UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLANTACIÓN DE MAAGTIC-SI EN LOS PROCESOS DEL SECTOR GOBIERNO BASADO EN LAS MEJORES PRÁCTICAS

TESIS

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTAN:

CLEMENTINA AGUILAR HERNÁNDEZ
LESLY ALVIZO GARCÍA

DIRECTOR DE TESIS:

M.C. ALEJANDRO VELÁZQUEZ MENA

CIUDAD UNIVERSITARIA 2013

Imagina la vida como un juego en el que estás malabareando cinco pelotas en el aire.

Estas son:

Tu Trabajo, Tu Familia, Tu Salud, Tus Amigos y Tu Vida Espiritual, y tú las mantienes todas éstas en el aire.

Pronto te darás cuenta que el Trabajo es como una pelota de goma. Si la dejas caer, rebotará y regresará. Pero las otras cuatro pelotas: Familia, Salud, Amigos y Espíritu son frágiles, como de cristal. Si dejas caer una de estas, irrevocablemente saldrá astillada, marcada, mellada, dañada e incluso rota. Nunca volverá a ser lo mismo. Debes entender esto: apreciar y esforzarte por conseguir y cuidar lo más valioso.

Brian Dyson

AGRADECIMIENTOS

Siempre vi muy lejano este momento en mi vida que sin las personas que han estado en mi camino no sería la misma vida.

Quiero agradecer y dedicar este trabajo a mis papás Enrique y Clara que son todo un ejemplo de lo que se debe ser en la vida y de los cuales estoy muy orgullosa. También a mis hermanos que al igual siempre han sido ejemplos, desde mi hermano mayor Omar que ha sido el camino y que buen camino, mi hermano Iván con su carácter tan decisivo y su tenacidad y mi hermano chiquito Uriel que con su nobleza y espíritu siempre brilla y me ha enseñado tanto. A César por su amor y comprensión, gracias. Son la familia perfecta, los amo.

También a mi tío José María y a Georgina junto con sus familias porque son muy cercanos a mí y personas ejemplares. A mis abuelas y abuelos que aunque a alguno no lo conocí me siento orgullosa de ellos por eso también les dedico esta tesis.

Gracias a todos mis profesores que estuvieron a lo largo de toda mi trayectoria escolar ya que de cada uno aprendí grandes lecciones, de esos maestros de vocación, de esos maestros difíciles de carácter a todos gracias, gracias a los sinodales que invirtieron su tiempo en este trabajo.

Gracias a la UNAM porque desde el bachillerato fue algo maravilloso ser parte de ella por todo lo que nos da, por ese ambiente universitario único, por haberme dado la oportunidad de estudiar y porque ser universitario te cambia la vida y la visión del mundo. Estoy muy orgullosa de la Universidad.

Gracias a mis grandes amigos que fueron más que compañeros de carrera, hermanos. José Luis, Isaac, Clementina, Gabriel, Paty y mis compañeros que me dieron grandes momentos.

A la Facultad de Ingeniería porque si estar en la UNAM es un orgullo pertenecer a esta Facultad da el doble de orgullo, te abre la mente y adquieres capacidades que en ningún otro lugar encontrarías por lo cual siempre el anhelo de regresar a mi Facultad de Ingeniería y le agradezco por formarme como Ingeniera.

Gracias a Dios porque sin él nada sería posible, gracias por todo lo que tengo, todo lo que soy y por lo que viene.

Lesly Alvizo García

P O R M I R A Z A H A B L A R Á E L E S P Í R I T U

Tal vez en el dinero encuentres un poco de felicidad, en las amistades encuentres alegrías, en las medicinas la cura para tu enfermedad, pero el amor solo lo encontraras en tu familia.

Dedico esta tesis a Clementina Hernández Reyes, a Carlos Aguilar Muñiz, a Carla Aguilar Hernández y a Flor Aguilar Hernández por hacerme feliz cada día, soy muy afortunada de haberlos conocido, siempre vivirán juntos en mi corazón.

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre, por su eterna belleza por dentro y por fuera, por ser un pilar muy importante en mi vida, por demostrarme siempre su cariño y apoyo incondicional y por ser la mujer que más admiro hasta el momento. A mi padre por su entera confianza, por su gran amor y por su apoyo día con día, por tenerme como prioridad ante todo e inculcarme el deporte, a ambos por amarme tanto, por protegerme, por alimentarme, por cuidarme y por darme siempre lo mejor. Ser padres no es una profesión pero si lo fuera los dos serían los mejores, nunca he visto tanta entrega, tanta confianza y compromiso de unos padres hacia sus hijas, siempre los vamos a amar mucho Carla, Flor y yo. Nos dejaron la mejor herencia y han sido muchos años de amor y nuestra educación.

A mi tío Hipólito, a quien quiero como a un segundo padre, por compartir momentos significativos conmigo desde el día en que llegué a este mundo, por preocuparse por mi crecimiento profesional y por siempre estar dispuesto a escucharme, ayudarme en cualquier momento, por su gran confianza en mí y por ser el mejor ejemplo que conozco de una persona capaz de generarse muchos retos, también por exigirme ser una persona emprendedora, sobresaliente y en equilibrio y por coincidir hermosamente en el camino de la ingeniería. A Flor, porque te amo infinitamente hermanita y por ampliar mi visión de crecimiento profesional a lo largo de este tiempo, también por recorrer y compartir algunos caminos juntas, estoy muy orgullosa de tus logros y tu seguridad. A Carla mi alma gemela; por compartir cada momento de mi vida sin envidia alguna y por brindarme uno de los cariños más importantes de mi vida el de hermanas y almas gemelas; al igual que de Flor me llenas de mucho orgullo con cada paso que das.

A mi abuelita Celia por consentirme, quererme mucho y darme un gran ejemplo de vida al ser emprendedora, alegre, inteligente y llenarme de lo más importante: de mucho amor.

A mi abuelito Marcelino, un angelito que ahora me cuida a donde voy y por su gran amor hacia mí, aunque ya no este; nunca se me olvidará la fe que tenía en que cumpliéramos nuestros sueños.

A mi tía María Félix por siempre seguirnos y darnos la mejor versión de ella y no perderse ningún momento especial para mí, a mi tía Cande por sus detalles siempre únicos hacia mí y su incondicional cariño, a mi tía Eligia por su alegría que siempre nos inyecta, a mi tía Gina por su apoyo incondicional y sus consejos, a mi tío Santos por inyectarme de su eterna juventud y actitud positiva y por esas pláticas de las cuales siempre aprendo, a mi tío Bernardo por tratarme siempre como una princesa y enseñarme que el respeto es esencial, a mi tío Rafael por su gran ejemplo de constancia y disciplina, a mi tío pancho por enseñarme que la vida también consta de disfrutar de esos grandes momentos.

A mis primos por dejarme compartir momentos inolvidables con ellos, los amo mucho a todos.

A Lesly, por su amistad y porque sin el equipo que formamos, no hubiéramos logrado esta meta.

A Abel Zabaleta por su amistad y por demostrarme que la distancia no impide estar siempre ahí preocupados el uno del otro, a Héctor Zarate por darse el tiempo de convivir conmigo y compartir experiencias inolvidables conmigo, a José Luis por cuidarme y darme la mejor amistad durante la carrera y su apoyo incondicional, a Javier Estrada por su entera confianza y por contagiarme de esas ganas de superarnos siempre, a Juan González Tinoco por su apoyo, por tratarme todos estos años como a una hermana y por considerarme para compartir los maravillosos pasos que da, a Abraham por su alegría y su sincera amistad a pesar del tiempo, a Roberto Cota por estar ahí siempre al pendiente de mí, a Jaime por enseñarme que a pesar del tiempo la esencia nunca cambia, a Pablo por estar ahí, a Emmanuel, Omar, Cesar, a Alan Becerril por su incondicional

apoyo, por esas largas pláticas y por su gran cariño, a Andrea García por ser una gran amiga, hermana y por estar ahí con su importante presencia en las buenas y en las malas, por todos esos momentos llenos de magia y de sincera amistad con los cuales me quedo, a Juliana y Adriana por su enorme alegría, a Dánae por ser una de las amistades más importantes, por su eterno apoyo, confianza y respeto, a Jimena Sota por esa luz que me contagia día con día en la oficina, por convertirse en una de las amistades más importantes en tan poco tiempo, a Berenice por estar siempre tratándome de localizar y estar ahí , a Ana Gabriela ser mi Buapa más bonita y su enorme cariño, a Jairo por sus hermosas pláticas, a Hugo Munguía por ser parte de la familia ahora y siempre, a Mike, Antonio, David, Verito, David Hernández, Mauricio, Patch, Daniel, Jovanni, Jonathan, Ulises, Gilberto, José Concepción, Erick, a Tania Haro por darse siempre el tiempo para estar conmigo pese a muchos cosas, a Vladimir por su sensatez ,a Ángeles por su alegría, a Luis por su confianza y todos mis amigos de la universidad, diplomado y cursos por su amistad incondicional y su sinceridad, soy muy afortunada de tenerlos a todos.

A Alejandro Mena, Carlos Saucedo, Cesar Govantes, Heriberto Olguín, Laura Sandoval, Sergio Cruz, por su gran disposición y amistad y a todos mis profesores los cuales me dejaron un buen sabor de boca al salir de la universidad.

A todo el equipo de Negocios Digitales por darme la oportunidad de crecer profesionalmente y aprender mucho de ellos; en especial agradezco a Cristina Vega por su incondicional amistad desde que tuve la gran oportunidad de conocerla, a David Arellano por sus consejos, su amistad incondicional y su entera confianza, a Roberto González por escucharme y darme el consejo y abrazo más sincero, a Sergio Guerra por su respeto y su amistad, a Humberto Guzmán por contagiarme de su entusiasmo de lograr un cambio en los procesos de gobierno, a Héctor por su envidiable actitud y su vibra siempre positiva, a Oscar Quintero por darme la oportunidad de llevar a cabo los trámites finales de mi titulación y apoyarme en mi crecimiento profesional.

A BANSEFI, al Instituto Nacional de Rehabilitación, a Pronósticos para la Asistencia Pública, a la Secretaria de Economía y su maravillosa gente que ha colaborado conmigo y me ha dado la oportunidad de aprender más de sus procesos de TI.

A Carlos Gutiérrez por darme la mejor versión de él, el tiempo que compartimos, por ser parte del libro de mi vida en el cual quiero seguir dando la oportunidad de ser yo misma y seguir mis objetivos ante todo.

A Miguel del Castillo por ser el coach que me cambió la vida, a Charly Calderón y a Jonathan Ortiz Rivera por su amistad y por tomarme de la mano en una de las etapas más difíciles que pasé y de la cual aprendí a visualizar el papel bond entero para generarme la mejor historia de vida y dejar de enfocarme en ese punto rojo que sólo me estaba cuadrando, por enseñarme a no tener miedo y a ser una persona creativa y segura de mi misma.

A Víctor Islava y Eleazar del Valle por darme la oportunidad de colaborar con ellos y aprender mucho de su profesionalismo.

A la UNAM por darme la oportunidad de formar parte de ella, por la belleza en sus espacios y por regalarme una de las etapas más hermosas de mi vida: ser estudiante.

A la Facultad de Ingeniería por ser mi casa, por permitirme conocer a las personas más inteligentes, creativas y emprendedoras de México, todas con capacidades diferentes y admirables, soy muy afortunada de tenerlos conmigo y saber que cuento con ustedes.

A Facebook por darme la oportunidad de compartir mi manera de pensar y las evidencias de este libro de mi vida que cada día vale más la pena.

A Sport City por darme la oportunidad de seguir practicando una de mis más grandes pasiones el arte del deporte, y seguir trabajando en mis inseguridades.

A mis alumnas de zumba por darme la oportunidad de cumplir uno de mis sueños: ser maestra de baile.

A Discovery Channel por hacerme consciente de la naturaleza y la implicación de no tenerla.

Al equipo de Toast Masters por inyectarme las ganas de convertirme en una líder competente, camino en el que me encuentro aun y tengo pendiente.

A Andrés por su gran amistad y por enseñarme que la edad no importa cuando se tiene el hambre de comerse al mundo.

A Martha Debayle y a Carmen Aristegui por brindarme información de calidad.

A mí misma porque me he generado personas hermosas por dentro y por fuera en mi vida y aunque trabajo día con día en mis inseguridades actualmente estoy enamorada de mi actitud, de mi educación, de mis valores, de mi entorno, de mi cuerpo, de mi alma y de mi esencia, me considero única en el mundo, con muchas cosas para dar y con una gran capacidad para seguir generándome retos importantes.

A la vida por darme la oportunidad de estar viva, de ver cada día el sol, la luna y las estrellas y de seguir escribiendo más capítulos, para el día que me vaya, lo haga con la mayor tranquilidad de que no me quede con ganas de viajar, de bailar, de amar, de trabajar, de hacer una maestría, de hacer mucho por México, por mí, de hacer lo que más me gusta y de amarlos tanto, prometo siempre dar lo mejor de mí.

Los amo infinitamente

Clem.

Índice

INTRODUCCIÓN

No se cuenta con el conocimiento de las mejores prácticas para el uso de las Tecnologías de Información para el grado de efectividad de las tecnologías de información mediante una correcta aplicación de habilidades, herramientas, técnicas y recursos en el desarrollo de proyectos, por lo tanto no se optimiza la aplicación de los recursos, con el fin de obtener mayores beneficios en la organización. Así, cada uno de los procesos se verifica, monitorea y evalúa considerando las acciones de mejora necesarias para una operación eficiente de la Unidad de Tecnologías de la Información y Control (UTIC).

En definitiva, este documento busca generar una mejor solución del uso de (MAAGTIC-SI) basado en las mejores prácticas para todas aquellas organizaciones que gestionen Tecnologías de la Información y conocer maneras de optimizar los recursos existentes, para que las buenas prácticas puedan convertirse en guías de nuevos hábitos desde las Universidades.

Un manual de mejores prácticas, es una guía que incorpora un conjunto de recomendaciones para los fines anteriormente expuestos. El presente manual de buenas prácticas recoge y difunde experiencias innovadoras que sirven de modelo. En este sentido, pretende involucrar todos los procesos ejecutados en las organizaciones posibles de las tecnologías, proyectos y soluciones a posibles necesidades tecnológicas para lo cual es necesario el desarrollo de una metodología que nos permita usar el Manual de manera adecuada para llevar acabo la implantación de dicha metodología en los procesos conforme a las mejores prácticas. Decidimos usar el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información, Comunicaciones y Seguridad de la Información, llevando a cabo el siguiente método: primero se definieron los objetivos, alcance y metas, así como el diagrama de Actividades genérico y su relación con los procesos de (MAAGTIC-SI), posteriormente se efectuaron los diagramas de Flujo de los procesos involucrados de acuerdo a los Factores Críticos que propone el (MAAGTIC-SI) seguida de una descripción detallada de los procesos, así como los roles involucrados en el método para cada uno de los procesos, llevando a cabo la evaluación de riesgos por probabilidad y grado de impacto.

El Mapeo de los procesos a los formatos propuestos por el (MAAGTIC-SI), requiere llevar un Control y Monitoreo de la Suficiencia de las actividades, así como la Administración de la Documentación del proceso en el Portafolio de Procesos. Para efectuar una mejora continua en cada uno de los procesos se guarda de acuerdo a una Bitácora de Control de Cambios.

En (MAAGTIC-SI) se integran las mejores prácticas como lo son PMBOK para la Administración de Proyectos, COBIT para la Gobernabilidad y Administración de Procesos, ITIL para la Administración y Operación de Servicios, RISK I para la Administración de riesgos, CMMI para la Administración y Desarrollo de Soluciones, ISO 9001 para auditoría en Calidad, ISO 27001 para la Seguridad de la Información, BSC para la Planeación Estratégica, TOGAF Arquitectura Empresarial y COBIT para el establecimiento del modelo de Gobernabilidad de TIC, Planeación estratégica y Determinación de la Dirección Tecnológica.

CAPÍTULO 1. MARCO TEÓRICO

Capítulo 1. Marco teórico

1.1 Definición de la Problemática

El pasado 14 de mayo de 2010 en México Distrito Federal, La Secretaria de la Función Pública concluyó el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información MAAGTIC-SI [1.1] , posterior a una serie de esfuerzos realizados desde el 22 de Septiembre del 2009; el cual se publicó el 13 de Julio del 2010 con aplicación obligatoria para toda la Administración Pública Federal (APF), como se muestra en la Fig. 1.1:

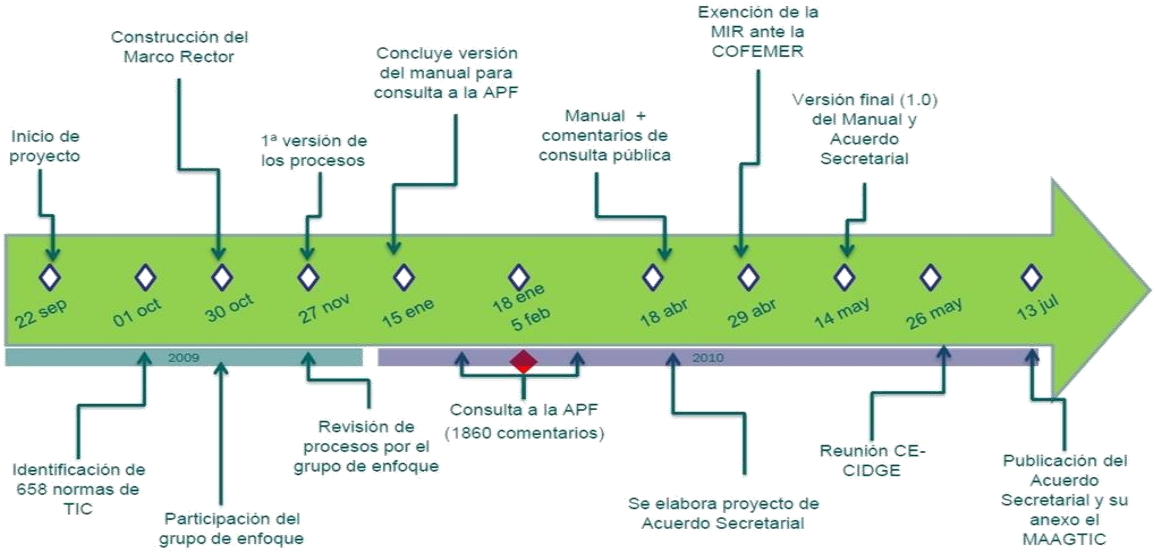


Fig. 1.1 Cronograma evolutivo del MAAGTIC

Hoy en día, las empresas no pueden darse el lujo de permanecer conformes con lo que tienen. Si no se preocupan por mejorar, solo es cuestión de tiempo antes de que desaparezcan.

Nuestra sociedad se encuentra ávida de cosas nuevas, de soluciones a problemas insolutos y de productos o servicios que los cautiven, los inspiren o les brinden la posibilidad de ser diferentes a los demás. Por esto, las empresas buscan mantenerse vigentes ante los ojos del cliente, dándole algo mejor y diferente a lo que ofrece el

competidor. De ahí la necesidad de innovar, de mejorar procesos, de buscar alternativas para ponerse adelante, de ser distinto.

En una empresa es importante mapear cada uno de los procesos de Tecnologías de la Información [1.2] y apegarlo a las mejores prácticas, ya que al documentarlo nos daremos cuenta que todos los procesos no se aplican con total limpieza, las corporaciones hoy en día han sufrido pérdidas informáticas, porque suelen tener un conocimiento muy limitado del impacto que puede tener la pérdida de los bienes informáticos o la imposibilidad para acceder a sus aplicaciones o información, las corporaciones deben aplicar el uso de las mejores prácticas para llevar a cabo cada uno de sus procesos.

Este documento nos va ayudar a entender como documentar cada uno de los procesos de TI y a tener un control en cada una de las actividades que se realizan en la empresa u organización, para así saber cómo se hace, y con qué recursos.

En los últimos años la tecnología de información se ha convertido en el detonador del crecimiento de las empresas alrededor del mundo, permitiendo a las organizaciones entrar a un mercado internacional, a un mundo globalizado. Las inversiones en TI las podemos ver en todos los sectores; automotriz, textil, banca, construcción, etc. Muchas veces estos avances representan para las empresas una ventaja estratégica, una diferenciación o una mejor manera de dar servicio al cliente. La tecnología de información puede ayudar en varios ámbitos: en mejorar un producto, en ofrecer mejores servicios o en gestionar mejor los recursos de una empresa.

1.2 Definición de los procesos y sus relaciones dentro de TI en los Macroprocesos.

Gracias a las TI los ejecutivos tienen la posibilidad de gestionar con mayor eficiencia y productividad las empresas, disminuyendo tiempos, costos, recursos, incertidumbre y falta de comunicación. La información es el recurso más importante de las organizaciones hoy en día, si se administra de la mejor manera puede significar una ventaja competitiva ante las demás organizaciones. Muchas empresas invierten enormes cantidades en tecnología de información y se quedan a la mitad de sus proyectos o los cancelan. Algunos empresarios no utilizan ningún método de evaluación para este tipo de inversiones, logrando que se conviertan en un problema para la empresa, en un desperdicio de recursos y de tiempo; debido a que no hubo una

correcta planeación del proyecto, ni una definición de los objetivos y metas del mismo. Hay que definir métodos para implementar estas tecnologías y evaluar el impacto que tendrán en la organización. El Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información [1.3] como se muestra en la Fig. 1.2, está conformado por 4 Niveles de Gestión [1.4], 11 Grupos de Procesos ó Macroprocesos [1.5] y 30 Procesos [1.6].

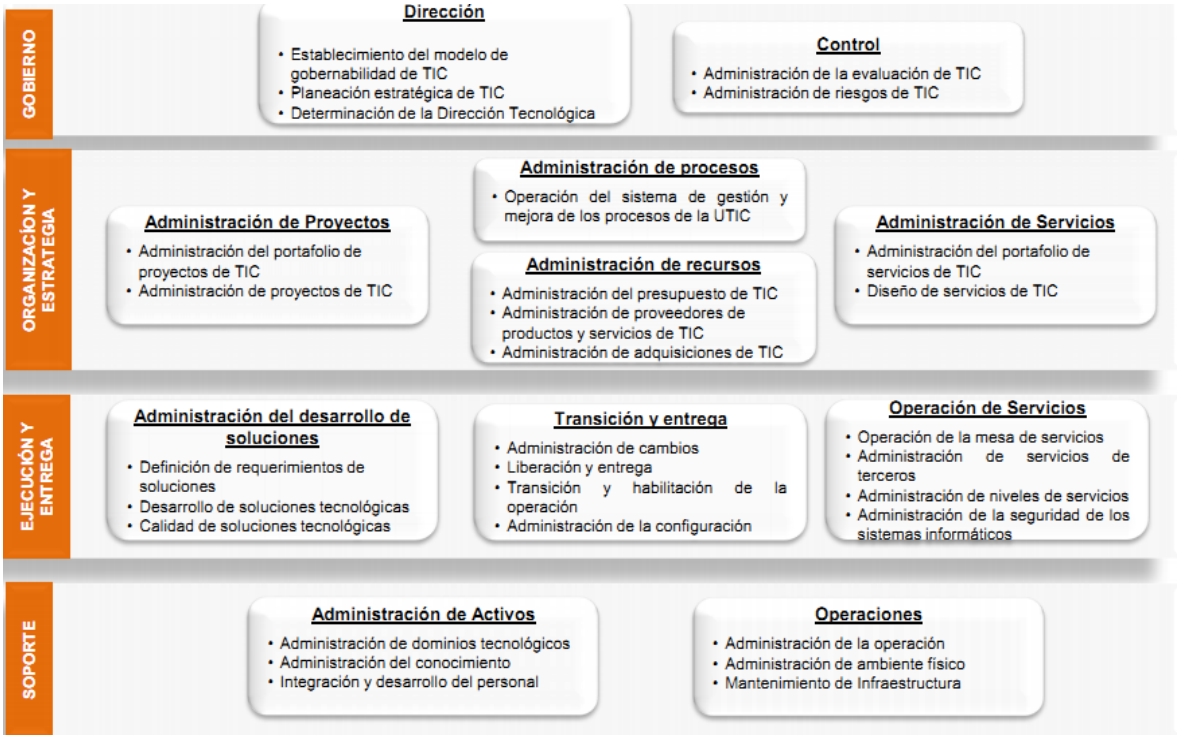


Fig. 1.2 Definición de los procesos y sus relaciones dentro de TI en los Macroprocesos.

Nivel de Gestión: Gobierno

Macroproceso: Dirección

Definir un modelo de gobernabilidad de Tecnologías de la Información y Comunicaciones (TIC) mediante la conformación de dos grupos de trabajo; el primero principalmente para apoyar la toma de decisiones en materia de TIC y determinar las prioridades de inversión; y el segundo para establecer y mantener una adecuada organización al interior de la Unidad de Tecnologías de la Información y Comunicaciones.

La Gobernabilidad de TIC es la coordinación de acciones orientadas a la dirección y el control, con una visión estratégica, esto es, enfocadas principalmente a la toma de decisiones estratégicas sobre las inversiones e iniciativas de servicios de TIC.

Procesos:

- Establecimiento del modelo de gobierno de TIC
- Planeación Estratégica de TIC
- Determinación de la Dirección Tecnológica
- Administración de la Evaluación

Nivel de Gestión: Gobierno

Macroproceso: Dirección y Control de la Seguridad de Información

Establecer mecanismos de seguimiento y evaluación, así como acciones de mejora a partir de los resultados de la ejecución de la planeación estratégica, de la operación de los procesos y de los proyectos, del uso y aprovechamiento de los activos, de los recursos y de la entrega de los servicios de TIC.

Procesos:

- Administración de la Seguridad de la Información
- Operación de los controles de seguridad de la información y del ERISC

Nivel de Gestión: Organización y Estrategia

Macroproceso: Administración de Proyectos

Obtener los resultados esperados de los proyectos de TIC, mediante una administración efectiva y una correcta aplicación de conocimientos, habilidades, herramientas, técnicas y recursos en el desarrollo de las actividades de los proyectos, con el fin de satisfacer, cumplir y superar las necesidades y objetivos de las iniciativas de TIC.

Procesos:

- Administración del Portafolio de Proyectos de TIC
- Administración de proyectos de TIC

El control de ejecución por proyectos apoyado por las TICs, introduce un cambio de estilo de dirección en la interacción entre el equipo de proyecto, los directivos y las partes interesadas, con el propósito de alcanzar los objetivos del proyecto en el menor plazo de tiempo posible, en el marco del presupuesto y con la calidad requerida por el cliente y las partes interesadas (stakeholders). El proyecto constituye la unidad básica organizativa del sistema de dirección en las empresas que trabajan por proyecto y su cronograma de ejecución actualizado, representa una herramienta fundamental para garantizar una mayor efectividad en la toma de decisiones, por el fácil acceso a la información necesaria para identificar los problemas en las tareas y brindar las decisiones oportunas que requiere la toma de decisiones en el sistema de dirección. El trabajo tiene como objetivo, el desarrollo de un procedimiento para ejecutar la toma de

decisiones en la Dirección Integrada por Proyectos apoyada por las TICs, tomando como base la programación estructurada del proyecto con los correspondientes cortes, la línea base, la línea de progreso y el seguimiento con el avance de las tareas, permitiendo ejercer su control, a partir de la información que se genera en los cortes, para con las decisiones tomadas en el corte anterior, el diagnóstico en el corte actual y el pronóstico para el siguiente, tomar las decisiones estratégicas que garantizan el cumplimiento de los objetivos, en un proceso integrado de y Administración de Proyectos de TIC.

El portafolio de proyectos es la agrupación de todos los proyectos dentro de una organización. Los administradores de un portafolio supervisan el conjunto de todos los proyectos. El propósito es satisfacer los objetivos estratégicos de la organización. Hay diferencia entre la gerencia de proyectos y la gerencia de portafolio. La gerencia de proyectos se enfoca en hacer el trabajo de forma correcta. La gerencia del portafolio se enfoca en identificar cuáles son los proyectos correctos.

Nivel de Gestión: Organización y Estrategia

Macroproceso: Administración de Procesos

Establecer y operar un Sistema de gestión y mejora de los procesos de la UTIC en el que se verifiquen, monitoreen y evalúen los procesos y se consideren las acciones de mejora necesarias para una operación eficiente de la UTIC.

Procesos:

- Operación del sistema de gestión y mejora de procesos de la UTIC

Considerando por lo menos para cada uno de los procesos, la información siguiente:

a) Objetivo general y objetivos específicos.

b) Responsable.

c) Entradas y salidas.

d) Proveedores y usuarios (clientes).

e) Mecanismos de medición e indicadores, incluyendo umbrales.

f) Recursos de los procesos: humanos, financieros, infraestructura y ambiente de trabajo.

g) Mapas del proceso.

h) Actividades y factores críticos del proceso.

Nivel de Gestión: Organización y Estrategia

Macroproceso: Administración de Recursos

Coordinar las acciones para el ejercicio del presupuesto asignado a las TIC, a fin de maximizar la aplicación de éste en los proyectos y operaciones planeadas.

Procesos:

- Administración del presupuesto de TIC
- Administración de proveedores de bienes y servicios
- Administración para las contrataciones de TIC

El Presupuesto es la predicción de gastos e ingresos para un lapso designado. Permite a las empresas, los gobiernos, las organizaciones privadas y las familias constituir prioridades y evaluar la consecución de sus objetivos. El presupuesto es un instrumento importante, utilizado como medio administrativo de determinación adecuada de capital, costos e ingresos necesarios en una organización, así como la debida utilización de los recursos disponibles acorde con las necesidades de cada una de las unidades y/o departamentos para la asignación de proyectos o servicios. Este instrumento también sirve de ayuda para la determinación de metas que sean comparables a través del tiempo, coordinando así las actividades de los departamentos con la consecución de dichas metas, evitando costos innecesarios y mala utilización de recursos.

Nivel de Gestión: Organización y Estrategia

Macroproceso: Administración de Servicios

Definir los compromisos y costos de servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de creación de servicios de TIC susceptibles de aportar beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución.

Procesos:

- Administración del portafolio de servicios de TIC
- Diseño de servicios de TIC

La Administración del Portafolio de Servicios es un método cuyo principal objetivo es cuidar las inversiones en servicio en toda la organización y administrándolos creando “valor”, Consiste en la administración proactiva de la inversión a través del ciclo de vida del servicio, incluyendo esos servicios en el concepto, diseño y transición, así como servicios vigentes definidos en los diferentes catálogos y servicios no vigentes.

Nivel de Gestión: Ejecución y Entrega

Macroproceso: Administración del Desarrollo de soluciones

Definir los requerimientos para el desarrollo de soluciones mediante acciones coordinadas con las unidades responsables solicitantes, los responsables de la implantación de la solución y las unidades responsables de las contrataciones.

Procesos:

- Apoyo Técnico para la contratación de soluciones tecnológicas
- Desarrollo de soluciones tecnológicas
- Calidad de soluciones tecnológicas

Diseño y desarrollo de soluciones tecnológicas, cuyo objetivo es ofrecer soluciones integrales avanzadas, basadas en definiciones de arquitectura de software e innovación tecnológica que contribuye a la potencialización del negocio.

Nivel de Gestión: Ejecución y Entrega

Macroproceso: Transición y entrega

Lograr una integración eficiente, segura y oportuna de los cambios que modifican el ambiente operativo mediante la definición y establecimiento de los métodos, procedimientos y estándares necesarios.

Procesos:

- Administración de cambios
- Liberación y entrega
- Transición y habilitación de la operación
- Administración de la configuración

Nivel de Gestión: Ejecución y Entrega

Macroproceso: Operación de Servicios

Establecer y operar un punto único de contacto para que los usuarios de los servicios hagan llegar sus solicitudes de servicio de TIC, para efecto de que las mismas sean atendidas de acuerdo a los niveles de servicio establecidos [1].

Procesos:

- Operación de la mesa de servicios
- Administración de niveles de servicio

Nivel de Gestión: Soporte

Macroproceso: Administración de Activos

Implementar arquitecturas tecnológicas robustas y efectivas para cada una de las agrupaciones lógicas denominadas dominios tecnológicos.

Procesos:

- Administración de dominios tecnológicos

- Administración del conocimiento
- Apoyo a la capacitación del personal de la UTIC

La administración eficiente de los activos de una empresa se ha constituido en una herramienta primordial de la gestión que impacta a la empresa mejorando los índices financieros de la empresa.

Nivel de Gestión: Soporte

Macroproceso: Operaciones

Establecer los mecanismos para administrar y operar la infraestructura, con el propósito de entregar los servicios de TIC conforme a los niveles de servicio acordados.

Procesos:

- Administración de la operación
- Administración de ambiente físico
- Mantenimiento de infraestructura

Los procesos clave para integrar la planeación estratégica con otros sistemas de gestión y que a la vez responsabiliza a todos los gerentes por el desarrollo e implementación estratégica son los procesos Planeación Estratégica de TIC, Administración del Presupuesto de TIC y Administración del Portafolio de Proyectos; son procesos de decisiones continuas que modelan el desempeño de la organización, teniendo en cuenta las oportunidades y las amenazas que enfrenta en su propio medio, además de las fuerzas y debilidades de la organización misma. La calidad del equipo de gestión así como la adopción de un enfoque de negocio y el seguimiento de los clientes son aspectos fundamentales para el desempeño. Permiten estandarizar las buenas prácticas así como la orientación estratégica en las áreas de TIC la orientación al valor que espera la organización sea generado, determinando la visión, las iniciativas y los recursos que estarían involucrados, bajo una actitud preventiva en la que se gestiona a la par la evolución organizacional, los retos y riesgos tecnológicos. A continuación se detallan estos procesos fundamentales para modelar el desempeño de la organización:

PE - Planeación Estratégica de TIC

Que el Instituto cuente con un PETIC [1.7], con el objeto de establecer líneas de acción en materia de TIC y su seguimiento, alineadas a los objetivos institucionales, de acuerdo lo establecido en el Plan Nacional de Desarrollo, los programas sectoriales y

especiales que resulten aplicables, así como las estrategias y líneas de acción de la Agenda de Gobierno Digital.

APTIC - Administración del Presupuesto de TIC

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las adquisiciones y servicios de TIC requeridos por la Institución.

APP - Administración del Portafolio de Proyectos

Administrar iniciativas, programas y proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios para la Institución.

La manera de extender las capacidades de TIC es a través de la subcontratación de proveedores ya sea por la integración de personal especialista, por ser dueños de productos de TIC o solo para extender la capacidad instalada. El Objetivo principal de la Metodología es lograr integrar estas capacidades de proveedores de manera mucho más efectiva, afectando favorablemente los proyectos o servicios en los que se incorporen.

Algunos procesos adicionales son necesarios para modelar el desempeño de la organización, éstas son:

AC - Administración para las contrataciones de TIC

Establecer un programa para la contratación de los bienes y servicios de TIC que se requieren para las Iniciativas de TIC contenidas en los portafolios de servicios y proyectos de TIC, alineado a los recursos financieros autorizados y apoyar técnicamente en la realización de los procedimientos de contratación correspondientes.

APBS - Administración de proveedores de bienes y servicios de TIC

Establecer un mecanismo que permita verificar el cumplimiento de los compromisos asumidos por los proveedores en los contratos celebrados en materia de TIC.

AT - Apoyo técnico para la contratación de soluciones tecnológicas de TIC

Definir los requerimientos de las soluciones tecnológicas de TIC, apoyar técnicamente su contratación y dar seguimiento al desarrollo de las mismas hasta su entrega, mediante acciones coordinadas con el área de Adquisiciones del Instituto, los responsables de la implantación técnica de dichas soluciones en la UTIC y, en su caso, con los Solicitantes.

Toda operación de un área de TIC está basada en procesos, creer en ellos significa que los activos ligados a los procesos se encuentran vivos en su organización. Mejorar la calidad de los procesos repercute en la calidad de los productos y/o servicios que

son generados. Implementar un esquema en el que se identifiquen oportunidades de mejora en los procesos permite mantenerlos útiles y aplicables en la organización. Detallar los activos de procesos involucra la documentación de las actividades y tareas, las reglas, los productos, los roles y los indicadores.

El Objetivo principal de la Metodología MAP2 es establecer un Sistema de Gestión y Mejora de los procesos de la UTIC que involucra la definición de estándares de documentación, metas de mejora y protocolos para su identificación, evaluación e implementación

OSGP-Operación del Sistema de Gestión y Mejora de los Procesos de la UTIC

Establecer y operar un sistema de gestión y mejora de los procesos de la SDI, en el que se verifiquen, monitoreen y evalúen los procesos establecidos por el MAAGTIC y se consideren las acciones de mejora necesarias para una operación eficiente.

EMG-Establecimiento del modelo de gobierno de TIC

Establecer un modelo de gobierno en la SDI del INR, mediante la conformación de Comités de trabajo para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC y asegurar la adecuada organización al interior de la SDI para la gestión de sus procesos.

AE-Administración de la evaluación de TIC

Establecer mecanismos de seguimiento y evaluación de la ejecución de la planeación estratégica de TIC, así como acciones de mejora a partir de sus resultados.

ACNC-Administración del conocimiento

La generación de conocimiento en la SDI y su difusión entre sus colaboradores, mediante el establecimiento, actualización y accesibilidad a un Repositorio de conocimiento.

APC-Apoyo a la capacitación del personal de la UTIC

Identificar las necesidades de capacitación de los colaboradores de la SDI, con el propósito de proponer las acciones de capacitación que permitan actualizarse en sus conocimientos, fortaleciendo sus habilidades.

Gestión y Operación de Proyectos: APTI, DST, CST, LE, THO.

En las áreas de TIC es natural el manejo de proyectos como parte de sus funciones y poder lograr las Soluciones Tecnológicas que la Institución requiere. Por ello es de relevancia establecer, de manera estandarizada, los procesos que involucra Administrar y Operar los Proyectos. El Objetivo principal que se persigue es lograr abordar a los proyectos de TIC con mayor eficiencia, logrando cubrir los compromisos

establecidos con la calidad pactada, dentro del periodo acordado y haciendo el mejor uso de los recursos.

APTI-Administración de Proyectos de TIC

Obtener los resultados esperados de los proyectos de TIC, mediante una administración efectiva y la correcta aplicación de conocimientos, habilidades, herramientas, técnicas y recursos en el desarrollo de las actividades de los proyectos, para cumplir los objetivos de las iniciativas y Programas de proyectos.

DST-Desarrollo de Soluciones Tecnológicas

Establecer el método a seguir para el desarrollo de soluciones tecnológicas de TIC, considerando la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios para su entrega, de manera que se obtenga el mejor aprovechamiento posible de los recursos de TIC.

