la capacitación de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 Distribución del plan de continuidad de TI
Determinar que una estrategia de distribución definida y administrada existe para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

DS4.8 Recuperación y reanudación de los servicios de TI
Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los participantes, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 Almacenamiento de respaldos fuera de las instalaciones
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder

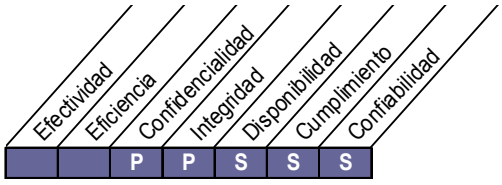
recuperar los datos archivados y periódicamente pruebar y renuevar los datos archivados.

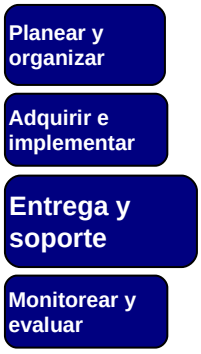
DS4.10 Revisión post-reanudación
Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

Objetivo de control de alto nivel

DS5 Garantizar la seguridad de los sistemas

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. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio por vulnerabilidades o incidentes de seguridad





Control sobre el proceso TI de

Garantizar la seguridad de los sistemas

que satisface el requisito de negocio de TI para

mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

enfocándose en

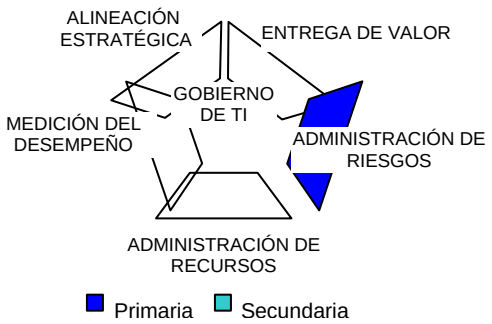
la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.

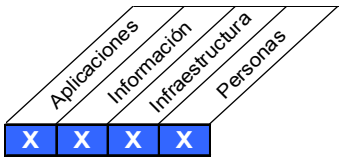
se logra con

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular.

y 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
- El número de de violaciones en la segregación de tareas.





Objetivos de control detallados

DS5 Garantizar la seguridad de los sistemas

DS5.1 Administración de la seguridad de TI
Administrar la seguridad de TI al nivel apropiado máximo dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI
Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los participantes y a los usuarios.

DS5.3 Administración de identidades
Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación de sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema y habilitados por la persona responsable de la seguridad. Las identidades de los usuarios y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los privilegios de acceso.

DS5.4 Administración de cuentas de usuario
Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de la información o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. Llevar a cabo una revisión regular por parte de la gerencia de todas las cuentas y de los privilegios asociados.

DS5.5 Pruebas, monitoreo y monitoreo de la seguridad
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de acceso al sistema esta alineado con los requerimientos del negocio en términos de requerimientos de retención y de privilegios de acceso.

DS5.6 Definición de incidente de seguridad
Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

DS5.7 Protección de la tecnología de seguridad
Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de claves criptográficas
Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de claves criptográficas estén implantadas, para garantizar la protección de las claves contra modificaciones y divulgaciones no autorizadas.

DS5.9 Prevención, detección y corrección contra software malicioso
Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

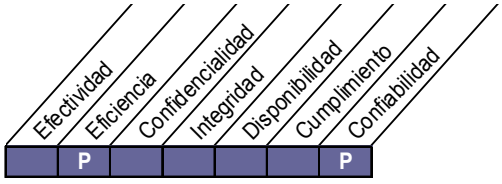
DS5.10 Seguridad de la red
Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos delicados
Garantizar que las transacciones de datos delicados sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de sumisión, prueba de recepción y no rechazo del origen.

Objetivo de control de alto nivel

DS6 Identificar y asignar costos

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 cosntrucción y operación de una sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respectos al uso de los servicios de TI.



Control sobre el proceso TI de

Identificar y asignar costos

que satisface el requisito de negocio de TI para

transparentar y entender los costos de TI y mejorar la rentabilidad a través del uso bien informado de los servicios de TI

enfocándose en

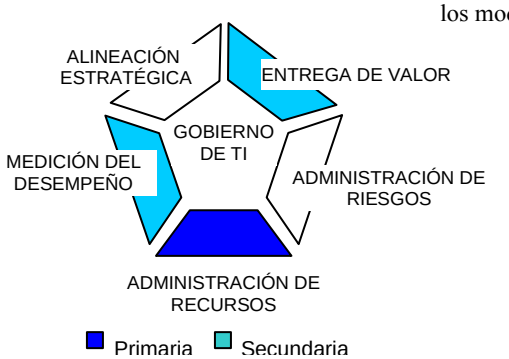
el registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios de negocio, y un sistema para reportar oportunamente el uso de TI y los costos asignados.

