## **INSTITUTO POLITÉCNICO NACIONAL**

###### **ESCUELA SUPERIOR DE CÓMPUTO**

**IT Governance**

Profesora Jessie Paulina Guzmán Flores

Tarea 11: Marco de trabajo: Objetivos de control para la información y tecnologías relacionadas II

**Grupo:** 3CM20 - Equipo 4

**Fecha de Entrega:** 29/Mayo/2022

**Integrantes:**

* Martínez Coronel Brayan Yosafat
* Ramírez Cotonieto Luis Fernando
* Sánchez Rojas Jesús Ubaldo

# Índice

[**Introducción**](#_t70btsdue1fh) **3**

[**Objetivos**](#_o00bt4wm3omi) **4**

# Introducción

Los objetivos de control para la información y las tecnologías relacionadas (COBIT) son un marco empresarial de TI diseñado específicamente para la gestión y el gobierno de TI.

COBIT es un conjunto de objetivos de control que ayuda a los profesionales de gestión y gobierno de TI a administrar las operaciones de TI, independientemente del tamaño de la organización. Fue lanzado en 1996 y es investigado, desarrollado, mantenido y publicado por la Asociación de Auditoría y Control del Sistema de Información (ISACA). COBIT es principalmente un marco comercial para administrar TI empresarial. Es un estándar abierto reconocido a nivel mundial que funciona en procesos de TI de negocios y en mantener alineados los objetivos de TI y de negocios. Es un conjunto integral de herramientas, procedimientos, pautas y principios en el gobierno y la gestión de TI. COBIT ayuda a las organizaciones a beneficiarse de sus sistemas de información y activos de TI, al tiempo que tiene control en toda la empresa sobre TI empresarial.

# Objetivos

Con esta investigación se pretende realizar la investigación documental y organizador gráfico de:

* Objetivos de control para la información y tecnologías relacionadas
* Descripción de procesos
* Uso de la metodología COBIT para implementar el Gobierno de las Tecnologías de Ia información

# Descripción de procesos

COBIT consta de aproximadamente 40 diferentes procesos que se centran en 5 categorías diferentes (las siglas están en inglés):

* EDM: Evaluar, dirigir y monitorear.
* APO: Alinear, planear y organizar.
* BAI: Construir, adquirir e implementar.
* DSS: Entregar, servicio y soporte.
* MEA: Monitorear, evaluar y valorar.

## Procesos de EDM: Evaluar, dirigir y monitorear.

**EDM01. Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**: Analizar y articular los requerimientos para el gobierno de las TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.

**EDM02. Asegurar la entrega de beneficios**: Optimizar la contribución al valor del negocio desde los procesos de negocios, los de servicios TI y activos de las TI resultado de la inversión hecha por TI a unos costos aceptables.

**EDM03. Asegurar la optimización del riesgo**: Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

**EDM04. Asegurar la optimización de recursos**: Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.

**EDM05. Asegurar la transparencia hacia las partes interesadas**: Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes, con aprobación por las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.

## Procesos de APO: Alinear, planear y organizar.

**APO01. Gestionar el Marco de Gestión de TI**: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.

**APO02. Gestionar la Estrategia**: Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

**APO03. Gestionar la Arquitectura Empresarial**: Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describen las líneas de partida y las arquitecturas objetivo. Define los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes.

**APO04. Gestionar la Innovación**: Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de la empresa.

**APO05. Gestionar el Portafolio**: Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.

**APO06 Gestionar el Presupuesto y los Costes**: Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa.

**APO07. Gestionar los Recursos Humanos**: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.

**AP008. Gestionar las relaciones**: Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándose hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.

**AP009. Gestionar los acuerdos de servicio**: Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.

**APO10. Gestionar los Proveedores**: Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.

**APO11. Gestionar la Calidad**: Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

**APO12 Gestionar el Riesgo**: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Propósito del Proceso. Integrar la gestión de riesgos empresariales relacionados

**APO13. Gestionar la Seguridad**: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

## Procesos de BAI: Construir, adquirir e implementar.

**BAI01. Gestión de Programas y Proyectos**: Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.

**BAI02. Gestionar la Definición de Requisitos**: Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios.

**BAI03. Gestionar la Identificación y Construcción de Soluciones**: Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

**BAI04. Gestionar la Disponibilidad y la Capacidad**: Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio.

**BAI05. Gestionar la Facilitación del Cambio Organizativo**: Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI.

**BAI06. Gestionar los Cambios**: Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

**BAI07. Gestionar la Aceptación del Cambio y la Transición**: Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.

**BAI08. Gestionar el Conocimiento**: Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.

**BAI09. Gestionar los Activos**: Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento, que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.