CST-Calidad de Soluciones Tecnológicas

Verificar y validar, mediante revisiones de calidad, que los componentes y productos de las soluciones tecnológicas adquiridas o en desarrollo, cumplan con los requerimientos definidos.

LE-Liberación y Entrega

Integrar al ambiente operativo las liberaciones de las soluciones tecnológicas o servicios de TIC y efectuar las pruebas para asegurar que cumplen con los requerimientos técnicos establecidos.

THO-Transición y Habilitación de la Operación

Establecer los programas que contengan las acciones que permitan ejecutar, monitorear y controlar la transición a la operación de las soluciones tecnológicas o componentes de TIC, a fin de que evitar riesgos, fallas o la interrupción de los servicios existentes en la Institución.

Gestión y Operación de Servicios: APS, DSTI, OMS, ANS.

El principal punto de contacto de una de TIC para con los usuarios es mediante los servicios que ofrece en la demanda de necesidades de la organización. La principal producción de una de Tecnología deberá medirse en función del nivel de satisfacción que ocurre en la atención de las solicitudes de servicio recibidas por los usuarios. Para ello se integran procesos que permitirán organizar las capacidades tecnológicas y dirigirlas en la atención de servicios.

APS-Administración del Portafolio de Servicios

Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de creación de servicios de TIC susceptibles de aportar beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución.

DSTI-Diseño de Servicios de TIC

Diseñar los servicios de TIC que la Institución requiere, con la finalidad de que se consideren, de manera integral y desde su diseño, aspectos relevantes sobre la capacidad, disponibilidad y continuidad requeridas, considerando las ventajas de la existencia de un portafolio de servicios de TIC.

OMS-Operación de la Mesa de Servicios

Establecer y operar una Mesa de servicios, como punto único de contacto para que los usuarios de los activos y servicios de TIC hagan llegar sus solicitudes de servicio, a efecto de que las mismas sean atendidas de acuerdo a los niveles de servicio establecidos.

ANS-Administración de Niveles de Servicio

Establecer respecto de los servicios disponibles en la SDI, niveles de servicio susceptibles de comprometerse para los diversos servicios de TIC que requieran las Unidades administrativas solicitantes, mediante Acuerdos de nivel de servicio SLA y Acuerdos de nivel operacionales OLA, así como dar seguimiento al cumplimiento de éstos para identificar áreas de oportunidad y definir las acciones aplicables.

Gestión de la Arquitectura Tecnológica: DDT, ADT, ACMB, ACNF.

Las soluciones y servicios de TIC se basan en gran medida en la Arquitectura Tecnológica seleccionada en el Instituto. Este grupo de procesos es responsable de plantear los estándares tecnológicos y su evolución, a partir de las tendencias y normativas tecnológicas. Esta tecnología es organizada en un modelo que integra dominios tecnológicos, a manera de esquemas interpuestos, interconectados, en dependencia y con un enfoque integral, incorporando “gajos” de tecnología que permiten observar el todo y cada una de sus partes. Uno de esos dominios, por su valor organizacional, es la Seguridad, que se le dedica un apartado especial para su Administración del Sistema de Seguridad Informática. Por otra parte, elementos de la arquitectura se encuentran en los diferentes ambientes o entornos (desarrollo, pruebas, producción), requiriendo de su control mediante protocolos de control de cambios y configuración.

DDT-Determinación de la Dirección Tecnológica

Determinar la dirección tecnológica del Instituto y establecer un Programa de tecnología que facilite la selección, el desarrollo, la aplicación y el uso de la infraestructura de TIC, de manera que ésta responda a la dinámica del INR.

ADT-Administración de Dominios Tecnológicos

Implantar las arquitecturas de los dominios tecnológicos de acuerdo con los servicios de TIC existentes y proyectados en el Instituto.

ASSI-Administración de la seguridad de los sistemas informáticos

Establecer mecanismos que permitan la administración de la seguridad de la información del Instituto, contenida en medios electrónicos y sistemas informáticos, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

ACMB-Administración de Cambios

Lograr la integración eficiente, segura y oportuna de los cambios que modifican el ambiente operativo de la SDI, mediante la definición y el establecimiento de criterios técnicos y mecanismos para la administración de Solicitudes de cambio.

ACNF-Administración de la Configuración

Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la SDI, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los demás procesos contenidos en este Manual, cuando éstos así lo requieran para la operación del proceso respectivo.

Gestión de la Infraestructura: MI, AAF, AO

Administración de la Operación

Entregar a los Usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

Administración del Ambiente Físico

Implementar en el centro de datos e instalaciones de la SDI, los controles de seguridad de acuerdo con el SGSI, a fin de minimizar el impacto a la Institución, por Incidentes o riesgos que se materialicen al interior del mismo o en su entorno externo.

Mantenimiento de Infraestructura

Mantener actualizada la infraestructura tecnológica para garantizar la continuidad de los servicios de TIC.

Gestión de la Seguridad de la Información: ASI, OPEC

En las áreas de TIC el tema de seguridad es un factor de criticidad para la operación óptima de las áreas vinculadas. La información de salida como de entrada debe ser vigilada bajo estrictos controles de seguridad.

El Objetivo principal que se persigue es lograr establecer los grupos que involucrados en establecer y preservar los controles que envuelven el entorno de la seguridad de la información dentro de la Institución.

ASI-Administración de Seguridad de la Información

Establecer y vigilar los mecanismos que permitan la administración de la Seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de PAP o constituir una amenaza para la Seguridad Nacional.

OPEC-Operación de los Controles de Seguridad de la Información y del ERISC

Implantar y operar los controles de seguridad de la información de acuerdo al Programa de implantación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

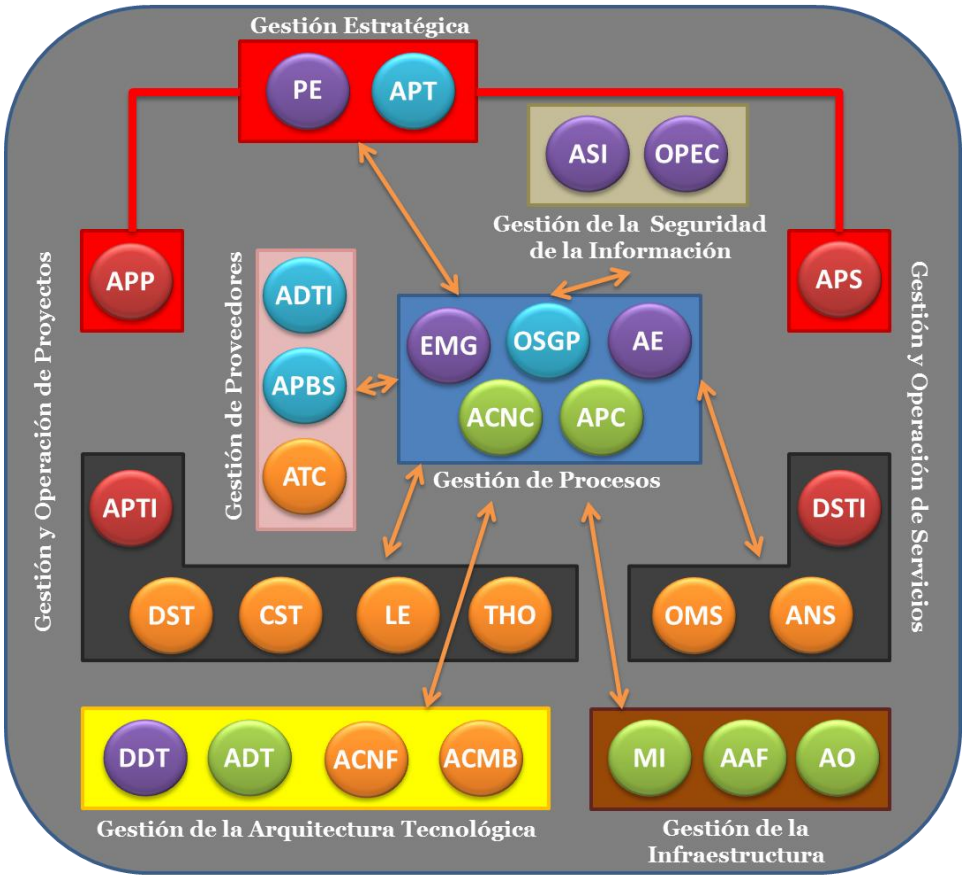


Fig. 1.3. Marco rector de procesos MAAGTIC-SI Optimizado

1.3 Marco rector de procesos, basado en las mejores prácticas

El Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTIC-SI) tiene como principal función homologar las actividades que realizan las dependencias y entidades de la Administración Pública Federal en materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, así como establecer indicadores estándar que permitan medir los resultados de la gestión de TIC; y garantizar el uso de las mejores prácticas, para alcanzar una mayor eficiencia en las actividades y procesos institucionales con una orientación al servicio y satisfacción del ciudadano.

Definir los procesos que en materia de TIC regirán hacia el interior de la Unidad de Tecnologías de la Información y Comunicaciones, con el propósito de lograr la cobertura total de la gestión, de manera que, independientemente de la estructura organizacional con que cuenten o que llegaran a adoptar, los roles definidos puedan acoplarse a los procesos establecidos para lograr la cohesión total para una mejor gestión.

El MAAGTIC-SI es un manual que describe 30 procesos de tecnologías de información y comunicaciones, distribuidos en 11 grupos por área de conocimiento o dominio de aplicación, basados en metodologías y estándares que ayudan a las instituciones a alcanzar mayor calidad y eficiencia en las operaciones de TI como CMMI [1.8], TOGAF [1.9], PMBOK [1.10], RISKIT [1.11], COBIT [1.12], ITIL [1.13], BSC [1.14], ISO 9001 [1.15] e ISO 27001 [1.16].

Fig 1.4 Marco Rector de procesos

Las mejores prácticas se han convertido en la llamada “receta de cocina” para el mejoramiento de procesos en empresas comunes teniendo como objetivo la búsqueda del compromiso en su UTIC y dirección de TIC y sus empleados, en la actualidad nos hemos dado cuenta a lo largo de la implantación del MAAGTIC-SI que mejorar nuestra organización no es una opción, es una necesidad por que tiene como consecuencias retroceder competitivamente, el objetivo es lograr la mejora continua en este tipo de organizaciones.

Las mejores prácticas se reflejan en el MAAGTIC-SI a nivel proceso, ya que definimos como proceso el conjunto de operaciones que transforman y dan valor a un producto, el cual está al servicio de la comunidad, un procesos es repetible, tiene dueño y se relaciona con otros procesos, Tener un modelo que una la misión, el esfuerzo, los objetivos y estrategias de todo el personal agrega valor y se ve reflejado en la manera en que una empresa detecta elimina y previene sus problemas.

El MAAGTIC-SI nos permite hacer una reingeniería de procesos esta ha tenido una evolución positiva en el transcurso del tiempo, considerándose con una de las poderosas y principales herramientas de gestión que le permiten a las empresas y/o sectores desarrollar mediante un cambio extremo y radical de las operaciones

convencionales con la finalidad de alcanzar metas aún más ambiciones dentro del alcance de las potencialidades de quienes lo implementan reingeniería en un concepto simple, es el rediseño de un proceso en un negocio o un cambio drástico de un proceso. A pesar que este concepto resume la idea principal de la reingeniería esta frase no envuelve todo lo que implica la reingeniería. Reingeniería es comenzar de cero, es un cambio de todo o nada, además ordena la empresa alrededor de los procesos. La reingeniería requiere que los procesos fundamentales de los negocios sean observados desde una perspectiva transfuncional y en base a la satisfacción del cliente. Para que una empresa adopte el concepto de reingeniería, tiene que ser capaz de deshacerse de las reglas y políticas convencionales que aplicaba con anterioridad y estar abierta a los cambios por medio de los cuales sus negocios puedan llegar a ser más productivos. Una definición rápida de reingeniería es "comenzar de nuevo". Reingeniería también significa el abandono de viejos procedimientos y la búsqueda de trabajo que agregue valor hacia el consumidor. Las actividades de valor agregado tienen dos características, es algo que el cliente aprecia y es importante que se ejecuten correctamente desde la primera vez. La reingeniería se basa en crear procesos que agreguen el mayor valor a la empresa. La definición más aceptada actualmente es la siguiente "La Reingeniería es el replanteamiento fundamental y el rediseño radical de los procesos del negocio para lograr mejoras dramáticas dentro de medidas críticas y contemporáneas de desempeño, tales como costo, calidad, servicio y rapidez" [1.17]. En la definición anterior planteada por Hammer y Champy existen cuatro palabras claves: Fundamental, Radical, Dramáticas y Procesos. Estas palabras son claves debido a que:

1. Una reingeniería buscará por qué se está realizando algo fundamental.
2. Los cambios en el diseño deberán ser radicales (desde la raíz y no superficiales).
3. Las mejoras esperadas deben ser dramáticas (no de unos pocos porcentajes).
4. Los cambios deben enfocarse únicamente sobre los procesos.

Se puede decir que una reingeniería es un cambio dramático en el proceso y que como efecto de esto se tendrá un rompimiento en la estructura y la cultura de trabajo. La base fundamental de la reingeniería es el servicio al cliente, a pesar del énfasis en esto, en general las empresas no logran la satisfacción del cliente y una de las razones es que los métodos y los procesos han dejado de ser inadecuados en tal grado que el reordenamiento no es suficiente, lo que se necesita es elaborar de nuevo la

"ingeniería" del proceso. A juicio de Hammer la esencia de la reingeniería es que la gente esté dispuesta a pensar de un modo diferente en el proceso y accedan a deshacerse de las anticuadas reglas y suposiciones básicas de los procesos en la organización. Además la reingeniería requiere el abandono de los viejos procesos y la búsqueda de nuevos que agreguen valor al consumidor, rompiendo la estructura y cultura de trabajo. Desde otro punto de vista la reingeniería "Es el rediseño rápido y radical de los procesos estratégicos de valor agregado - y de los sistemas, las políticas y las estructuras organizaciones que los sustentan - para optimizar los flujos del trabajo y la productividad de una organización" [1.18]. En su forma más sencilla la reingeniería cambia el proceso para corregir el ajuste entre el trabajo, el trabajador, la organización y su cultura para maximizar la rentabilidad del negocio. El concepto de avance decisivo no es nuevo, anteriormente las ideas innovadoras casi siempre encontraban respuestas como: Si se pudiera hacer, ¿Alguien ya lo habría hecho? ¿Ya se le habría ocurrido a alguien más? ¿Si se hiciera cual sería el impacto en la estructura organizacional? El objeto de la reingeniería lo constituyen aquellos procesos que son a la vez estratégicos y de valor agregado. En general solo el 50% de los procesos son estratégicos y agregan valor. La optimización que la reingeniería pide se mide en términos de resultados del negocio, incremento de rentabilidad, participación del mercado, ingresos y rendimiento sobre la inversión. Sin la relación entre la reingeniería y mejorar los resultados del negocio la reingeniería está condenada al fracaso. Otra característica de la reingeniería es que en general debe ser rápida porque los ejecutivos esperan resultados en tiempos muy cortos. Además los resultados deben ser radicales para que logren resultados notables y sorprendentes. Además debe rediseñar los procesos que agreguen valor y desechar los demás. La importancia básica de estas definiciones consiste en dejar claro que no todo cambio o transformación que se instrumente en una organización responde al concepto de reingeniería, no es una moda, es una revolución en el pensamiento y en la manera de actuar y operar de una organización en todos y cada uno de sus procesos, no son cambios parciales, sino radicales. En cuanto a sus directivos y recursos humanos implica no sólo una forma de ver el mundo, sino una nueva manera de vivir en el mundo. El ritmo del cambio en la vida de los negocios se ha acelerado a tal punto que ya no pueden ir al paso las iniciativas capaces de alcanzar mejoras incrementales en rendimiento. La única manera de igualar o superar la rapidez del cambio en el mundo que nos rodea es lograr avances decisivos, discontinuos. Sucede que muchas veces

se culpa a los empleados, a los encargados o la maquinaria cuando las cosas no marchan bien; cuando en realidad la culpa no es de ellos sino de la forma en que se trabaja. También es importante hacer notar que no es porque el proceso sea malo, sino que es malo en la actualidad debido a que el proceso fue diseñado para otras condiciones de mercado que se daban en el pasado. Muchos procesos magníficamente diseñados en el pasado ya no responden al presente. El mundo cambia, la ciencia y la tecnología avanzan, las necesidades de los clientes son otras, los competidores crecen y mejoran sus enfoques, productos y servicios.

Capítulo 2. METODOLOGÍAS

Capítulo 2. Metodologías

2.1 COBIT

El inicio de los trabajos para la implantación de controles internos se remonta a la década de 1970, cuando el Congreso de Estados Unidos y la Securities and Exchange Commission (SEC) aprobaron reformas a la ley de campaña de 1977 y la Ley de Prácticas Corruptas en el Extranjero, debido a prácticas de financiamiento de campañas políticas y prácticas de corrupción extranjeras.

La ley tipificaba como delito el soborno transnacional y las empresas para implementar programas de control interno. En 1985 se formó una iniciativa del sector privado llamada National Commission on Fraudulent Financial Reporting, que tenía como objetivo inspeccionar, analizar y emitir recomendaciones sobre información empresarial fraudulenta. La iniciativa fue conocida como Treadway Comission.

La comisión estudió los sistemas de información para reportes financieros durante dos años, y en 1987 publicó un informe de conclusiones y recomendaciones. Como resultado de este primer informe, se formó el Committe of Sponsoring Organizations of the Treadway Commission (COSO). Fue retenido una importante firma de contadores públicos llamada Coopers & Lybrand. Posteriormente, en 1992 COSO publicó el informe titulado Control Interno-Marco Integrado y más tarde se volvió a publicar en 1994 con algunas modificaciones. El informe presenta una definición común de control interno y proporciona un marco conceptual que puede ser evaluado y mejorado. Se trata del informe estándar que las compañías de Estados Unidos utilizan para evaluar el cumplimiento de la FCPA [2.1].

COBIT (Control Objectives for Information and Related Technology); tiene cinco versiones importantes.

COBIT es empleado en todo el mundo por quienes tienen como responsabilidad primaria los procesos de negocio y la tecnología, aquellos de quien depende la tecnología y la información confiable, y los que proveen calidad, confiabilidad y control de TI.

Los Objetivos de Control para la Información y Tecnologías relacionadas o COBIT, es un marco de buenas prácticas diseñado para reducir el riesgo de eventos indeseables e incrementar el valor de TI en los negocios. Está reconocido a nivel mundial, representa el consenso de expertos de la industria y es revisado por miembros de

ISACA [2.2] de todo el mundo. Tiene como misión: Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Los puntos fundamentales de COBIT se enfocan en actividades para Gobierno de TI, control interno y niveles de madurez. Además se trata de un documento de dominio público, conformado por 34 procesos y 210 objetivos de control.

La terminología que emplea COBIT está alineada, tanto como ha sido posible, a otras mejores prácticas y estándares (administración de proyectos, desarrollo de software, administración de la calidad, seguridad de la información, etcétera). Para la versión 4.1 de COBIT, se utilizaron alrededor de 40 estándares, marcos, guías y mejores prácticas.

Gobierno de TI

El gobierno corporativo es el punto de vista general de gobierno y aplica a todas las empresas, se trata del nivel más alto en el marco del gobierno, de él se deriva el Gobierno de TI, fundamental de COBIT. Fundamentalmente, el gobierno de TI se refiere a dos resultados: entrega de valor de TI al negocio y mitigación de riesgos relacionados con TI. Esto se logra a través de una alineación de TI con el negocio, la disponibilidad y administración adecuada de los recursos y las medidas de desempeño para el monitoreo hacia las metas deseadas. El IT Governance institute (ITGI), define al Gobierno de TI de la siguiente manera:

“Es el conjunto de responsabilidades prácticas ejercidas por el consejo de directores y los ejecutivos, con los objetivos de proporcionar dirección estratégica, asegurar que se logran los objetivos, determinar que los riesgos son administrados apropiadamente y verificar que los recursos de la empresa son utilizados responsablemente”.

Es importante hacer la siguiente aclaración: la administración de TI se centra en el suministro eficaz y eficiente de los servicios y operación de TI. El gobierno de TI es más amplio, se centra en el desempeño y transformación de TI para satisfacer las demandas presentes y futuras de la organización.

La implementación del Gobierno de TI puede realizarse con una mezcla de estructuras, procesos y mecanismos relacionales:

a) Estructuras. Involucra la existencia de responsabilidades para las funciones, tales como la existencia de ejecutivos de TI y comités de TI.
b) Procesos. Se refiere a la toma de decisiones y supervisión sobre TI, como planeación de sistemas de información y Balanced Scorecard [2.3].

c) Mecanismos relacionales. Incluyen la participación, diálogo y aprendizaje compartido de las partes interesadas.

d) Los principales beneficios de un efectivo gobierno de TI son los siguientes:

- Mejora las relaciones de confianza con los clientes
- Protege la reputación de la organización
- Provee rendición de cuentas para salvaguardar la información durante las actividades críticas de la organización

Áreas Focales del Gobierno de TI

El Gobierno de TI se enfoca en cinco áreas: alineación estratégica, entrega de valor, administración del riesgo, administración de los recursos y medición del desempeño

a) Alineación Estratégica. La primera área focal busca garantizar la alineación entre los planes de negocio y de TI; definir, mantener y validar la propuesta de valor de TI, así como alinear las operaciones de TI y de la organización

b) Entrega de valor. La segunda área de enfoque se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de TI.

c) Administración del riesgo. La tercera área se enfoca en la conciencia por parte de los altos ejecutivos de la organización, un claro entendimiento de la aversión al riesgo; comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos de la empresa y la inclusión de las responsabilidades de administración de la organización

d) Administración de recursos. La siguiente área focal es la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas clave se refieren a la optimización de conocimiento (retención y documento) y de infraestructura.

e) Medidas de desempeño. Por último, la quinta área focal rastrea y monitorea la estrategia de implementación, la terminación del proyectos, el uso de los recursos, el desempeño de los procesos y la entrega del servicio , con el uso, por ejemplo de indicadores balanceados de desempeño (balanced scorecard) que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Es el modelo para el Gobierno de la TI desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI por sus siglas en

Inglés) (www.itgi.org) se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa.

Un gobierno de TI efectivo, ayuda a garantizar que TI soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI.

Enfocado al negocio

La primera característica del marco de trabajo COBIT es su enfoque en el negocio. La orientación al negocio consiste en alinear las metas de la organización con las metas de TI, brindar métricas y modelos de madurez para la medición de logros e identificación de responsabilidades asociadas a los dueños de los procesos de negocio y de TI. Se basa en el siguiente principio: Para proporcionar la información que la organización requiere para lograr sus objetivos, necesita invertir, administrar y controlar los recursos de TI utilizando un conjunto estructurado de procesos que proporcionen los servicios que entregan la información organizacional requerida.

Metas de negocio

La estrategia de la organización se debe traducir en objetivos relacionados con iniciativas habilitadas por TI (metas del negocio para TI), estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de TI (metas de TI), posteriormente, estas metas a su vez deben definir los recursos y capacidades de TI (arquitectura empresarial de TI) necesarios para realizar de forma exitosa la parte que le corresponde a TI de la estrategia de la organización. De acuerdo con COBIT, existen 17 metas de negocio que se dividen en cuatro perspectivas:

a) Perspectiva financiera.

b) Perspectiva del cliente.

c) Perspectiva interna.

d) Perspectiva de aprendizaje y crecimiento.

Beneficios de Implementar COBIT

Existen diversos beneficios para las organizaciones que utilizan los marcos de control, para el caso de COBIT, se pueden enlistar los siguientes:

 Mayor alineación basada en los objetivos del negocio. La alta dirección entiende las funciones de TI y la forma en la que soportan los objetivos del negocio.

 Orientación a procesos. Define claramente a los dueños de los procesos y sus responsabilidades, así como las metas en actividades, procesos y TI.

 Aceptabilidad general. Debido al uso generalizado entre las organizaciones, terceras partes y entidades regulatorias comprenden los términos del marco.

 Entendimiento compartido. Las partes interesadas manejan un lenguaje común.

Recursos de TI

Los recursos de TI identificados en COBIT son 4 (aplicaciones, información, infraestructura y personas), se definen como:

a) Aplicaciones. Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que requieren información.

b) Información. Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

c) Infraestructura. Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

d) Personas. Son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas o contratadas, de acuerdo a como se requieran.

Criterios de Información

Los criterios de información proporcionan un método para definir los requerimientos de la organización. COBIT define siete criterios:

a) Efectividad. La información debe ser relevante y pertinente a los procesos del negocio, además de ser proporcionada de manera oportuna, correcta, consistente y utilizable.

b) Eficiencia. La información debe ser generada con el óptimo (más productivo y económico) uso de los recursos.

c) Confidencialidad. La información sensible debe ser protegida contra una revelación no autorizada.

d) Integridad. La información debe ser exacta y completa, así como válida de acuerdo a los valores y expectativas del negocio.

e) Disponibilidad. La información debe estar accesible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

f) Cumplimiento. Se deben acatar leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

g) Confiabilidad. Se debe proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Fig. 2.1 Diagrama de COBIT

Niveles de madurez

0. **No Existente.** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1. **Inicial.** Exista evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen
2. **Repetible.** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal entre los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3. **Definido.** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4. **Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5. **Optimizado.** Los procesos se han refinado hasta un nivel de mejor práctica**.**

2.2 RISK IT

Creado por ISACA emitido en el 2009. La publicación, denominada en inglés "Enterprise Risk: Identify, Govern and Manage IT Risk; The Risk IT Framework" [2.4].

Esta publicación viene a llenar un vacío que existía entre las metodologías de riesgos genéricas (como la ISO 31000) [2.5] y las específicas asociadas a la administración de riesgos de seguridad de la información (como la ISO 27001) [2.6].

Los riesgos de TI pueden ser clasificados en tres grandes grupos:

Riesgos en la entrega de los servicios de TI, asociados con el desempeño y disponibilidad de los servicios, y que pueden ocasionar destrucción o reducción de valor a la organización.

Riesgos en la entrega de una solución de negocio, asociados con la contribución esperada de TI a la mejora o creación de nuevas soluciones de negocio.

Riesgos en la entrega de beneficios, asociadas con la pérdida de oportunidades de usar la tecnología para mejorar la eficiencia y eficacia de los procesos de negocio, o para usar la tecnología como habilitador de nuevas iniciativas de negocio.

Especifica los requerimientos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en el contexto de la actividad general de la organización y el riesgo al que se enfrenta.

Sistema de Gestión de Seguridad de la Información (SGSI). Aquella parte del sistema gerencial general, el cual incluye:

- la estructura organizacional,
- actividades de planeación,
- responsabilidades,
- políticas,
- procedimientos, procesos
- recursos

El Gobierno Empresarial efectivo para Riesgos de TI, Siempre se relaciona con objetivos de negocio, Alinea la administración de los riesgos relacionados con TI con la administración general de riesgos de la Empresa Equilibra el costo y los beneficios de la administración de Riesgos.

Administración efectiva de Riesgos de TI: Promueve una comunicación clara y abierta sobre riesgos de TI, Establece el tono adecuado desde la parte más alta de la empresa al tiempo que define y refuerza la rendición de cuentas personal sobre la operación dentro de niveles de tolerancia bien definidos, con el objeto de ayudar a las organizaciones en la mitigación de los riesgos corporativos que tengan su origen en el uso de las TIC.

Beneficios de usar RISK IT

Es un esquema (o marco de trabajo) de Arquitectura Empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información. Esta arquitectura es modelada por lo general con cuatro niveles o dimensiones: Negocios, Tecnología (TI), Datos y Aplicaciones. Cuenta con un conjunto de arquitectura base que busca facilitarle al equipo de arquitectos definir el estado actual y futuro de la arquitectura. El marco de los riesgos de TI, RISK IT, se complementa con COBIT, que proporciona un marco integral para el control y la gestión de las organizaciones de soluciones y servicios de TI. Aunque COBIT establece las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI, RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio. El marco de riesgos de TI es utilizado para ayudar a implementar el gobierno de TI, y las organizaciones que han adoptado (o están planeando adoptar) COBIT como marco de su gobierno de TI pueden utilizar RISK IT para mejorar la gestión de sus riesgos. COBIT, propiedad de ISACA, se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que tratar con eventos internos o externos a la organización. Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones. Los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan. Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo, y cómo gestionarlo, es el tema principal de RISK IT. Cuándo se

identifican las oportunidades de cambios del negocio relacionados con TI, el Marco VAL IT describe cómo progresar y maximizar el retorno de la inversión realizada en los mismos. El resultado de la evaluación tendrá probablemente un impacto en algunos de los procesos de TI, por lo que las flechas de la —Gestión de Riesgos" y —Gestión del Valor|| se dirigen a la "Gestión de los Procesos de TI", tal y como se muestra en la figura 2.2. Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos. Los riesgos de TI pueden clasificarse de diversas maneras.

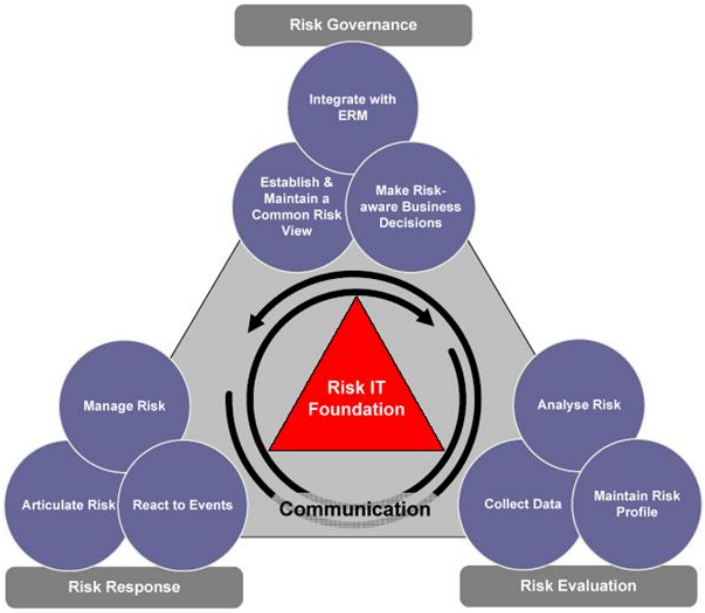


Fig. 2.2 Gestión del Risk IT

2.3 ITIL

ITIL (Information Technologies Infraestructure Library), es un conjunto de mejores prácticas para la dirección y gestión de servicios de tecnologías de la información en lo referente a Personas, Procesos y Tecnología, desarrollada por la OGC (Office of Goverment Commerce), y es un estándar de facto utilizado mundialmente para definir y mejorar la Gestión de Servicios. A través de las mejores prácticas especificadas en ITIL se hace posible para departamentos y organizaciones reducir costos, mejorar la calidad del servicio tanto a clientes externos como internos y aprovechar al máximo las

habilidades y experiencia del personal mejorando su productividad hacia un modelo orientado al servicio.

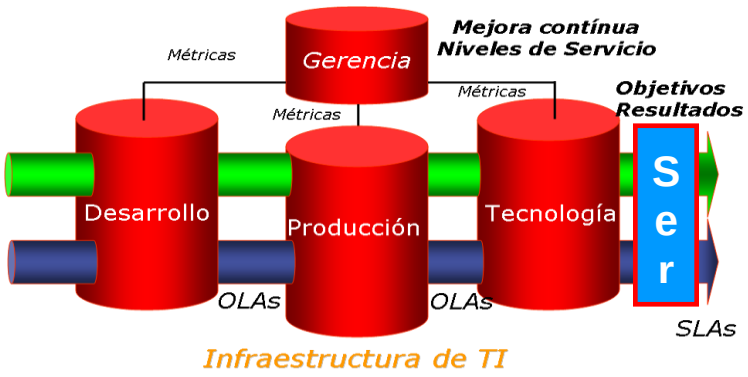


Fig. 2.3 Infraestructura de TI

La sociedad está en la actualidad en un momento donde la disponibilidad de los servicios es cada vez más exigente, las peticiones de los clientes o usuarios son más cuantiosas y urgentes y el ritmo de los negocios cambia constantemente. Es indudable la importancia de que las Tecnologías de Información (TI) estén adecuadamente organizadas y alineadas con la estrategia del negocio. ITIL es un camino al logro de este objetivo vital. Las Tecnologías de la Información (TI) disponen de una gran relevancia en la sociedad y en la economía actual, aumentando su influencia cada día que pasa; han dejado de ser simples herramientas a ser factores clave para el desarrollo de la sociedad y la economía, convirtiéndose en estos momentos en los principales canales de comunicación

ITIL nos permite mejorar notablemente la calidad de los servicios de tecnologías de la información y que presta una organización a sus clientes o un departamento a su organización. Los servicios son los medios para entregar valor a los clientes, facilitando sus tareas para obtener resultados, sin que ellos deban asumir los costos específicos ni los riesgos asociados. Los proveedores de servicios asumen y asignan costos y riesgos a cada cliente por los servicios que ellos proveen. Los resultados se logran a través de la ejecución de tareas y están limitados por la presencia de ciertas restricciones. Los servicios facilitan la obtención de resultados por medio del aumento del rendimiento de las tareas asociadas y la reducción de los efectos de las restricciones. El resultado es el incremento de la probabilidad de obtener los resultados deseados.La Gestión del Servicio es un conjunto de habilidades organizacionales

especializadas para proveer valor a los clientes en la forma de servicios. Las habilidades toman la forma de funciones y procesos para gestionar los servicios a través de un ciclo de vida, con especializaciones como se muestra en la figura 2.1 Ciclo de vida del servicio de TI.

- Estrategia
- Diseño
- Transición
- Operación
- Mejora continua

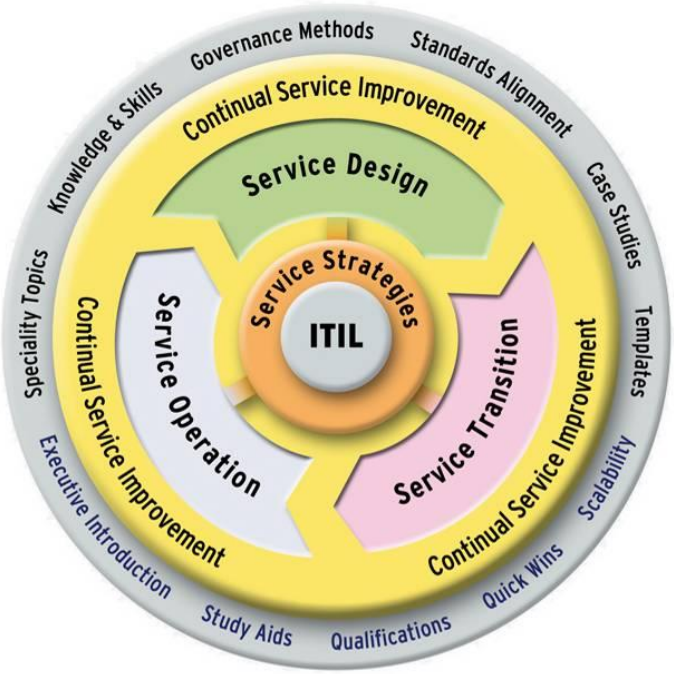


Fig. 2.4 Ciclo de Vida del servicio de TIC, ITL librería

El concepto de función

Son unidades organizacionales especializadas para ejecutar ciertos tipos de tareas o trabajos y son responsables de sus resultados específicos.

Proveen estructura y estabilidad a la organización e implementan el principio de la especialización.

Son unidades autónomas con habilidades y recursos necesarios para su funcionamiento y entrega de resultados.

Generalmente definen los roles y la autoridad y responsabilidad asociadas para la obtención de resultados y rendimientos específicos. Tienden a optimizar sus métodos de trabajo localmente para focalizarlos sobre los resultados asignados.

El concepto de proceso

Es un conjunto de actividades coordinadas que combina e implementa recursos y capacidades para producir un resultado, el cual directa o indirectamente crea valor para un cliente o un stakeholder. Provee la transformación hacia un objetivo y utiliza el feedback para tomar acciones de autocorrección (funciona como un sistema de ciclo cerrado).

Describe las acciones, las dependencias y la secuencia de actividades

Características de los procesos

- **Medibles:** Tenemos que ser capaces de medir los procesos de una manera relevante. Los gerentes necesitan medir el costo, la calidad y otras variables asociadas.
- **Resultados específicos:** La razón de existir de un proceso es entregar un resultado específico. Este resultado debe ser individualmente identificable y contable.
- **Clientes:** Cada proceso entrega sus resultados a un cliente o a un stakeholder. Los clientes pueden ser internos o externos a la organización; más allá de eso, el proceso debe cubrir sus expectativas.
- **Responden a eventos específicos:** Mientras un proceso puede ser continuo o iterativo, éste debería responder a un disparador específico.

El concepto de rol

- Un **rol** es un conjunto de comportamientos conectados realizados por una persona, un equipo o un grupo en un contexto específico.
  Por ejemplo: un departamento técnico puede ejecutar el rol de Gestión de Problemas cuando diagnostica la causa raíz de los incidentes.
- También puede esperarse que un mismo departamento juegue otros roles diversos en distintos momentos, por ejemplo podría evaluar el impacto de los cambios (rol de Gestión de Cambios), administrar el rendimiento de los dispositivos bajo su control (rol de Gestión de Capacidad), etc.
- El alcance del **rol** y lo que dispara su desempeño está definido por el proceso correspondiente y acordado por el gerente de línea.

Dueño del proceso

- El **Dueño del Proceso** lleva a cabo el rol esencial de apoyar el proceso, liderar su diseño, entrenar al personal y defender el proceso dentro de la organización.
- Típicamente debería ser un gerente de nivel senior, con credibilidad, influencia y autoridad a lo largo de las distintas áreas impactadas por las actividades del proceso.
- Este rol clave es responsable de la calidad general de su proceso, de su supervisión, de su conformidad organizativa, de su flujo, de sus procedimientos, de su modelo de datos, de sus políticas y de sus tecnologías asociadas.
- Se requiere que tenga la habilidad de influenciar y asegurar la conformidad con las políticas y los procedimientos establecidos, a lo largo de los silos culturales y departamentales de la organización de TI.

Incluye las siguientes responsabilidades

- Documentar y publicar el proceso.
- Definir los KPI (Indicadores Clave de Rendimiento - Key Performance Indicators) para evaluar la efectividad y la eficiencia del proceso y luego analizarlos para ejecutar las acciones correctivas necesarias.
- Asistir y ser en última instancia el responsable del diseño del proceso.
- Mejorar la eficiencia y la eficacia del proceso y revisar las mejoras propuestas para el proceso.
- Asegurar el entrenamiento requerido de todo el personal relevante para actuar en el proceso y, además, la conciencia que cada integrante tenga de su rol.
- Asegurar la existencia de revisiones y auditorías regulares del proceso, de los roles y sus responsabilidades y de la documentación correspondiente.
- El Propietario del Servicio tiene la responsabilidad ante el cliente de la iniciación, la transición, el mantenimiento y el soporte continuo de un servicio particular.
- Responde por un servicio específico, independientemente de dónde residan los componentes tecnológicos, los procesos y las capacidades profesionales que lo soporten.
- La definición de una responsabilidad única es absolutamente esencial para proporcionar el nivel de atención y de focalización requerido para la provisión del servicio y para asegurar su gestión focalizada en el negocio.
- El Propietario del Servicio es responsable de la mejora continua y de la gestión de los cambios que afecten a los servicios por los que sea responsable.