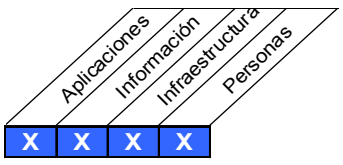
se logra con

- La alineación de cargos con la calidad y cantidad de los servicios brindados
- La construcción y aceptación de un modelo de costos completo
- La aplicación de cargos con base en la política acordada.

y 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.





Objetivos de control detallados

DS6 Identificar y asignar costos

DS6.1 Definición de servicios
Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos de negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados.

DS6.2 Contabilización de TI
Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

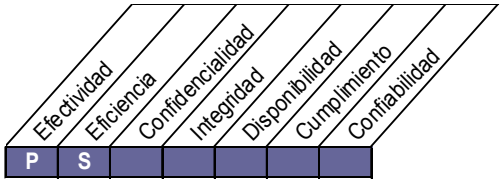
DS6.3 Modelación de costos y cargos
Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa. El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios.

DS6.4 Mantenimiento del modelo de costos
Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

Objetivo de control de alto nivel

DS7 Educar y capacitar a los usuarios

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de capacitación de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo una capacitación efectiva y para medir los resultados. Un programa efectivo de capacitación 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.



Planear y organizar

Adquirir e implementar

Entrega y soporte

Monitorear y evaluar

Control sobre el proceso TI de

Educar y capacitar a los usuarios

que satisface el requisito de negocio de TI para

el uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos

enfocándose en

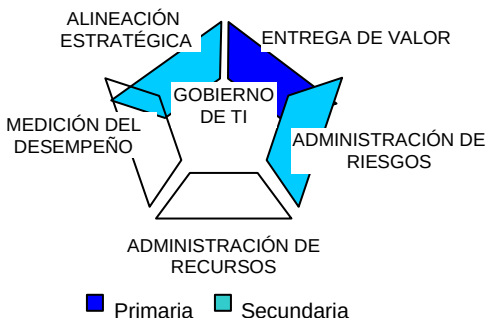
un claro entendimiento de las necesidades de capacitación en TI para los usuarios, la ejecución de una efectiva estrategia de capacitación y la medición de resultados.

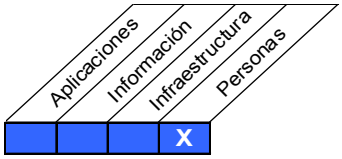
se logra con

- Establecer un programa de capacitación
- Organizar la capacitación
- Impartir la capacitación
- Monitorear y reportar la efectividad de la capacitación.

y se mide con

- Número de llamadas de soporte debido a problemas de capacitación
- Porcentaje de satisfacción de los participantes con la capacitación recibida
- Lapso de tiempo entre la identificación de la necesidad de capacitación y la impartición de la misma.





Objetivos de control detallados

DS7 Educar y capacitar a los usuarios

DS7.1 Identificación de necesidades de capacitación y educación
Establecer y actualizar de forma regular un programa de capacitación para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles con especialización y certificaciones actuales y/o necesidades de comprobación de credenciales.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

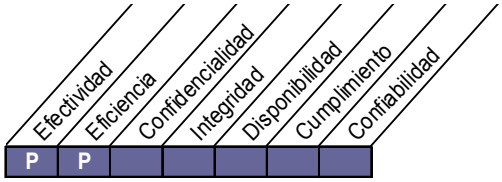
DS7.2 Impartición de capacitación y educación
Con base en las necesidades de capacitación identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar la capacitación con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

DS7.3 Evaluación de la capacitación recibida
Al finalizar la capacitación, evaluar el contenido de la capacitación respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de capacitación.

Objetivo de control de alto nivel

DS8 Administrar la atención a usuarios y los incidentes

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



Control sobre el proceso TI de

Administrar la atención a usuarios y los incidentes

que satisface el requisito de negocio de TI para

permitir el efectivo uso sistemas de IT garantizando la resolución y el análisis de causas, consultas de los usuarios finales, incidentes y preguntas.

enfocándose en

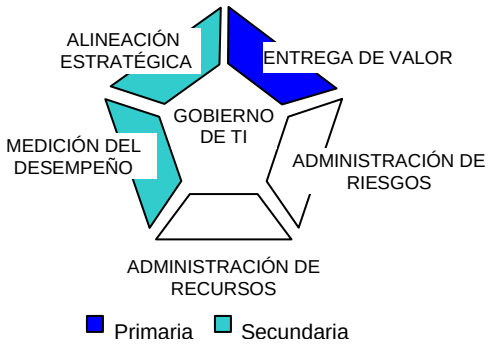
una atención a usuarios profesional con tiempo de respuesta rápido, procedimientos de escalación claros y análisis de tendencias y de resolución.