**BAI10. Gestionar la Configuración**: Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

## Procesos de DSS: Entregar, servicio y soporte.

**DSS01. Gestionar Operaciones**: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

**DSS02. Gestionar Peticiones e Incidentes de Servicio**: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

**DSS03. Gestionar Problemas**: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

**DSS04. Gestionar la Continuidad**: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

**DSS05. Gestionar Servicios de Seguridad**: Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

**DSS06. Gestionar Controles de Proceso de Negocio**: Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información.

## Procesos de MEA: Monitorear, evaluar y valorar.

**MEA01. Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad**: Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

**MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno**: Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

**MEA03. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos**: Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

# Uso de la metodología COBIT para implementar el Gobierno de las Tecnologías de Ia información

La implementación de COBIT consta de siete fases que satisfacen cada una de las siguientes preguntas:

* ¿Cuáles son los motivadores?
* ¿Dónde estamos ahora?
* ¿Dónde queremos estar?
* ¿Qué es preciso hacer?
* ¿Cómo conseguiremos llegar?
* ¿Hemos conseguido llegar?
* ¿Cómo mantendremos el impulso?

Existen varias propuestas para la implementación de COBIT, sin embargo, la presentada es la de John Kotter, las fases son las siguientes.

## Fase 1: Establecer el deseo de cambiar

El propósito de esta fase es entender la amplitud y profundidad del cambio previsto, las partes interesadas que son afectadas, la naturaleza del impacto, y el involucramiento requerido por cada grupo de partes interesadas, además de la disponibilidad actual y la habilidad para adoptar el cambio.

Los puntos de dolor y los eventos desencadenantes actuales pueden proporcionar una buena base para establecer el deseo de cambiar. La llamada de atención, una comunicación inicial sobre el programa puede estar relacionada con problemas del mundo real que la empresa podría estar experimentando. Además, los beneficios iniciales pueden estar relacionados con áreas que son muy visibles en la empresa, creando una plataforma para impulsar los cambios y así tener un compromiso y una aceptación más amplios.

Mientras que, la comunicación es un hilo común a través de la iniciativa de implementación o mejora, la comunicación inicial es una de las más importantes, y debería demostrar el compromiso de la alta dirección. Por ello, la comunicación inicial debería hacerse idealmente por el comité ejecutivo o por el CEO.

## Fase 2: Formar un equipo de implementación eficaz

Las dimensiones a considerar a la hora de conformar un equipo principal de implementación eficaz implican involucrar a las áreas adecuadas del negocio y de TI e identificar el conocimiento y la pericia, la experiencia, la credibilidad y la autoridad de los miembros del equipo. Obtener una visión independiente y objetiva, como la proporcionada por terceros (como consultores y agentes de cambio) podría también ser muy beneficiosa, mediante su contribución al proceso de implementación o cubrir brechas de habilidades que pudieran existir en la empresa. Por tanto, otra dimensión a considerar es la mezcla adecuada de recursos internos y externos.

* La esencia del equipo debería ser un compromiso con:
* Una visión clara del éxito y las metas deseadas
* Involucrar lo mejor en todos los miembros del equipo, en todo momento
* Claridad y transparencia de los procesos, rendición de cuentas y comunicaciones del equipo
* Integridad, apoyo mutuo y compromiso con el éxito del otro
* Rendición de cuentas mutua y responsabilidad colectiva
* Medición continua de su propio desempeño y la forma en que se comporta como equipo
* Actuar fuera de su zona de confort, buscar siempre formas de mejorar, descubrir nuevas posibilidades y adoptar los cambios

Es importante identificar a potenciales agentes de cambio dentro de las distintas partes del negocio con las que el equipo principal pueda trabajar para respaldar la visión y los cambios en cascada.