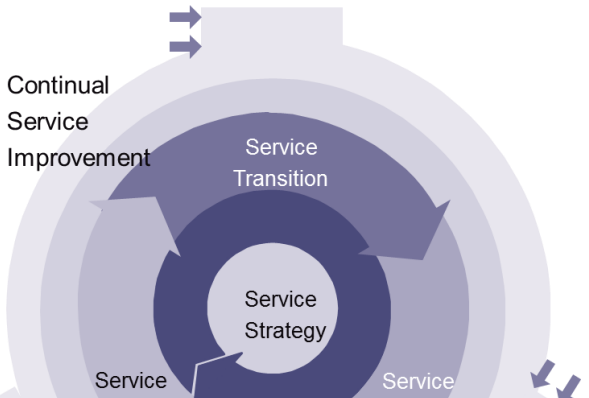
Propietario del servicio

- El Propietario del Servicio tiene la responsabilidad ante el cliente de la iniciación, la transición, el mantenimiento y el soporte continuo de un servicio particular.
- Responde por un servicio específico, independientemente de dónde residan los componentes tecnológicos, los procesos y las capacidades profesionales que lo soporten.
- La definición de una responsabilidad única es absolutamente esencial para proporcionar el nivel de atención y de focalización requerido para la provisión del servicio y para asegurar su gestión focalizada en el negocio.
- El Propietario del Servicio es responsable de la mejora continua y de la gestión de los cambios que afecten a los servicios por los que sea responsable.
- Actuar como un primer contacto con el cliente para todos los temas y requerimientos relacionados con el servicio.
- Asegurar que el soporte y la entrega continúa del servicio alcance los requerimientos acordados con el cliente.
- Identificar oportunidades para la mejora de los servicios, discutirlas con el cliente y generar un RFC para su evaluación si es apropiado.
- Comunicarse con los dueños de proceso apropiados a través del ciclo de vida del servicio.
- Solicitar datos requeridos, reportes y estadísticas para el análisis y facilitar un efectivo monitoreo y rendimiento del servicio.
- Ser responsable ante el director de TI de la entrega del servicio.

El modelo ITIL

El framework ITIL, como una fuente de mejores prácticas en la Gestión de Servicios, presenta las siguientes cinco publicaciones:

Estrategia del Servicio
(Service Strategy)
Diseño del Servicio
(Service Design)



Transición del Servicio

(Service Transition)

Operación del Servicio

(Service Operation)

Mejora Continua del Servicio

(Continual Service Improvement)

Fig. 2.5 Ciclo de vida del Servicio

- Service Strategy (SS): representa las políticas y los objetivos. Es el eje central alrededor del cual gira el ciclo de vida del servicio.
- Service Design (SD): Service Transition (ST) y Service Operation (SO) implementan la estrategia definida.
- Continual Service Improvement (CSI): ayuda a desarrollar y priorizar los programas y los proyectos de mejora basándose en los objetivos estratégicos.

Ciclo de vida

- Mientras que la experiencia es utilizada para influenciar la acción futura, la **estructura** es esencial para organizar la información no relacionada o dispersa.
- La estructura del ciclo de vida de los servicios es un marco organizativo.
- Sin estructura, el conocimiento de la gestión del servicio es una mera colección de observaciones, prácticas y metas en conflicto.
- Los procesos describen cómo cambiar las cosas, mientras que las estructuras describen cómo éstas deben conectarse, determinando el comportamiento.
- Sin estructura es difícil aprender de la experiencia.
- El ciclo de vida es un modelo para la gestión del servicio: busca comprender su estructura, las interconexiones entre todos sus componentes y cómo los cambios en cualquier área afectarán el sistema completo a través del tiempo.

El patrón predominante en el ciclo de vida es el progreso secuencial que comienza en SS > SD > ST > SO y que regresa a SS a través de CSI

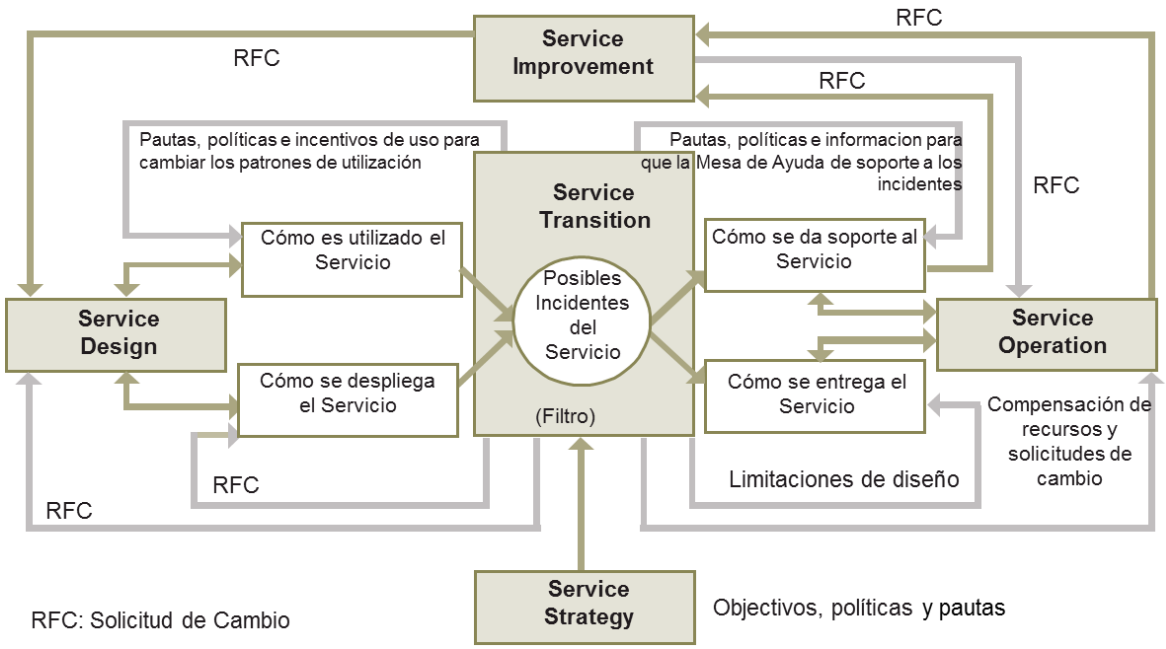


Fig. 2.6 RFC en el ciclo de vida del servicio

Beneficios de la Gestión del servicio de las TI e ITIL

Primeramente veamos que beneficio proporciona la Gestión del Servicio de las TI:

"Asegura que los servicios ofrecido por las TI estén alineados con las necesidades del negocio, aportando valor al mismo".

Una buena Gestión del servicio de las Tecnologías de la Información:

• Nos permite maximizar la Calidad de los servicios que ofrecemos apoyando al negocio de nuestra empresa u organización. • Supone habilidad para clarificar y alinear los costes de los servicios de TI.

Capacidad de absorber el cambio y complejidad con el mínimo impacto mejorando el "time to market".

• Mejora de la Disponibilidad de los servicios a través de reducir el número e impacto de los incidentes.

• Ofrece una clara visión de la capacidad del área de TI, obteniendo de eses modo un personal más motivado y satisfecho frente a las expectativas de gestión.

• Facilita de toma de decisiones de acuerdo a indicadores de las TI y referentes al negocio.

• Estándares de gobernabilidad verificables establecidos por la dirección de las organizaciones.

Todos estos beneficios alinean íntegramente las necesidades del negocio con el área de servicios de TI, haciendo que la empresa hable un lenguaje común y mejorando el entendimiento y relaciones entre todas las partes involucradas.

ITIL es una de las herramientas que nos permite, mediante su conjunto de buenas prácticas orientadas al negocio, a procesos y a clientes/usuarios conseguir una óptima Gestión del Servicio y los beneficios que ello implica. Es importante destacar que ayuda a la creación de una base sólida enfocada a la mejora continua.

Por su parte los Beneficios de ITIL son:

- Una mejora la calidad de los servicios proveídos.
- Una visión clara y más confianza de los servicios ofrecidos de TI.
- Una visión clara de la capacidad actual de TI.
- Mayor flexibilidad para las organizaciones a través de un entendimiento con las TI.
- Un personal más satisfecho, a través de un mayor entendimiento de la capacidad y mejores
- expectativas de gestión.
- Mayor flexibilidad y adaptabilidad.
- Mejora en los sistemas, tales como seguridad, fiabilidad, velocidad y disponibilidad como se requiere en el nivel de servicio a ofrecer.
- Reducción del tiempo de los cambios que se efectúan y una tasa mayor de éxito.
- Alineación de los servicios de TI con las necesidades de las organizaciones definidas.
- Asegura una mejor comunicación entre TI y las organizaciones a través de un lenguaje común
- Mejora la calidad y reduce los costes a largo plazo de la provisión de los servicios.
- Crea una base sólida para la mejora continua.
- Incrementa la transparencia y control de las organizaciones de TI.

2.4 CMMI

CMMI representa la fusión de un conjunto de modelos orientados a la mejora de procesos de Ingeniería de Software, ingeniería de sistemas, desarrollo de productos y adquisición de aplicaciones. Creado en 1991 por el Software Engineering Institute (SEI)

como CMM y posteriormente actualizado como CMMI en 2002, está orientado a la garantía de calidad del software en función del nivel de madurez de sus proceso de producción.

Su implementación aumenta la fiabilidad del software producido, la visibilidad de los procesos de producción y soporte, la reusabilidad de componentes y como resultado de la combinación de este tipo de mejoras, disminuye los costes de producción y mantenimiento de las aplicaciones.

CMMI (Capability Maturity Model Integration) es un modelo de madurez de mejora de los procesos para el desarrollo de productos y de servicios. Consiste en las mejores prácticas que tratan las actividades de desarrollo y de mantenimiento que cubren el ciclo de vida del producto, desde la concepción a la entrega y el mantenimiento.

Esta última versión del modelo, presentada en esta obra, integra los cuerpos del conocimiento que son esenciales para el desarrollo y el mantenimiento, pero que se han tratado por separado en el pasado, tales como la ingeniería del software, la ingeniería de sistemas, la ingeniería del hardware y de diseño, los aspectos no funcionales y la adquisición. Las denominaciones anteriores de CMMI para la ingeniería de sistemas y la ingeniería del software (CMMI-SE/SW) son reemplazadas por el título “CMMI para desarrollo”, reflejando así realmente la integración completa de estos cuerpos de conocimiento y la aplicación del modelo en el seno de una organización. CMMI para desarrollo (CMMI-DEV) propone una solución integrada y completa para las actividades de desarrollo y de mantenimiento aplicadas a los productos y a los servicios.

CMMI para desarrollo, versión 1.2, es una continuación y actualización de CMMI versión 1.1 y ha sido simplificada gracias al concepto de “constelaciones” de CMMI, donde un conjunto de componentes fundamentales puede ser ampliado mediante material adicional a fin de proponer unos modelos específicos de aplicación con elevado contenido común. CMMI-DEV es la primera de esas constelaciones y representa al dominio de interés de desarrollo.

El propósito de CMMI para desarrollo es ayudar a las organizaciones a mejorar sus procesos de desarrollo y de mantenimiento, tanto para los productos como para los servicios. El Marco de CMMI soporta el Conjunto de productos de CMMI, permitiendo generar múltiples modelos, cursos de formación y métodos de evaluación que dan soporte a dominios de interés específicos.

1. El Marco de CMMI es la estructura básica que organiza los componentes CMMI y los combina en las constelaciones y modelos.

Actualmente hay tres constelaciones planificadas que se sostienen en el marco del modelo de la v1.2: desarrollo, servicios y adquisición. Las “extensiones “se utilizan para extender las constelaciones mediante contenido específico adicional

CMMI para desarrollo es un modelo de referencia que cubre las actividades del desarrollo y del mantenimiento aplicadas tanto a los productos como a los servicios. Las organizaciones de numerosas industrias, incluyendo la aeroespacial, los bancos, la construcción de ordenadores, el software, la defensa, la fabricación del automóvil y las telecomunicaciones, utilizan el CMMI para desarrollo.

Los modelos de la constelación del CMMI para desarrollo contienen prácticas que cubren la gestión de proyectos, la gestión de procesos, la ingeniería de sistemas, la ingeniería del hardware, la ingeniería de software y otros procesos de soporte utilizados en el desarrollo y el mantenimiento.

Beneficios de CMMI

1. Fundamentos del CMMI y de los procesos de mejora continua en el software.
2. Esquema de plan de producción de software con una metodología ágil.
3. Fases, Procesos y repertorio de entregables de proyecto.
4. Roles y responsabilidades.
5. Esquema de calidad ajustado a distintas escalas de proyecto.
6. Como diseñar un plan de mejora continua en los procesos.
7. Estrategias de micro-mejoras en la producción de software.
8. Factores de éxito en la definición de procesos.
9. Herramientas de soporte en la mejora de procesos.
10. Plan director para lograr una certificación CMMI progresiva.

Áreas de proceso de Soporte básicas

Las áreas de proceso de Soporte Básicas tratan las funciones de soporte fundamentales que se usan por todas las áreas de proceso. Aunque todas las áreas de proceso de Soporte usan como entrada otras áreas de proceso, las áreas de proceso básicas de soporte proporcionan relaciones entre áreas de proceso de soporte que también ayudan a implementar varias prácticas genéricas. Los proyectos y a las organizaciones durante la alineación de las necesidades y objetivos de medición con una forma de medir que proporcionará resultados objetivos. Estos resultados pueden usarse en la toma de decisiones informadas y en la toma de acciones correctivas. La

Figura 2.7 proporciona una visión general de las interacciones entre las áreas de proceso de Soporte Básicas y todas las demás áreas de proceso.

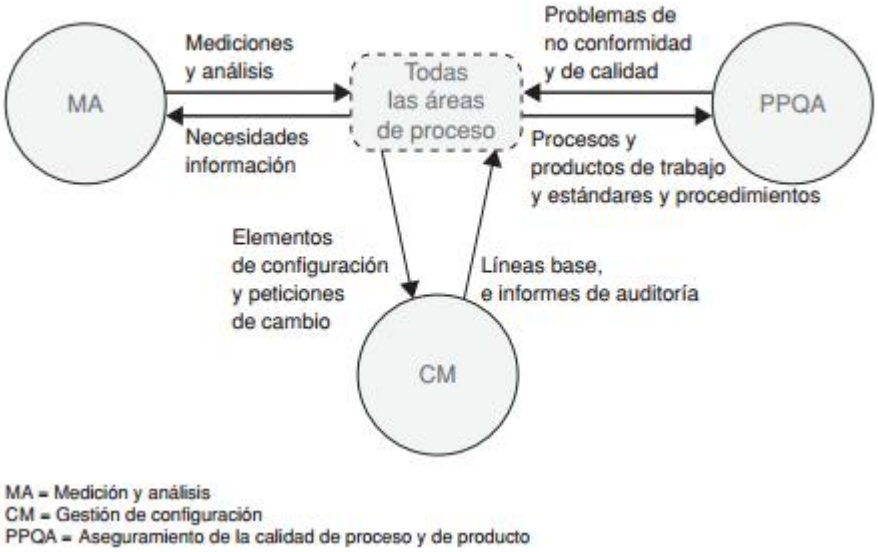


Fig. 2.7 Áreas de proceso de soporte básicas

El área de proceso de Aseguramiento de la calidad de proceso y de producto da soporte a todas las áreas de proceso, proporcionando prácticas específicas para evaluar objetivamente los procesos, los productos de trabajo y los servicios realizados frente a las descripciones aplicables de procesos, estándares y procedimientos, y para asegurar que cualquier problema planteado en estas revisiones tiene un tratamiento adecuado. El aseguramiento de la calidad de proceso y de producto da soporte a la entrega de productos y servicios de alta calidad proporcionando al personal del proyecto y a todos los niveles de gerencia la visibilidad apropiada, y una realimentación, sobre los procesos y productos de trabajo asociados a lo largo de la vida del proyecto.

Áreas de proceso de Soporte avanzadas

Las áreas de proceso de Soporte Avanzadas proporcionan a los proyectos y a la organización una capacidad de soporte mejorada. Cada una de estas áreas de proceso se apoya en las entradas o prácticas específicas de otras áreas de proceso.

La Figura 2.7 proporciona una visión general de las interacciones entre las áreas de proceso de Soporte Avanzadas y con todas las demás área de proceso.

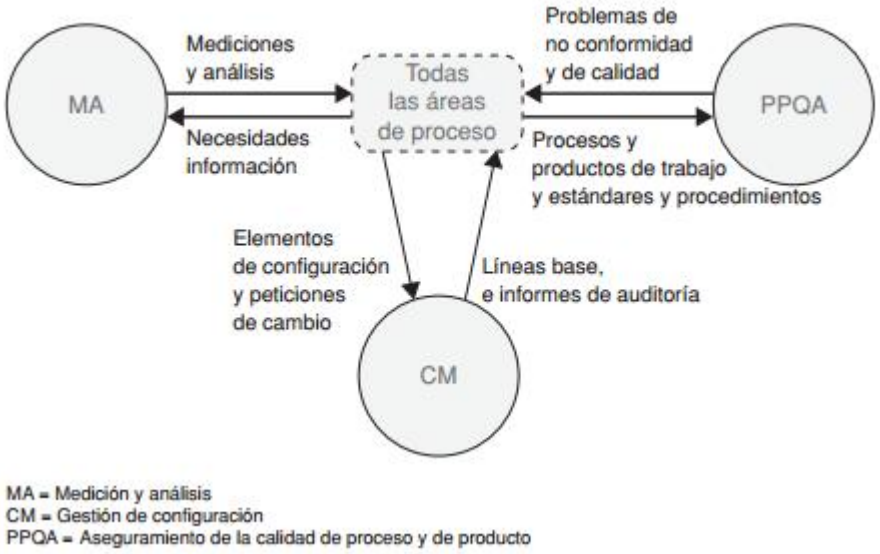


Fig. 2.8 Áreas de proceso de Soporte avanzadas

Usando el área de proceso de Análisis causal y resolución, los miembros del proyecto identifican las causas de los defectos y otros problemas seleccionados, y toman acciones para prevenir su ocurrencia en el futuro. Mientras que los procesos definidos del proyecto son los principales puntos de mira para identificar la causa del defecto, las propuestas de mejora de procesos que éstos generan van encaminadas al conjunto de procesos estándar de la organización, lo que prevendrá la reaparición del defecto en la organización.

El área de proceso de Análisis de decisiones y resolución da soporte a todas las áreas de proceso, determinando qué problemas deberían estar sujetos a un proceso de evaluación formal para luego aplicarles dicho proceso de evaluación formal. La complejidad de los productos actuales demanda una visión integrada de cómo realizan su negocio las organizaciones. CMMI puede reducir el coste de la mejora de procesos en las empresas que dependen de múltiples funciones o grupos para producir productos y servicios. Para lograr esta visión integrada, el marco de CMMI incluye una terminología común, componentes del modelo comunes, métodos de evaluación comunes y material de formación común. Este capítulo describe cómo las organizaciones pueden usar el conjunto de productos CMMI no solamente para mejorar su calidad, reducir sus costos y optimizar sus calendarios, sino también para calibrar cómo está funcionando su programa de mejora de procesos.

La investigación ha mostrado que la etapa inicial más poderosa para la mejora de procesos es construir un fuerte soporte de la organización mediante un fuerte patrocinio de la dirección. Para obtener el patrocinio de la dirección, es a menudo beneficioso exponer a la dirección los resultados de rendimiento experimentados por otros que han usado CMMI para mejorar sus procesos.

2.5 ISO 9001

Esta norma internacional especifica los requisitos para un sistema de gestión de calidad, cuando una organización necesita demostrar su capacidad para proporcionar de forma coherente productos que satisfagan los requisitos del cliente y los reglamentos aplicables. Y aspira a aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema, incluyendo los procesos para la mejora del sistema y el aseguramiento de la conformidad con los requisitos del cliente y los reglamentos aplicables.

La ISO 9001 se puede aplicar en cualquier tipo de organización, ya sea con o sin fines de lucro, pública, manufacturera o de servicios, grande, mediana o pequeña.

¿Qué se requiere para iniciar un proceso de gestión de calidad?

- ✓ Compromiso y participación de la alta dirección.
- ✓ Involucramiento de todos los empleados, comunicación, capacitación de todos los departamentos de la organización, Disponibilidad de recursos para la implementación del SGC (responsable designado, tiempo, dinero, instalaciones, etc).
- ✓ Clara definición de responsabilidades.
- ✓ Entender los requisitos de los clientes.
- ✓ Determinar la política de calidad y los objetivos de calidad (desarrollar un plan de calidad).
- ✓ Organización de la documentación existente.
- ✓ Diseño e Implementación de mecanismos para la mejora continua.
- ✓ Definición, planificación e implementación de actividades de medición.

Debido al reducido énfasis sobre la documentación, también cambió el enfoque de auditoría. Mientras en el pasado existía la percepción de que las auditorías de certificación se enfocaban primeramente en el estricto cumplimiento de los requisitos de la documentación de la norma, las auditorías ahora se deben concentrar en la verificación de que se tenga una visión común de los procesos de la organización, que estos se lleven a cabo bajo las condiciones controladas y que se estén logrando los resultados esperados.

Se evalúa la eficacia del SGC como resultado de la aplicación del modelo del proceso "Planificar-Hacer-Verificar-Ajustar", y el logro de los objetivos de la organización y la conformidad de sus productos o servicios con los requisitos del cliente y los requisitos legales y regulatorios aplicables.

La organización debe establecer, documentar, implementar y mantener un sistema de gestión de calidad y mejorar continuamente su eficacia

La organización debe

a) Identificar los procesos necesarios para el sistema de gestión de calidad y su aplicación a través de la organización.
b) Determinar la secuencia e iteración de estos procesos
c) Determinar los criterios y métodos necesarios para asegurarse de que tanto la operación como el control de estos procesos sean eficaces.
d) Asegurarse de la disponibilidad de los recursos e información necesarios para apoyar la operación y seguimiento de los procesos.
e) Realizar el seguimiento, la medición y el análisis de estos procesos.
f) Implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de estos procesos.

Cada organización determina el alcance de la documentación dependiendo del tamaño de la misma y de sus actividades, la complejidad de sus procesos y como están entre-lazados, la competencia del personal, así como los requisitos de los clientes, los legales y los regulatorios, y hasta que punto es necesario demostrar cumplimiento con los requisitos del Sistema de Gestión de Calidad.

Plan de Calidad: describe como el Sistema de Gestión de Calidad aplica a un producto, proyecto o contrato especifico

Especificaciones: Describen los requisitos

Guías: Proporciona recomendaciones o sugerencias.

Instrucciones de trabajo, dibujos: Proporcionan Información sobre como desarrollar ciertas actividades y procesos de manera consistente.

Control de Registros

Los registros deben establecerse y mantenerse para proporcionar evidencia de la conformidad con los requisitos así como la operación eficaz del sistema de gestión de calidad.

- ✓ Los registros deben permanecer legibles, fácilmente identificables y recuperables.

- ✓ Debe establecerse un procedimiento documentado para definir los controles necesarios para; la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros

2.6 ISO 27001

Especifica los requerimientos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en el contexto de la actividad general de la organización y el riesgo al que se enfrenta.

Esta norma Internacional ha sido preparada para proporcionar un modelo que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).La adopción de un SGSI debe ser una decisión estratégica para la organización. El diseño e implementación del SGSI de una organización está influenciado por sus necesidades y objetivos, requisitos de seguridad, los procesos empleados y el tamaño de la estructura de la organización, los cuales, al igual que sus sistemas de soporte se prevé que cambien con el tiempo. Se espera que la escala de implantación de un SGSI se establezca de acuerdo a las necesidades de la organización, es decir, una situación sencilla requiere una solución de SGSI sencilla.

La presente Norma Internacional puede utilizarse para evaluar el cumplimiento por las partes interesadas, interna y externa

Enfoque de proceso

Esta Norma internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. Una organización necesita identificar y administrar muchas actividades a fin de funcionar eficazmente. Cualquier actividad que utilice recursos y se administre con el fin de permitir la transformación de entradas en salidas, puede considerarse como un proceso.

Con frecuencia la salida de un proceso forma directamente la entrada del proceso siguiente. A la aplicación de un sistema de procesos dentro de una organización conjuntamente con la identificación e interacciones de estos procesos, y su administración, se le puede denominar como un “enfoque de proceso”. El enfoque de proceso para gestión de seguridad de la información presentada en esta Norma Internacional, alienta a que sus usuarios resalten la importancia de:

- ✓ la comprensión de los requisitos de seguridad de la información de una organización y la necesidad de establecer políticas y objetivos de seguridad de la información;
- ✓ implementar y operar controles para manejar los riesgos de seguridad de la información de una organización dentro del contexto de riesgos totales de negocios de la misma;
- ✓ monitorear y revisar al desempeño y efectividad del SGSI; y
- ✓ mejoramiento continuo basado en la medición de los objetivos.

Esta Norma Internacional adopta el modelo de "Planear-Hacer-Comprobar-Actuar", el cual se describe a continuación

- ➢ Planear: Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes para gestionar el riesgo y mejorar la seguridad de la información, a fin de entregar resultados conforme a las políticas y objetivos generales de la organización.
- ➢ Hacer: Implementar y operar la política, controles, procesos y procedimientos del SGSI.
- ➢ Comprobar: Evaluar y donde corresponda, medir el desempeño del proceso según la política, objetivos y experiencia práctica del SGSI y el examen de la gerencia u otra información pertinente, para lograr el mejoramiento continuo del SGSI.

Alcance

Esta norma puede aplicarse a todos los tipos de organizaciones (empresas comerciales, agencias gubernamentales, organizaciones no comerciales). Esta norma internacional especifica los requisitos para implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de riesgos totales de negocios de una organización. Especifica requisitos para la implementación de controles de seguridad adaptados a las necesidades de organizaciones individuales o partes de las mismas.

Sistema de Gestión de Seguridad de la Información (SGSI). Aquella parte del sistema gerencial general, el cual incluye: la estructura organizacional, actividades de planeación, responsabilidades, políticas, procedimientos, procesos y recursos.

2.7 BSC

Proceso que permita planear, administrar, medir y comunicar la capacidad de la organización para crear valor y lograr la visión. Este proceso se conoce como Proceso Estratégico, y abarca desde la definición de las estrategias, la comunicación de las mismas, la implantación y su administración como un proceso continuo. Una herramienta que ayuda a la Dirección General de las empresas e instituciones en la conducción de todo el Proceso Estratégico es el Balanced Scorecard.

Éste es un sistema de gestión (no sólo un sistema de medición) que permite ubicar la estrategia en el centro del proceso, trayendo como consecuencia que las organizaciones puedan aclarar y formular su visión y estrategia y traducirla en acciones.

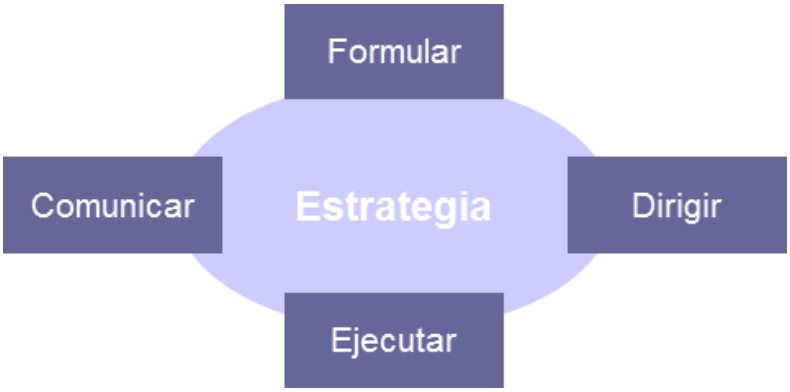


Fig. 2.9. Estrategia del BSC

Beneficios del BSC

Conducir el Proceso Estratégico apoyándose en el BSC permite:

- Alinear toda la organización en torno a la estrategia, ya que ésta se lleva del nivel ejecutivo de la organización a los procesos o funciones y de allí a las personas.
- Articular los objetivos estratégicos a través de la identificación de relaciones causa-efecto, lo que evita tener esfuerzos aislados.
- Medir la estrategia a través de la definición de métricas y metas para cada objetivo estratégico.
- Comunicar la estrategia más fácilmente al traducirla en aspectos operacionales y relevantes para cada persona.
- Tener la visión de la organización en diferentes horizontes de tiempo al traducir lo estratégico en términos tácticos y operativos.

2.8 TOGAF

TOGAF ha sido desarrollada por los miembros de Open Group como un método y conjunto de herramientas para desarrollar arquitectura de empresas que permite evaluar las fortalezas y debilidades, y así poder trazar estrategias de transformación, desde la Arquitectura actual hacia un modelo Arquitectónico que represente la visión de TI. Es un framework de Arquitectura Empresarial que proporciona un enfoque para el diseño, planeación, implementación y gobierno de una arquitectura empresarial de información. Se ha convertido en el paradigma con mayor aceptación para desarrollar arquitecturas empresariales. No sólo es un marco para categorizar los elementos que hay que capturar, sino que también define un método para hacer las cosas (Architecture Development Method), el cual define cómo desarrollar, implementar y mantener una arquitectura empresarial así como facilitar al equipo de arquitectos, definir el estado actual y futuro de la arquitectura.

Arquitectura de Negocios; se encarga definir la estrategia de negocios, la gobernabilidad, la estructura y los procesos clave de la organización. Provee un mapa (blueprint) para cada uno de los sistemas de aplicación que se requiere implantar, las interacciones entre estos sistemas y sus relaciones con los procesos de negocio centrales de la organización.

Arquitectura de Datos; describe la estructura de los datos físicos y lógicos de la organización, y los recursos de gestión de estos datos. Arquitectura Tecnológica, la cual describe la estructura de hardware, software y redes requerida para dar soporte a la implantación de las aplicaciones principales, de misión crítica, de la organización.

No obstante, TOGAF tiene una definición propia de lo que es una arquitectura, que en resumen la define como la siguiente "una descripción formal de un sistema, o un plan detallado del sistema a nivel de sus componentes que guía su implementación"[2.7], o "la estructura de componentes, sus interrelaciones, y los principios y guías que gobiernan su diseño y evolución a lo largo del tiempo [2.8]

El método más conocido como ADM “Architecture Development Method” es el método definido por TOGAF para el desarrollo de una arquitectura empresarial que cumpla con las necesidades empresariales y de tecnologías de la información de una organización.

El proceso es iterativo y cíclico. Cada paso inicia con la verificación de los requerimientos. La fase C involucra una combinación de Arquitectura de Datos y **Arquitectura de Aplicaciones.**

Cuando usted está construyendo una aplicación para un propósito muy específico --- por ejemplo, procesamiento de un cargo a una cuenta - usted sabe lo que tiene que hacer y cómo tiene que hacerlo. Su arquitectura puede ser sencilla, incluso simple. En el caso de las aplicaciones empresariales, sin embargo, una gran cantidad de pensamiento tiene que ir al igual que En el caso de grandes proyectos, la persona que realiza este pensamiento suele ser un arquitecto de TI. Esta persona es responsable de traducir los requerimientos del negocio en los requisitos de software. Para proyectos pequeños y las pequeñas empresas, esto puede ser una tarea muy sencilla. En el caso de grandes empresas, sin embargo, esta tarea puede ser francamente compleja. Afortunadamente, hay ayuda. TOGAF, proporciona una metodología para el análisis de su situación específica y crucial que el análisis de los artefactos en acciones concretas.

Definir la arquitectura de TI, no se trata de aplicaciones de la empresa, se trata de hacer que funcione la arquitectura a nivel de empresa. En muchas de las empresas los arquitectos de TI se están moviendo en la oficina de la estrategia corporativa y los departamentos de planificación. La empresa considera la arquitectura empresarial y técnica de la empresa, crea una visión estratégica, y lleva a cabo esa visión a través de la aplicación. Este trabajo no se limita al software, sino que se extiende a los sistemas completos de pensamiento dentro de la empresa. Incluso una sencilla aplicación es necesario crear, implementar, y se rige en el contexto de la arquitectura de toda la empresa.

La mayoría de desarrolladores reconocen la necesidad de una planificación previa. Sin embargo, muchos desarrolladores no entienden el nivel en el que este trabajo se lleva a cabo la arquitectura. A menudo, los que están familiarizados con la idea de la planificación de una aplicación, pero la planificación de la empresa requiere de un diferente conjunto de habilidades.

"El papel del arquitecto de TI debe ser capaz de entender el problema de negocio y el dominio del negocio y explicar a los técnicos, y ser capaz de entender los dominios tecnológicos y explicar las posibilidades técnicas para la gente de negocios. O en el ámbito civil noción de la arquitectura, es el arquitecto que puede explicar al comprador, la persona que está financiando un edificio o una ciudad, "Estas son las posibilidades de cómo se puede construir este edificio." El arquitecto finalmente viene con los planos para dar al constructor y le dice: 'Bueno, esto es lo que los propietarios de este edificio quiere. Aquí está la forma en que desea que este edificio construido, aquí están las

características que desean en este edificio. “Es importante tener a alguien con experiencia en tecnología de TI para cumplir esa función, porque su papel es esencialmente como el jefe técnico del equipo “.

Teniendo en cuenta que, los conocimientos técnicos son una necesidad, no importa donde un arquitecto de TI comienza. "Un arquitecto de buen edificio necesita saber la resistencia estructural del acero antes de diseñar en ella,"

Así que ahí tienen una definición general de la función de la arquitectura de TI. Pero, ¿qué, te preguntarás, es TOGAF?

Originalmente diseñado como un medio para desarrollar la arquitectura de la tecnología de una organización, TOGAF se ha convertido en una metodología para el análisis de la arquitectura general de la empresa. La primera parte de TOGAF es una metodología para desarrollar el diseño de su arquitectura, que se llama el Método de Desarrollo de la Arquitectura (ADM).

Tiene las siguientes nueve fases básicas:

Fase preliminar: Marco y los principios. Que todo el mundo a bordo con el plan.

- Fase A: La visión de la arquitectura. Defina su alcance y la visión y planifica tu estrategia global.
- Fase B: la arquitectura de negocios. Describa sus arquitecturas de negocio actuales y el objetivo y determinar la distancia entre ellos.
- Fase C: Arquitecturas de sistemas de información. Desarrollar arquitecturas de destino para sus datos y aplicaciones.
- Fase D: arquitectura de la tecnología. Crear la arquitectura general de selección que se implementará en fases futuras.
- Fase E: Oportunidades y soluciones. Desarrollar la estrategia general, la determinación de lo que va a comprar, construir o volver a utilizar, y cómo va a implementar la arquitectura descrita en la fase D.
- Fase F: planificación de la migración. Priorizar proyectos y desarrollar el plan de migración.
- Fase G: Aplicación de la gobernabilidad. Determine cómo va a proporcionar la supervisión de la aplicación.
- Fase H: Gestión de la Arquitectura cambio. Supervisar el sistema en funcionamiento para los cambios necesarios y determinar si se debe iniciar un nuevo ciclo o regresar a la fase preliminar.

Estas fases proporcionan una forma estandarizada de analizar la empresa y la planificación y la gestión de la aplicación real.

La segunda parte importante de TOGAF es el proceso continuo de empresa. Esta colección de bloques de construcción arquitectónicos y modelos le permiten no sólo construir su diseño de arquitectura con más facilidad, sino también para eliminar la ambigüedad cuando se habla de varios conceptos y elementos que intervienen en el análisis y la aplicación - que puede ser un problema incluso entre los grupos dentro de una sola organización.

Un punto común de confusión sobre TOGAF es que no es en realidad una arquitectura, sino más bien un marco para diseñar y describir una arquitectura. "Un marco arquitectónico es, en esencia, un sistema de clasificación para las descripciones arquitectónicas", explica David. "Además, TOGAF es un método de desarrollo de la arquitectura. El método proporciona el proceso de implementar un arquitecto para llegar a los artefactos descriptivos que pueblan un marco arquitectónico."

En otras palabras, en lugar de ayudar a describir una determinada arquitectura orientada a servicios (SOA) del sistema, por ejemplo, TOGAF puede ayudarle a decidir si SOA es el adecuado para el proyecto en absoluto. La metodología TOGAF ayuda a extraer el arquitecto del proyecto hasta el punto que puede ser una decisión tomada acerca como un estilo arquitectónico puede ser mejor aplicado para resolver el problema original del arquitecto.

Si todo esto suena como TOGAF es en gran medida de una metodología de arriba hacia abajo, tienes razón. Al igual que con todos los métodos de arriba hacia abajo, se inicia con el cuadro grande y lo divide en pedazos cada vez más pequeños. Pero TOGAF se destina a ser un método genérico, una que funciona con cualquier arquitectura. ¿Qué sucede cuando usted está usando un más de abajo hacia arriba estilo, tales como SOA [2.9], que comienza con funciones específicas y se basa en un sistema más grande?

Lo que ocurre es la clásica discusión de "arriba hacia abajo contra la de abajo hacia arriba". Es un debate que empuja a uno de los botones de acceso directo. Cuando empezamos a hablar de arquitectura, realmente estábamos hablando de la arquitectura de aplicaciones, de los programas en lugar de la arquitectura de los sistemas o de la empresa o de los sistemas de negocios que estamos tratando ahora. Así TOGAF es mucho más centrado en la arquitectura empresarial, la arquitectura de sistemas, y cómo se relacionan con el negocio de los requisitos de la empresa”.

La arquitectura de negocios y arquitectura empresarial y la creación de artefactos se enlazan con la arquitectura del sistema. Así que es muy probable que haya una abundante cosecha de los arquitectos en el futuro, es decir, personas que entienden el negocio, los procesos de negocio y requerimientos de la industria y que puede traducirse en artefactos para definir el diseño y desarrollo de la infraestructura de TI. Así que usted puede incluso ver una situación en la que los arquitectos y arquitectos de la empresa de negocios trabajando juntos para crear activos que son luego entregados a las tiendas de subcontratación u otras personas que simplemente se traducen en la infraestructura de TI.