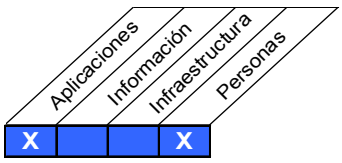
se logra con

- Instalación y operación de una atención a usuarios
- Monitoreo y reporte de tendencias
- Definición de procedimientos y de criterios de escalación claros

y 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





Objetivos de control detallados

DS8 Administrar la atención a usuarios y los incidentes

DS8.1 Atención a usuarios
Establecer la función de atención a usuarios, la cual es la conexión del usuario con TI, para registrar comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalación basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la atención a usuarios y de los servicios de TI.

DS8.2 Registro de consultas de clientes
Establecer una función y sistema para permitir el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Debe trabajar de forma apegada a los procesos de administración de incidentes, administración de problemas, administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio, y redirigidos al equipo de administración de problemas apropiado, se debe mantener informados a los clientes sobre el estatus de sus consultas.

DS8.3 Escalación de incidentes
Establecer procedimientos de atención a usuarios, de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados de forma apropiada de acuerdo a los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizar que la asignación de incidencias y el monitoreo de ciclos de vida permanecen en la mesa de servicio para usuarios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.

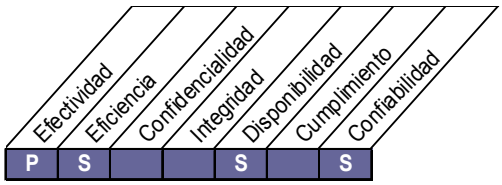
DS8.4 Cierre de incidentes
Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente, la mesa de atención a usuarios debe registrar la causa si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

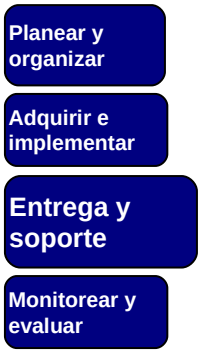
DS8.5 Análisis de tendencias
Emitir reportes de la actividad de atención a usuarios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes, de forma que el servicio pueda mejorarse de forma continua.

Objetivo de control de alto nivel

DS9 Administrar la configuración

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración, y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.





Control sobre el proceso TI de

Administrar la configuración

que satisface el requisito de negocio de TI para

optimizar la infraestructura recursos y capacidades de TI, y dar cuenta de los activos de TI.

enfocándose en

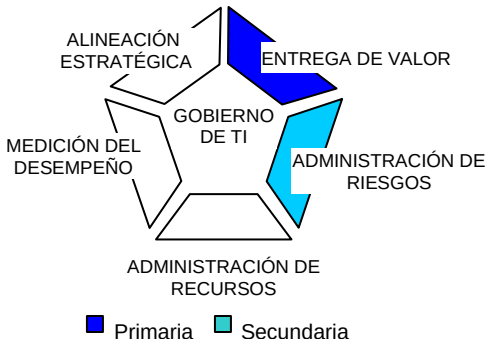
establecer y mantener un repositorio completo y preciso de puntos de referencia y de líneas base para la configuración de los activos, y para comparar contra la configuración actual.

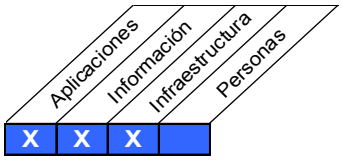
se logra con

- El establecimiento de un repositorio central de todos los elementos de la configuración
- La identificación de los elementos de configuración y su mantenimiento
- Revisión de la integridad de los datos de configuración.

y se mide con

- El número de problemas de cumplimiento del negocio debido a incidentes con la adecuada configuración de los activos.
- El número de desviaciones identificadas entre el repositorio de configuración y la configuración actual de los activos.
- Porcentaje de licencias compradas y no concentradas en el repositorio.





Objetivos de control detallados

DS9 Administrar la configuración

DS9.1 Repositorio de configuración y línea base
Establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

DS9.2 Identificación y mantenimiento de elementos de configuración
Contar con procedimientos en orden para:
• Identificar elementos de configuración y sus atributos
• Registrar elementos de configuración nuevos, modificados y eliminados
• Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones.
• Actualizar los elementos de configuración existentes en el repositorio de configuraciones.
• Prevenir la inclusión de software no-autorizado

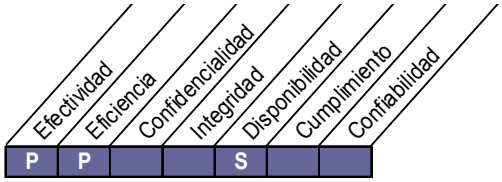
Estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones sobre el repositorio de configuración y estar integrados de forma apropiada con los procedimientos de administración de cambios y administración de problemas.

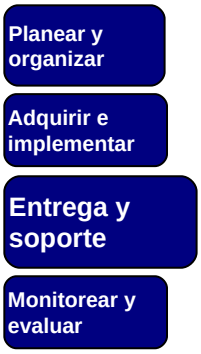
DS9.3 Revisión de integridad de la configuración
Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica, para comparar con la situación actual. Revisar de forma periódica contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

Objetivo de control de alto nivel

DS10 Administración de problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de registros mejora los niveles de servicio, reduce costos y mejora la comodidad y satisfacción del usuario.