## Fase 3: Comunicar la visión deseada

En esta fase, se desarrolla un plan de habilitación del cambio de alto nivel junto con el plan general del programa. Un componente clave del plan de habilitación del cambio es la estrategia de comunicación, que considera quiénes son los grupos de audiencia principal, y sus perfiles de comportamiento y requisitos de información, canales de comunicación y principios.

La visión deseada para el programa de implementación o mejora debería comunicarse en el idioma de aquellos que se ven afectados. La comunicación debería incluir la justificación y beneficios del cambio, los impactos de no hacer el cambio (propósito), así como la visión (perspectiva), el mapa de ruta para hacer realidad la visión (plan) y la participación necesaria de las distintas partes interesadas (partes).133 La alta dirección debería comunicar mensajes clave (como la visión deseada). La comunicación debería tomar nota de que se abordarán tanto aspectos de comportamiento/culturales como lógicos y que el énfasis está en la comunicación bidireccional. Deberían captarse las reacciones, sugerencias y otras retroalimentaciones y deberían tomarse las medidas oportunas.

## Fase 4: Empoderar a los roles asignados e identificar las ganancias rápidas

A medida que se diseñan y crean las mejoras, los planes de respuesta al cambio se desarrollan para empoderar a varios roles asignados. Su alcance podría incluir:

* Cambios de diseño organizativo, como el contenido de un puesto de trabajo o estructuras de equipos
* Cambios operativos, como flujos de procesos o logística
* Cambios en la gestión de personal, como formación y/o cambios requeridos en la gestión del desempeño y los sistemas de recompensa

La obtención de ganancias rápidas es importante desde el punto de vista de una habilitación del cambio. Estos podrían estar relacionados con los puntos de dolor y los eventos desencadenantes comentados en el capítulo 3. Las ganancias rápidas visibles e inequívocas pueden generar una dinámica y una credibilidad para el programa y ayudar a acabar con cualquier escepticismo que pudiera existir.

Es imprescindible usar una estrategia participativa en el diseño y construcción de las mejoras. Involucrar a los afectados por el cambio en el diseño (por ejemplo, a través de talleres y sesiones de revisión) podría aumentar la aceptación.

## Fase 5: Habilitar la operación y el uso

Así como las iniciativas se implementan dentro del ciclo de vida de implementación principal, también se implementan los planes de respuesta al cambio. Los éxitos rápidos que se han obtenido se construyen sobre los aspectos culturales y de comportamiento abordándolos desde el sentido amplio de la transición (temas como el manejo de los temores de pérdida de responsabilidad, nuevas expectativas y tareas desconocidas).

Es importante equilibrar las intervenciones de grupo e individuales para incrementar la aceptación e involucramiento, y asegurar que todas las partes interesadas tengan una visión holística del cambio.

Durante el proceso de despliegue de la solución, el mentoring y el coaching son fundamentales para garantizar la aceptación en el entorno del usuario. Los requisitos y objetivos del cambio que se establecieron al inicio de la iniciativa deberían volver a revisarse para garantizar que se abordan de forma adecuada.

Las medidas de éxito deberían definirse y deberían incluir tanto medidas difíciles de negocio como medidas de percepción, que hacen seguimiento a cómo se sienten las personas ante un cambio.