TOGAF es importante para la empresa arquitecto de TI por una sencilla razón: se necesita. Las grandes organizaciones ya no pueden darse el lujo de crear aplicaciones aisladas que realizan funciones individuales y no se comunican con otras aplicaciones. Tampoco pueden ignorar el efecto que las condiciones reales de negocio tienen en sus necesidades de tecnología. Arquitectura empresarial está interviniendo para proporcionar el enlace entre una empresa y su infraestructura tecnológica, y TOGAF proporciona una forma estándar, utilizando las mejores prácticas, para que ese enlace. Los arquitectos y desarrolladores que quieren ser arquitectos pueden aprovechar TOGAF ahora, haciéndose más eficaz y más útil en la industria, tanto hoy como en el futuro.

2.9 PMBOK

El Project Management Body of Knowledge (Libro de estándares para la Gestión de Proyectos) Es el conjunto de conocimientos en Dirección, Gestión y Administración de Proyectos, la guía PMBOK comprende dos grandes secciones, la primera sobre los procesos y contextos de un proyecto, la segunda sobre las áreas de conocimientos específicos para la gestión de un proyecto.

El incremento en la aceptación de la Administración de Proyectos indica que la aplicación apropiada de conocimiento, procesos, habilidades técnicas, tienen un impacto significativo en el éxito del proyecto.

Los proyectos se llevan a cabo en un contexto más amplio de sus propios límites, por lo que es importante considerar: la estructura del proyecto, impacto del trabajo operativo, la influencia de los interesados en el proyecto, la estructura organizacional.

Gobernabilidad del proyecto a través del ciclo de vida

- Determina quién autoriza los cambios de alcance.
- Debe ser descrita en el Plan de Administración del Proyecto.

- Debe enmarcarse dentro del contexto del programa o de la organización patrocinadora.
- Las limitaciones de tiempo y dinero, se debe determinar el mejor método de realización del proyecto.
- Si hay más de una fase implicada, especificar la estructura del proyecto individual.
- Se debe realizar una revisión administrativa al inicio de cada fase, sobre todo si no ha concluido la anterior.

Entre los interesados clave en el proyecto se encuentran:

- **Administradores de programas**: Responsables por la administración relativa a proyectos coordinados con un objetivo común.

- **PMO**: Puede ser un interesado en el proyecto si tiene responsabilidad directa o indirecta con el resultado del proyecto. Interesados en el Proyecto

- PM: Debe ser capaz de entender el detalle del proyecto y administrarlo desde una perspectiva integral.

- Equipo de proyecto: Es un equipo compuesto por el PM, el equipo de administración del proyecto y el grupo que realiza el trabajo del proyecto.

Interesados en el Proyecto: Entre los interesados clave en el proyecto se encuentran:

- Administradores funcionales: Individuos con llaves que tienen un roll administrativo o funcional en las áreas de negocio RH, Finanzas, Contabilidad, Compras, etc.

- Administradores operativos: Individuos con un rol administrativo en un área productiva de negocio: Investigación y Desarrollo, Diseño, Manufactura, Capacitación, etc.

- Proveedores/Socios de negocio: Compañías externas que se integrarán con un acuerdo contractual para proveer un servicio o componente necesario para el proyecto.

La cultura organizacional, el estilo y la estructura incluyen en el desempeño de los proyectos. Influye también el grado de madurez y sus sistemas para la Administración de Proyectos, cuando el proyecto incluye entidades externas como una alianza o sociedad, será influenciado por más de una empresa.

A continuación se presentan los siguientes cuadros comparativos para cada Mejor práctica y se compara con la metodología MAAGTIC-SI.

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
COBIT	Garantizar que los procesos de TI soporten las metas de negocio, optimicen la inversión del negocio de TI y administre de forma adecuada los riesgos y oportunidades asociados a TI	Eficiencia Confidencialidad Integridad Disponibilidad Cumplimiento Confiabilidad	Dirección	Procesos del dominio Planear y Organizar (PO)
				P01 Definir el plan estratégico
				P02 Definir la arquitectura de información
				P03 Determinar la dirección tecnológica
				P04 Definir procesos, organización y relaciones de TI
				P05 Administrar la inversión en TI
				P06 Comunicar las aspiraciones y la dirección de la gerencia
				P07 Administrar los recursos humanos de TI
				P08 Administrar la calidad
				P09 Evaluar y administrar los riesgos de TI
				P010 Administrar proyectos
				Procesos del dominio Adquirir e Implementar (AI)
				A1 Identificar soluciones automatizadas
				A2 Adquirir y mantener el software aplicativo
				A4 Facilitar la operación y el uso
				A5 Adquirir recursos de TI
				A6 Administrar cambios
				A7 Instalar y acreditar soluciones y cambios
				Procesos del dominio entregar y dar soporte DS
				DS1Definir y administrar niveles de servicio
				DS2 Administrar servicios a terceros
				DS3 Administrar desempeño y calidad
				DS4 Garantizar la continuidad del servicio
				DS5 Garantizar la seguridad de los sistemas
				DS6 Identificar y asignar recursos
				DS7 Educar y entrenar a los usuarios
				DS8 Administrar la mesa de servicio y los incidentes
				DS9 Administrar la configuración
				DS10 Administrar los problemas
				DS11 Administrar los datos
				DS12 Administrar el ambiente físico
				DS13 Administrar las operaciones
				Procesos del dominio Monitorear y Evaluar (ME)
				ME 1 Monitorear y evaluar el desempeño de TI
				ME 2 Monitorear y evaluar el control interno
				ME 3 Garantizar el cumplimiento regulatorio
				ME 4 Proporcionar gobierno de TI

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
PMBOK	Lograr una aplicación apropiada de conocimiento, procesos, habilidades técnicas para lograr un impacto significativo en el desarrollo de cada uno de los proyectos de TI.	Dirección Gobernabilidad Administración Planeación Estratégica	Administración de Proyectos	42 procesos de dirección de proyectos con los 5 grupos de procesos de dirección de proyectos y las 9 Áreas de Conocimiento de la Dirección de Proyectos.
				Grupo de procesos de Iniciación
				3.3.1 Desarrollar el Acta de Constitución del Proyecto
				3.3.2 Identificar a los interesados
				Grupo de procesos de Planificación
				3.4.1 Desarrollar el Plan para la Dirección del Proyecto
				3.4.2 Recopilar Requisitos
				3.4.3 Definir el Alcance
				3.4.4 Crear la EDT (Estructura de Desgloce de Trabajo)
				3.4.5 Definir las Actividades
				3.4.6 Secuenciar las Actividades
				3.4.7 Estimar los Recursos de las Actividades
				3.4.8 Estimar la duración de las Actividades
				3.4.9 Desarrollar el Cronograma
				3.4.10 Estimar Costos
				3.4.11 Estimar el Presupuesto
				3.4.12 Planificar la Calidad
				3.4.13 Desarrollar el Plan de Recursos Humanos
				3.4.14 Planificar las Comunicaciones
				3.4.15 Planificar la Gestión de Riesgos
				3.4.16 Identificar Riesgos
				3.4.17 Realizar Análisis Cualitativo de Riesgos
				3.4.18 Realizar Análisis Cuantitativo de Riesgos
				3.4.19 Planificar la Respuesta a los Riesgos
				3.4.20 Planificar las Adquisiciones
				Grupo de procesos de Ejecución
				3.5.1 Dirigir y Gestionar la Ejecución del Proyecto
				3.5.2 Realizar Aseguramiento de Calidad
				3.5.3 Adquirir el Equipo del Proyecto
				3.5.4 Desarrollar el Equipo del Proyecto
				3.5.5 Dirigir el Equipo del Proyecto
				3.5.6 Distribuir la Información
				3.5.7 Gestionar las Expectativas de los Interesados
				3.5.8 Efectuar Adquisiciones
				Grupo de procesos de Seguimiento y Control
				3.6.1 Dar Seguimiento y Controlar el Trabajo del Proyecto
				3.6.2 Realizar Control Integrado de Cambios
				3.6.3 Verificar al Alcance
				3.6.4 Controlar el Alcance
				3.6.5 Controlar el Cronograma
				3.6.6 Controlar Costos
				3.6.7 Realizar Control de Calidad
				3.6.8 Informar el Desempeño
				3.6.9 Dar Seguimiento y Controlar los Riesgos
				3.6.10 Administrar las Adquisiciones
				Grupo de procesos de Cierre
				3.7.1 Cerrar el Proyecto o Fase
				3.7.2 Cerrar las Adquisiciones
Metodología	**Objetivo**	**Criterios de Evaluación**	**Rubros**	Procesos
ISO 9001	La organización debe establecer, documentar, implementar y mantener un sistema de gestión de calidad y mejorar continuamente su eficacia.	Aseguramiento de la calidad Viabilidad Evaluación Cumplimiento	Administración de Recursos	Responsabilidad de la dirección
				Gestión de los recursos
				Realización del producto
				Medición, análisis y mejora

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
CMMI	mejora de procesos de Ingeniería de Software, ingeniería de sistemas, desarrollo de productos y adquisición de aplicaciones	Confiablidad Planificación	Administración de Procesos	Análisis causal y resolución (CAR) Gestión de configuración (CM) Análisis de decisiones y resolución (DAR) Gestión integrada del proyecto Medición y análisis Innovación y despliegue en la organización Definición de procesos en la organización Enfoque de procesos en la organización Rendimiento del proceso en la organización Formación organizativa Integración de producto Monitorización y control del proyecto Planificación de proyecto Aseguramiento de la calidad de proceso y de producto Gestión cuantitativa de proyecto Desarrollo de requerimientos Gestión de requerimientos Gestión de riesgos Gestión de acuerdos con proveedores Solución técnica Validación Verificación

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
ITIL	Mejorar la calidad del servicio tanto a clientes externos como internos y aprovechar al máximo las habilidades y experiencia del personal mejorando su producto vidad	Gobernabilidad Calidad de los servicios Nivel de los Servicios		Procesos de Soporte de Servicios Administración de Incidentes Administración de Problemas Administración de Configuración Administración de Cambios Administración de Liberaciones Función de mesa de Servicios Procesos de Entrega de Servicios Administración de Niveles de Servicio Administración de Disponibilidad Administración de Capacidad Administración de Continuidad de servicios de TI Administración Financiera de Servicios de TI

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
BSC	Planear, administrar, medir y comunicar la capacidad de la organización para crear valor y lograr la visión. Este proceso se conoce como Proceso Estratégico, y abarca desde la definición de las estrategias, la comunicación de las mismas, la implantación y su administración como un proceso continuo.	Eficiencia Comunicación Integración Planeación Estratégica	Administración del Desarrollo de Soluciones	Procesos de innovación
				Procesos Operativos
				Servicios de Venta

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
ISO 27001	Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de Gestión de la Seguridad de la Información (SGSI). La cual debe ser una decisión estratégica para organización.	Disponibilidad Confidencialidad Seguridad de la Información Integridad Aceptación del riesgo Evaluación de riesgos Mejora Continua Control	Operación de Servicios	Requisitos y expectativas de la Seguridad de la Información
				Crear el SGSI
				Implementar y operar el SGSI
				Supervisar y revisar el SGSI
				Mantener y mejorar el SGSI
				Seguridad de la información gestionada

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
TOGAF	Desarrollar, implementar y mantener una arquitectura empresarial así como facilitar al equipo de desarrolladores un enfoque el cual describa la estructura de software, hardware y redes requerida para dar soporte a la implantación de aplicaciones principales.	Gobernabilidad Planificación Diseño	Administración de Activos	Visión de la Arquitectura
				Arquitectura de Negocios
				Arquitectura de Sistemas de Información
				Arquitectura de la Tecnología
				Oportunidades y Soluciones
				Planeamiento de Migración
				Implementación de Gobierno
				Desarrollo y Mantenimiento de EA
				Gestión de Requerimientos

Metodología	Objetivo	Criterios de Evaluación	Rubros	Procesos
MAAGTIC-SI	Definir los procesos que en materia de TIC y de seguridad de la información, regirán a las Instituciones, con el propósito de regular y homologar su gestión, independientemente de la estructura organizacional con que éstas cuenten.	El presente Manual es de aplicación general en las Instituciones.	Gobierno Organización y Estrategia Ejecución y Entrega Soporte	EMG- Establecimiento del Gobierno de TIC PE- Planeación Estratégica DDT- Determinación de la dirección tecnológica AE- Administración de la Evaluación ASI- Administración de la Seguridad de la Información OPEC- Operación de los controles de seguridad de la información y del ERISC APP- Administración del portafolio de proyectos de TIC APTI- Administración de Proyectos de TIC OSGP- Operación del sistema de gestión y mejora de los procesos de la UTIC APTI- Administración del Presupuesto de TIC ADTI Administración para las Contrataciones de TIC APBS Administración de Proveedores de Bienes y Servicios de TIC APS- Administración del portafolio de servicios de TIC DSTI- Diseño de Servicios de TIC ATC- Apoyo técnico para la contratación de soluciones tecnológicas de TIC DST- Desarrollo de soluciones tecnológicas CST- Calidad de soluciones tecnológicas ACMB- Administración de Cambios LE- Liberación y Entrega THO- Transición y Habilitación de la Operación ACNF- Administración de la configuración ADT- Administración de Dominios Tecnológicos ACNC- Administración del Conocimiento APC-Apoyo a la capacitación del personal de la UTIC OMS- Operación de la mesa de servicios ANS- Administración de Nieles de Servicio AO- Administración de la Operación AAF- Administración del Ambiente Físico MI- Mantenimiento de la Infraestructura ACNC- Administración del Conocimiento APC-Apoyo a la capacitación del personal de la UTIC OMS- Operación de la mesa de servicios ANS- Administración de Nieles de Servicio AO- Administración de la Operación AAF- Administración del Ambiente Físico MI- Mantenimiento de la Infraestructura

Capítulo 3. MAAGTIC-SI

Capítulo 3. MAAGTIC-SI

3.1 EMG - Establecimiento del Modelo de Gobernabilidad

En este proceso se busca determinar un modelo de gobierno de TIC en la Institución, lo cual se logrará mediante la conformación de dos grupos de trabajo encargados de realizar el análisis de las oportunidades de aprovechamiento de las TIC y asegurar la adecuada organización al interior de la UTIC [3.1] para la gestión de sus procesos.

Objetivos Específicos

- Establecer un modelo para obtener la integración y operación del Grupo de Trabajo que llevará a cabo la Dirección de TIC.
- Establecimiento de un modelo para obtener la integración y operación del Grupo de Trabajo que llevará a cabo la Estrategia de TIC.
- Determinación de roles y responsabilidades de cada área de la UTIC.

El Grupo de trabajo Estratégico de TIC opera y mantiene el modelo de gobierno de TIC esto es establecer, implementar y mantener una adecuada organización de la UTIC.

Por otro lado el Grupo de Trabajo para la Dirección de TIC determinará las acciones de gobernabilidad de TIC que implica tomar decisiones con respecto a requerimientos, inversión y gastos en materia de TIC, también deberá definir y establecer controles de gobierno para evaluar los resultados de la UTIC así como procurar una adecuada dirección y control de los procesos y servicios de TIC.

Descripción de las Actividades del Proceso

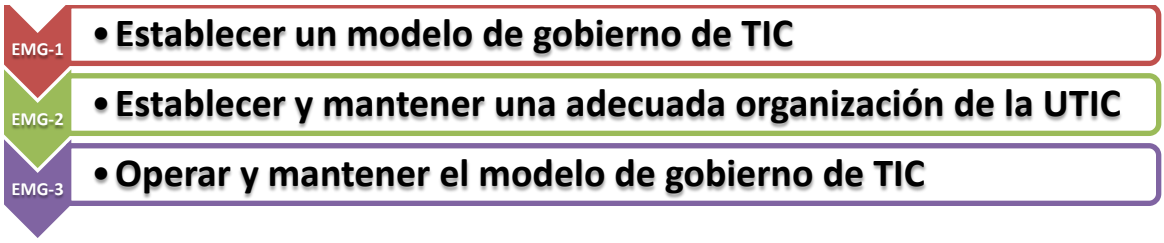


Figura 3.1 Descripción de las actividades del proceso EMG

EMG-1

El Grupo de trabajo para la Dirección de TIC establece un Documento para integración y operación de éste:

Documento que contenga los objetivos, roles y responsabilidades del Grupo de Trabajo y de su funcionamiento.

1. El primer documento tiene como objetivo establecer el Grupo de trabajo para la Dirección de TIC y asegurar que:
   a) El Documento contenga, al menos: objetivos y responsabilidades del Grupo de Trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del Grupo de trabajo.
   b) El Grupo de trabajo se integre por servidores públicos que deberán ser de alto nivel dentro de la Institución. Este grupo estará encabezado por el Titular de la UTIC.
   c) Se comuniquen los roles y responsabilidades de los integrantes del Grupo de trabajo para la dirección de TIC.
   d) Se realicen, entre otras actividades, las siguientes:
      - Determinar las oportunidades y los riesgos en el uso de TIC.
      - Determinar las prioridades de las Iniciativas de TIC alineadas con la estrategia y las prioridades institucionales.
      - Verificar que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución.
      - Evaluar el cumplimiento de los niveles de servicio establecidos para los servicios de TIC.
2. El segundo documento busca establecer el Grupo de trabajo Estratégico de TIC y asegurarse de que:
   a) El Documento contenga, al menos: los objetivos y responsabilidades del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo.
   b) El grupo se integre por servidores públicos de la UTIC. Este grupo estará encabezado por el servidor público de la UTIC que designe su Titular.
   c) Se comuniquen los roles y responsabilidades de los integrantes del Grupo de trabajo estratégico de TIC.
   d) Definir como se implementará y mantendrá una adecuada organización al interior de la UTIC, mediante la asignación de roles y responsabilidades para la gestión de los procesos, atendiendo a las necesidades para la gobernabilidad de los procesos y proyectos de la UTIC.

EMG-2

Factores críticos	
	1. Asignar roles y responsabilidades a los servidores públicos de la UTIC.
	2. Implantar la segregación de roles y responsabilidades.
	3. El Grupo de trabajo.
	4. Evaluar
	5. Comunicar a los servidores públicos de la UTIC

1. Asignar roles y responsabilidades a los servidores públicos de la UTIC

El Grupo de trabajo Estratégico de TIC debe asignar roles y responsabilidades a los servidores públicos de la UTIC, para cada proceso, delimitando con precisión su participación y teniendo en consideración sus conocimientos, experiencia y habilidades, para lo cual deberá:

a) Utilizar la matriz RACI [3.2], la cual debe incluir el cruce total de roles sobre las posibilidades de acción definidas en la matriz: responsable de la ejecución, responsable de rendir cuentas, responsable de asesorar o proporcionar consultoría y responsable de mantenerse informado.

b) Integrar la asignación de los roles y responsabilidades en el Documento de descripción de roles y responsabilidades.

2. Implantar la segregación de roles y responsabilidades

El Grupo de trabajo Estratégico de TIC debe procurar implementar la segregación de roles y responsabilidades con la finalidad de que se reduzca la posibilidad de que un solo individuo ejecute o administre un proceso o actividad crítica, mediante lo siguiente:

a) Definir los tramos de actividades a los diversos actores en cada proceso o actividad.

b) Definir las acciones para identificar y prevenir irregularidades en la gestión de los procesos, originadas por roles y responsabilidades inadecuadamente asignados, de manera que sea posible evitar discrecionalidades o errores.

c) Implementar controles para asegurar que los roles y responsabilidades se ejerzan de acuerdo a las asignaciones efectuadas.

d) Integrar la información de este factor crítico en el Documento de segregación de roles y responsabilidades.

Es recomendable usar el modelo Top-Down [3.3] para la segregación de roles ya que lo ideal es dividir por funcionalidades asignando a cada quien responsabilidades y tareas que tengan una cohesión consistente.

3. **El Grupo de trabajo**

   El Grupo de trabajo Estratégico de TIC debe supervisar la correspondencia de tareas con las asignadas.

4. **Evaluar**

   El Grupo de trabajo Estratégico de TIC debe evaluar, al menos una vez al año, la asignación de roles y responsabilidades y ajustarla, para nuevas necesidades.

5. **Comunicar a los servidores públicos de la UTIC**

   Dar a conocer a los servidores públicos de la UTIC los roles y responsabilidades asignados en esta actividad.

EMG-3

Factores Críticos	1. Tomar acuerdos
	2. Participar
	3. Aprobar el PETIC y mantenerse informado
	4. Aprobar el sistema de gestión y mejora de los procesos
	5. Establecer la coordinación necesaria con el Responsable
	6. Conocer los criterios técnicos
	7. Informar al Titular de la Institución

1. **Tomar acuerdos**

   Tomar acuerdos sobre los asuntos que en materia de TIC le sean puestos a su consideración, a través de la Lista de asuntos y acuerdos directivos.

2. **Participar en los Procesos APP y APS**

   Participar en los procesos APP [3.4] y APS [3.5], conforme se señala en los mismos.

3. **Aprobar el PETIC y mantenerse informado**

   Aprobar el PETIC [3.6] y mantenerse informado del seguimiento del mismo, conforme a lo señalado en el proceso Planeación Estratégica de TIC.

4. **Aprobar el sistema de gestión y mejora de los procesos**

   Aprobar el sistema de gestión y mejora de los procesos de la UTIC, así como los indicadores del Cuadro de mando integral de la UTIC [3.7].

5. **Establecer la coordinación necesaria con el Responsable**

Establecer la coordinación necesaria con el Responsable de seguridad de la información para armonizar el gobierno de TIC, la administración de riesgos y el SGSI [3.8].

6. **Conocer los criterios técnicos**

   Conocer los criterios técnicos que proponga el responsable de la seguridad de la información en la Institución para gestionar los riesgos.

7. **Informar al Titular de la Institución**

   Informar al Titular de la Institución acerca de los resultados, recomendaciones y acuerdos del Grupo de trabajo para la dirección de TIC.

3.2 Planeación Estratégica de TIC

En toda empresa o institución deberá existir un Plan/Programa Estratégico de Tecnologías de la Información y Comunicaciones (PETIC), con el objeto de establecer líneas de acción en materia de TIC, tomando en cuenta la Agenda de Gobierno Digital [3.9].

Objetivos Específicos

1. Identificar los objetivos y prioridades de la Institución con la finalidad de proponer proyectos eficaces e innovadores, considerando especialmente aquellos relacionados con la mejora sustancial de los trámites y los servicios públicos.
2. Análisis del entorno y de la organización para así identificar las oportunidades y riesgos para el cumplimiento de los objetivos estratégicos de la Institución en materia de TIC.
3. Establecer los mecanismos para elaborar, operar y supervisar el avance del PETIC de la Institución, especialmente en lo relativo a las estimaciones del presupuesto de la inversión por proyecto, de los beneficios esperados, de las fuentes de financiamiento y de la estrategia de adquisición.
4. Instrumentar los mecanismos para asegurar que los servidores públicos de la UTIC entiendan completamente el PETIC de la institución.
5. Impulsar el cumplimiento de los objetivos y proyectos institucionales, mediante la implementación de un mecanismo que permita dar seguimiento al PETIC.

Descripción de las Actividades del Proceso

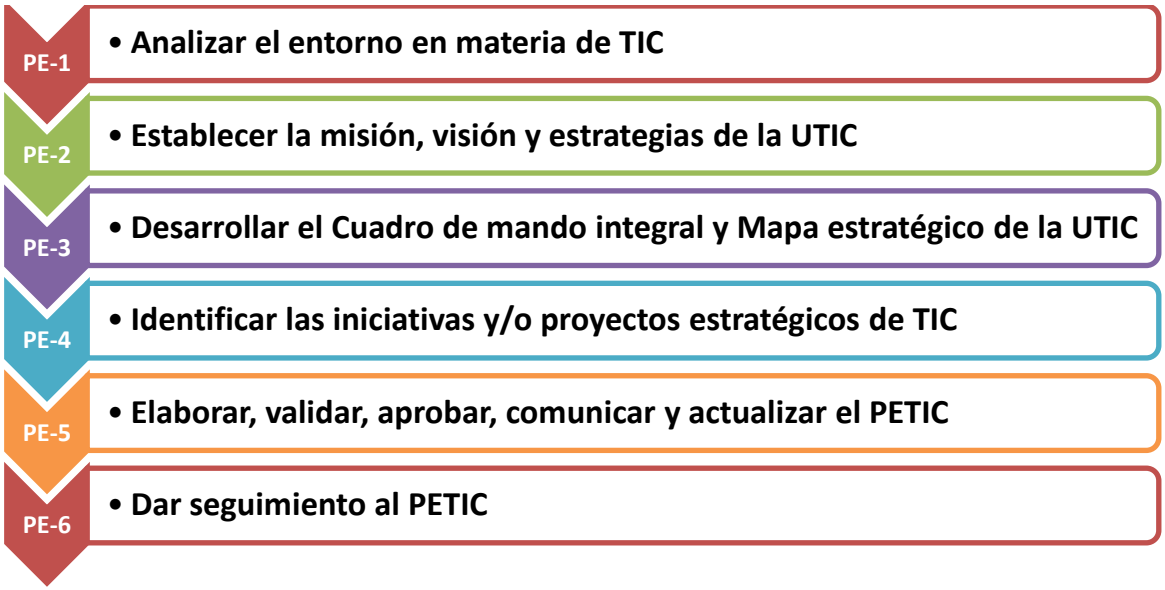


Fig. 3.2 Descripción de las actividades del proceso PE

PE-1 Analizar el entorno en materia de TIC

Identificar y analizar los factores que conforman el entorno de la Institución o empresa en materia de TIC y la situación actual.

Factores Críticos

El Responsable de la planeación estratégica de la UTIC deberá de:

1. Identificar los elementos regulatorios, normativos y tecnológicos que influyen en la ejecución de las actividades y servicios que brinda la UTIC en apoyo a las funciones sustantivas de la Institución.
2. Realizar un análisis de fortalezas, oportunidades, debilidades y amenazas que influyen en el cumplimiento de las funciones de la Institución en materia de TIC, para lo cual se deberá de considerar la Agenda de Gobierno Digital.
3. Identificar los principales hechos o eventos del ambiente externo que podrían representar alguna amenaza u oportunidad para la Institución tales como: factores legales, regulatorios, políticos, económicos, sociales, tecnológicos, entre otros.
4. Identificar las principales fortalezas y debilidades de la Institución para el cumplimiento de sus objetivos y funciones tales como: disponibilidad de recursos tecnológicos, financieros, y humanos, activos, procesos, calidad de la infraestructura y/o de servicios, estructura interna y percepción de los usuarios.

PE-2 Establecer la misión, visión y estrategias de la UTIC

Establecer y comunicar a los integrantes de la UTIC la misión, visión y estrategias, para así lograr comprender los propósitos y objetivos de la UTIC.

Factores críticos

El Grupo de trabajo para la dirección de TIC deberá de:

1. Establecer la misión de la UTIC.
    - Describir de manera clara y concreta el objetivo fundamental que persigue la UTIC, a fin de lograr el compromiso inmediato de los servidores públicos que la conforman.
2. Establecer la visión de la UTIC.
    - Describir de manera breve la situación deseada que busca alcanzar la UTIC a largo plazo, debe ser fácil de recordar y estar alineada a los objetivos estratégicos, deberá ser elaborada pensando en el escenario ideal de desempeño de manera efectiva, en el cumplimiento de sus objetivos y en la alineación de sus planes.
3. Difundir la misión y visión de la UTIC.
    - Comunicar constantemente a todos los miembros de la Institución a fin de sensibilizar a los servidores públicos para trabajar alineados a la misión y visión de la UTIC.
4. Establecer las estrategias de la UTIC a través de:
    - Analizar los resultados de la Matriz FODA [3.10].
    - Analizar los objetivos estratégicos de la Institución.

PE-3 Desarrollar el Cuadro de mando integral y Mapa estratégico de la UTIC

Diseño e implementación de un Mapa estratégico y un Cuadro de mando integral de la UTIC que abarque la perspectiva financiera, de usuario o cliente, de procesos, de desarrollo de personal y de aprendizaje, para así, establecer los objetivos y las metas de la UTIC de forma más clara y concisa.

Factores críticos

El Responsable de la planeación de la UTIC deberá:

1. Analizar la situación actual de la UTIC y obtener información.
2. Analizar y determinar las funciones sustantivas de la Institución.
3. Identificar las necesidades de TIC.
4. Diseñar un Mapa estratégico de la UTIC el cual estará sustentado por un análisis de:

- Perspectiva financiera: factores críticos que permitan tener una situación económica saludable en la UTIC; esto incluye el uso adecuado de los recursos financieros, el análisis del costo de operación de los servicios de TIC y, en su caso, la salud financiera de la UTIC.
- Perspectiva de cliente o usuario: factores críticos que permiten mantener niveles de satisfacción adecuados de los usuarios proporcionados por la Institución.
- Perspectiva de procesos: factores críticos que permitan mantener procesos y procedimientos adecuados para operar de manera efectiva, eficiente y con un adecuado nivel de control, a fin de cumplir con las necesidades de los usuarios.
- Perspectiva de desarrollo de personal y de aprendizaje: factores críticos que permitan desarrollar las capacidades de los servidores públicos de la Institución y el conocimiento necesario para ejecutar los procesos y procedimientos empleados para operar en la Institución.
- Las relaciones entre las cuatro perspectivas y la subordinación que existen entre éstas.

5. Identificar las variables e indicadores críticos en cada una de las perspectivas.
6. Establecer una correspondencia eficaz y eficiente entre las variables críticas y las acciones precisas para su control en el Mapa estratégico de la UTIC.
7. Diseñar un Cuadro de mando integral que deberá considerar:
   - Integrar la información del Mapa estratégico de la UTIC [3.11].
   - La definición de las metas y acciones que permitan cumplir los objetivos de la UTIC.
   -

PE-4 Identificar las iniciativas y/o proyectos estratégicos de TIC

Identificar las principales iniciativas y/o proyectos estratégicos de TIC que deben ser ejecutados, para cumplir con los objetivos estratégicos de la Institución que tengan relación con las TIC y con el Mapa estratégico de la UTIC.

Factores críticos

La UTIC deberá:

1. Correlacionar los objetivos estratégicos de la Institución que tengan relación con las TIC con el Mapa estratégico de la UTIC.

2. Determinar las iniciativas y/o proyectos estratégicos de TIC necesarios para cumplir con los objetivos estratégicos de la Institución que tengan relación con las TIC, para lo cual se:
   - Integrará la relación de las iniciativas y/o proyectos estratégicos de TIC priorizadas, tomando en cuenta:
     - Su relevancia para cumplir con los objetivos estratégicos que puedan aprovechar el uso de TIC.
     - El valor que podrían aportar a los ciudadanos.
     - La mejora en los trámites y servicios que presta la Institución.
3. Estimar la inversión requerida para las iniciativas y/o proyectos estratégicos de TIC.
   - Para cada iniciativa y/o proyecto estratégico de TIC, se deberá estimar el presupuesto y los recursos necesarios para su ejecución. Este presupuesto deberá considerar los recursos financieros para la contratación de los servicios, o en su caso, la adquisición, puesta en operación y mantenimiento de la solución tecnológica y/o el servicio de TIC.
   - De igual forma se deberá estimar el esfuerzo interno y los recursos necesarios para adquirir, supervisar y administrar la solución tecnológica y/o el servicio de TIC.
4. Integrar las iniciativas y/o proyectos estratégicos de TIC que hayan sido relacionadas conforme al Portafolio de proyectos [3.12] de TIC.

PE-5 Elaborar, validar, aprobar, comunicar y actualizar el PETIC

Elaborar, validar, aprobar, comunicar y actualizar el PETIC.

Factores críticos

1. La UTIC será la encargada de la elaboración del PETIC, que deberá integrar cuando menos, la información siguiente:
   a) Misión y visión de la UTIC.
   b) La Matriz FODA.
   c) Proyectos estratégicos de la UTIC que hayan sido autorizados y que se encuentren en el Portafolio de proyectos de TIC.
   d) Objetivos, descripción y beneficios de la implementación de cada proyecto estratégico de la UTIC.
   e) Riesgos e impacto de cada proyecto estratégico de la UTIC.
   f) Presupuesto estimado para cada proyecto estratégico de la UTIC.

g) Descripción de roles y responsabilidades de los servidores públicos que ejecutarán los proyectos que se señalan en el inciso c) anterior.

h) Mecanismos de seguimiento al PETIC.

Esta información o cualquier otra adicional que se determine por la UGD se deberá integrar a la herramienta de registro y seguimiento del PETIC denominada DAS-IT [3.13].

2. Revisar y validar el PETIC.
   - Deberá ser revisado y validado por el Grupo de trabajo para la dirección de TIC.
3. Aprobar y Comunicar el PETIC
   - Deberá ser aprobado y firmado por los titulares de cada Institución.
   - Una vez firmado el PETIC deberá de ser comunicado por la UTIC.
4. Actualizar el PETIC.
   - Deberá mantenerse actualizado por la UTIC cuando: la estrategia cambie significativamente, la situación externa y/o interna afecte el cumplimiento de los objetivos, se requiera afinar la estrategia definida, exista un cambio en la administración de la Institución.

PE-6 Dar seguimiento al PETIC

Dar seguimiento a los avances en el cumplimiento del PETIC.

Factores críticos

La UTIC para el seguimiento de los avances en el cumplimiento del PETIC deberá:

1. Dar seguimiento, de manera programada, al PETIC y reportar trimestralmente su avance a la UGD [3.14].
2. Informar periódicamente al Grupo de trabajo para la dirección de TIC, el cumplimiento del PETIC y la situación de los indicadores del Cuadro de mando integral.
3. Registrar y dar seguimiento a los acuerdos del Grupo de trabajo para la dirección de TIC.
4. Identificar, registrar y administrar las acciones correctivas en caso de desviación.

3.3 Determinación de la dirección tecnológica

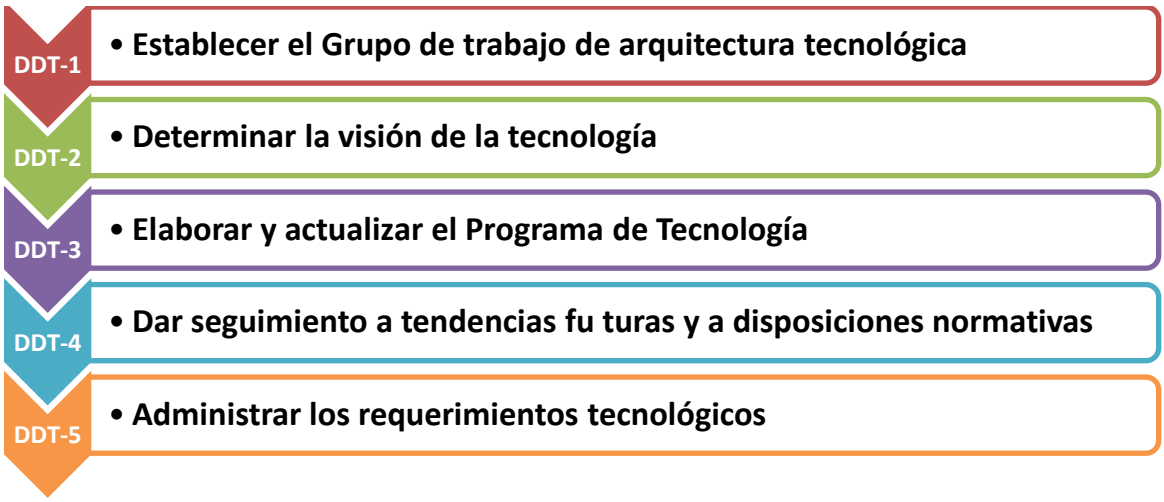


Fig. 3.3 Descripción de las actividades del proceso DDT

Determinar la dirección tecnológica de la Institución para crear un Programa de Tecnología que facilite la selección, el desarrollo, la aplicación y el uso de la infraestructura de TIC.

Objetivos Específicos

1. Determinar los requerimientos tecnológicos derivados de las necesidades de la Institución que deberán ser incorporados en el Programa de Tecnología.
2. Definir un modelo para el Programa de Tecnología que incluya la arquitectura tecnológica considerando los diversos dominios tecnológicos necesarios para estandarizar y evolucionar la infraestructura de TIC, de manera que cuente con la capacidad necesaria para satisfacer las necesidades actuales y futuras de la Institución.
3. Procurar que el Programa de Tecnología tenga un balance entre necesidades, innovación, beneficios, riesgos y costos y oriente a la Institución hacia el desarrollo de nuevas formas de cumplir con sus objetivos.

Descripción de las Actividades del Proceso

DDT-1 Establecer el Grupo de trabajo de arquitectura tecnológica

Conformar el Grupo de trabajo de arquitectura tecnológica

Factores críticos

Se establecerá un Grupo de trabajo de arquitectura en cada una de las Instituciones, integrado por servidores públicos de la UTIC.

1. La UTIC al establecer el Grupo de trabajo de arquitectura tecnológica deberá:

- Acordar y definir el rol y responsabilidades del Grupo de trabajo de arquitectura tecnológica.
- Establecer y comunicar el alcance, objetivos, roles y responsabilidades de los integrantes del Grupo de trabajo de arquitectura tecnológica.
- Determinar la visión de la tecnología.
- Elaborar y actualizar el Programa de Tecnología.
- Dar seguimiento a tendencias futuras y a disposiciones normativas.
- Administrar los requerimientos tecnológicos.

DDT-2 Determinar la visión de la tecnología

Analizar las tecnologías existentes y emergentes; planear cuál dirección tecnológica es la apropiada para materializar los objetivos y estrategias, y proveer los servicios de información acordes a los requerimientos de la Institución.

Factores críticos

1. Definir los requerimientos tecnológicos derivados de las necesidades, objetivos, estrategias, proyectos y servicios de la Institución que deberán ser soportados por la dirección tecnológica que se defina.
2. Traducir los requerimientos tecnológicos en términos de directrices rectoras para la arquitectura tecnológica.
3. Definir el alcance, estructura y nivel de detalle de los dominios descritos en el proceso de Administración de dominios tecnológicos, a fin de determinar una arquitectura tecnológica, los cuales estarán definidos en los niveles siguientes:
   - Arquitectura de datos/información: La descripción de la estructura de los datos físicos y lógicos de la Institución y los recursos de gestión de dichos datos.

     Dicha descripción debe contener, entre otras cosas: el ciclo de vida integral de la información, la forma de registro, actualización y distribución de la información.
   - Arquitectura de aplicaciones: El modelo que contiene las aplicaciones que la Institución requiere para soportar sus capacidades sustantivas; la forma en que estarán organizadas, y como estarán relacionadas.
   - Arquitectura de infraestructura tecnológica: La definición de los marcos técnicos de referencia, principios, modelos, estándares, entre otros; necesarios para gobernar los recursos tecnológicos en la provisión de los servicios de TIC.

- Arquitectura de negocio: La definición de entregables relativos a la información, contexto y requerimientos tecnológicos necesarios para sostener los cambios en los procesos sustantivos o, causados por modificaciones de estrategia o metas.