Control sobre el proceso TI de

Administración de problemas

que satisface el requisito de negocio de TI para

garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el retrabajo y los defectos en la prestación de los servicios y de las soluciones.

enfocándose en

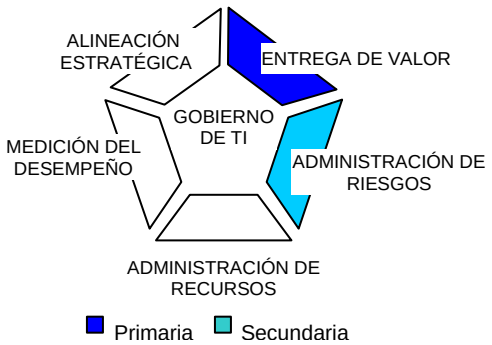
registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.

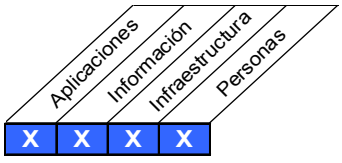
se logra

- Realizando un análisis de causas raíz de los problemas reportados
- Analizando las tendencias
- Tomando propiedad de los problemas y con una resolución de problemas progresiva.

y se mide con

- Número de problemas recurrentes con impacto en el negocio
- Porcentaje de problemas resueltos dentro del período de tiempo solicitado
- Frecuencia de los reportes o actualizaciones sobre un problema en curso, con base en la severidad del problema.





Objetivos de control detallados

DS10 Administración de problemas

DS10.1 Identificación y clasificación de problemas
Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

DS10.2 Rastreo y resolución de problemas
El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:
• Todos los elementos de configuración asociados
• Problemas e incidentes sobresalientes
• Errores conocidos y sospechosos

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs.

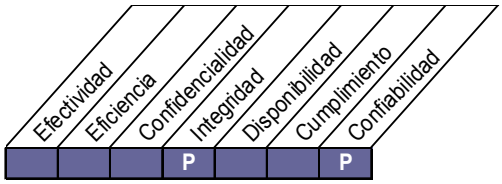
DS10.3 Cierre de problemas
Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.

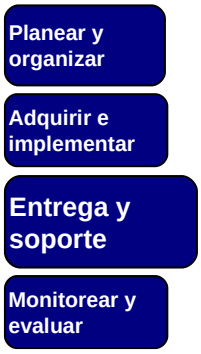
DS10.4 Integración de las administraciones de cambios, configuración y problemas
Para garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas. Monitorear cuánto esfuerzo se aplica en apagar fuegos, en lugar de permitir mejoras al negocio y, en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas.

Objetivo de control de alto nivel

DS11 Administración de la información

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. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.





Control sobre el proceso TI de

Administración de la información

que satisface el requisito de negocio de TI para

Optimizar el uso de información y garantizar la disponibilidad de la información cuando se requiera.

enfocándose en

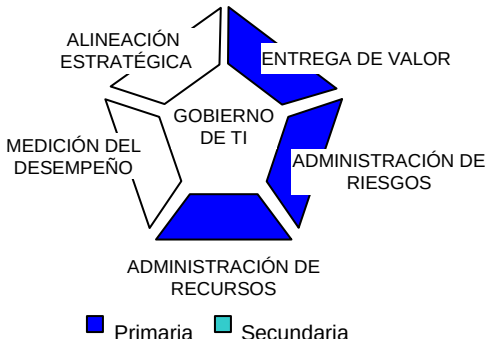
mantener la integridad, precisión, disponibilidad y protección de la información.

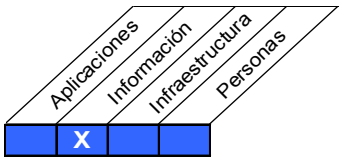
se logra

- Respaldando la información y probando la restauración
- Administrando almacenamiento de información en sitio y fuera de sitio.
- Desechando de manera segura la información y el equipo.

y se mide con

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





Objetivos de control detallados

DS11 Administración de la información

DS11.1 Requerimientos del negocio para administración de información
Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

DS11.2 Acuerdos de almacenamiento y conservación
Definir e implementar procedimientos para el archivo y almacenamiento de la información, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encriptación y autenticación.

DS11.3 Sistema de administración de librerías de medios
Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y utilidad. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

DS11.4 Eliminación
Definir e implementar procedimientos para prevenir el acceso a la información delicada y al software, desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que la información eliminada o a ser desechada, no puede recuperarse.

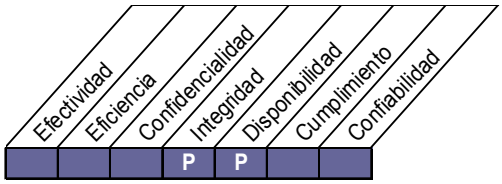
DS11.5 Respaldo y restauración
Definir e implementar procedimientos de respaldo y restauración de los sistemas, información y configuraciones, que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo, y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

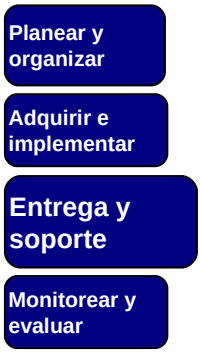
DS11.6 Requerimientos de seguridad para la administración de datos
Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes delicados. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

Objetivo de control de alto nivel

DS12 Administración del ambiente físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.