## Fase 6: Incorporar nuevas estrategias

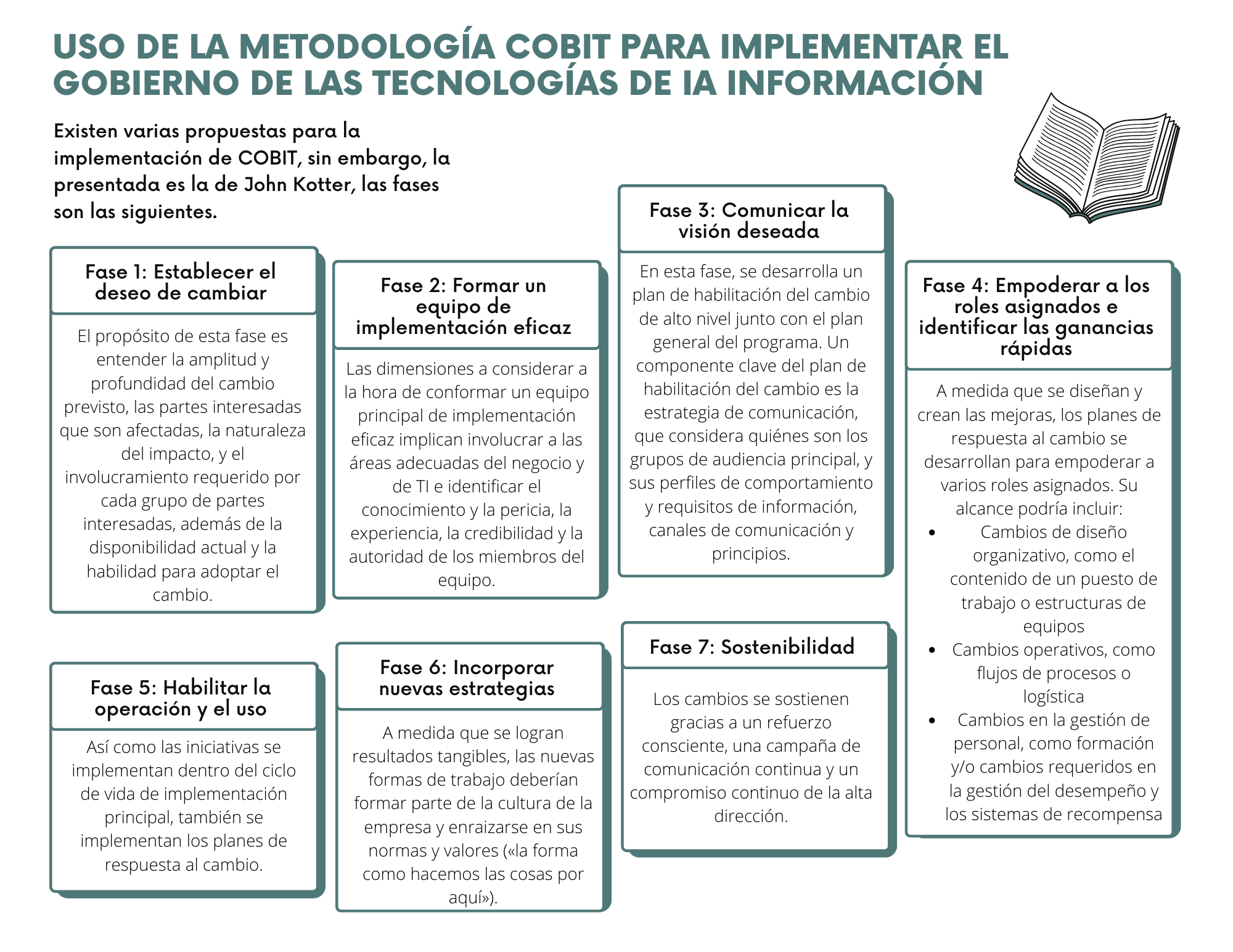
A medida que se logran resultados tangibles, las nuevas formas de trabajo deberían formar parte de la cultura de la empresa y enraizarse en sus normas y valores («la forma como hacemos las cosas por aquí»). Una forma de lograrlo es implementar políticas, estándares y procedimientos adecuados. Debería hacerse un seguimiento de los cambios implementados, debería evaluarse la eficacia de los planes de respuesta ante el cambio y deberían tomarse las medidas correctivas según corresponda. Esto podría incluir reforzar el cumplimiento cuando aún sea preciso.

La estrategia de comunicación debería mantenerse para sostener una concienciación continua.

## Fase 7: Sostenibilidad

Los cambios se sostienen gracias a un refuerzo consciente, una campaña de comunicación continua y un compromiso continuo de la alta dirección.

En esta fase, se implementan los planes de acciones correctivas, se registran las lecciones aprendidas y se comparte el conocimiento con toda la empresa.



# Referencias

COBIT 2019: Marco de Referencia, Introducción y Metodología, ISACA: <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko5fEAC>

ISACA. (s. f.). Implementación y optimización de una solución de gobierno de información y tecnología - PDFCOFFEE.COM. pdfcoffee.com. <https://pdfcoffee.com/implementacion-y-optimizacion-de-una-solucion-de-gobierno-de-informacion-y-tecnologia-4-pdf-free.html>