4. Los niveles antes mencionados deberán ser consistentes con los niveles de detalle necesarios para sustentar los requerimientos tecnológicos determinados. Realizar regularmente un análisis de FODA de todos los elementos críticos de la arquitectura tecnológica.
5. Dar seguimiento a la evolución del mercado y de las tecnologías emergentes con el propósito de identificar las tecnologías de punta que puedan ser aprovechables.
6. Realizar la selección de las áreas y tópicos de investigación de TIC, en función de las iniciativas y/o proyectos de TIC identificados y/o de los requerimientos tecnológicos identificados.
7. Compilar las investigaciones en materia de TIC, a fin de establecer posibles directrices rectoras.
8. Determinar las directrices rectoras para la arquitectura tecnológica.

DDT-3 Elaborar y actualizar el Programa de Tecnología

Elaborar y actualizar el Programa de Tecnología acorde con los objetivos estratégicos y tácticos de la UTIC. El programa se basa en la dirección tecnológica e incluye directrices para la adquisición de recursos tecnológicos y toma en cuenta los cambios en la tecnología.

Factores críticos

1. Elaborar el Programa de Tecnología basado en un análisis por cada uno de los dominios antes señalados que contendrá:
   - La descripción del estado actual de los componentes de cada dominio para establecer una línea base que sustente la planeación.
   - Las descripciones de la arquitectura tecnológica que se desea para cada uno de los dominios, conforme a la visión tecnológica de la Institución.
   - La información de la selección de las perspectivas de la arquitectura tecnológica que se desea, de forma que demuestre que da respuesta a los requerimientos tecnológicos y a los objetivos esperados por las unidades responsables en un plazo determinado.

- Un estudio de las brechas entre la arquitectura tecnológica en operación y la arquitectura tecnológica que se desea.
- La definición de la arquitectura tecnológica que se desea y de ser necesario la definición de arquitecturas tecnológicas de transición como etapas intermedias para llegar a la arquitectura tecnológica deseada.

2. Integrar en el Programa de Tecnología las arquitecturas tecnológicas de cada uno de los dominios tecnológicos antes señalados, lo cual permitirá:
   - Visualizar cómo los componentes de tecnología se integran en un enfoque sistémico.
   - Plantear modelos arquitectónicos tecnológicos enfocados en la capacidad de la Institución.
   - Definir los estándares que habilitarán la integración de componentes para maximizar su reutilización y potenciar su interoperabilidad.
   - Asegurar que las descripciones de los diferentes dominios antes mencionados pueden combinarse en una sola representación lógica.
3. Evaluar y seleccionar la alternativa de implementación de las arquitecturas tecnológicas deseadas que conforman el Programa de Tecnología, por medio de los factores críticos para la transición y las iniciativas de TIC y/o proyectos de tecnología requeridos para pasar del estado actual al deseado, así como evaluar las correlaciones, costos y beneficios de las distintas alternativas.
4. Integrar las iniciativas de TIC y/o los proyectos de tecnología al Programa de Tecnología de manera que se considere la prioridad, el orden, las interdependencias y los beneficios de las mismas.
5. Incluir en el Programa de Tecnología los costos relacionados con las iniciativas de TIC de TIC y/o los proyectos de tecnología y otros costos derivados de la estrategia de transformación, riesgos tecnológicos, y las mejoras esperadas en la interoperabilidad de plataformas y aplicaciones.
6. Someter a evaluación, selección y autorización el Programa de Tecnología, así como las iniciativas de TIC y/o los proyectos de tecnología al proceso de Administración de portafolio de proyectos de TIC.
7. Revisar el Programa de Tecnología de acuerdo a las iniciativas de TIC y/o los proyectos de tecnología autorizados.
8. Dar seguimiento a la implementación del Programa de Tecnología.
9. Revisar y actualizar periódicamente el Programa de Tecnología.

10. Procurar que todos los grupos de trabajo involucrados participen en el desarrollo y aprobación de los proyectos de migración y de cambio que se realicen para la transición de la arquitectura tecnológica.
11. Establecer un proceso de Control de cambios en la arquitectura tecnológica, conforme al proceso Administración de cambios.
12. Determinar las condiciones bajo las cuales los componentes arquitectónicos tecnológicos podrían cambiarse una vez implementados, así como aquéllas para iniciar el ciclo de actualización de la arquitectura tecnológica.

DDT-4 Dar seguimiento a tendencias fu turas y a disposiciones normativas

Establecer un mecanismo para dar seguimiento a las tendencias tecnológicas, de infraestructura, así como a las disposiciones legales en la materia y, en su caso, incluirlas en el Programa de Tecnología.

Factores críticos

Los integrantes del Grupo de trabajo de arquitectura tecnológica deberán de:

1. Estar capacitados para desarrollar esta actividad.
2. Consultar, de ser posible, con especialistas externos el entendimiento de las oportunidades y beneficios derivados de las nuevas tecnologías en la UTIC.
3. Participar en los foros y grupos de especialistas que se establezcan.
4. Mantener informado a los integrantes de los diversos grupos de trabajo sobre las tendencias tecnológicas.
5. Evaluar la posible contribución de tecnologías emergentes al logro de los objetivos estratégicos de la Institución relacionados con las TIC.
6. Dar seguimiento a las reformas de las disposiciones y normas relativas a los componentes tecnológicos de la arquitectura tecnológica en operación y, en su caso, analizar el impacto en el Programa de Tecnología, para prever los cambios pertinentes.
    - Mecanismo de seguimiento al desarrollo tecnológico y sus tendencias.

DDT-5 Administrar los requerimientos tecnológicos

Identificar, almacenar y comunicar los requerimientos tecnológicos derivados de los objetivos, estrategias y servicios que deberán ser soportados por la arquitectura tecnológica.

Factores críticos

1. Registrar requerimientos tecnológicos, incluyendo aquéllos necesarios para la arquitectura tecnológica deseada.

2. Determinar la prioridad de los requerimientos tecnológicos de acuerdo a su tipo y etapa en el ciclo de vida de la arquitectura tecnológica.
3. Dar seguimiento a los requerimientos tecnológicos y, en caso de ser necesario, reasignar prioridades, agregar nuevos requerimientos tecnológicos, así como ajustar o dar de baja dichos requerimientos.
4. Generar un análisis de impacto de los cambios en los requerimientos tecnológicos para presentarlos al Grupo de trabajo de arquitectura tecnológica.

3.4 Administración de la Evaluación de TIC

Establecer mecanismos de seguimiento y evaluación, así como acciones de mejora a partir de los resultados de la ejecución de la planeación estratégica, de la operación de los de los procesos y de los proyectos, del uso y aprovechamiento de los activos, de los recursos y de la entrega de los servicios de TIC.

Objetivos Específicos

1. Establecer un sistema que permita evaluar en forma integral, o por componentes, la operación y servicios de TIC.
2. Proporcionar informes de resultados de la operación y de rendimiento de los procesos y de los servicios de las TIC y de avance en el cumplimiento de los objetivos, que les permita tomar decisiones oportunas e informadas.
3. Establecer las acciones de mejora para prever y corregir desviaciones en la operación y el rendimiento de los procesos y de los servicios así como dar seguimiento a los resultados de éstas acciones.

Descripción de las Actividades del Proceso

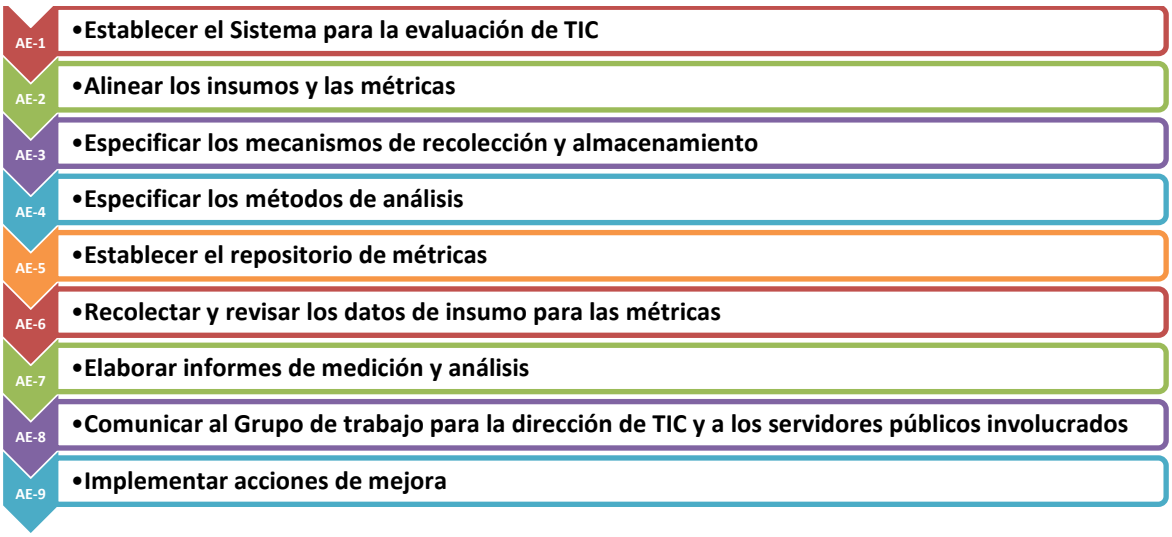


Fig. 3.4 Descripción de las actividades del proceso AE

AE-1 Establecer el Sistema para la evaluación de TIC

Establecer los elementos necesarios para instrumentar el sistema que permita dar seguimiento al avance y rendimiento en la implementación de la estrategia y de los proyectos; a la operación y resultados de los procesos; al uso de los recursos, así como a la entrega de los servicios de TIC.

Factores críticos

El Administrador del sistema de evaluación de TIC deberá:

1. Identificar, categorizar y documentar un conjunto de indicadores de proceso, de producto y de resultados.
2. Verificar el diseño de los indicadores establecidos para cada proceso del "Marco rector de procesos en materia de TIC", de manera que se asegure su consistencia e integralidad.

   Deben orientarse a:

   - Reducción de costos;
   - Cumplimiento regulatorio;
   - Satisfacción de los usuarios;
   - Madurez y la optimización del proceso;
   - Niveles de servicio, y
   - Cumplimiento de los objetivos estratégicos.
3. Actualizar continuamente la información insumo para operar los indicadores.
4. Formalizar y aprobar el establecimiento de los indicadores.
5. Considerar al establecer el Sistema de evaluación de TIC, los elementos siguientes:
   - Riesgos de TIC y cumplimiento normativo.
   - Niveles de satisfacción de los usuarios.
   - Indicadores de operación y resultados de los procesos de TIC.
6. Sensibilizar a los servidores públicos de la UTIC y a los usuarios sobre la importancia de la evaluación de TIC.

AE-2 Alinear los insumos y las métricas

Alinear las métricas y la información que sirve de insumo, de acuerdo a la operación de la UTIC, con estricto apego a los indicadores de los procesos del "Marco rector de procesos en materia de TIC".

Factores críticos

El Administrador de métricas deberá de:

1. Identificar las métricas de los indicadores
2. Establecer los nombres, categorías, unidades de medida, entre otros atributos de las propias métricas.
3. Especificar los modelos o fórmulas de cálculo de las métricas.
4. Revisar, aprobar y formalizar las métricas.
5. Verificar la prioridad y vigencia de las métricas periódicamente.

AE-3 Especificar los mecanismos de recolección y almacenamiento

Especificar cómo son obtenidos y almacenados los datos de las métricas

Factores críticos

El Administrador de métricas deberá de:

1. Identificar orígenes de los datos.
2. Identificar métricas para las cuales se requieren datos que no se encuentran disponibles y, en su caso, revisar la definición de la métrica.
3. Especificar cómo recolectar y almacenar datos para cada métrica requerida.
4. Crear mecanismos y una guía para la recolección y almacenamiento de datos, integrados en los procesos a medir.
5. Establecer sistemas y mecanismos para la recolección automática de datos cuando sea apropiado y viable.
6. Priorizar, revisar, aprobar y formalizar tanto las métricas como los mecanismos de recolección y almacenamiento de datos.
7. Actualizar métricas e indicadores periódicamente.

AE-4 Especificar los métodos de análisis

Especificar los métodos para el análisis y reporte de los datos del Sistema de evaluación de TIC.

Factores críticos

El Administrador de métricas deberá de:

1. Especificar y priorizar los análisis de información y los reportes.
2. Seleccionar métodos y herramientas apropiados para el análisis de datos.
3. Revisar y actualizar el contenido y el formato de los informes para realizar los análisis especificados.
4. Especificar los criterios para evaluar la utilidad de los resultados y de las actividades de medición y análisis.

5. Efectuar, anualmente, una verificación sobre las métricas, indicadores y criterios para evaluar los resultados del análisis y, en su caso, actualizar las métricas, indicadores y criterios.

AE-5 Establecer el repositorio de métricas

Establecer y mantener actualizado el repositorio de métricas del Sistema de evaluación de TIC.

Factores críticos

El repositorio de métricas deberá ser diseñado como un componente del sistema de conocimiento de acuerdo al proceso de Administración del conocimiento y contendrá la información necesaria para entender, interpretar y evaluar las métricas, así como la referencia hacía otra información relacionada.

El Administrador del sistema de evaluación de TIC deberá:

1. Determinar las necesidades de almacenamiento y recuperación de métricas.
2. Diseñar e implementar el repositorio de métricas.
3. Especificar los procedimientos para almacenar, actualizar y recuperar las métricas.
4. Mantener disponible para su uso el contenido del repositorio de métricas.
5. Revisar, periódicamente, el repositorio de métricas y los mecanismos.

AE-6 Recolectar y revisar los datos de insumo para las métricas

Obtener los datos de insumo para las métricas y analizar e interpretar los mismos.

Factores críticos

El Analista de evaluación de TIC deberá:

1. Obtener y/o generar los datos de insumo para las métricas
2. Revisar los datos de insumo para las métricas y verificar su integridad y exactitud.
3. Almacenar la información de acuerdo con los mecanismos de almacenamiento de datos para las métricas.
4. Efectuar periódicamente la actualización de los criterios de revisión.

AE-7 Elaborar informes de medición y análisis

Elaborar los informes de medición y análisis de la estrategia y de los proyectos; de la operación y resultados de los procesos; del uso de los recursos, así como de la entrega de los servicios de TIC.

Factores críticos

El Analista de evaluación de TIC deberá:

1. Elaborar los informes de manera que cumplan con los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.
    - Los informes deberán de ser diseñados para mostrar aquéllos asuntos y riesgos relacionados con la contribución de TIC, particularmente, con la capacidad de desarrollo de soluciones tecnológicas y la entrega de servicios de TIC, así como con el grado de cumplimiento de los objetivos de los procesos.
2. Desarrollar un análisis inicial de los datos de insumo para las métricas, interpretar los resultados y desarrollar las conclusiones preliminares.
3. Revisar las conclusiones preliminares.
4. Desarrollar, en su caso, análisis complementarios con datos de insumo adicionales para las métricas y preparar resultados, cuando así proceda, para su presentación.
5. Asesorar a los grupos trabajo involucrados respecto a esta actividad.

AE-8 Comunicar al Grupo de trabajo para la dirección de TIC y a los servidores públicos involucrados

Mantener informado a los grupos de trabajo involucrados con respecto de los resultados de la medición y análisis de la estrategia y de los proyectos; de la operación y resultados de los procesos; del uso de los recursos, así como de la entrega de los servicios de TIC.

Factores críticos

El Administrador del Sistema de evaluación de TIC deberá:

1. Consolidar los resultados de los informes de medición y análisis en informes ejecutivos que reflejen el impacto en la operación de la Institución (positivo o negativo).
2. Establecer un mecanismo para dar conocer, en forma oportuna y confiable los informes ejecutivos.
3. Informar, en su caso, las acciones que se realizaron para mitigar aquéllos riesgos que fueron identificados.

AE-9 Implementar acciones de mejora

Identificar desviaciones, problemas y oportunidades de mejora con base en los informes de medición y análisis, para definir e implementar las acciones correctivas y preventivas.

Factores críticos

El Analista de evaluación de TIC deberá:

1. Identificar desviaciones, problemas y oportunidades de mejora con base en los informes de medición y análisis.
2. Determinar las acciones correctivas y preventivas a fin de establecer el Programa de Mejora, incorporando en el mismo aquéllas actividades de revisiones periódicas.
3. Efectuar negociaciones con los servidores públicos involucrados en los procesos del "Marco rector de procesos en materia de TIC", para implementar el Programa de Mejora.
4. Definir los resultados esperados de la implementación del Programa de Mejora.
5. Ejecutar el Programa de Mejora.
6. Evaluar los resultados de los programas de mejora, incluyendo la identificación de sus desviaciones.

3.5 Administración de Riesgos de TIC

Disminuir el impacto de eventos adversos que potencialmente podrían afectar el logro de los objetivos de la Institución en materia de TIC.

Objetivos Específicos

1. Establecer en la UTIC un sistema que permita identificar, analizar, evaluar, atender y monitorear los riesgos en materia de TIC.
2. Establecer mediante el sistema previsto en el numeral anterior, los medios que permitan tomar decisiones de manera informada y oportuna sobre la mitigación de los riesgos en materia de TIC.

Descripción de las Actividades del Proceso

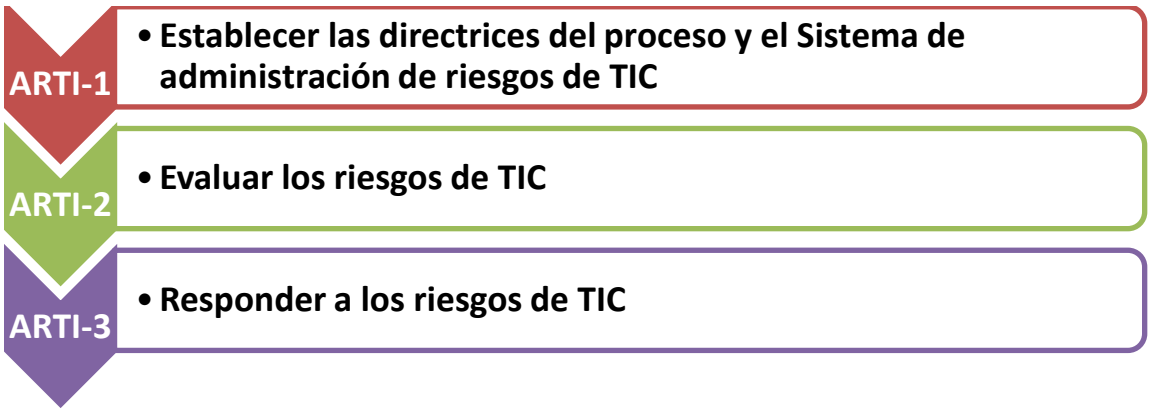


Fig. 3.5 Descripción de las actividades del proceso ARTI

ARTI-1 Establecer las directrices del proceso y el Sistema de administración de riesgos de TIC Establecer las directrices del proceso de Administración de riesgos de TIC y el Sistema de administración de riesgos de TIC.

Factores críticos

Se integrará un Grupo de trabajo de riesgos de TIC en cada una de las Instituciones, conformado por servidores públicos de la UTIC.

1. La UTIC al establecer el Grupo de trabajo de riesgos de TIC deberá:
    - Acordar y definir el rol y responsabilidades del Grupo de trabajo de riesgos de TIC.
    - Establecer y comunicar el alcance, objetivos, roles y responsabilidades de los integrantes del Grupo de trabajo de riesgos de TIC.
2. El Grupo de trabajo de riesgos de TIC deberá: Identificar en el ambiente interno y externo los riesgos, que en materia de TIC, podrían influir en la Institución:
    - En el ambiente externo los aspectos que se podrán considerar son, entre otros: legales, financieros, tecnológicos, económicos, naturales y competitivos, tanto a nivel federal y estatal, como en al ámbito internacional, así como tendencias e impulsores externos que tienen impacto en los objetivos de la Institución en materia de TIC y percepciones y valores que los involucrados externos tienen de la Institución en materia TIC.
    - En el ambiente interno los aspectos que podrán considerar, entre otros, son: estándares y modelos de referencia adoptados por la Institución en materia de TIC, políticas, objetivos y estrategias definidas en materia de TIC y soluciones tecnológicas y flujos existentes de información en la Institución, así como en aquellos procesos del “Marco rector de procesos en materia de TIC” en donde se tomen decisiones.
3. Documentar y difundir una directriz rectora en donde se definan los antecedentes, sustentos y justificaciones de la necesidad de implantar, a través de la UTIC, la administración de riesgos de TIC en la Institución. La directriz rectora deberá:
    - Mantenerse alineada con la estrategia de administración de riesgo de la Institución.
    - Establecer los roles y responsabilidades de los servidores públicos que intervienen en el presente proceso.
    - Integrar los requerimientos regulatorios aplicables.

- Contener, entre otros, elementos siguientes: Umbrales de tolerancia al riesgo en materia de TIC de la Institución; mecanismos o métodos que medirán el presente proceso y la administración de riesgos en materia de TIC; procesos, métodos y herramientas que se usarán para administrar los riesgos en materia de TIC; acciones que serán tomadas para corregir las desviaciones de los límites de exposición al riesgo, así como los ajustes preventivos a los niveles de tolerancia al riesgo.
- Establecer la forma y periodicidad en que se informará a los grupos de trabajo involucrados y a los usuarios, sobre los riesgos en materia de TIC a los que se encuentran expuestos los procesos y servicios que utilizan.
- Contener las acciones que deberán aplicarse cuando pudiera existir incumplimiento en la administración de un riesgo en materia de TIC.
- Establecer criterios para incluir consideraciones de riesgos en materia de TIC, en la toma de decisiones estratégicas de la Institución.
- Definir la periodicidad con la que se efectuará la revisión de la Directriz rectora y, en su caso, respecto a su actualización.
- Definir los reportes de gestión del proceso de Administración de riesgos de TIC y la periodicidad con la que se elaborarán y comunicarán.
- Establecer la forma en que se difundirá la Directriz rectora.

4. Enviar para revisión y, en su caso, aprobación la Directriz rectora del proceso de administración de riesgos de TIC al Grupo de trabajo para la dirección de TIC. El Sistema de administración de riesgos de TIC se constituye mediante la instrumentación y operación de la Directriz rectora.

ARTI-2 Evaluar los riesgos de TIC

Evaluar los riesgos de TIC que permitan identificar los impactos sobre los procesos y los servicios de la Institución.

Factores críticos

El Grupo de trabajo de riesgos de TIC deberá:

1. Recopilar los datos relevantes relacionados con los riesgos de TIC, tales como:
   - Incidentes que hayan tenido algún impacto en la Institución.
   - Riesgos del activo o recurso a evaluar.
   - Controles actualmente implementados en los activos o recursos a evaluar.
2. Identificar y clasificar las amenazas y riesgos en materia de TIC, conforme a lo siguiente:

- No causadas por el hombre: Fallas de TIC o de infraestructura de soporte y desastres naturales.
- Causados por el hombre: Dolosas, son aquéllas realizadas con la intención de causar un daño; culposas, son aquéllas que sin intención alguna se causa un daño.

3. Identificar los factores de riesgo que afecten a la Institución, los cuales pueden clasificarse en:
   - Financieros.
   - Niveles de servicios en materia de TIC.
   - Imagen o reputación en materia de TIC.
   - Regulatorios.
4. Identificar y analizar escenarios de riesgo de TIC que permitan evaluar y obtener los impactos potenciales considerando, entre otros, los elementos siguientes:
   - Servicios
   - Procesos
   - Datos (operativos, nómina, contables, entre otros)
   - Software (sistemas, aplicaciones, entre otros)
   - Hardware
   - Equipos informáticos que hospedan datos, aplicaciones y servicios
   - Equipos de comunicaciones
   - Dispositivos de almacenamiento
   - Usuarios y de personal externo a la Institución

   Para cada escenario de riesgo se debe definir y acordar la prioridad para su implantación, algunos de los parámetros que pueden ser considerados para dicha prioridad son:
   - Severidad del riesgo
   - Nivel de impacto de la implantación
   - Costo de la implantación
5. Integrar las matrices de riesgo de TIC, que sean necesarias, con la información referida en los numerales de 1 a 4 anteriores.

ARTI-3 Responder a los riesgos de TIC

Responder a los riesgos de TIC de acuerdo las decisiones para su tratamiento y los criterios de priorización.

Factores críticos

El Grupo de trabajo de riesgos de TIC deberá:

1. Identificar el nivel de severidad del riesgo.
2. Identificar opciones para el tratamiento y control del riesgo a efecto de tomar las decisiones para:
    - Aceptar el riesgo: No se efectúa ninguna acción debido a que el nivel de riesgo está dentro de los niveles aceptables por la entidad o dependencia.
    - Evitar el riesgo: Se elimina la causa que produce el riesgo.
    - Transferir el riesgo: Se transfiere y comparte el riesgo.
    - Mitigar el riesgo: Se implementan acciones para reducir el riesgo a un nivel aceptable.
3. Identificar acciones preventivas y correctivas y correlacionarlas para cada uno de los escenarios de riesgos identificados. Estas acciones se deberán integrar a las Declaraciones de aplicabilidad.
4. Definir programas de mitigación del riesgo, los cuales considerarán las acciones para implantar los controles de riesgos en las Declaraciones de aplicabilidad.
5. Definir un Programa de contingencia para hacer frente a los eventos o incidentes de los riesgos identificados que en materia de TIC pudieran presentarse.

3.6 Administración de proyectos de TIC

Obtener los resultados esperados de los proyectos de TIC, mediante una administración efectiva y una correcta aplicación de conocimientos, habilidades, herramientas, técnicas y recursos en el desarrollo de las actividades de los proyectos, con el fin de cumplir los objetivos de las iniciativas y Programas de proyectos.

Objetivos Específicos

Contar con un documento de planeación para cada proyecto autorizado, con el propósito de dirigir la ejecución del proyecto hacia la obtención de los resultados.

Evitar desviaciones en lo planeado, optimizar recursos, mitigar riesgos y preservar la seguridad de la información durante la ejecución de los proyectos de TIC.

Descripción de las actividades del proceso

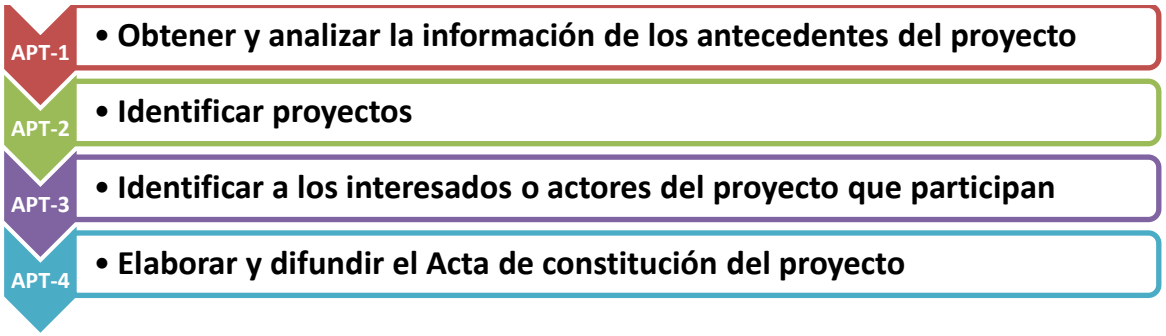


Fig. 3.6 Descripción de las actividades del proceso APT

APT-1 Obtener y analizar la información de los antecedentes del proyecto

El Administrador del proyecto debe obtener y analizar los antecedentes y la información disponible del proyecto asignado, para conocer, entre otros aspectos, su alcance, objetivos y beneficios esperados.

APT-2 Identificar proyectos

Identificar proyectos relacionados con el proyecto asignado, para determinar interdependencias, coordinar esfuerzos, identificar riesgos y explorar alternativas que permitan evitar conflictos entre los proyectos durante su ejecución.

APT-3 Identificar a los interesados o actores del proyecto que participan

El Administrador de proyecto debe identificar a quienes pudieran resultar afectados o beneficiados con el desarrollo del proyecto, a fin de conocer sus expectativas sobre el proyecto y, en caso necesario conciliarlas considerando los objetivos y alcances del proyecto.

APT-4 Elaborar y difundir el Acta de constitución del proyecto

El Administrador del Portafolio de proyectos de TIC, debe elaborar y difundir el Acta de constitución del proyecto, para formalizar su inicio y la designación formal del Administrador de proyecto.

3.7 Administración de la Seguridad de los Sistemas de Información

Establecer y vigilar los mecanismos que permitan la administración de la Seguridad de la Información de la Institución, así como disminuir el impacto de eventos que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

Objetivos Específicos

1. Establecer, operar y mantener un modelo de gobierno de Seguridad de la Información.
2. Efectuar la identificación de Infraestructuras críticas y Activos clave de la Institución y elaborar el Catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un SGSI que proteja los Activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
5. Establecer mecanismos para la respuesta inmediata a Incidentes a la seguridad de la Información.
6. Vigilar los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.

Descripción de las Actividades del Proceso

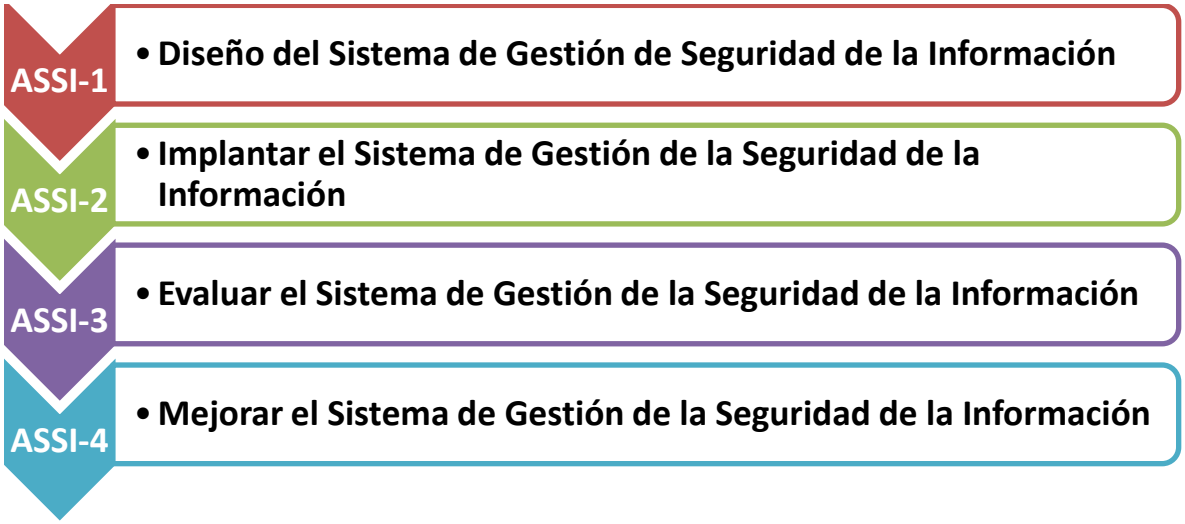


Fig. 3.7 Descripción de las actividades del proceso ASSI

ASSI-1 Diseño del Sistema de Gestión de Seguridad de la Información

Factores Críticos

1. Definir el alcance del SGSI, que establezca límites de protección desde la perspectiva Institucional, para proteger adecuadamente los activos tecnológicos y sistemas informáticos, incluyendo medios electrónicos de almacenamiento y de comunicación y la información contenida en los mismos.
2. Involucrar a las unidades responsables de la información contenida en medios electrónicos y sistemas informáticos, ya que son fuente principal para establecer el alcance, riesgos, vulnerabilidades, amenazas e impacto de la seguridad en la información de la Institución.
3. Definir los roles y responsabilidades del personal que participará en el diseño del SGSI.
4. Realizar un diagnóstico de los requerimientos de seguridad de la información de la Institución, a través de un análisis de riesgos de seguridad informática que valore sus activos, conociendo las vulnerabilidades y amenazas que pueda sufrir la información contenida en medios electrónicos y sistemas informáticos.
5. Asociar cada riesgo con las estrategias y/o objetivos de la Institución para generar las estrategias de seguridad informática, considerando los principios de integridad, confidencialidad y disponibilidad de la Información.
6. Elaborar el programa de mitigación de riesgos que contenga las estrategias de corto, mediano y largo plazo para enfrentar y mitigar los riesgos de seguridad de la información identificados en medios electrónicos y sistemas informáticos.
7. Definir métricas y los controles de verificación de cumplimiento de los requerimientos de seguridad de la información identificados en medios electrónicos y sistemas informáticos.
8. Elaborar el Programa de implantación del SGSI que incluya los procesos y procedimientos que permitan su adecuada operación.

ASSI-2 Implantar el Sistema de Gestión de la Seguridad de la información

Factores Críticos

1. Ejecutar, dar seguimiento y actualizar el estatus del Programa de Implantación del SGSI en la Institución.
2. Implementar y operar los controles de seguridad identificados y documentados en el SGSI.
3. Documentar y comunicar las acciones realizadas en el SGSI.

ASSI-3 Evaluar el Sistema de Gestión de la Seguridad de la información

Factores Críticos

1. Realizar revisiones para verificar la eficiencia y eficacia de los controles implementados en el SGSI.
2. Medir la efectividad de los controles de seguridad para verificar que se hayan cumplido los requerimientos de seguridad de los sistemas informáticos.
3. Efectuar el monitoreo de la seguridad de la información en medios electrónicos y sistemas informáticos para validar la efectividad del SGSI.
4. Revisar los intentos exitosos y no exitosos de violaciones e incidentes de seguridad.
5. Documentar y comunicar las acciones de evaluación del SGSI a los Usuarios del SGSI.

ASSI-4 Mejorar el Sistema de Gestión de la Seguridad de la información

Factores Críticos

1. Establecer las acciones correctivas y preventivas con la finalidad de minimizar los riesgos de seguridad de la información identificados.
2. Implantar y dar seguimiento a las acciones correctivas y preventivas.

3.8 OSGP – Operación del sistema de gestión y mejora de los procesos de la UTIC

Establecer y operar un Sistema de gestión y mejora de los procesos de la UTIC en el que se verifiquen, monitoreen y evalúen los procesos del presente manual y se consideren las acciones de mejora necesarias para una operación eficiente de la UTIC.

Objetivos específicos

1. Establecer la mejora continua para la operación de los procesos del presente Manual.
2. Ejecutar las acciones de mejora determinada para la adecuada operación de los procesos.

Descripción de las Actividades del Proceso

1. **Definir criterios técnicos**

   El Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, con apoyo de los Responsables de los demás procesos de este Manual, deberá de definir los criterios técnicos para diseñar e incorporar elementos al Repositorio de activos de procesos.

2. **Integrar en el Repositorio características de los proceso**

   El Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, con apoyo de los Responsables de los demás procesos de este Manual, debe integrar en el Repositorio de activos de procesos, las características esenciales de los procesos del presente Manual, considerando por lo menos para cada uno de los procesos, la siguiente información:

   - Objetivo general y objetivos específicos
   - Responsable
   - Entradas y salidas
   - Proveedores y usuarios (clientes)
   - Mecanismos de medición e indicadores, incluyendo umbrales.
   - Recursos de los procesos: humanos, financieros, infraestructura y ambiente de trabajo
   - Mapas del proceso
   - Actividades y factores críticos del proceso
   - Reglas del proceso

- Diagrama que muestre la interrelación con otros procesos
- Los elementos del proceso que permiten precisar aspectos específicos de su operación

3. Integrar el Repositorio de activos al Sistema

El Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, debe integrar el Repositorio de activos de procesos al sistema de conocimiento de la UTIC, en coordinación con el Responsable del proceso ACNC-Administración del conocimiento.

4. Elaborar el Mapa de procesos

El Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, debe elaborar el Mapa de procesos, en el que se muestre la jerarquía, relación e interacción de los procesos.

5. Seleccionar sujetos y activos para control de cambios

El Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, debe seleccionar los documentos y activos de procesos que estarán sujetos a control de cambios de versiones.

6. Integrar información en el Repositorio de activos y en el de métricas

Los Responsables de cada uno de los procesos, con apoyo del Responsable del proceso OSGP-Operación del Sistema de gestión y mejora de los procesos de la UTIC, deben integrar los objetivos, metas, objetivos de calidad del proceso y de sus productos, criterios técnicos de aceptación de los productos del proceso, métricas y resultados esperados, en el Repositorio de activos de procesos y en el Repositorio de métricas de procesos y generar el Documento de administración del proceso, el cual podrá ser una vista de los Repositorios mencionados.

7. Establecer y actualizar Modelos

Los Responsables de cada uno de los procesos, con apoyo del Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, deben establecer y actualizar los Modelos de ciclo de vida aplicables.

8. Establecer Sistema de Gestión y mejora

Los Responsables de cada uno de los procesos, con apoyo del Responsable del proceso OSGP-Operación del Sistema de Gestión y mejora de los procesos de la UTIC, deben establecer el Sistema de Gestión y mejora de

procesos de la UTIC, integrando la información y elementos generados a través de los factores críticos anteriores.

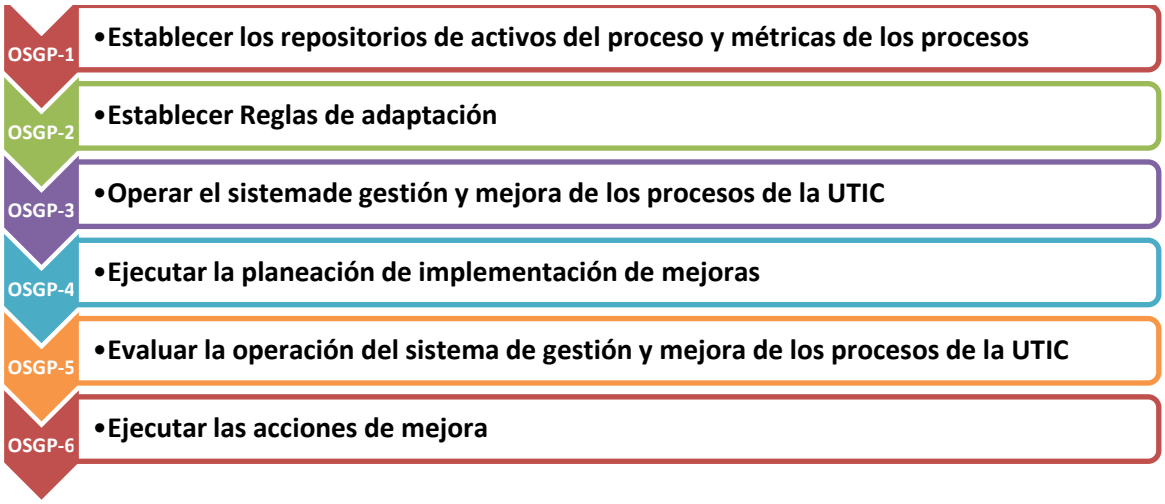


Fig. 3.9 Descripción de las actividades del proceso OSGP

OSGP-1 Establecer los repositorios de activos del proceso y métricas de los procesos

El Responsable de este proceso, con apoyo de los Responsables de los demás procesos del Manual, deberá:

1. Definir los criterios técnicos para diseñar e incorporar elementos al Repositorio de activos de procesos.
2. Integrar en el Repositorio de activos de procesos, las características esenciales de los procesos del presente Manual, considerando por lo menos para cada uno de los procesos, la información siguiente:
   a) Objetivo general y objetivos específicos
   b) Responsable
   c) Entradas y salidas
   d) Proveedores y usuarios (clientes)
   e) Mecanismos de medición e indicadores, incluyendo umbrales
   f) Recursos de los procesos: humanos, financieros, infraestructura y ambiente de trabajo
   g) Mapas del proceso
   h) Actividades y factores críticos del proceso
   i) Reglas del proceso
   j) Diagrama que muestre la interrelación con otros procesos

k) Los elementos del proceso que permiten precisar aspectos específicos de su operación

3. Integrar el Repositorio de activos de procesos al sistema de conocimiento de la UTIC, en coordinación con el Responsable del proceso ACNC-Administración del conocimiento.
4. Elaborar el Mapa de procesos, en el que se muestre la jerarquía, relación e interacción de los procesos.
5. Seleccionar los documentos y activos de procesos que estarán sujetos a control de cambios y de versiones.
6. Integrar los objetivos, metas, objetivos de calidad del proceso y de sus productos, criterios técnicos de aceptación de los productos del proceso, métricas y resultados esperados, en el Repositorio de activos de procesos y en el Repositorio de métricas de procesos y generar el Documento de administración del proceso, el cual podrá ser una vista de los repositorios mencionados.
7. Establecer y actualizar los Modelos de ciclo de vida aplicables.
8. Establecer el sistema de gestión y mejora de procesos de la UTIC, integrando la información y elementos generados a través de los factores críticos anteriores.