Control sobre el proceso TI de

Administración del ambiente físico

que satisface el requisito de negocio de TI para

proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.

enfocándose en

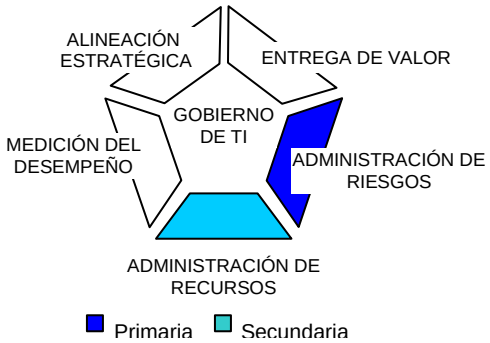
proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI de acceso, daño o robo.

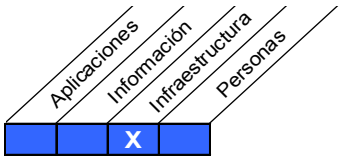
se logra

- Implementando medidas de seguridad físicas.
- Seleccionando y administrando las instalaciones.

y se mide con

- Tiempo sin servicio ocasionado por incidentes relacionados al ambiente físico
- Número de incidentes ocasionados por fallas o brechas de seguridad física
- Frecuencia de revisión y evaluación de riesgos físicos.





Objetivos de control detallados

DS12 Administración del ambiente físico

DS12.1 Selección y diseño del centro de datos
Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas físicas de seguridad
Definir e implementar medidas físicas de seguridad alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones de TI críticas. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso Físico
Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

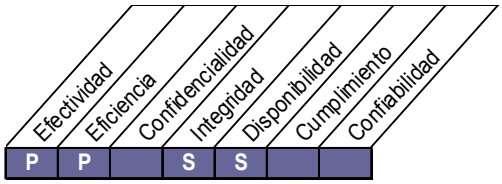
DS12.4 Protección contra factores ambientales
Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

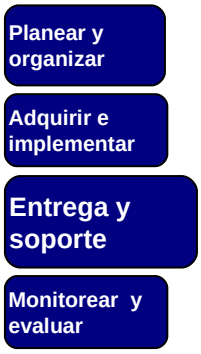
DS12.5 Administración de instalaciones físicas
Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

Objetivo de control de alto nivel

DS13 Administración de operaciones

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 confidenciales, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de la información y reduce los retrasos en el trabajo y los costos operativos de TI.





Control sobre el proceso TI de

Administrar operaciones

que satisface el requisito de negocio de TI para

mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperase de errores y fallas.

enfocándose en

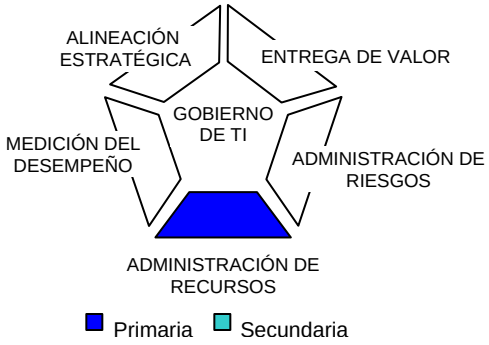
cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos confidenciales, y monitoreo y mantenimiento de la infraestructura.

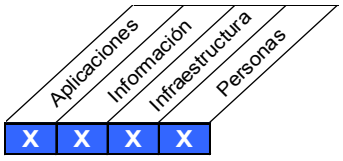
se logra

- Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas
- Manteniendo la infraestructura de TI

y 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.





Objetivos de control detallados

DS13 Administración de operaciones

DS13.1 Procedimientos e instrucciones de operación
Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de transferencia (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalación, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

DS13.2 Programación de tareas
Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar de trabajos.

DS13.3 Monitoreo de la infraestructura de TI
Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

DS13.4 Documentos confidenciales y dispositivos de salida.
Establecer resguardos físicos, prácticas de rendición de cuentas y administración de inventarios adecuados sobre los activos de TI más delicados tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.

DS13.5 Mantenimiento preventivo del hardware
Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

MONITOREAR Y EVALUAR

ME1 Monitorear y evaluar el desempeño de TI

ME2 Monitorear y evaluar el control interno

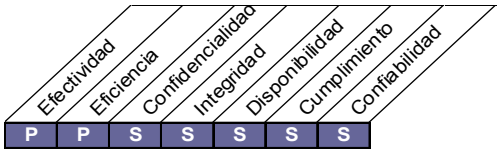
ME3 Garantizar el cumplimiento regulatorio

ME4 Proporcionar un gobierno de TI

Objetivo de control de alto nivel

ME1 Monitorear y evaluar el desempeño de TI

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. La monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.



Control sobre el proceso TI de

Monitorear y evaluar el desempeño de TI

que satisface el requisito de negocio de TI para

transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo a los requisitos de gobierno

enfocándose en

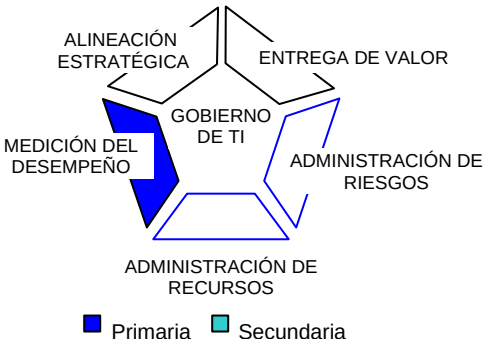
monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño

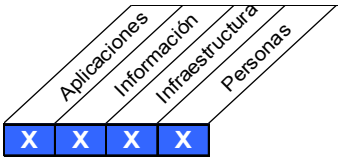
se logra con

- Cotejar y traducir los reportes de desempeño de proceso a reportes gerenciales
- Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias

y 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 vigilados





Objetivos de control detallados

ME1 Monitorear y evaluar el desempeño de TI

ME1.1 Monitorear el enfoque
Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI. El marco de trabajo se debería integrar con el sistema de administración del desempeño corporativo.

ME1.2 Definición y recolección de datos de monitoreo
Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño, y que estas se encuentren acordadas formalmente con el negocio y otros públicos de interés relevantes. Los indicadores de desempeño deberían incluir:

- La contribución al negocio que incluya, pero que no se limite a, la información financiera
- Desempeño contra el plan estratégico del negocio y de TI
- Riesgo y cumplimiento de las regulaciones
- Satisfacción del usuario interno y externo
- Procesos clave de TI que incluyan desarrollo y entrega del servicio
- Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio

Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

ME1.3 Método de monitoreo
Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.

ME1.4 IT Evaluación del desempeño
Comparar de forma periódica el desempeño frente a las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.

ME1.5 Reportes al consejo directivo y a ejecutivos
Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado al que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado, y se deben iniciar y reportar las medidas administrativas adecuadas.

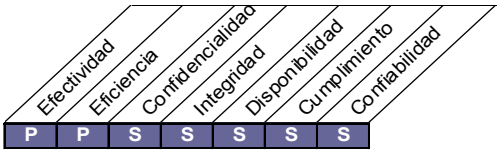
ME1.6 Medidas correctivas
Identificar e iniciar medidas correctivas basadas en la monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de toda la monitoreo, de los reportes y de las evaluaciones con:

- Revisión, negociación y establecimiento de respuestas administrativas
- Asignación de responsabilidades para la corrección
- Rastreo de los resultados de las acciones comprometidas

Objetivo de control de alto nivel

ME2 Monitorear y evaluar el control interno

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



Control sobre el proceso TI de

Monitorear y evaluar el control interno

que satisface el requisito de negocio de TI para

proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI

enfocándose en

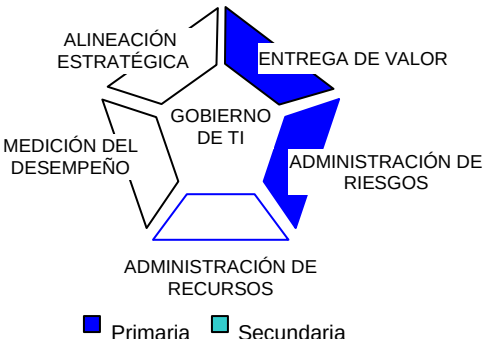
la monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejora

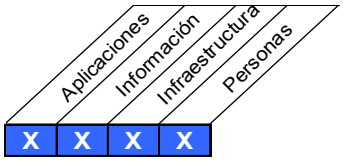
se logra con

- La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI
- Monitorear y reportar la efectividad de los controles internos sobre la TI
- Reportar las excepciones de control a la gerencia para accionar medidas

y se mide con

- Número de violaciones importantes del control interno
- Número de iniciativas para la mejora del control
- Porcentaje de procesos críticos vigilados





Objetivos de control detallados

ME2 Monitorear y evaluar el control interno

ME2.1 Monitorear el marco de trabajo de control interno
Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando las mejores prácticas de la industria y se debe utilizar la evaluación por comparación (benchmarking) para mejorar el ambiente y el marco de trabajo de control interno de TI.

ME2.2 Revisión de supervisión
Monitorear y reportar la efectividad de los controles internos sobre la TI por medio de revisiones de supervisión incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

ME2.3 Excepciones de control
Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de medidas correctivas. La gerencia debe decidir cuáles excepciones se deben comunicar al individuo responsable de la función y cuáles excepciones se deben escalar. La gerencia también es responsable de informar a las partes afectadas..