OSGP-2 Establecer Reglas de adaptación

1. Elaborar y someter a la autorización del Titular de la UTIC, Reglas de adaptación que permitan no observar uno o más factores críticos de alguna actividad o, una o más actividades de un proceso, cuando tal adaptación responda a necesidades específicas de la Institución y no se afecte la consistencia y cohesión del proceso o la interrelación de éste con los demás procesos del “Marco rector de procesos”.

   El Titular de la UTIC deberá:

2. Autorizar, en su caso, las Reglas de adaptación a que se refiere el factor crítico anterior, considerando al efecto que las Reglas de adaptación están sujetas a lo siguiente:

   a) Sólo podrán establecerse en Instituciones cuyo presupuesto anual destinado a procesos, proyectos y servicios de TIC sea menor a 25 millones de pesos.

b) En ningún caso los procesos de los grupos: DR, DCSI y AP serán objeto de dichas Reglas.
c) No podrán establecerse para dejar de observar factores críticos vinculados directamente con controles de seguridad de la información o con niveles de servicio ni para omitir la observancia de cualquiera de las reglas contenidas en los apartados “Reglas del proceso”.
d) Deberán incluir una justificación para cada actividad o factor crítico que se dejará de observar.

3. Enviar las Reglas de adaptación autorizadas a la UGD, para efectos de su registro y control.
4. Registrar las Reglas de adaptación autorizadas y registradas en la UGD, como activos del proceso.

OSGP-3 Operar el sistema de gestión y mejora de los procesos de la UTIC

1. Comunicar oportunamente a los involucrados en cada proceso: el objetivo general, los objetivos específicos, los resultados esperados y sus indicadores.

   El Responsable de este proceso, con apoyo de los Responsables de cada uno de los procesos, deberá:

2. Informar a los involucrados del proceso del resultado de la supervisión a la asignación de roles, actividades y responsabilidades para la ejecución de los procesos efectuada por el Grupo de trabajo estratégico de TIC.
3. Establecer y actualizar los objetivos de calidad de los procesos, los activos de procesos, así como las actividades de verificación, validación, monitoreo, inspección, pruebas específicas y los criterios técnicos de aceptación de los productos de cada proceso.
4. Establecer registros para proveer evidencia sobre el cumplimiento de los procesos y de sus productos.
5. Establecer y actualizar las métricas que permitan conocer los resultados y el desempeño de cada proceso, así como la oportuna implementación de acciones para corregir las desviaciones a las metas e indicadores.
6. Alinear los objetivos, las métricas e indicadores de los procesos con el sistema de evaluación de TIC, establecido en el proceso AE-Administración de la evaluación de TIC.

7. Establecer los Estándares de ambiente de trabajo, considerando, las instalaciones, espacio de trabajo, herramientas asociadas, software e infraestructura, y actualizarlos.

OSGP-4 Ejecutar la planeación de implementación de mejoras

El Responsable de este proceso, con apoyo de los Responsables de los procesos a los que se aplicarán las mejoras, deberá:

1. Elaborar el Documento de planeación para la implementación de mejora de procesos, considerando, al menos, los siguientes elementos:
   a) Las solicitudes de mejora recibidas.
   b) La información contenida en el Repositorio de activos de procesos, así como el Repositorio de métricas de procesos.
   c) Los proyectos de servicios de TIC en desarrollo, y los compromisos de la UTIC.
   d) Los procesos a los que aplicará la acción de mejora.
   e) El objetivo y alcance de la implementación de la mejora.
   f) Las acciones que habrán de efectuarse para lograr una adecuada comunicación con los involucrados en la mejora.
   g) Las acciones que habrán de efectuarse para la adecuada administración de los cambios que deriven de la mejora.
   h) Los criterios técnicos para evaluar la calidad del proceso mejorado.
2. Instrumentar el Proyecto de implementación de mejora de procesos, siguiendo el proceso APTI-Administración de proyectos de TIC.
3. Comunicar el Proyecto de implementación de mejora de procesos, a los involucrados.
4. Dirigir, supervisar y controlar la ejecución del Proyecto de implementación de mejora de procesos.
5. Documentar, formalizar y difundir la mejora aplicada.
6. Integrar el Documento de lecciones aprendidas y mantenerlo a disposición de los involucrados e interesados.
7. Actualizar el Repositorio de activos de procesos, así como el Repositorio de métricas de procesos.

OSGP-5 Evaluar la operación del sistema de gestión y mejora de los procesos de la UTIC

El Responsable de este proceso, con apoyo de los Responsables de los demás procesos del Manual, deberá:

1. Establecer un Grupo de trabajo de aseguramiento de calidad, compuesto por integrantes del Recurso humano en la UTIC.

   El Grupo de trabajo de aseguramiento de calidad deberá:

2. Obtener un diagnóstico del estado actual de los procesos de la UTIC.
3. Obtener un inventario de las capacidades del personal que interviene en la ejecución de los procesos.
4. Identificar los procesos que tienen oportunidades de mejora.
5. Monitorear y medir los productos y servicios de los procesos, con el propósito de constatar que:
   a) Los requerimientos de mejora se han cumplido.
   b) Se obtuvo y conserva evidencia de la mejora, de conformidad con los criterios técnicos de aceptación.
6. Monitorear y medir el desarrollo de las actividades de los procesos, a través de:
   a) Mecanismos para el seguimiento a la ejecución de los procesos que permitan mostrar claramente los resultados de la gestión.
   b) Acciones para corregir la desviación identificada y, eliminar de ser posible, la causa raíz.
   c) La evidencia que se obtenga y conserve, de la conformidad con los criterios técnicos de aceptación.
   d) La revisión que se realice para constatar que las capacidades de los involucrados están alineadas con los procesos que operan. En coordinación con las acciones de los procesos EMG-Establecimiento del modelo de gobierno de TIC y APC- Apoyo a la capacitación del personal de la UTIC.
7. Elaborar el Documento de planeación de evaluación, y conducir, al menos una vez por año, las evaluaciones que permitan determinar si la forma como se están operando los procesos es la que indica en este Manual y si se cumple con los niveles de desempeño previstos para cada proceso, a cuyo efecto:
   a) Definirá el alcance, la frecuencia, así como los criterios técnicos y métodos para las evaluaciones.

b) Seleccionará a los evaluadores de calidad, asegurándose de que éstos no evaluarán su propio trabajo.
c) Dará seguimiento a las evaluaciones que realicen los evaluadores seleccionados para dar certeza de la objetividad e imparcialidad de las evaluaciones.
d) Establecerá el Programa de evaluaciones tomando en cuenta tanto el estado y la importancia de los procesos así como los resultados de evaluaciones anteriores.
e) Elaborará el Análisis comparativo de los procesos evaluados.
f) Registrará y comunicará los resultados de las evaluaciones a los Responsables de los procesos evaluados y directamente relacionados.

8. Elaborar el Reporte de evaluación de procesos, el cual deberá incluir:
   a) Los resultados y conclusiones de las evaluaciones, destacando: hallazgos, no conformidades y, en su caso, actividades no evaluadas.
   b) Las oportunidades de mejora identificadas en las diversas fuentes disponibles, como pueden ser:
      i. Los resultados de las evaluaciones efectuadas a los procesos.
      ii. Los resultados de cada Análisis comparativo realizado.
      iii. Propuestas y solicitudes de mejora de procesos, presentadas por los involucrados.
      iv. Lecciones aprendidas en la implantación y ejecución de los procesos.

OSGP-6 Ejecutar las acciones de mejora

El Responsable de este proceso deberá:

1. Establecer un Grupo de trabajo de procesos y mejora continua de la UTIC, conformado por integrantes del Recurso humano en la UTIC, el cual será responsable de administrar las mejoras a los procesos de la UTIC, de manera ordenada y orientada al beneficio de la Institución.

   El Grupo de trabajo de procesos y mejora continua de la UTIC deberá:

2. Registrar en el Repositorio de solicitudes de mejora, las solicitudes recibidas.
3. Elaborar el Informe de análisis de mejoras propuestas, mediante la revisión, análisis, priorización y selección de las solicitudes de mejora de procesos. Para efectuar la selección de dichas solicitudes se considerará lo siguiente:

a) Menor costo y horas de trabajo.
b) Mayores beneficios tangibles e intangibles.
c) Mayor contribución de las mejoras propuestas al cumplimiento del PETIC.
d) Menores obstáculos o riesgos potenciales.

4. Documentar las solicitudes de mejoras de procesos como proyectos de implementación de mejora de procesos, conforme a lo establecido en el proceso APP- Administración del portafolio de proyectos de TIC, para su evaluación y, en su caso, autorización correspondiente.
5. Ejecutar los proyectos de implementación de mejora procesos y dar seguimiento a las “no conformidades” hasta su cierre, así como validar las acciones correctivas implementadas.
6. Elaborar el documento de Resultado de mejoras implementadas, con los datos provenientes de la actividad OSGP-5.
7. Iniciar un nuevo ciclo del proyecto de mejora implementado, si las acciones realizadas no tienen el resultado esperado, para lo cual se deberá regresa a la actividad de OSGP-5.
8. Integrar la información del resultado de mejoras implementadas a los repositorios de este proceso y asegurarse que dichos resultados se incorporen al Repositorio de conocimiento a que se refiere el proceso ACNC-Administración del conocimiento.
9. Difundir los resultados obtenidos a los involucrado

3.9 Administración del presupuesto de TIC

Coordinar las acciones para el ejercicio del presupuesto asignado a las TIC, a fin de maximizar su aplicación en las adquisiciones y servicios de TIC requeridos por la Institución.

Objetivos Específicos

1. Identificar y consolidar los requerimientos de recursos financieros de los proyectos y servicios de TIC existentes en los portafolios correspondientes.
2. Proponer escenarios para organizar los portafolios de proyectos y servicios de TIC, de acuerdo con los requerimientos de recursos de los proyectos y servicios de TIC y los recursos financieros con los que se cuente para ello, a fin de mejorar el rendimiento de los portafolios, considerando minimizar los costos y maximizar los beneficios por medio de estrategias adecuadas.

3. Participar en la priorizar de proyectos de TIC y programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica, a fin de lograr la optimización en el manejo del presupuesto destinado a las TIC.
4. Mantener actualizados los registros del presupuesto de TIC en el Repositorio de iniciativas de TIC, para cada rubro de gasto e inversión.

Descripción de las Actividades del Proceso

1. El Responsable del seguimiento del presupuesto debe mantener comunicación efectiva con las unidades administrativas responsables de administrar los recursos financieros y materiales de la Institución.
2. Los Responsables de los procesos de este Manual, deberán gestionar ante las unidades administrativas aplicables, la asignación de recursos para la ejecución de los Programas de proyectos y de proyectos de TIC autorizados, contenidos en los portafolios de proyectos y de servicios de TIC, así como para los programas de aprovisionamiento de mantenimiento de la infraestructura tecnológica.
3. El Responsable del seguimiento del presupuesto debe coordinar, en el ámbito de competencia de la UTIC, el seguimiento del ejercicio de los recursos presupuestarios de TIC, mediante las siguientes acciones:
    - Participar en el control de los gastos efectuados con cargo al presupuesto asignado a la UTIC, para la ejecución de los proyectos y servicios de TIC, así como para el aprovisionamiento de la infraestructura tecnológica.
    - Mantener actualizados los Portafolios de proyectos y de servicios de TIC, en lo que respecta a verificar que el costo de mantenimiento de los activos de TIC esté adecuadamente reflejado en el Programa de Mantenimiento de la infraestructura tecnológica y en el presupuesto asignado a la UTIC.
4. El Responsable del seguimiento del presupuesto debe verificar con la unidad administrativa competente, que los elementos que conforman las iniciativas de los Portafolios de proyectos y de servicios de TIC, así como los de aprovisionamiento y de mantenimiento de la infraestructura tecnológica estén identificados de acuerdo con la partida de gasto correspondiente.
5. El Responsable del seguimiento del presupuesto debe elaborar, con los datos del factor crítico anterior, la Lista de conceptos de TIC etiquetados en el presupuesto de TIC.

6. El Responsable del seguimiento del presupuesto debe informar a los Administradores de los Portafolios de proyectos y de servicios de TIC, sobre la existencia de recursos para la contratación de bienes y servicios de TIC.
7. El Responsable del seguimiento del presupuesto debe mantener actualizados y disponibles los registros sobre el ejercicio del presupuesto de TIC, incluida la programación de gasto comprometido, montos y fechas de pago para operación y mantenimiento del activo de TIC, mediante el documento Reporte del seguimiento del ejercicio del presupuesto.
8. El Responsable del seguimiento del presupuesto debe proveer a los responsables de la elaboración de los Casos de negocio de iniciativas de TIC, de la información sobre el presupuesto de TIC.
9. El Responsable del seguimiento del presupuesto debe comunicar a los Grupos de trabajo para la Dirección de TIC y estratégico de TIC, la información sobre el presupuesto de TIC, con la finalidad de priorizar su asignación y coordinar su aplicación.

3.10 Definición de Requerimientos de Soluciones

Definir los requerimientos de las soluciones tecnológicas de TIC, apoyar técnicamente su contratación y dar seguimiento al desarrollo de las mismas hasta su entrega, mediante acciones coordinadas con la Unidad administrativa responsable de realizar los procedimientos de contratación en la Institución, los Responsables de la implantación técnica de dichas soluciones en la UTIC y en su caso, con la Unidad administrativa solicitante.

Objetivos Específicos

1. Definir las características técnicas de las soluciones tecnológicas de TIC que se requieran contratar, considerando los requerimientos y restricciones identificadas.
2. Evaluar técnicamente las propuestas de soluciones tecnológicas que presenten los diversos proveedores, con el propósito de identificar la mejor propuesta técnica de acuerdo a las necesidades de la Institución.
3. Apoyar, conforme al ámbito de atribuciones de la UTIC y de acuerdo a las disposiciones jurídicas aplicables, la contratación de soluciones tecnológicas.
4. Administración la entrega de las soluciones tecnológicas adquiridas, incluyendo su configuración, personalización, puesta en operación y demás actividades que se hayan establecido en su contratación.

Descripción de las Actividades del Proceso

1. El Líder técnico de requerimientos para la solución tecnológica de TIC debe coordinarse con el Administrador del portafolio de proyectos de TIC, para que el proyecto correspondiente a la solución tecnológica se inscriba en el portafolio de proyectos de TIC y que se asigne un Responsable de proyecto.
2. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe identificar las necesidades de TIC de la Unidad administrativa solicitante, así como de los requerimientos técnicos para la contratación de la solución tecnológica de TIC de que se trate, considerando al menos, lo siguiente:
3. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuanto así corresponda; debe priorizar los requerimientos identificados.
4. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe elaborar la propuesta de Documento de requerimientos de la solución tecnológica de TIC con la información obtenida de los factores críticos anteriores.
5. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe verificar que los requerimientos contenidos en la propuesta señalada en el factor crítico anterior cubran los escenarios operacionales indispensables, así como que los métodos de operación de la solución tecnológica de TIC estén definidos y documentados.
6. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe analizar los posibles riesgos, así como las estrategias de mitigación y contingencia de los escenarios operacionales definidos.
7. El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe proponer los criterios técnicos de aceptación para la solución tecnológica, con base en los requerimientos funcionales y no funcionales identificados.
8. El Líder técnico de requerimientos para la solución tecnológica de TIC debe dar su conformidad a la propuesta de Documento de requerimientos de la solución

tecnológica de TIC y obtener, en su caso, la aprobación de la Unidad administrativa solicitante.

9. El Líder técnico de requerimientos para la solución tecnológica de TIC debe revisar el Sistema de Inventario de Aplicaciones de la APF, para identificar si en las demás Instituciones existe alguna solución tecnológica similar a la requerida, que podría satisfacer las necesidades de la Unidad administrativa solicitante y ser compatible con la infraestructura de TIC de la Institución.
10. El Líder técnico de requerimientos para la solución tecnológica de TIC debe comunicar al Titular de la UTIC el resultado de la revisión efectuada conforme al factor crítico anterior, con la finalidad de que:
    - Se realicen las gestiones necesarias para la obtención de la solución tecnológica identificada y en su caso, adaptarla a las necesidades de la Institución, por medio del proceso DST.
    - Se continúe con el factor crítico siguiente.
11. El Titular de la UTIC debe designar al servidor público de la UTIC que fungirá como Representante del Área técnica para efectos de la contratación respectiva. Dicha designación podrá recaer en el Líder técnico de requerimientos para la solución tecnológica de TIC.
12. El servidor público que se designe como representante del Área técnica debe elaborar la Propuesta de Anexo técnico que contenga las especificaciones y requerimientos técnicos del bien o servicio de TIC que se pretenda contratar, debiendo incluir al menos: los requerimientos funcionales, no funcionales, niveles de servicio, términos y condiciones de entrega y aceptación y /o de tiempos de respuesta de soporte y servicio y demás aspectos señalados por la Unidad administrativa solicitante, y realizar su envío al Responsable del Programa para as contrataciones de TIC, previsto en el proceso ADTI-Administración para las contrataciones de TIC.
13. El servidor público que se designe como representante del Área técnica debe elaborar la Propuesta de estudio de mercado para su envío al Responsable del Programa para las contrataciones de TIC, debiendo incluir en dicha propuesta para el caso de software, alternativas de solución tanto de software de código abierto como de soluciones comerciales.
14. El Líder técnico de requerimientos para la solución tecnológica de TIC debe coordinarse cuando así corresponda, con el servidor público designado como

representante del Área técnica, para la elaboración de las propuestas a que se refieren los factores críticos 12 y 13.

3.11 Desarrollo de soluciones tecnológicas de TIC

Desarrollo de soluciones tecnológicas de TIC (DST) tiene por objetivo contar con un marco de referencia para la construcción de una solución tecnológica, incluyendo la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios para su entrega, de manera que se haga el mayor aprovechamiento posible de los recursos de TIC en la UTIC.

Responsabilidades

1. Administrador de Proyecto
    - Verificar la Matriz de trazabilidad
    - Mantener el Repositorio de configuraciones
    - Coordinarse con el Administrador del Portafolio de proyectos de TIC
    - Asegurar que se elabore el Documento de Planeación del proyecto
2. Analista de requerimientos de soluciones tecnológicas de TIC
    - Identificar necesidades y especificar requerimientos de solución tecnológica
    - Desarrollar los requerimientos de la solución tecnológica
    - Establecer la definición de los requerimientos funcionales
    - Analizar y validar los requerimientos
3. Líder técnico de desarrollo
    - Conducir la construcción de la solución tecnológica
    - Generar y mantener la documentación del producto
    - Validar y administrar las interfaces
4. Arquitecto de soluciones tecnológicas
    - Determinar y seleccionar alternativas de solución tecnológica
5. Diseñador de soluciones tecnológicas de TIC
    - Generar un diseño detallado de la solución tecnológica
    - Realizar análisis de hacer, re-utilizar o comprar componentes de la solución tecnológica
6. Responsable del Repositorio de configuraciones
    - Establecer líneas base de los componentes y productos identificados
    - Actualizar la configuración de los componentes y productos, cada que se apruebe una solicitud de cambio.

7. Desarrolladores de la solución tecnológica
    - Construir la solución tecnológica
    - Generar y mantener la construcción del producto
    - Validar y administrar interfaces
8. Integrador de la solución tecnológica
    - Determinar los componentes o productos que serán integrados en la solución tecnológica y su secuencia.
    - Ensamblar componentes de la solución tecnológica
9. Representante de la Unidad administrativa solicitante
    - Apoyar en la identificación de necesidades y requerimientos de la solución tecnológica
    - Aprobar los requerimientos de la solución tecnológica

Establecer el método a seguir para el desarrollo de soluciones tecnológicas de TIC, considerando la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios para su entrega, de manera que se obtenga el mejor aprovechamiento posible de los recursos de TIC.

Objetivos Específicos

1. Definir los requerimientos de la solución tecnológica de TIC de que se trate.
2. Utilizar de manera integral la arquitectura tecnológica definida por la UTIC.
3. Aprovechar los componentes y productos existentes en la arquitectura tecnológica en operación.
4. Efectuar la revisión de la calidad de los desarrollos de las soluciones tecnológicas de TIC.
5. Contar con mecanismos para el monitoreo, identificación y corrección de desviaciones durante los desarrollos de las soluciones tecnológicas de TIC.

Descripción de las Actividades del Proceso

1. Coordinar inscripción en el Portafolio y asignación de Responsable

    El Responsable de este proceso debe coordinarse con el Administrador del Portafolio de proyectos de TIC, para inscribir el proyecto correspondiente al desarrollo de la solución tecnológica en el Portafolio de proyectos de TIC y que asignar un Responsable de proyecto.

2. El Responsable de este proceso debe asegurar la elaboración del Documento de planeación del proyecto, de acuerdo al proceso APTI-Administración de proyectos de TIC.
3. El Responsable de este proceso debe asegurarse que se asignen los roles y responsables para la ejecución del proyecto y se registren en el Documento de planeación del proyecto.
4. Identificar necesidades de solución tecnológica

   El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad Administrativa solicitante, cuando así corresponda; debe identificar las necesidades de la solución tecnológica que se pretende desarrollar, tomando en cuenta:

   - La normativa que incide en la solución tecnológica de que se trate.
   - Las expectativas, interfaces y restricciones, existentes y proyectadas.
5. Definir requerimientos

   El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe definir los requerimientos de las soluciones tecnológicas de TIC, para lo cual debe:

   - Traducir las necesidades identificadas, en requerimientos específicos.
   - Integrar la información y el diseño de la solución tecnológica de TIC que se haya desarrollado, mediante el proceso DSTI. Diseño de servicios de TIC.
   - Analizar el modelo de flujo de negocio que será provisto, en su caso por la Unidad administrativa solicitante.
6. Revisar y validar requerimientos

   El Analista de requerimientos de soluciones tecnológicas de TIC, con apoyo del Representante de la Unidad administrativa solicitante, cuando así corresponda; debe revisar y validar los requerimientos específicos definidos conforme a los factores críticos 4 y 5, así como integrarlos en el Documento de visión de la solución tecnológica de TIC.

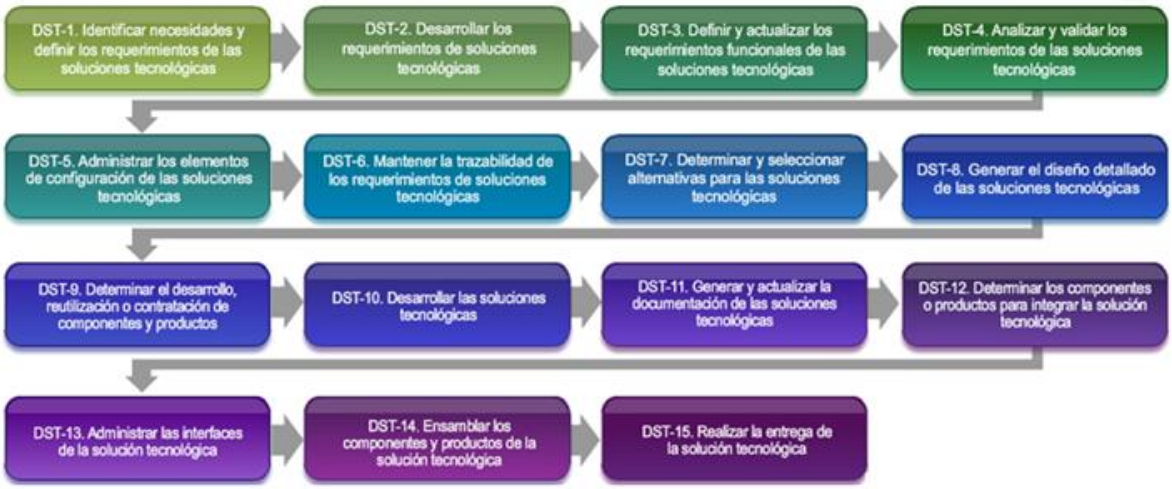


Fig. 3.10 Descripción de las actividades del proceso DST

3.12 Administración del portafolio de servicios de TIC

Administración del portafolio de servicios de TIC (APS) busca definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de creación de servicios de TIC susceptibles de aportar beneficios importantes en el cumplimiento de los objetivos de la Institución.

Responsables:

1. Grupo de Trabajo para la Dirección de TIC
   - Determinar las acciones de gobernabilidad de TIC con respecto de las iniciativas y/o servicios que se encuentran en el Portafolio de servicios de TIC.
   - Aprobar el rendimiento del Portafolio de servicios de TIC.
2. Administrador del Portafolio de servicios de TIC
   - Establecer un Portafolio de servicios de TIC.
   - Crear y mantener las categorías aplicables a las iniciativas y/o servicios del Portafolio de servicios de TIC.

Objetivos Específicos

1. Contar con mecanismos para la toma de decisiones de carácter estratégico relacionadas con los servicios de TIC.
2. Contar con un esquema de evaluación adecuado, comparable, transparente y repetible, que considere el valor, los beneficios y los riesgos de los Casos de

negocio de servicios de TIC, armonizado con lo establecido en el proceso APP-Administración del portafolio de proyectos de TIC.

3. Proporcionar a los mandos medios y superiores información clara y precisa sobre los servicios de TIC.

Descripción de las Actividades del Proceso

Fig. 3.11 Descripción de las actividades del proceso APS

1. **Recabar información de las Unidades administrativas**

   Recabar información de las Unidades administrativas solicitantes y usuarios, respecto a su visión a corto y largo plazo, relacionada con:

   - Los servicios de TIC necesarios para alcanzar las metas de los objetivos institucionales.
   - Las capacidades y recursos estimados para implantar los servicios de TIC que se requieren para cumplir con los objetivos referidos.
   - La ruta crítica para la entrega de los servicios de TIC.

2. **Recabar la información con que cuenten las Unidades administrativas**

   Recabar la información con que cuenten las Unidades administrativas solicitantes, respecto a la definición de los servicios de TIC existentes y los propuestos, con el propósito de obtener información única y consistente.

3. **Recabar la información técnica de los servicios de TIC**

   Recabar la información técnica de los servicios de TIC existentes y los propuestos.

4. **Integrar e incluir la información obtenida en el Repositorio**

   Integrar la información obtenida e incluir en el Repositorio del portafolio de servicios de TIC, los datos de los servicios de TIC durante todo su ciclo de vida, desde su conceptualización, diseño, transición, operación hasta su retiro de la operación. El Repositorio del portafolio de servicios de TIC incluye el Catálogo de servicios de TIC.

5. **Constatar que se elabore el correspondiente caso de negocio**

   Constatar que se elabore para cada servicio contenido en el portafolio de servicios de TIC, su correspondiente caso de negocio, en el que se defina la justificación técnica y económica del servicio de TIC para visualizar su valor.

6. **Incluir en el portafolio los servicios de TIC**

   Incluir en el portafolio de servicios de TIC, los servicios de TIC que proveen terceros.

3.13 Integración y Desarrollo del Personal

Identificar las necesidades de capacitación de los servidores públicos de la UTIC, con el propósito de proponer ante la Unidad administrativa competente las acciones de capacitación que permitan que los servidores públicos adscritos a la misma, actualicen sus conocimientos y fortalezcan sus habilidades.

Responsables:

1. Responsable del proceso APC-Apoyo a la capacitación del personal de la UTIC
   - Establecerá la vigilancia en la ejecución del proceso y mantendrá informado al titular de la UTIC al respecto del mismo.
2. Responsable del apoyo a la capacitación de la UTIC
   - Identificar, considerando los objetivos estratégicos de la Institución, el Mapa estratégico de la UTIC y el Programa de tecnología.
   - Identificar con base en el factor crítico anterior, las necesidades de capacitación de los servidores públicos de la UTIC.
   - Integrar el documento de Necesidades de capacitación en la UTIC
3. Unidad administrativa responsable de la capacitación en la Institución
   - Área encargada de la determinación de las necesidades de capacitación institucional, así mismo proporciona los recursos y material para la capacitación del personal de la UTIC.

Objetivos Específicos

1. Proponer acciones de capacitación para los servidores públicos de la UTIC, con base en el Mapa estratégico de la UTIC, las necesidades de operación de cada dominio tecnológico, así como en las necesidades de desarrollo de los servidores públicos de la UTIC.
2. Colaborar con la unidad administrativa responsable de la capacitación en la Institución, para la ejecución de las acciones de capacitación a los integrantes de la UTIC.

Capítulo 4. ESTUDIO DE CASO

Capítulo 4. Estudio de Caso

4.1 Objetivo, alcance y metas

OBJETIVO

El Responsable de la seguridad de la información en la Institución deberá:

1. Establecer el Grupo de trabajo Estratégico de Seguridad de la Información, que estará integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante éste documento de integración y operación y asegurarse de que:
    a) El Documento contenga, al menos: los objetivos y responsabilidades del grupo de trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo.
    b) Se comuniquen los roles y responsabilidades de los integrantes del Grupo de trabajo estratégico de seguridad de la información.
2. Encabezar el Grupo de trabajo estratégico de seguridad de la información (GESI) y dar seguimiento a las acciones establecidas en el mismo.

ALCANCE

Ámbito de los procesos MAAGTIC-SI involucrados en las responsabilidades del GESI:

El Grupo de Trabajo Estratégico de Seguridad de la Información deberá:

- ASI-1
- ASI-2 Operar y mantener el modelo de gobierno de seguridad de la información
- ASI-3 Diseño del SGSI (Sistema de Gestión de Seguridad de la Información)
- ASI-4 Identificar las Infraestructuras críticas y los Activos clave
- ASI-5 Establecer la Directriz rectora para la administración de riesgos
- ASI-6 Elaborar el Análisis de riesgos
- ASI-7 Integrar al SGSI los controles mínimos de Seguridad de la información
- ASI-8 Mejorar el SGSI
- ASI-9 Reglas del Proceso
- OPEC-1 Establecer el grupo de implantación de la seguridad
- OPEC-2 Establecer los elementos de operación del ERISC.

METAS

- Revisión y mejoramiento continuo de todos los procesos y servicios de TI

- Rediseñar y mantener actualizada la infraestructura de la red de comunicaciones de datos y telefonía existentes, para permitirnos brindar más y mejores servicios de alta tecnología.
- Continuar mejorando los servicios de programación en los sistemas administrativos
- Asesorar y agilizar las peticiones de nuestros usuarios para el procesamiento de datos o cambios a los sistemas.
- Mejorar la disponibilidad de todos los sistemas administrativos
- Garantizar la integridad de los datos.
- Asegurar la confidencialidad de la información asegurando que solo los individuos autorizados tengan acceso a los recursos que se intercambian.
- Garantizar el correcto funcionamiento
- . de los sistemas de información
- Garantizar de que no pueda negar una operación
- Evitar el rechazo: garantizar de que no pueda negar una operación realizada.
- Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

4.2 Diagrama de Actividades para el Sistema de Gestión de Seguridad de la Información

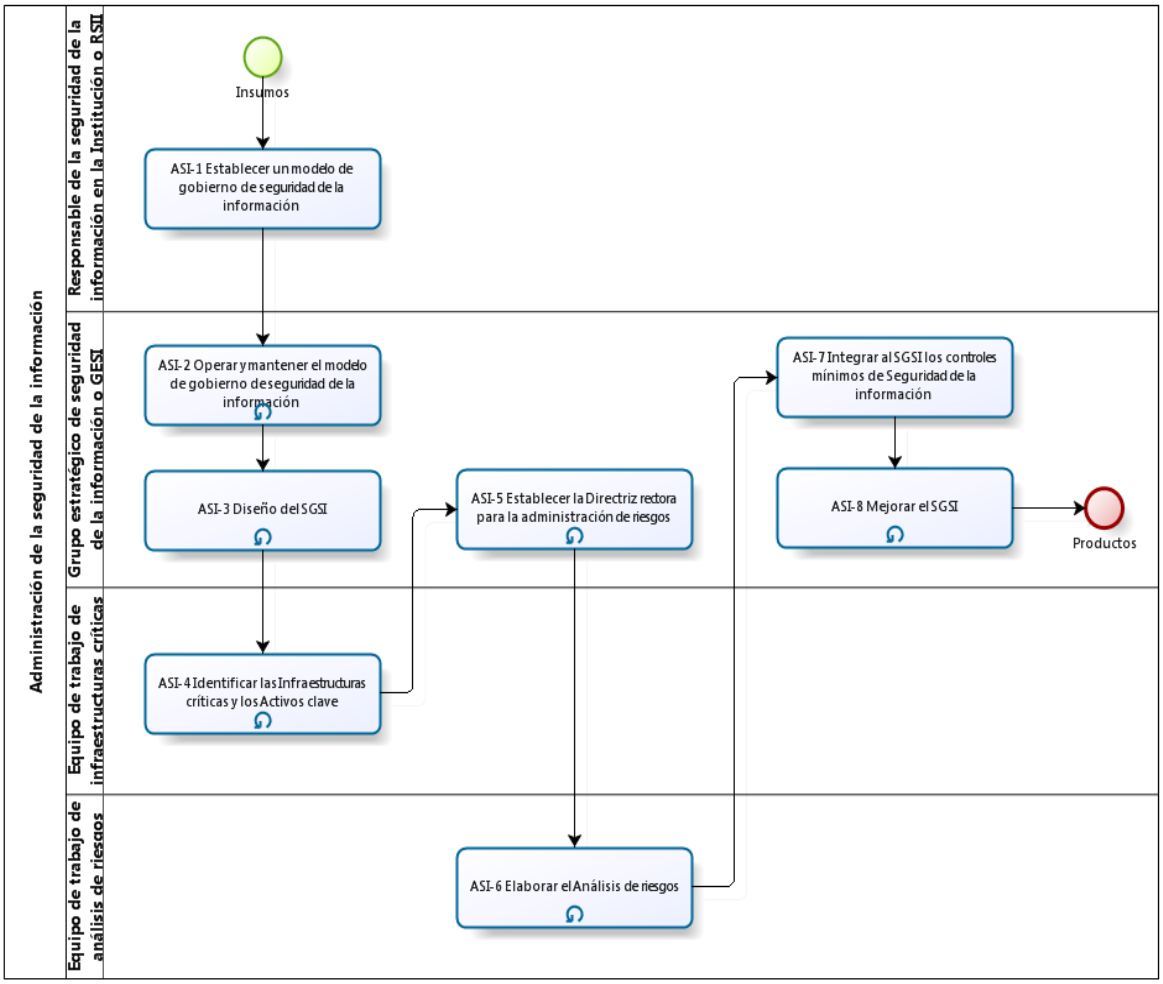


Figura 4.1 Actividades ASI

4.3 Factores Críticos para el proceso

ASI-1 Establecer un modelo de la seguridad de la Información

Al Titular de la Institución le corresponderá:

1. Designar al Responsable de la seguridad de la información en la Institución, quien deberá tener nivel jerárquico mínimo de Director General o equivalente.
2. Establecer el Grupo de trabajo estratégico de seguridad de la información, que estará Integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo de trabajo estratégico de seguridad de la información, y asegurarse de que:

a) El Documento contenga, al menos: los objetivos y responsabilidades del grupo de trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo.
b) Se comuniquen los roles y responsabilidades de los integrantes del Grupo de trabajo estratégico de seguridad de la información.

3. Encabezar el Grupo de trabajo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas en el mismo.

ASI-2 Operar y mantener el modelo de gobierno de seguridad de la información

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Coordinar la elaboración y actualización del Catálogo de infraestructuras críticas de la Institución.
2. Establecer, conjuntamente con los Responsables de los grupos de procesos PR, AS, TE, OS, AA y OP, así como en su caso con los servidores públicos que administren Activos de información, los mecanismos para garantizar la protección de las Infraestructuras críticas que éstos tengan bajo su responsabilidad.
3. Vigilar que los controles de seguridad de la información que se definan e implanten, consideren los mecanismos establecidos en el factor crítico anterior, así como el Análisis de riesgos que se realiza en la actividad ASI-6.
4. Constatar que se efectúe la implantación de SGSI en la Institución y que se lleven a cabo revisiones al mismo en periodos no mayores a un año, a fin de verificar su cumplimiento.
5. Dar seguimiento a las acciones de mejora continua derivadas de las revisiones al SGSI.

ASI-3 Diseño del SGSI

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Diseñar, en coordinación con las diferentes áreas y unidades administrativas de la Institución, la Estrategia de seguridad de la información que será implantada al interior de la misma, así como efectuar su revisión al menos una vez al año. Dicha Estrategia será la base para establecer el SGSI, cuyo diseño se efectuará atendiendo a lo siguiente:

a) Realizar un diagnóstico de los requerimientos de seguridad de la información de la Institución, considerando la participación de las unidades administrativas

usuarias de la información para establecer adecuadamente el alcance del SGSI.

b) Definir el alcance del SGSI, de manera tal que establezca límites de protección desde la perspectiva institucional, para proporcionar la seguridad requerida a los activos de información.

c) Generar las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos de la Institución.

d) Desarrollar reglas técnicas para verificar que los controles de seguridad de la información que se definan operen según lo esperado.

e) Definir métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los Activos de Información.

f) Elaborar las reglas técnicas que contengan las acciones para la adecuada operación del SGSI.