ME2.4 Auto-evaluación de control
Evaluar la integridad y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

ME2.5 Aseguramiento del control interno
Obtener, según sea necesario, aseguramiento adicional de la integridad y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoría interna o por auditores y consultores externos subcontratados o incluso por organismos de certificación. Las aptitudes de los individuos que realicen la auditoria, por ej. Un Auditor de Sistemas de Información Certificado™ (CISA® por sus siglas en Inglés) se deberán verificar.

ME2.6 Control interno para terceros
Valorar el estatus de los controles internos de los proveedores externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede se provisto por una auditoría de terceros o se puede obtener de una revisión por parte de la función de auditoría interna de la gerencia y por los resultados de la auditoria.

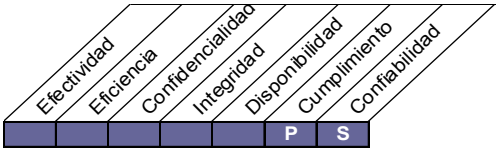
ME2.7 Medidas correctivas
Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con:

- La revisión, negociación y establecimiento de respuestas administrativas
- La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos)
- El rastreo de los resultados de las acciones comprometidas

Objetivo de control de alto nivel

ME3 Garantizar el cumplimiento regulatorio

Una supervisión efectiva del cumplimiento regulatorio requiere del establecimiento de un proceso independiente de revisión para garantizar el cumplimiento de las leyes y reglamentos. Este proceso incluye la definición de un estatuto de auditoría, independencia de los auditores, éticas y estándares profesionales, planeación, realización de trabajo de auditoría, y reportes y seguimiento a las actividades de auditoría. El propósito de este proceso es proporcionar un aseguramiento positivo relativo al cumplimiento de TI de las leyes y reglamentos..



Planear y organizar

Adquirir e implementar

Entrega y soporte

Monitorear y evaluar

Control sobre el proceso TI de

Garantizar el cumplimiento regulatorio

que satisface el requisito de negocio de TI para

cumplir las leyes y reglamentos

enfocándose en

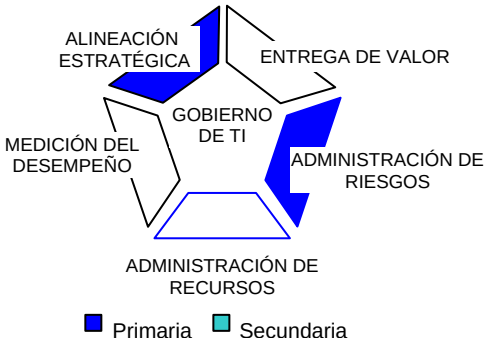
la identificación de todas las leyes y reglamentos aplicables y el nivel correspondiente de cumplimiento de TI, además de la optimización de los procesos de TI para reducir el riesgo de no cumplimiento

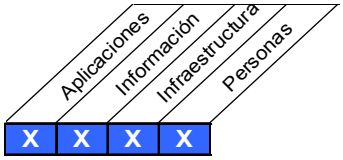
se logra con

- La identificación de los requisitos legales y regulatorios relacionados con la TI
- La evaluación del impacto de los requisitos regulatorios
- La monitoreo y reporte del cumplimiento de los requisitos regulatorios

y se mide con

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





Objetivos de control detallados

ME3 Garantizar el cumplimiento regulatorio

ME3.1 Identificar las leyes y reglamentos con impacto potencial en TI
Definir e implantar un proceso para garantizar la identificación oportuna de requisitos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salubridad y seguridad.

ME3.2 Optimizar la respuesta a requisitos regulatorios
Revisar y optimizar las políticas, estándares y procedimientos de TI, para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.

ME3.3 Excepciones de control
Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requisitos legales y regulatorios, con base en la supervisión y la operación de los controles internos del gobierno de la gerencia de TI y del negocio.

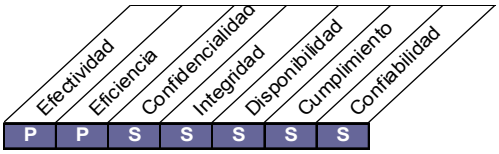
ME3.4 Aseguramiento positivo del cumplimiento
Definir e implantar procedimientos para obtener y reportar un aseguramiento positivo y , según sea necesario, para verificar que se hayan tomado las medidas correctivas por parte del propietario del proceso de forma oportuna para resolver cualquier brecha de cumplimiento. Integrar los reportes de avance y estatus del cumplimiento de TI con las salidas similares provenientes de otras funciones de negocio

ME3.5 Reportes integrados.
Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.

Objetivo de control de alto nivel

ME4 Proporcionar un gobierno para TI

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 alienadas y de acuerdo con las estrategias y objetivos empresariales..



Planear y organizar

Adquirir e implamentar

Entrega y soporte

Monitorear y evaluar

Control sobre el proceso TI de

Proporcionar un gobierno para TI

que satisface el requisito de negocio de TI para

la integración de un gobierno de TI con objetivos gubernamentales corporativos
y
que cumpla con las leyes y reglamentos

enfocándose en

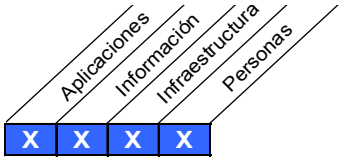
la elaboración de reportes para el consejo sobre la estrategia, el desempeño y los riesgos de TI, y responder a los requisitos de gobierno de acuerdo a las directrices del consejo directivo

se logra con

- El establecimiento de un marco de trabajo para el gobierno de TI, integrado al gobierno corporativo
- la obtención de garantías independientes sobre el estatus del gobierno de TI

y se mide con

- La frecuencia de reportes de consejo sobre TI a los participantes (incluyendo la madurez)
- La frecuencia de los reportes de TI hacia el consejo (incluyendo la madurez)
- Frecuencia de revisiones independientes del cumplimiento de TI



Objetivos de control detallados

ME4 Proporcionar un gobierno para TI

ME4.1 Establecer un marco de trabajo de gobierno para TI
Trabajar con el consejo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requisitos de información, y estructuras organizacionales para garantizar que los programas de inversión en TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. El marco de trabajo debe proporcionar ligas claras entre la estrategia empresarial, el portafolio de inversiones en TI que ejecuten la estrategia, los programas de inversión individual, y los proyectos de negocio y de TI que forman los programas. El marco de trabajo debe definir una rendición de cuentas y prácticas incontrovertibles para evitar fallas de control interno y de supervisión. El marco de trabajo debe ser consistente con el ambiente completo de control empresarial y con los principios de control generalmente aceptados, y se debe basar en el proceso y en el marco de control de TI.

ME4.2 Alineación estratégica
Facilitar el entendimiento del consejo directivo y de los ejecutivos de temas estratégicos de TI tales como el rol de TI, reflexiones y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio. Asegurarse de que exista un entendimiento claro de que el valor de TI sólo se obtiene cuando las inversiones en TI se administran como un portafolio de programas que incluye el alcance completo de los cambios que el negocio debe realizar para optimizar el valor proveniente de las capacidades que tiene TI para lograr la estrategia. Trabajar con el consejo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI, y que se desarrollo la certidumbre y la confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la corresponsabilidad entre el negocio y TI e la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones en TI.

ME4.3 Entrega de valor
Administrar los programas de inversión en TI, así como otros activos y servicios de TI, para garantizar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. .Asegurarse de que los resultados de negocio esperados de las inversiones en TI y el alcance completo del esfuerzo requerido para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los participantes, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a las demandas de los clientes. Implantar un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones en TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI. Garantizar que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.

ME4.4 Administración de recursos
Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros, y seguir el ritmo de las demandas del negocio. La dirección debe implantar políticas claras, consistentes y reforzadas de recursos humanos y políticas de procuración para garantizar que se satisfagan los requisitos de recursos de manera efectiva y para adaptarse a las políticas y estándares de la arquitectura. La infraestructura de TI se debe evaluar de forma periódica para asegurar que esté estandarizada siempre que sea posible, y que exista la interoperabilidad según sea requiera.

ME4.5 Administración de riesgos.
Trabajar en conjunto con el consejo para definir el apetito empresarial de riesgos de TI. Comunicar este apetito hacia la organización y acordar el plan de administración de riesgos de TI. Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten de forma periódica los riesgos asociados con TI y el impacto sobre el negocio. Garantizar que la gerencia de TI dé seguimiento a la exposición a los riesgos, poniendo especial atención a las fallas y debilidades de control interno y de supervisión, así como su impacto potencial y real en el negocio. La posición de riesgo empresarial en TI debe ser transparente para todos los participantes..

ME4.6 Medición del desempeño.
Reportar el desempeño relevante del portafolio de los programas y de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa. Los reportes administrativos que se deben entregar para su revisión por parte de la alta dirección deben incluir el avance de la empresa hacia metas identificadas. Los reportes de estatus deben incluir el grado al cual se han logrado los objetivos planeados, se han obtenido los entregables, se han alcanzado las metas de desempeño y se han mitigado los riesgos.

Integrar los reportes con salidas similares de otras funciones. Las mediciones de desempeño deben ser aprobadas por los participantes clave. El consejo y los ejecutivos deben retar a estos reportes de desempeño y la gerencia de TI debe tener la oportunidad de explicar las desviaciones y los problemas de desempeño. Después de la revisión, se deben iniciar y controlar las medidas administrativas apropiadas.

ME4.7 Aseguramiento independiente.
Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo – esto ocurrirá probablemente a través de un comité de auditoría – seguridad independiente y oportuna sobre el cumplimiento que tiene TI respecto a las políticas, estándares y procedimientos, así como a las prácticas generalmente aceptadas.