2. Integrar, con la información del factor crítico anterior, el Documento de definición del SGSI y el Programa de implantación del SGSI.

3. Someter a la consideración del Titular de la Institución el Documento de definición del SGSI y su Programa de implantación.

4. Asegurarse de que se presente a la unidad administrativa responsable de la capacitación en la Institución, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la Seguridad de la información, así como la estructura y alcances del SGSI.

5. Dar a conocer el SGSI y su programa de implantación a los servidores públicos de la institución involucrados con el mismo.

6. Elaborar el Programa de evaluaciones del SGSI y difundirlo en la Institución.

7. Elaborar, probar y mantener actualizada una Directriz rectora de respuesta a incidentes, en coordinación con el ERISC, ésta deberá contener al menos:

a) El rol y el servidor público asignado a éste, quien puede iniciar las tareas de respuesta a Incidentes.

b) El mecanismo de notificación, escalamiento y atención de Incidentes en la Institución.

c) Los mecanismos de interacción con otras Instituciones o entidades externas.

d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de Incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.
e) Los elementos del Programa de contingencia a los Activos de información que son sustantivos para el cumplimiento de la misión, visión y los objetivos institucionales.

8. Asegurarse de que la información obtenida de los factores críticos anteriores se integre en el Documento de definición del SGSI y éste se mantenga actualizado.
9. Hacer de conocimiento del órgano interno de control de la Institución y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI para el efecto de que se determinen, en su caso, las responsabilidades que procedan en términos de los ordenamientos legales aplicables.

ASI-4 Identificar las Infraestructuras críticas y los Activos clave

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Establecer el Equipo de trabajo de infraestructuras críticas, y designar a uno de sus integrantes como Responsable del mismo y de las acciones realizadas por éste, debiendo asegurarse de que:

a) Se formalice el establecimiento del Equipo, mediante el Documento de integración del equipo de trabajo de infraestructuras críticas, y que éste contenga al menos: los objetivos y responsabilidades del Equipo; roles y responsabilidades de cada miembro, así como el funcionamiento del mismo.
b) Se comunique la integración del Equipo así como los roles y responsabilidades de los integrantes del mismo.
c) El Equipo que se constituya realice, la identificación de Infraestructuras críticas y activos clave, para la elaboración del Catálogo de infraestructuras críticas de la Institución.
d) Los integrantes del Equipo de trabajo tengan un concepto claro y uniforme con respecto de las acciones que en materia de Seguridad nacional señala el artículo 3 de la Ley de Seguridad Nacional, así como sobre la forma en que las TIC apoyan los procesos sustantivos de la Institución y coadyuvan para garantizar la Seguridad nacional.

El Equipo de trabajo de infraestructuras críticas, en la identificación de Infraestructuras críticas y Activos clave, deberá:

2. Identificar procesos críticos de la Institución, mediante la ejecución de las siguientes acciones:

Analizar los procesos existentes y determinar cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos, en los niveles de servicio que tenga establecidos, derivado de sus atribuciones. Dicho análisis se realizará considerando, al menos los siguientes elementos:

i. Proveedores del proceso.

ii. Insumos del proceso.

iii. Eventos de inicio que disparan la ejecución del proceso.

iv. Subprocesos o actividades que lo conforman.

v. Actores que intervienen en su ejecución.

vi. Productos o servicios que genera.

vii. Evento de fin del proceso.

viii. Clientes o usuarios del proceso.

ix. Activos de información involucrados en el proceso.

a) Analizar los diagramas de los procesos, a fin de identificar las Interdependencias que existan entre éstos así como con otros fuera de la Institución.

3. Identificar, a partir de los procesos críticos determinados en el factor crítico anterior, aquéllos que se encuentren vinculados con la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo que señalan los artículos 3 y 5 de la Ley de Seguridad Nacional. En caso de no identificarse este tipo de procesos críticos, no será necesario atender los factores críticos 4 a 15 restantes, debiendo dar inicio a la actividad ASI-5.
4. Obtener un listado de los procesos críticos de la Institución e integrar la información de los factores críticos 2 y 3 anteriores en el Documento de identificación de infraestructuras críticas.
5. Identificar las actividades críticas de los procesos contenidos en el Documento de identificación de infraestructuras críticas, mediante la ejecución de las acciones siguientes:

a) Enlistar y describir las actividades de cada proceso crítico, así como los factores de éxito para que el proceso se lleve a cabo de manera adecuada.
b) Determinar las actividades que resultan críticas para la operación del proceso.
c) Integrar en el Documento de Identificación de infraestructuras críticas, los datos obtenidos de los incisos anteriores.

6. Identificar los Activos de información involucrados en los procesos de seguridad nacional, mediante la ejecución de las acciones siguientes:

a) Elaborar una relación de los Activos de información que soportan la generación, procesamiento, transmisión y almacenamiento de la información en los procesos, con apoyo de los responsables, según corresponda, de su desarrollo, mantenimiento, operación, uso y seguridad, así como de su administración y resguardo.
b) Incluir en la relación de los Activos de Información al responsable de su resguardo.
c) Clasificar los Activos de información como: Activos primarios o de soporte, de acuerdo a su funcionalidad, alcance o impacto en el proceso.
d) Definir la nomenclatura para la identificación de los Activos de información, a partir de dos campos: en el primero “Id. Activo”, se asignará un número consecutivo que, relacionado con el segundo campo “Id. Proceso”, correspondiente al proceso, provea una identificación única para cada activo.
e) Registrar los datos obtenidos de los incisos anteriores en el Documento de identificación de infraestructuras críticas.

7. Efectuar la valoración de los Activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad, para identificar aquéllos que deban considerarse como Activos de información clave y registrar los resultados de la valoración efectuada en el documento de Matrices de infraestructuras críticas y activos clave.
8. Utilizar como parámetros para identificar la criticidad de una infraestructura, los tipos de impacto potencial que podrían ocurrir ante la presentación de un Incidente. Estos se deberán representar en las matrices de impacto que forman parte del documento denominado Matrices de infraestructuras críticas y activos clave.
9. Determinar el nivel de criticidad de cada infraestructura, mediante la identificación de su Interdependencia y el nivel de Impacto que tenga con cada

una de las infraestructuras con las que se relacione, en el documento de Matrices de infraestructuras críticas y activos clave.

10. Revisar los resultados obtenidos y los documentos generados en los factores críticos anteriores.
11. Verificar los resultados obtenidos y documentos generados por el Equipo de trabajo de infraestructuras críticas, y constatar que las infraestructuras críticas que se hubieren identificado efectivamente tengan ese carácter.

El Grupo de trabajo estratégico de seguridad de la información, con apoyo del Equipo de trabajo de infraestructuras críticas, deberá:

12. Elaborar el Catálogo de infraestructuras críticas, con base en la información contenida en el documento de identificación de infraestructuras críticas y en el de Matrices de infraestructuras críticas y activos clave, y realizar las siguientes acciones:

a) Asignar, de acuerdo con la tabla que se contiene en el Catálogo de Infraestructuras críticas, el sector y subsector que corresponda a cada infraestructura crítica.
b) Verificar que el Catálogo de Infraestructuras críticas incorpore los datos de identificación de las Infraestructuras críticas, señalando su descripción, componentes, sector y subsector, Institución y ubicación.
c) Incluir en el Catálogo de Infraestructuras críticas un mapa de localización geográfica, en donde se muestre la ubicación de las diversas Infraestructuras críticas.

El Responsable de la seguridad de la información de la Institución deberá:

1. Presentar a la aprobación del Titular de la Institución, el Catálogo de infraestructuras críticas.
2. Asegurarse de que se observe lo establecido en la Ley de Seguridad Nacional, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, para la clasificación y resguardo de la información generada en esta actividad.

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Revisar, por lo menos una vez al año, el Catálogo de infraestructuras críticas de la Institución e instruir, en su caso, al Equipo de trabajo de infraestructuras críticas para que se efectúen los trabajos para su actualización.

ASI-5 Establecer la Directriz rectora para la administración de riesgos

El Grupo de trabajo estratégico de seguridad de la información, deberá:

1. Elaborar la Directriz rectora para la administración de riesgos, mediante las siguientes acciones:

a) Integrar los antecedentes y demás elementos que justifiquen la necesidad de implantar la administración de riesgos en la Institución.
b) Definir metodologías y herramientas que se usarán para administrar los Riesgos.
c) Integrar el marco normativo que resulte aplicable a los Riesgos identificados.
d) Establecer las reglas para medir la efectividad de los controles en la gestión de los riesgos.
e) Establecer la forma y periodicidad con las que se informará a los grupos y equipos de trabajo, a las áreas y unidades administrativas de la Institución y externos involucrados, sobre los Riesgos a los que se encuentran expuestos los procesos y servicios que utilizan.
f) Establecer consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la Institución.

2. Verificar que la Directriz rectora para la administración de riesgos permanezca actualizada, mediante las siguientes acciones:

a) La revisión de su adecuada alineación con el Modelo de gobierno de seguridad de la información.
b) La evaluación de las acciones adoptadas por incumplimientos detectados en la administración de los riesgos.
c) La revisión de los formatos de los reportes de ASI-6, al menos cada seis meses.

El Responsable de la Seguridad de la Información deberá:

1. Autorizar la Directriz rectora para la administración de riesgos.
2. Difundir la Directriz rectora para la administración de riesgos y sus actualizaciones a los involucrados y a los integrantes del Grupo de trabajo para la dirección de TIC, a fin de que sea conocida por los mismos.

El Grupo de trabajo estratégico de seguridad de la información, deberá:

3. Establecer el Repositorio de riesgos e integrar la información de la Directriz rectora para la administración de riesgos.

ASI-6 Elaborar el Análisis de riesgos

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Integrar el Equipo de trabajo de análisis de riesgos, mediante la elaboración del documento de integración del equipo de trabajo de análisis de riesgos, y asegurarse de que:

a) El Documento contenga, al menos: los objetivos y responsabilidades del Equipo de trabajo, los roles y responsabilidades de cada miembro, así como el funcionamiento del Equipo.

b) El Equipo se conforme con un número de entre 5 y 10 integrantes, quienes preferentemente deberán ser servidores públicos con conocimientos en materia de TIC, de seguridad de la información, de seguridad física y por aquéllos que se considere puedan aportar al Equipo mayor capacidad de análisis y alcance de objetivos.

c) Los integrantes del Equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan.

d) Se delimite el objetivo y alcance del Análisis de riesgos que se efectuará por el Equipo de trabajo.

2. Seleccionar al líder del Equipo y hacer de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados.
3. Integrar la información de los factores críticos anteriores en el Documento de Integración del equipo de trabajo de análisis de riesgos.

El Equipo de trabajo de análisis de riesgos, con el apoyo de las diversas áreas o unidades administrativas de la Institución involucradas, deberá:

4. Elaborar el Documento de identificación de procesos críticos, integrando en éste la información siguiente:

a) La de aquellos procesos de los que la Institución depende para alcanzar sus objetivos y niveles de servicio comprometidos, derivada de la identificación realizada conforme al factor crítico 2 de la actividad ASI-4, en los casos en que la Institución no hubiere identificado procesos críticos vinculados con la seguridad nacional.

b) La obtenida como resultado del desarrollo de la actividad ASI-4, por haberse identificado procesos críticos vinculados con la seguridad nacional.

5. Identificar los Activos de información e incluirlos en una relación detallada que se incorporará en el Documento de identificación de activos de información.

6. Consultar a los responsables de los Activos de información, para identificar los elementos que se pretende proteger ante la posible materialización de Amenazas e integrar la información obtenida en el Documento de identificación de activos de información.
7. Identificar las Vulnerabilidades, mediante las acciones siguientes:

a) Elaborar una relación de las características de los Activos de información, así como del ambiente y de la Institución en que se ubican los mismos, que pudieran ser aprovechadas para poner en riesgo la confidencialidad, integridad y disponibilidad de éstos.
b) Considerar como vulnerabilidad la ausencia y falla de controles.
c) Integrar a los responsables de la administración, operación y, en su caso, resguardo de los Activos de información en el proceso de identificación de vulnerabilidades.

8. Identificar Amenazas, mediante las acciones siguientes:

a) Elaborar el Documento de identificación de amenazas, registrando las posibles amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los Activos de información contenidos en el documento de identificación de activos de información.
b) Identificar y registrar en el documento del inciso anterior, los agentes que podrían materializar una Amenaza, utilizando la Lista de amenazas y agentes que se provee en el formato del mismo.

9. Elaborar el Documento de identificación y evaluación de escenarios de riesgo, en el que se deberán registrar y evaluar los escenarios de riesgo que se identifiquen, mediante las acciones siguientes:

a) Definir los escenarios, para lo cual es necesario efectuar los cálculos para establecer el valor del Riesgo para cada escenario, utilizando la fórmula: R=PI; en la que “P” es la probabilidad de ocurrencia de la Amenaza e “I” es el Impacto ocasionado por la materialización de la misma.
b) Integrar las variables complementarias que se indican en el formato del Documento de identificación de amenazas y sus ponderaciones, ya que éstas determinan el valor final del Riesgo, utilizando la tabla denominada “Probabilidad de ocurrencia contra impacto”, que se contiene en el formato del documento mencionado.

c) Definir la estrategia de seguridad para cada Riesgo, seleccionando alguna de las establecidas en el formato del Documento de identificación de amenazas: evitar, mitigar o reducir, financiar o asumir y transferir o compartir, debiendo evaluarse en este mismo orden.
d) Obtener la relación de riesgos que requieren atención, su prioridad y estrategia de seguridad.

10. Elaborar el Análisis de costo-beneficio de controles de seguridad, mediante las acciones siguientes:

a) Elaborar la lista de escenarios de riesgo, cuya acción de seguridad implica el uso de controles o la modificación de un proceso para evitar, mitigar o reducir, financiar o asumir y transferir o compartir los Riesgos.
b) Comparar el costo del control que se proponga contra el impacto que se podría ocasionar por la materialización del riesgo.
c) Utilizar el Documento de análisis de costo-beneficio de controles de seguridad, debiendo definir los valores indicados en éste, para cada escenario de riesgo.

11. Elaborar el Documento de resultados del análisis de riesgos, mediante las acciones siguientes:

a) Integrar la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad establecido, indicando además los requerimientos para su implantación.
b) Incluir, de ser el caso, el nivel de riesgo residual de cada escenario.
c) Elaborar e integrar las Declaraciones de aplicabilidad con los controles necesarios, de acuerdo a los resultados obtenidos de los factores críticos anteriores.
d) Elaborar e incluir las propuestas para los Programas de mitigación de riesgos, considerando los controles establecidos en las Declaraciones de aplicabilidad obtenidas.
e) Elaborar e incluir en el Documento de resultados del análisis de riesgos, la propuesta de Programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERISC.

12. Obtener del Grupo de trabajo estratégico de seguridad de la información, la aprobación del documento de resultados del análisis de riesgos y enviarlo a los responsables de los procesos en las diversas áreas y unidades administrativas de la Institución para su revisión.

Los responsables de los procesos en las diversas áreas y unidades administrativas de la Institución, con el apoyo del Equipo de trabajo de análisis de riesgos, deberán:

13. Seleccionar de entre los controles recomendados por el Grupo de trabajo estratégico de seguridad de la información, contenidos en el Documento de resultados del análisis de riesgos, aquéllos a implantar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas.
14. Justificar ante el Grupo de trabajo estratégico de seguridad de la información las razones por las cuales existan controles recomendados no seleccionados.

El Equipo de trabajo de análisis de riesgos, en coordinación con las áreas y unidades administrativas de la Institución involucradas, deberá:

15. Elaborar el Programa de implantación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada conforme al factor crítico 13 de esta actividad. Dicho Programa deberá incluir la designación de responsables de la implantación de cada control, de acuerdo al Documento de resultados del análisis de riesgos y los datos necesarios para su implantación, así como documentarse conjuntamente con la implantación de las acciones y controles del SGSI.
16. Obtener del Grupo de trabajo estratégico de seguridad de la información la aprobación del Programa de implantación para el manejo de riesgos y verificar su adecuada integración con las demás actividades de implantación o mejora de los controles y acciones del SGSI.

El Grupo de trabajo estratégico de seguridad de la información deberá:

17. Cuidar que el Análisis de riesgos se realice o actualice conforme a los factores críticos de esta actividad, al menos una vez al año, o bien, en caso de un cambio en los procesos, Activos de Información o cuando se detecte una nueva Amenaza o Vulnerabilidad a la seguridad de la información y/o los Activos de TIC que la soportan.
18. Asegurar que se obtengan los productos de esta actividad actualizados y se documente, en caso de ser procedente, la mejora continua que se efectúe derivada del factor crítico anterior.
19. Vigilar que se actualice el Repositorio de riesgos.

ASI-7 Integrar al SGSI los controles mínimos de Seguridad de la información

Descripción Definir los controles mínimos de Seguridad de la información e integrarlos al SGSI, para su implantación a través de los diversos procesos del Manual.

El Grupo de trabajo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:

1. Definir los controles de seguridad necesarios para salvaguardar a los Activos de TIC, las, Infraestructuras críticas y los Activos de información de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:

a) La definición, en términos de seguridad, de la viabilidad del software que se pretenda adquirir e instalar en los equipos de cómputo, dispositivos electrónicos o sistemas de información.
b) La designación de personal en las áreas relacionadas con el manejo, administración y gestión de los Activos de información de la Institución, con apego a las disposiciones jurídicas aplicables y, considerando los procedimientos que, en su caso, se tengan implantados en el área o unidad administrativa de que se trate.
c) La instalación y configuración del software, así como para la administración de la seguridad de las soluciones tecnológicas y servicios de TIC que se utilicen en la Institución.
d) El ingreso y salida de Activos de información.
e) El borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario.
f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los Activos de información.
g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
h) Los criterios de asignación de Usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.
i) La configuración de las herramientas de protección implementadas en las redes institucionales.

j) Las conexiones a redes públicas y privadas, así como para los dispositivos electrónicos que contengan Información considerada como reservada o sensible para la Institución.
k) La seguridad física y lógica que permita mantener la confidencialidad, integridad y disponibilidad de los respaldos de información.
l) El uso del servicio de Internet en la Institución, el cual debe contar con herramientas de seguridad y de filtrado de contenido.
m) El intercambio seguro de la información, ya sea de manera interna o hacia el exterior.
n) Que la información clasificada o aquélla que tiene valor para la Institución, sea respaldada y restaurada en el momento en que se requiera.
o) Contar con registros de auditoría y Bitácoras de seguridad, en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.

2. Documentar los controles determinados conforme al factor crítico anterior, incluyendo su definición detallada e integrarlos al Documento de definición del SGSI y elaborar conjuntamente con los responsables de los procesos institucionales involucrados, el Programa de implantación del SGSI.

ASI-8 Mejorar el SGSI

El Grupo de trabajo estratégico de seguridad de la información deberá:

1. Constatar, en coordinación con las áreas y unidades administrativas involucradas, que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica de la Institución se apliquen, a fin de hacer del conocimiento del Titular de la misma el cumplimiento de los controles de seguridad establecidos.
2. Obtener, del Informe de evaluación del SGSI, los datos sobre su desempeño, a fin de definir y documentar las acciones correctivas y preventivas para ajustar el mismo, integrarlas al documento Acciones preventivas y correctivas al SGSI.
3. Elaborar el Documento de implantación de la mejora al SGSI. Este documento debe utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.
4. Comunicar las mejoras que deberán aplicarse al SGSI al Responsable del grupo de trabajo para la implantación de la seguridad de la información, previsto

en la actividad OPEC-1, por medio de los productos: Acciones preventivas y correctivas al SGSI y el

Documento de implantación al SGSI.

5. Vigilar la implantación de las mejoras mediante el Informe de seguimiento a las acciones de mejora al SGSI.

4.4 Roles Involucrados

Roles y Responsabilidades de los procesos involucrados. Anexo 1 Formato 3

ROLES

Nombre del Rol	**Descripción del Rol**	**Perfil deseable**
Presidente	Responsable de la seguridad de la información en la Institución	Subdirector General de Informática.
Secretario	Responsable de dar seguimiento a los acuerdos del comité	Coordinador de Tecnología de la Información y Comunicaciones.
Vocal ejecutivo	Atender los asuntos de las sesiones y cuando exista alguna problemática en el cumplimiento de las responsabilidades del Grupo Estratégico de Seguridad de Información;	Dirección de Innovación, Supervisión y Proyectos.
Miembros	Responsables de los procesos de MAAGTIC-SI	Funcionario con nivel de jefe de departamento o superior.
Invitados	Se determinarán por el Presidente y el Vocal Ejecutivo, de acuerdo a la naturaleza de los asuntos a tratar contenidos en el Orden del Día, los casos en que se estime necesaria su asistencia.	Funcionario con nivel de jefe de departamento o superior.

RESPONSABILIDADES

Nombre del Rol	Descripción de la responsabilidad
Presidente	1. Declarar el quórum y presidir las sesiones; 2. Determinar, conjuntamente con el Vocal Ejecutivo, los asuntos del Orden del Día a tratar en las sesiones y, cuando corresponda, la participación de los responsables de las áreas competentes de la Institución; 3. Poner a consideración de los miembros el Orden del Día y las propuestas de acuerdos para su aprobación; 4. Autorizar el calendario de sesiones ordinarias; 5. Autorizar la celebración de sesiones extraordinarias; 6. Autorizar la participación de invitados externos ajenos al GESI y/o a la Institución; 7. Presentar los acuerdos relevantes que el GESI determine e informar de su seguimiento hasta su conclusión.
Secretario	1. Previo al inicio de la sesión, solicitar y revisar las acreditaciones de los miembros e invitados y verificar el quórum; 2. Convocar a las sesiones de conformidad con el punto de convocatoria; 3. Elaborar la propuesta de Orden del Día de las sesiones; 4. Coordinar la integración y captura de la minuta electrónica para su consulta por los convocados, de acuerdo a los tiempos señalados; 5. Vigilar que los acuerdos se cumplan en tiempo y forma; 6. Proponer el calendario de sesiones ordinarias; 7. Elaborar las minutas de las sesiones, enviarlas para revisión de los miembros y recabar las firmas, así como llevar su control y resguardo.
Vocal ejecutivo	1. Determinar, conjuntamente con el Presidente, los asuntos del Orden del Día a tratar en las sesiones del GESI y, cuando corresponda, la participación de los responsables de las áreas competentes de Pronósticos; 2. Presentar por sí, o en coordinación con el Presidente, asuntos a ser discutidos;

Nombre del Rol	**Descripción de la responsabilidad**
	3. Asesorar a los miembros para coadyuvar al mejor cumplimiento de los objetivos y metas del GESI; **4.** Dar seguimiento y verificar que el cumplimiento de los acuerdos se realice en tiempo y forma por los responsables, y registrar su atención en el Repositorio Central en la Intranet.
Miembros	1. Participar con voz y voto en las sesiones del GESI y proponer los asuntos a tratar en las mismas; 2. Proponer, en el ámbito de su competencia, los acuerdos para la atención de los asuntos de las sesiones y cuando exista alguna problemática en el cumplimiento de las responsabilidades del GESI; 3. Impulsar en el ámbito de su competencia, el cumplimiento en tiempo y forma de los acuerdos o recomendaciones aprobados; 4. Proponer la celebración de sesiones extraordinarias, cuando sea necesario por la importancia, urgencia y/o falta de atención de los asuntos; 5. Proponer la participación de invitados externos al GESI y/o a la Institución; 6. Proponer áreas de oportunidad para mejorar el funcionamiento del GESI; 7. Analizar la minuta electrónica de la sesión publicada en el Repositorio Central de la INTRANET, emitir comentarios respecto a la misma y proponer acuerdos; 8. Promover el cumplimiento de las presentes disposiciones, y las demás necesarias para el logro de los objetivos del GESI.
Invitados	1. Participar con voz, pero sin voto en las sesiones del GESI y proponer los asuntos a tratar en las mismas; 2. Proponer, en el ámbito de su competencia, los acuerdos para la atención de los asuntos de las sesiones y cuando exista alguna problemática en el cumplimiento de las responsabilidades del GESI;

Nombre del Rol	Descripción de la responsabilidad

4.5 Mapeo de los procesos a los formatos propuestos por el MAAGTIC-SI

ASI − Administración de la seguridad de la información.	
ASI	“Documento de integración y operación del grupo de trabajo estratégico de seguridad de la información”, anexo 5, formato 1.
ASI	“Directriz rectora para la administración de riesgos”, anexo 5, formato 2.
ASI	“Documento de integración del equipo de trabajo de infraestructuras críticas”, anexo 5, formato 3.
ASI	“Documento de identificación de infraestructuras críticas”, anexo 5, formato 4.
ASI	“Matrices de infraestructuras críticas y activos clave”, anexo 5, formato 5.
ASI	“Catálogo de infraestructuras críticas”, anexo 5, formato 6.
ASI	“Documento de integración del equipo de trabajo de análisis de riesgos”, anexo 5, formato 7.
ASI	"Documento de identificación de procesos críticos”, anexo 5, formato 8.
ASI	“Documento de identificación de activos de Información”, anexo 5, formato 9.
ASI	“Documento de identificación de amenazas”, anexo 5, formato 10.
ASI	“Documento de identificación y evaluación de escenarios de riesgo”, anexo 5, formato 11.

ASI	"Documento de análisis de costo-beneficio de controles de seguridad", anexo 5, formato 12.
ASI	"Declaraciones de aplicabilidad", anexo 5, formato 13.
ASI	"Programas de mitigación de riesgos", anexo 5, formato 14.
ASI	"Programa de contingencia a los riesgos", anexo 5, formato 15.
ASI	"Documento de resultados del análisis de riesgos", anexo 5, formato 16.
ASI	"Programa de implantación para el manejo de riesgos", anexo 5, formato 17.
ASI	"Documento de definición del SGSI", anexo 5, formato 18.
ASI	"Programa de implantación del SGSI", anexo 5, formato 19.
ASI	"Programa de evaluaciones del SGSI", anexo 5, formato 20.
ASI	"Directriz rectora de respuesta a incidentes", anexo 5, formato 21.
ASI	"Informe de evaluación del SGSI", anexo 5, formato 22.
ASI	"Acciones preventivas y correctivas de mejora al SGSI", anexo 5, formato 23.
ASI	"Informe de seguimiento a las acciones de mejora al SGSI", anexo 5, formato 24.
ASI	"Documento de implantación de la mejora al SGSI", anexo 5, formato 25.

4.6 Evaluación de riesgos por probabilidad y grado de impacto

1. FORMA DE OPERACIÓN DEL GRUPO:

PROGRAMACIÓN DE SESIONES ORDINARIAS

- **Convocatoria.** Se programarán de forma semestral, con convocatoria de un mes de anticipación a su celebración.

PROGRAMACIÓN DE SESIONES EXTRAORDINARIAS

- **Convocatoria.** Se programarán en caso de existir algún proceso en estado crítico, comprometiendo la operación de proyectos o servicios de alto impacto, será necesario celebrar una sesión extraordinaria con convocatoria de por lo menos un día de anticipación.

DESCRIPCIÓN DE LA OPERACIÓN DEL GRUPO

- **Difusión de responsabilidades.** Una vez firmado el presente documento por los miembros del GESI, el Vocal Ejecutivo informará a todos los colaboradores de la Subdirección General de Informática mediante el Portal interno de Pronósticos (Intranet) que funge como repositorio central de las actividades de la Subdirección.
- **Puntos de Acuerdo.** Estos se establecerán conforme al planteamiento de alguno de los miembros y bajo votación, teniendo voto de calidad, el Presidente del GESI. Los puntos de acuerdo pretenden ser decisiones que se comportarán como Reglas, Normas, Lineamientos que de manera continua aplicarán a toda la Institución, documentándose en la minuta de la sesión.
- **Puntos de Acción.** Los puntos de acción son resultado de decisiones, teniendo fronteras de tiempo y asignación específica.
- **Seguimiento a Asuntos.** Tanto los puntos de acuerdo, como los puntos de acción serán monitoreados y vigilados para su cumplimiento, para ello el área a la que pertenece el Vocal Ejecutivo será la responsable de tal monitoreo, reportando al GESI de manera continua y como parte preparativa a la sesión periódica, e incluso promoviendo sesiones extraordinarias.

OTROS ASPECTOS RELEVANTES PARA LA OPERACIÓN DEL GRUPO

- **Obligatoriedad y asistencia mínima.** La participación de los miembros durante la sesión será de carácter obligatorio, siendo posible la participación de suplentes, de acuerdo al protocolo establecido. La asistencia mínima para hacer válidos los acuerdos será de por lo menos tres miembros, en caso contrario, se cancelará la sesión, demandando su nueva planeación.

- **Suplentes.** Los miembros podrán nombrar a sus respectivos suplentes de nivel jerárquico inmediato inferior, quienes intervendrán en las ausencias de aquellos. Para fungir como suplentes, los servidores públicos deberán contar con acreditación por escrito dirigida al Vocal Ejecutivo, de la que se dejará constancia en la minuta y en la carpeta electrónica correspondiente. Los suplentes asumirán en las sesiones a las que asistan las funciones que corresponden a los miembros.
- **Documentación de la minuta y divulgación de acuerdos.** El Secretario documentará en la minuta electrónica de la sesión el quórum asistente, los Puntos de Acuerdo y los Puntos de Acción, publicándola en la Intranet de Pronósticos a más tardar tres días posteriores a la sesión, una vez que se integren las firmas electrónicas (FIEL) de los participantes.

Directrices de administración de riesgos

Necesidad	Directriz de administración de riesgos	Escenario
a) Detección temprana de interrupción en el servicio de los aplicativos b) Prevención de falta de disponibilidad del servicio c) Aplicación oportuna de mejoras al funcionamiento de los aplicativos d) Eliminar fallas o incidencias recurrentes mediante soluciones conocidas	a) Monitoreo diario de TCB b) Monitoreo diario de aplicativos c) Monitoreo de los procesos que se ejecutan en Sistema Central (Mainframe)	Fallos en Infraestructura de la Plataforma Tecnológica (hardware, software y telecomunicaciones).
a) Detección temprana de interrupciones y puesta en marcha de planeas de acción oportunos para restablecer el servicio	a) Migración a Red de Telecomunicaciones MPLS con redundancias en esquema ADSL	Interrupción en las líneas de Telecomunicación con las sucursales.
a) Mejor desempeño de los aplicativos en el acceso de información almacenada en la Base de Datos.	a) Convenios Modificatorios con actuales proveedores para redefinición de responsabilidades en el cumplimiento de las políticas y procedimientos: b) Mantenimiento a la Base de Datos	Deficiencias en la aplicación de políticas y procedimientos para el mantenimiento de la integridad de las bases de datos.
Detección oportuna de incidencias o posibles fallas en algunos de los componentes mencionados; y prevención de intermitencias en el servicio por falta de capacidades en cualquiera de los componentes.	Crecimiento de la infraestructura acorde a los resultados de la Planeación de capacidades. Análisis de capacidades de los componentes que integran la Plataforma Tecnológica, Bases de Datos, Memoria, CPU, Anchos de Banda, Espacio en Disco (SAN), etc.	Inapropiado crecimiento de la infraestruct hardware, respecto a los requerimientos del negocio derivado de la generación de nuevos productos, con altos volúmenes de transaccionalidad.
a) Detección temprana de interrupción en el Servicio de los aplicativos b) Prevención de falta de disponibilidad del servicio b) Aplicación oportuna de mejoras al funcionamiento de los aplicativos b) Eliminar fallas o incidencias recurrentes median soluciones conocidas	b) Monitoreo diario de aplicativos c) Monitoreo de los procesos que se ejecutan en Sistema Central (Mainframe)	Incumplimiento de niveles de servicio acc con los clientes y usuarios de la

Necesidades de administración de riesgos por Dominio tecnológico.

Necesidad	Estructura actual del dominio que se requiere proteger	Estructura a alcanzar
a) Detección temprana de interrupción en el servicio de los aplicativos. b) Prevención de falta de disponibilidad del servicio. c) Aplicación oportuna de mejoras al funcionamiento de los aplicativos. d) Eliminar fallas o incidencias recurrentes mediante soluciones conocidas.	Ocurrencia: Media-Posible Impacto : Medio-Serio Cuadrante: Rojo	Control, mitigación, medición.
a) Detección temprana de interrupciones y puesta en marcha de planes de acción oportunos para restablecer el servicio.	Ocurrencia: Media-Posible Impacto : Medio-Serio Cuadrante: Rojo	Control, mitigación, medición.
a) Mejor desempeño de los aplicativos en el acceso de información almacenada en la Base de Datos.	Ocurrencia: Media-Posible Impacto : Medio-Serio Cuadrante: Rojo	Control, mitigación, medición.
Detección oportuna de incidencias o posibles fallas en algunos de los componentes mencionados; y prevención de intermitencias en el servicio por falta de capacidades en cualquiera de los componentes.	Ocurrencia: Media-Posible Impacto : Medio-Serio Cuadrante: Rojo	Control, mitigación, medición.

No. Riesgo	Activo de TIC	Tipo de amenaza	Agente de amenaza identificada	Probabilidad	Descripción del riesgo	Nivel de riesgo (severidad)	Descripción del impacto	Nivel de impacto (severidad)	Tratamiento del riesgo
Riesgo # 1	Hardware	Fallas en los sistemas	Interrupción de sistemas, saturación de procesos y caída de enlaces	Media	Fallos en la infraestructura de la Plataforma Tecnológica (hardware, software y comunicaciones)	Medio	Poca o nula disponibilidad de aplicativos para procesos críticos de soporte	Medio	A) a) Monitoreo diario del core bancario
	Software								B) b) Monitoreo diario de aplicativos.
	Telecomunicaciones								C) c) Monitoreo de los procesos que se ejecutan en el sistema central

Riesgo # 2	Líneas de telecomunicación con las sucursales	Interrupción	Intermitencia de la comunicación con las sucursales	Media	Interrupción en las líneas de telecomunicación con las sucursales	Medio	Retraso o falta de atención a clientes en sucursal	D) Medio	E) Migración a red de telecomunicaciones.
Riesgo # 3	Integridad de Bases de Datos	Ejecución, entrega y gestión de procesos	Alteración en los datos, lo que puede ocasionar la falta de disponibilidad y confidencialidad de la información	Media	Deficiencias en la aplicación de políticas y procedimientos para el mantenimiento de la integridad de las bases de datos	Medio	Alteración en Bases de Datos	F) Medio	a) Convenios modificatorios con actuales proveedores para redefinición de responsabilidades en el cumplimiento de las políticas y procedimientos. b) Mantenimiento a la Base de Datos.
Riesgo # 4	Infraestructura de hardware	Incidencias en el negocio	Inapropiado crecimiento de la infraestructura (respecto a los requerimientos del negocio derivado de nuevos negocios)	Medio	Inapropiado crecimiento de la infraestructura del hardware, respecto a los requerimientos del negocio derivado de la generación de nuevos productos con altos volúmenes de transaccionalidad.	Media	Inadecuada gestión de los procesos	G) Medio	Crecimiento de la infraestructura acorde a los resultados de la planeación de capacidades. Análisis de capacidades de los componentes que integran la plataforma tecnológica .
Riesgo # 5	Niveles de servicio establecido	Recepción, ejecución y mantenimiento de operaciones	Falla en los sistemas y comunicación ineficiente	Medio	Incumplimiento de los niveles de servicio acordados con los clientes y usuarios de la PTB	Media	Incumplimiento en niveles establecidos por contratos y perdidas de negocio.	H) Medio	a) Monitoreo diario del core b) Monitoreo diario de aplicativos. c) Monitoreo de los procesos que se ejecutan en el sistema central (Mainframe).

Algunas categorías sugeridas para los campos de la Matriz de riesgo son las siguientes:

Tipo de amenaza	Acción	Activo/recurso
Maliciosa	Divulgación	Gente y organización
Accidental	Interrupción	Procesos
Falla	Modificación	Infraestructura
Natural	Regulación	Componentes de la arquitectura de negocio

Controles actualmente implementados				
Control	**Responsable**	**Tipo**	**Frecuencia**	**Justificación**
Monitoreo diario	Ingeniero en Sistemas	Detección / Prevención	Diario	Detección temprana de una posible interrupción o intermitencias en el funcionamiento del core bancario “TCB”. Prevención de una posible falta de disponibilidad del servicio.
B) B) Monitoreo diario de aplicativos.	Ing. Aquiles Alfredo Montaño	Detección / Prevención	Diario	Detección temprana de posibles fallos en el funcionamiento de otros aplicativos críticos. Aplicación oportuna de mejoras al funcionamiento de los aplicativos.

C) C) Monitoreo de los procesos que se ejecutan en el sistema central (Mainframe).	Ing. Aquiles Alfredo Montaño	Detección / Prevención	Diario	Eliminar fallas o incidencias recurrentes en los procesos del Mainframe a través de soluciones conocidas.

Identificación de la SoA	Hardware, Software y Telecomunicaciones.

Número de Riesgo	1
Descripción	Fallos en infraestructura de la Plataforma Tecnológica (hardware, software y comunicaciones).
Evaluación	Impacto Medio – Probabilidad Media.

Identificación del Programa	PTAR (Programa de Trabajo de Administración de Riesgos)
Número de Riesgo	1
Descripción	Fallos en infraestructura de la Plataforma Tecnológica (hardware, software y comunicaciones).
Impacto	Poca o nula disponibilidad de aplicativos para procesos críticos de soporte a procesos.
Controles Asociados	A) A) Monitoreo diario al TCB. B) B) Monitoreo diario de aplicativos. C) Monitoreo de los procesos que se ejecutan en el sistema central (Mainframe).
Número Actividad	**Responsable**

VALORACIÓN

La siguiente tabla muestra la escala de valores que se debe considerar para hacer la valoración de los Activos e identificar aquellos que resultan críticos para la Institución:

Tabla 1:

Valor	Descripción
1	La brecha puede resultar en poca o nula pérdida o daño.
2	La brecha puede resultar en una pérdida o daño menor.
3	La brecha puede resultar en una pérdida o daño medio, y los procesos de la Dependencia pueden verse afectados negativamente, sin llegar a fallar o causar su interrupción.
4	La brecha puede resultar en una pérdida o daño serio o considerable, y los procesos de la Dependencia pueden fallar o interrumpirse.
5	La brecha puede resultar en altas pérdidas monetarias, o en un daño crítico a un individuo o a la sociedad, reputación, privacidad y/o competitividad de la Dependencia. Los procesos de negocio de la Dependencia fallarán.

Debido a que la **Valoración deberá ser la suma de los valores asignados a la confidencialidad, integridad y disponibilidad**, debe emplear los rangos de la tabla siguiente al calcular el valor final:

Tabla 2:

*Rango	Valor
3 – 5	Bajo (1)
6 – 10	Medio (2)
11 – 15	Alto (3)

***Rango es la suma de valores por pérdida de confidencialidad, integridad y disponibilidad**

Para cada Activo identificado se debe efectuar su Valoración para establecer de manera cuantitativa su criticidad dentro de un proceso, debe elaborar la siguiente tabla:

Tabla 3:

Activo			Valoración					
Id. Proceso	**Id. Activo**	**Activo de información**	**C**	**I**	**D**	**Total**	**Valor 1**	**Valor 2**

[Donde C, I y D representan confidencialidad, integridad y disponibilidad, Valor 1 estará expresado en términos cualitativos (bajo, medio o alto) y Valor 2 será el valor cuantitativo (entre 1 y 3]).

PARÁMETROS DE INFLUENCIA PARA DETERMINAR UNA IC.

Tabla 4:

Parámetro		Descripción
a.	Amplitud geográfica:	1. Alcance geográfico y cantidad de personas afectadas.
b.	Período de afectación:	1. Interrupción de los servicios en horas.
c.	Cantidad de IC afectadas:	1. La ocurrencia de un Evento afecta además a otras IC de cualquier Sector y Subsector (efecto cascada).
d.	Campos de gobierno: la ocurrencia de un Incidente afecta además a otros campos de gobierno, entendiendo como tales a:	1. Impacto social (pérdidas de vidas, enfermedades, lesiones graves, evacuación). 2. Económico (efecto en el PIB, volumen de pérdida económica y/o degradación de productos o servicios). 3. Ambiental (Impacto en el lugar y sus alrededores). 4. Gobernabilidad (capacidad del Estado para responder a una contingencia, así como atender uno o varios problemas al mismo tiempo en diferentes escenarios).

1. ELABORACIÓN DE MATRICES.

En esta sección se efectúa la construcción de las matrices que integran los parámetros de influencia de una IC. El empleo de estas matrices como instrumentos permitirá identificar una IC.

a. Matriz de Impacto.

Referencias:

Amplitud geográfica	Calificación
Municipal o hasta 100,000 habitantes	1
Estatal o hasta 5,000,000 habitantes	2
Nacional e Internacional o más de 5,000,000 habitantes	3

Período de afectación	Calificación
24 horas o menos	1
Hasta 72 horas	2
Más de 72 horas	3

Asignación de valores:

Impacto		Período de afectación		
		1	**2**	**3**
Amplitud geográfica	**1**	1	2	3
	2	2	3	4
	3	3	4	5

Descripción de valores:

Calificación	Descripción
1	Afectación municipal con interrupción por 24 horas o menos
2	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos
3	Afectación municipal con interrupción de más de 72 horas
	Afectación estatal con interrupción de hasta 72 horas
	Afectación nacional/internacional con interrupción de 24 horas o menos
4	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas
5	Afectación nacional/internacional con interrupción de más de 72 horas

b. Matriz de Interdependencia.

Referencias:

IC afectadas	Calificación
Sólo una IC es afectada	1
La IC afecta a otra	2
La IC afecta a 3 o más IC	3

Campos de gobierno afectados	Calificación
1	1
2	2
3 o más	3

Asignación de valores:

Interdependencia		Campos de gobierno		
		1	2	3
IC afectadas	1	1	2	3
	2	2	3	4
	3	3	4	5

Descripción de valores:

Calificación	Descripción
1	Sólo es en una IC y un sólo campo de gobierno
2	Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno
3	Sólo es en una IC pero implica a tres o más campos de gobierno
	Dos IC son afectadas implicando a dos campos de gobierno
	Tres o más IC son afectadas en un sólo campo de gobierno

Calificación	Descripción
4	Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno
5	Tres o más IC son afectadas implicando tres o más campos de gobierno

c. Integración de la Matriz de Criticidad.

Criticidad		Interdependencia				
		1	2	3	4	5
Impacto	1	I	II	III	III	IV
	2	II	III	III	IV	IV
	3	III	III	IV	IV	V
	4	III	IV	IV	V	V
	5	IV	IV	V	V	V

Descripción de valores:

Calificación	Descripción
I	Afectación municipal con interrupción por 24 horas o menos Sólo es en una IC y un solo campo de gobierno

Calificación	Descripción
II	Afectación municipal con interrupción por 24 horas o menos Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno
II	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos Sólo es en una IC y un sólo campo de gobierno

Calificación	Descripción
III	Afectación municipal con interrupción por 24 horas o menos
	Sólo es en una IC pero implica a tres o más campos de gobierno
	Dos IC son afectadas implicando a dos campos de gobierno
	Tres o más IC son afectadas en un sólo campo de gobierno
	Afectación municipal con interrupción por 24 horas o menos Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno
	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno
	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos Sólo es en una IC pero implica a tres o más campos de gobierno Dos IC son afectadas implicando a dos campos de gobierno

Calificación	Descripción
	Tres o más IC son afectadas en un sólo campo de gobierno
	Afectación municipal con interrupción de más de 72 horas Afectación estatal con interrupción de hasta 72 horas Afectación nacional/internacional con interrupción de 24 horas o menos Sólo es en una IC y un sólo campo de gobierno
	Afectación municipal con interrupción de más de 72 horas Afectación estatal con interrupción de hasta 72 horas Afectación nacional/internacional con interrupción de 24 horas o menos Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno
	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas Sólo es en una IC y un sólo campo de gobierno

Calificación	Descripción
IV	Afectación municipal con interrupción por 24 horas o menos Tres o más IC son afectadas implicando tres o más campos de gobierno
	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno
	Afectación municipal con interrupción de hasta 72 horas Afectación estatal con interrupción de 24 horas o menos

Calificación	Descripción
	Tres o más IC son afectadas implicando tres o más campos de gobierno
	Afectación municipal con interrupción de más de 72 horas Afectación estatal con interrupción de hasta 72 horas Afectación nacional/internacional con interrupción de 24 horas o menos Sólo es en una IC pero implica a tres o más campos de gobierno Dos IC son afectadas implicando a dos campos de gobierno Tres o más IC son afectadas en un sólo campo de gobierno
	Afectación municipal con interrupción de más de 72 horas Afectación estatal con interrupción de hasta 72 horas Afectación nacional/internacional con interrupción de 24 horas o menos Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno
	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas Sólo es en una IC pero implica a tres o más campos de gobierno Dos IC son afectadas implicando a dos campos de gobierno Tres o más IC son afectadas en un sólo campo de gobierno
	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno
	Afectación nacional/internacional con interrupción de más de 72 horas Sólo es en una IC y un sólo campo de gobierno
	Afectación nacional/internacional con interrupción de más de 72 horas

Calificación	Descripción
	Sólo es en una IC pero implica a dos campos de gobierno Dos IC son afectadas, ambas en sólo un campo de gobierno

Calificación	Descripción
V	Afectación municipal con interrupción de más de 72 horas Afectación estatal con interrupción de hasta 72 horas Afectación nacional/internacional con interrupción de 24 horas o menos Tres o más IC son afectadas implicando tres o más campos de gobierno
	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno
	Afectación estatal con interrupción de más de 72 horas Afectación nacional/internacional con interrupción de hasta 72 horas Tres o más IC son afectadas implicando tres o más campos de gobierno
	Afectación nacional/internacional con interrupción de más de 72 horas
	Sólo es en una IC pero implica a tres o más campos de gobierno
	Dos IC son afectadas implicando a dos campos de gobierno
	Tres o más IC son afectadas en un sólo campo de gobierno
	Afectación nacional/internacional con interrupción de más de 72 horas Dos IC son afectadas implicando a tres o más campos de gobierno Tres o más IC son afectadas implicando a dos campos de gobierno

Calificación	Descripción
	Afectación nacional/internacional con interrupción de más de 72 horas Tres o más IC son afectadas implicando tres o más campos de gobierno

Beneficios

En materia de seguridad informática, se concluyó con la configuración, pruebas y puesta a punto de la herramienta de administración centralizada de políticas de seguridad. Con estas acciones se reducirá de manera importante los costos asociados a estas actividades, mismas que se realizan al menos dos veces al año. Lo anterior, conforme lo establecen las políticas de seguridad vigentes, así como las mejores prácticas y la normatividad aplicable a las Instituciones.

Capítulo 5. CONTROL Y MONITOREO

Capítulo 5. Control y Monitoreo

Monitorear y controlar todos los aspectos de un proyecto resulta un proceso importante ya que podemos determinar si los alcances y metas estipulados en el momento de la planeación realmente se están cumpliendo, todo esto es a lo largo y durante el ciclo de vida del proyecto por esto nos da la un correcto control sobre el proyecto así como las acciones correctivas que se pueden tomar para retomar el camino hacia dichos objetivos y metas planteados.

Objetivo

Monitorear y Controlar la agenda del proyecto así como los productos de trabajo y el seguimiento de la planeación con la finalidad de tener una perspectiva sobre el estado del proyecto y tomar acciones y decisiones correctivas y preventivas según sea el caso.

Alcance

Todas las fases del ciclo de vida, dado que durante este, se realizaran todas las tareas de monitoreo de los productos de trabajo productos de los otros procesos que conforman el proyecto en su conjunto.

Los indicadores son necesarios para llevar a cabo este proceso. Los indicadores son los elementos que se utilizan para medir la información cuantitativa y cualitativa recopilada durante o después de la implementación de una acción, proyecto o programa, a fin de medir los resultados y efectos de su puesta en práctica. Los indicadores están directamente relacionados con las metas, los objetivos y las actividades del proyecto o programa.

5.1 Bitácora de Control de Cambios

ACMB – Administración de Cambios

ACMB-1 Establecer un punto único de gestión de solicitudes de cambio

Se debe establecer un punto único a través del cual se administre el ciclo de vida de las solicitudes de cambio, que permita su seguimiento y control.

El Administrador del proceso de Administración de cambio, conjuntamente con el Administrador de cambios, deberán:

1. Establecer el punto central para la administración de cambios y realizar la difusión del mismo entre los involucrados, incluidos aquellos que tendrán el rol de solicitante del

cambio, con el propósito de minimizar la probabilidad de conflictos entre cambios, que derive en una posible afectación al ambiente operativo.

2. Definir a través de medios de comunicación se efectuará la difusión de la administración de cambios.

3. Definir los criterios para seleccionar la herramienta de software para el proceso de Administración de cambios, que permita la recepción y gestión de la solicitud de cambio.

ACMB-2 Definir el mecanismo de gestión de la solicitud, evaluación y atención del cambio

Establecer el mecanismo mediante el cual se realizará la solicitud de modificación de un elemento del entorno operativo actual, así como establecer qué información se requerirá integrar a dicha solicitud para su gestión.

El Administrador del proceso de Administración de cambio, conjuntamente con el Administrador de cambios, deberán:

1. Definir los datos mínimos que se requieren de las unidades responsables y usuarios, así como de los servidores públicos de la propia UTIC, que por las actividades de los procesos en los cuales intervienen requieran solicitar algún tipo de cambio.

2. Establecer un control para asegurar que en la solicitud de cambio se identifiquen los riesgos potenciales derivados del cambio, incluyendo tanto riesgos de tipo técnico como funcionales.

3. Establecer un identificador único por cada solicitud de cambios, para evitar la duplicidad de los mismos y facilitar su monitoreo.

4. En caso de tratarse de un cambio derivado de un incidente, problema o iniciativa, incluidas la de mejora, referir el identificador de esos otros registros.

5. Procurar que la solicitud incluya una ventana de tiempo del cambio, en la que se considere el tiempo que demandará aplicar todas las actividades, cuando sea pertinente.

6. Definir y comunicar las autorizaciones con las que deberán contar las unidades responsables y usuarios, así como los servidores públicos de la propia UTIC solicitantes del cambio para hacer su solicitud, cuando así aplique.

7. Solicitar que se enlisten, en el Repositorio o inventario de los elementos del ambiente productivo, los elementos que serán impactados directa o indirectamente por el cambio.

8. Establecer la documentación mínima que se requerirá para soportar la solicitud de cambio.
9. Definir qué documentación será la mínima requerida para solicitar un cambio de emergencia.
10. Determinar qué documentación sería opcional para ciertos tipos de cambio.
11. Definir los tipos de cambio posibles, para la clasificación de las solicitudes de cambio, se deberá considerar al menos los tres tipos siguientes:
• Cambio de rutina.
• Cambio normal.
• Cambio de emergencia.
12. Desarrollar un procedimiento en particular para cada tipo de cambio.
13. Establecer un mecanismo para diferenciar aquellos cambios que resultan de un incidente o problema, de los que derivan con motivo de una mejora.
14. Definir durante el diseño del proceso de Administración de cambios, los estatus que reflejen los diferentes estados por los que puede pasar un cambio.
15. Los estatus del cambio deberán estar disponibles para su uso en la herramienta de software del proceso y deberán ser susceptibles de cambiar conforme se requiera.
16. Definir las reglas que aplicarán para el cambio de estatus de un registro de cambio en la herramienta de software.
17. Deberán considerarse, para resolver los cambios, al menos los cuatro tipos de prioridad siguientes:
• Baja.
• Normal.
• Alta.
• Urgente.
18. Definir los niveles que se necesitarán para categorizar los cambios.
19. Definir las categorías de cambio que se prevé puedan abarcar la mayor parte de los posibles tipos de cambio, considerando su naturaleza.
20. Las categorías de los cambios deberán describir el rubro afectado, tales como: procesos, hardware, software, aplicaciones.
21. Las subcategorías deberán estar relacionadas con la categoría del nivel anterior y refieren el detalle de ese nivel.

ACMB-3 Definir los equipos responsables de evaluar y ejecutar el cambio

Definir los equipos responsables de evaluar y ejecutar los cambios que se autoricen, con base en el origen, complejidad y alcance de los cambios que se presentan.

El Administrador del proceso de Administración de cambio, conjuntamente con el Administrador de cambios, deberán:

1. Identificar dentro de la UTIC a los especialistas para la evaluación y ejecución de cambios.
2. Registrar en la herramienta de software para el proceso de Administración de cambios a los especialistas identificados.

ACMB-4 Registro y clasificación de la solicitud de cambio

Efectuar el registro de la solicitud del cambio y determinar su impacto, la urgencia y prioridad respecto a otros cambios y la ruta que se seguirá para su evaluación.

El Administrador de cambio deberá:

1. Recibir la solicitud de cambio por los canales de comunicación establecidos para este fin.
2. Validar que la solicitud de cambio se entregó en el formato que se haya definido con ese propósito, para lo cual:

• Verificará que la solicitud contenga el detalle del cambio.

• Verificará que contenga la justificación de la solicitud de cambio, en términos de beneficios para la Institución.

3. Rechazar las solicitudes de cambios incompletos.
4. Validar que el solicitante del cambio esté autorizado para requerirlo.
5. Contar preferentemente con una herramienta de software que permita capturar en un registro electrónico, la información prevista en la solicitud de cambio.
6. Clasificar y registrar la solicitud de cambio con base en la información prevista en el formato y la documentación de soporte adjunta, tomando en cuenta los tipos de prioridad descrito en la actividad ACMB-1.
7. Generar las órdenes de trabajo para la evaluación del cambio, cuando por el tipo de cambio así se requiera.

Toda la información que se genera en esta actividad actualizará el Repositorio de solicitudes de cambio.

ACMB-5 Evaluación y coordinación del cambio

Efectuar la evaluación de la solicitud del cambio y coordinar a los involucrados para su ejecución, debiendo establecer el programa asociado al cambio solicitado.

Los Especialistas responsables de ejecutar el cambio deberán:

1. Considerar para la evaluación lo siguiente:

• Solicitante del cambio.

• Justificación del cambio.

• Beneficios del cambio.

• Riesgos asociados al cambio.

• Recursos que se requieren para realizar el cambio.

• Responsables de la ejecución prueba e implementación del cambio.

• Relación de este cambio con otros previos.

• Tipo de cambio y prioridad del cambio.

ACMB-6 Canalización de la solicitud de cambio

Efectuar la canalización de la solicitud de cambio y su orden de trabajo dependiendo de su tipo, así como de su prioridad y categoría, la solicitud se dirige la actividad que aplique, según el procedimiento que corresponda.

El Administrador de cambios y los Especialistas responsables del cambio deberán de:

1. Determinar qué procedimiento aplica para el tratamiento de la solicitud, con base en el tipo, prioridad y categoría.

2. Canalizar la solicitud de cambio y su orden de trabajo a la actividad que corresponda, según el procedimiento.

3. Documentar todas las actividades realizadas en el registro del cambio.

4. Dar seguimiento al avance del cambio.

ACMB-7 Pruebas previas y posteriores al cambio

Ejecución de pruebas previas a la implantación del cambio, y de pruebas una vez implantado en mismo.

Los especialistas responsables de ejecutar el cambio, con el apoyo del Administrador de cambios, deberán:

1. El Programa de pruebas y su ejecución son obligatorios para cualquier tipo de cambio.

2. Incluir, todo cambio, al Programa de retorno, a través del cual será posible regresar el entorno a su estado original.

3. Registrar la información detallada e inmediata acerca de la solicitud del cambio y los resultados de ésta como un elemento de configuración, de acuerdo con el proceso de Administración de la configuración.

ACMB-8 Revisión y cierre del cambio

Revisar y valorar los resultados del cambio efectuado.

El Administrador de cambios, con el apoyo de los Especialistas responsables de ejecutar el cambio, deberán:

1. Considerar para la revisión y valoración lo siguiente:

• El cumplimiento de los objetivos.

• La percepción de los usuarios respecto al cambio.

• Averiguar si se utilizaron los programas de retorno en alguna fase del proceso.

• Si las actividades realizadas en el cambio se hicieron conforme a lo planeado o si se presentó alguna desviación importante que haya derivado en un riesgo para el ambiente operativo o para el cambio mismo, o haya resultado en la falla del cambio.

2. Confirmar si el cambio logró su objetivo.

3. Verificar con el representante de los involucrados si surgieron incidentes o problemas, a partir de la aplicación del cambio.

4. Medir la satisfacción del solicitante del cambio y demás involucrados, respecto a la ejecución del cambio y a los resultados logrados.

Obtener el visto bueno de todos los involucrados para el cierre del cambio.

5. Documentar todas las actividades realizadas, en el registro del cambio.

6. La evaluación del rendimiento del proceso se efectuará mediante el proceso de Administración de la evaluación de TIC.

Toda la información generada en esta actividad deberá integrarse al Repositorio de solicitudes de cambio y actualizarse.

Capítulo 6. RESULTADOS

Capítulo 6. Resultados

Resultados

- Homologación de los procesos MAAGTIC-SI formado por las mejores prácticas.
- percibir, entender y actuar sobre los procesos que ocurren en el medio ambiente del cliente, y cómo utilizar las TI como una herramienta de cambio dentro de estos.
- consultoría de procesos permite a los clientes aprender a diagnosticar y comprender por sí mismos sus procesos y cómo las TI pueden colaborar a mejorarlos o cambiarlos. desde el punto de vista de su alineamiento con las estrategias de negocio y del cumplimiento de buenas prácticas en la gestión de procesos.
- Rediseño de Procesos orientado a definir cambios o mejoras en el flujo de proceso, estructura organizacional, cultura organizacional y tecnologías de información de apoyo.

IMPLANTACIÓN DE MAAGTIC EN LOS PROCESOS DEL SECTOR GOBIERNO BASADO EN LAS MEJORES PRÁCTICAS

CONCLUSIONES

Conclusiones

Al enfrentarme por primera vez con una empresa cuyos procesos no se encontraban claros ni definidos, tuve la oportunidad de darme cuenta de la importancia de documentar de manera adecuada los procesos, nadie quiere documentar; pero es necesario llevar un orden de la evolución o avance del día a día, considero que MAAGTIC-SI reúne las características para homologar cada uno de los procesos.

En el mundo sólo el 16.2% de los proyectos en general son exitosos, el resto son cancelados antes de ser terminados o cuando estar finalizados no cubren las expectativas que se vislumbraban, lo que lleva a pérdidas multimillonarias. Los datos reflejan la falta de cultura de gestión de proyectos.

Para tener claro el por qué del fracaso de un proyecto es necesario documentarlo y registrar cada proceso del proyecto, esto lo permite MAAGTIC-SI. Esto para poder identificar en donde están los problemas para hacer correcciones oportunas del proyecto; MAAGTIC-SI es muy determinante en cuando a sus niveles de gestión y sus procesos por esto al documentar podrías darte cuenta que el problema esta en la Dirección, en la toma re requerimientos, una mala definición del alcance del proyecto, en el control de cambios, en los jefes de proyecto, en una gestión de servicios inadecuada, la falta de monitoreo, desarrollo de software inadecuado, la falta de un alineamiento estratégico entre otros varios.

Para que una empresa sea exitosa debe tener control sobre sus recursos y servicios sin esto estará destinada al fracaso.

Lesly Alvízo García

En la medida en la que trabajamos juntos para generar un cambio en la cultura empresarial de nuestro país, tendremos empresas institucionales. Es cuestión de supervivencia; las empresas que no apuesten por consolidar cada día más su estructura de gobierno corporativo no lograrán su desarrollo sustentable.

En nuestro país, el concepto de Gobierno Corporativo ha sido adoptado por la comunidad empresarial que reconoce el aporte y valor significativo, el cual atiende no solo a las regulaciones aplicables u obligatorias para las compañías, sino que además promueva la buena imagen corporativa y las sanas relaciones de negocio en las TIC. Para competir es importante asegurar eficiencia, transparencia, equidad y resultados en la empresa.

Administrar los procesos de TI de una organización requiere más allá de conocimiento, es saber trabajar en equipo, delegar y dar mérito a quien lo merece, es fundamental en la educación de un líder.

Como mencionamos a lo largo de este documento uno de los problemas más frecuentes es trasferir la visión del líder a tu equipo de trabajo, también compartir el ánimo por realizarlo, porque es más complicado llegar a los objetivos si esto no se cumple".

Las sociedades tienen un papel central en la promoción del desarrollo económico y el progreso social de nuestro país; son el motor del crecimiento y tienen la responsabilidad de generar riqueza, empleo, bienestar social, infraestructura, bienes y servicios.

La permanencia, el desempeño, la eficiencia y la responsabilidad social de las sociedades son del interés público y privado, por lo tanto, el gobierno corporativo es una de las prioridades en la agenda nacional.

Conocer la parte estratégica de TIC e involucrarse en los procesos junto con las mejores prácticas; te permite tener una mejor visión acerca de las oportunidades de negocio con las cuales cuenta México, llevar a cabo la implementación y certificaciones no solo para cumplir hace crecer tu negocio y te permite interactuar no solo en la parte operativa que es fundamental, si no en la toma de decisiones, esperamos que este compendio de mejores prácticas y su implantación sean de utilidad para que sumemos más líderes de proyectos o especialistas en procesos y podamos sumarnos a crecer mundialmente y lo más importante a ser mejores cada día.

Lo que aprendí en mi formación como ingeniera fue que la universidad me preparó para resolver problemas con las soluciones más óptimas y al haberme enfrentado a infinidad de problemas con recursos, presupuesto y resistencia al cambio apliqué el trabajo en equipo, en el cual la facultad de ingeniería fue clave.

Al administrar los procesos de la organización bancaria, y en algunas organizaciones en las que he tenido oportunidad de laborar me doy cuenta de la importancia de llevar a cabo los ciclos de TI con una correcta metodología así como de la importancia de identificar los procesos de TI, para así poder asociarlos a los roles y responsabilidades adecuadas; ya que no sólo se trata de organizar tus recursos, sino de identificar claramente el nivel de madurez de cada uno de los procesos, clasificar los activos de TIC y todo lo que afecte a la operación para que sea entendible para su misma fluidez, operación, ejecución y para los próximos responsables y que todo lo que se esté

produciendo se encuentre alineado al negocio con TI y a su vez agregue valor, creo que pocas veces nos hacemos este tipo de preguntas o nos preguntamos hacia dónde va nuestro trabajo, ignorando la posibilidad que la persona que nos ha delegado la tarea también este consciente del verdadero valor que agrega .

Hay mucho por hacer y no nos podemos dar por vencidos, y aun así cuando nuestro Jefe, Líder o Director no tenga esa visión; es nuestro deber compartirla para el propio beneficio de los involucrados en el proyecto, servicio o proceso.

Clementina Aguilar Hernández

IMPLANTACIÓN DE MAAGTIC EN LOS PROCESOS DEL SECTOR GOBIERNO BASADO EN LAS MEJORES PRÁCTICAS

GLOSARIO

Glosario

Activo de información clave	El Activo de información que resulta esencial o estratégico para la operación y/o el control de una Infraestructura crítica o incluso de una que no tenga este carácter, pero cuya destrucción, perdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.
Activo primario	El Activo de información asociado a las funciones sustantivas de una Institución.
Activos de proceso	Los elementos de información que son parte de un proceso y que reflejan características específicas del mismo
Activos de información	Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
Activos de TIC	Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
Activo de soporte	Aquél que apoya o complementa a un Activo primario en su función.
Acuerdo de nivel de servicio SLA:	El acuerdo de nivel de servicio que se compromete con la Unidad administrativa solicitante, al entregar una solución tecnológica o servicio de TIC (Service Level Agreement por sus siglas en inglés).
Acuerdo de nivel operacional OLA:	El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un servicio de TIC, que se deben definir y cumplir para responder a los Acuerdos de nivel de servicio SLA comprometidos (Operational Level Agreement por sus siglas en inglés).
Ambiente de trabajo	El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.
Amenaza:	Cualquier posible acto que pueda causar algún tipo de daño a los Activos de información de la Institución.

Análisis de riesgos:	El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los Activos de TIC, a la Infraestructura crítica o a los Activos de información; efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.
Área técnica:	La responsable en la Institución de elaborar las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, de evaluar la propuesta técnica de las proposiciones y de responder en la junta de aclaraciones, las preguntas que sobre estos aspectos realicen los licitantes, en términos de las disposiciones jurídicas aplicables en materia de adquisiciones y arrendamiento de bienes muebles y servicios de cualquier naturaleza.
Bitácora de seguridad	El registro continúo de eventos e incidentes de seguridad de la información que ocurren a los Activos de información
Centro de datos	El lugar físico en el que se ubican los Activos de TIC, desde donde se proveen los servicios de TIC.
Confidencialidad:	La característica o propiedad por la cual la información sólo es revelada a Individuos o procesos autorizados.
Cuadro de mando integral de la UTIC:	La herramienta mediante la cual se obtiene el grado de cumplimento de la planeación estratégica de TIC, representado por el valor de los indicadores definidos para los objetivos estratégicos que se pretenden alcanzar.
Declaraciones de aplicabilidad:	El documento que contiene los controles aplicados mediante el SGSI de la Institución como resultado del Análisis de riesgos.
Directriz rectora	Documento estratégico en el que se establecen principios tecnológicos de alto Nivel.
Diseminación	La transmisión o entrega de información considerada de seguridad nacional, a quienes cumplan con los requisitos para conocer esa información, de acuerdo con el nivel de acceso autorizado.
Disponibilidad	La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.
Documento de planeación del proyecto:	El documento que contiene la definición de un proyecto, el control de su avance, así como sus documentos de planeación subsidiarios y documentación complementaria.
Documentos de planeación subsidiarios:	Los documentos de planeación que se deben instrumentar cuando un proyecto es autorizado, los cuales se incorporan al Documento de planeación del proyecto.

Entregable:	El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.
Evento	Suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.
Funcionalidad	Las características de un servicio de TIC que permiten que cubra las necesidades o requerimientos de un usuario.
Gestión de riesgos	La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los Activos de TIC, a la Infraestructura crítica o a los Activos de información de la Institución.
Gobierno digital	Las políticas, acciones y criterios para el uso y aprovechamiento de las TIC, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las instituciones.
Impacto	El grado de los daños y/o de los cambios sobre un Activo de información, por la materialización de una amenaza.
Incidente	La afectación o interrupción a los Activos de TIC, a las Infraestructuras críticas, así como a los Activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.
Iniciativas de TIC	Conceptualización o visualización temprana de una oportunidad para ofrecer un servicio de TIC o una solución tecnológica en beneficio de la Institución, éstas se concretan por medio de la planeación y ejecución de uno o más Programas de proyectos, y de proyectos de TIC.
Infraestructuras críticas	Las instalaciones, redes, servicios y equipos asociados o vinculados con Activos de TIC o Activos de Información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.
Infraestructura de TIC	El hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
Instancias de la seguridad	Las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad

nacional:	nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquéllas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.
Institución	Las dependencias y entidades de la Administración Pública Federal, así como la Procuraduría General de la República.
Integridad	Mantener la exactitud y corrección de la información y sus métodos de proceso.
Interdependencia:	La interconexión estrecha que existe entre las Infraestructuras críticas, y que conlleva a que la falla o falta de una de ellas impacte negativamente en otras Infraestructuras críticas, presentándose como consecuencia un efecto cascada de fallas en la prestación de servicios.
Interoperabilidad	La capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de TIC.
Mapa estratégico de la UTIC:	La representación visual que integra los Objetivos estratégicos de la UTIC e ilustra cómo interactúan las perspectivas de presupuesto, de usuarios, de procesos internos y de crecimiento o aprendizaje de los servidores públicos de la UTIC.
Marco rector de procesos:	El conjunto de procesos tendientes a la homologación de la gestión de la seguridad de la información, así como de la gestión interna de las UTIC, que constituyen el presente Manual.
Mesa de servicios	El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.
Objetivos estratégicos de TIC:	El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la UTIC.
Problema	La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.
Programa de capacidad	El documento de planeación que contiene la información sobre la capacidad de la infraestructura de TIC considerando los escenarios de necesidades futuras y los acuerdos de niveles de servicio establecidos
Programa de	El documento de planeación en el que se plantea la estrategia,

contingencia:	el Recurso humano en la UTIC, los activos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso crítico, en caso de presentarse un desastre o la materialización de un riesgo.
Programa de continuidad	El documento de planeación que contiene los elementos y las acciones necesarios para asegurar que la operación de los servicios y procesos críticos de TIC de la Institución no se interrumpa.
Programa de disponibilidad:	El documento de planeación que contiene los elementos y acciones necesarios para que los componentes de la infraestructura de TIC estén operando y sean accesibles.
Programa de proyectos	La integración de uno o más proyectos de TIC que pueden ser administrados en su conjunto para la obtención de beneficios adicionales a los que se lograrían de ser administrados individualmente durante su ejecución.
Programa de retorno del cambio:	El documento de planeación que contiene el objetivo y descripción de las actividades para un regreso al estado inicial del ambiente operativo de la *Secretaría de la Función Pública, MÉXICO Página 4 de 141* UTIC, en caso de falla o incidente que no permita finalizar un cambio en proceso de implantación
Programa de tecnología	El documento de planeación en el que se establecen las acciones estratégicas para la conformación de las arquitecturas de cada dominio tecnológico y de todos ellos en su conjunto, considerando los servicios de TIC existentes y proyectados.
Programa de trabajo del cambio	El documento de planeación que contiene el objetivo y descripción de las actividades necesarias para la integración de un elemento al ambiente operativo de la UTIC
Proyecto	Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.
Proceso	Un proceso es un conjunto de actividades o eventos con un fin común
Recursos de TIC	La infraestructura, los activos, el Recurso humano en la UTIC y el presupuesto de TIC.
Recursos humanos en la UTIC:	Los servidores públicos adscritos a la UTIC, o inclusive los servidores públicos de otras áreas de la Institución o personal de terceros cuando participen en alguno de los procesos previstos en el Manual y hayan sido acreditados por algún servidor público facultado al efecto, para llevar a cabo actividades específicas en dichos procesos.
Reglas de adaptación	El documento que contiene los supuestos en que resulta factible adaptar alguno de los procesos del “Marco rector de procesos”,

	cuando por las características particulares de la Institución así se justifique, conforme a lo previsto en el proceso OSGP-Operación del sistema de gestión y mejora de los procesos de la UTIC.
Repositorio	El espacio en medio magnético u óptico en el que se almacena y mantiene la información digital.
Requerimientos funcionales:	La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.
Riesgo	La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los Activos de TIC, las Infraestructuras críticas o los Activos de información de la Institución
Seguridad de la información:	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Seguridad nacional:	Las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, conforme a lo dispuesto en el artículo 3 de la Ley de Seguridad Nacional.
Sistema o aplicativo	El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos
Software de código abierto	El software cuya licencia asegura que el código pueda ser modificado y mejorado por cualquier persona o grupo de personas con las habilidades correctas, el conocimiento es de dominio público.
Solución tecnológica	El sistema, aplicativo o componente desarrollado en la Institución o adquirido por la misma, para habilitar la automatización de procesos o proveer un servicio de TIC.
Unidad administrativa solicitante:	La unidad administrativa de la Institución que solicita una solución tecnológica o servicio de TIC y que es responsable de definir sus requerimientos, funcionalidad y niveles de servicio
Usuarios:	Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.
Validación	La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la Unidad administrativa solicitante.

Verificación:	La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.
Vulnerabilidades:	Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los Activos de TIC, a la Infraestructura crítica, así como a los Activos de información.
AA	El grupo de procesos de Administración de activos del “Marco rector de procesos”. Agrupa los siguientes procesos: ADT, ACNC y APC.
AAF	El proceso de Administración de ambiente físico, del “Marco rector de procesos”.
ACMB:	El proceso de Administración de cambios, del “Marco rector de procesos”. **ACNC:** El proceso de Administración del conocimiento, del “Marco rector de procesos”.
ACNF	El proceso de Administración de la configuración, del “Marco rector de procesos”.
AD:	El grupo de procesos de Administración para el desarrollo de soluciones tecnológicas del “Marco rector de procesos”. Agrupa los siguientes procesos: ATC, DST y CST.
ADT	El proceso de Administración de dominios tecnológicos, del “Marco rector de procesos”.
ADTI	El proceso de Administración para las contrataciones de TIC, del “Marco rector de procesos”.
AE	El proceso de Administración de la evaluación, de TIC del “Marco rector de procesos”.
ANS	El proceso de Administración de niveles de servicio, del “Marco rector de procesos”.
AO	El proceso de Administración de la operación, del “Marco rector de procesos”.
AP	El grupo de procesos de Administración de procesos del “Marco rector de procesos”. Está conformado por el proceso OSGP.
APBS	El proceso de Administración de proveedores de bienes y servicios de TIC, del “Marco rector de procesos”.
APC	El proceso de Apoyo a la capacitación del personal de la UTIC, del “Marco rector de procesos”.

APP	El proceso de Administración del portafolio de proyectos de TIC, del “Marco rector de procesos”.
APS	El proceso de Administración del portafolio de servicios de TIC, del “Marco rector de procesos”.
APT	El proceso de Administración del presupuesto de TIC del “Marco rector de procesos”.
APTI:	El proceso de Administración de proyectos de TIC, del “Marco rector de procesos”.
AR	El grupo de procesos de Administración de recursos, del “Marco rector de procesos”. Agrupa los siguientes procesos: APT, APBS y ADTI.
AS	El grupo de procesos de Administración de servicios, del “Marco rector de procesos”. Agrupa los siguientes procesos: APS y DSTI.
ASI	El proceso de Administración de la seguridad de la información, del “Marco rector de procesos”.
ATC	El proceso de Apoyo técnico para la contratación de soluciones tecnológicas de TIC, del “Marco rector de procesos”.
CST:	El proceso de Calidad de las soluciones tecnológicas de TIC, del “Marco rector de procesos”.
DCSI	El grupo de procesos de Dirección y control de la seguridad de la información, del “Marco rector de procesos”. Agrupa los siguientes procesos ASI y OPEC.
DDT	El proceso de Determinación de la dirección tecnológica, del “Marco rector de procesos”.
DR:	El grupo de procesos de Dirección y control de TIC del “Marco rector de procesos”. Agrupa los siguientes procesos: EMG, PE, DDT y AE.
DST:	El proceso de Desarrollo de soluciones tecnológicas de TIC, del “Marco rector de procesos”.
DSTI	El proceso de Diseño de servicios de TIC, del “Marco rector de procesos”.
EMG	El proceso de Establecimiento del modelo del gobierno de TIC, del “Marco rector de procesos”.

ERISC:	El Equipo de respuesta a incidentes de seguridad en TIC en la Institución
LE	El proceso de Liberación y entrega, del “Marco rector de procesos”.
MI:	El proceso de Mantenimiento de infraestructura, del “Marco rector de procesos”.
OMS	El proceso de Operación de la mesa de servicios, del “Marco rector de procesos”.
OP	El grupo de procesos de Operaciones del “Marco rector de procesos”. Agrupa los siguientes procesos: AO, AAF y MI.
OPEC:	El proceso Operación de controles de seguridad de la información y del ERISC, del “Marco rector de procesos”.
OS	El grupo de procesos de Operación de servicios del “Marco rector de procesos”. Agrupa los siguientes procesos: OMS y ANS.
OSGP	El proceso de Operación del sistema de gestión y mejora de los procesos de la UTIC, del “Marco rector de procesos”.
PE:	El proceso de Planeación estratégica de TIC, del “Marco rector de procesos”.
PETIC:	El documento de planeación estratégica en el que se definen los objetivos y proyectos estratégicos de TIC que la Institución efectuará en un periodo de tiempo determinado.
PR:	El grupo de procesos de Administración de proyectos del “Marco rector de procesos”. Agrupa los siguientes procesos: APP y APTI.
SFP:	La Secretaría de la Función Pública.
SGSI	El Sistema de Gestión de Seguridad de la Información que por medio del análisis de riesgos y de la definición de controles, implementa, opera, monitorea, revisa y mejora de manera continua la seguridad de la información.
TE	El grupo de procesos de Transición y entrega del “Marco rector de procesos”.
THO	El proceso de Transición y habilitación de la operación, del “Marco rector de Procesos”.
TIC	Las Tecnologías de la Información y Comunicaciones.
UGD	La Unidad de Gobierno Digital de la Secretaría de la Función

	Pública.
UTIC:	La unidad administrativa de la Institución responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas de la Institución.

REFERENCIAS

Referencias

[1.1] Secretaría de la Función Pública, MÉXICO. Acuerdo publicado en el Diario Oficial de la Federación el 12 de julio de 2010 (MAAGTIC).

[1.2] Tecnologías de la Información (TI).

[1.3] MAAGTIC-SI: Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información.

[1.4] Niveles de Gestión: Gobierno, Organización y Estrategia, Ejecución y Entrega y Soporte.

[1.5] Grupos de procesos o Macroprocesos: Dirección, Control, Administración de Proyectos, Administración de Procesos, Administración de Recursos, Administración de Servicios, Desarrollo y Adquisición de Soluciones, Transición y Entrega, Operación de Servicios, Administración de Activos, Operaciones.

[1.6] Procesos: Establecimiento de la estructura de gobierno de TIC, Planeación estratégica de TIC, Determinación de la dirección tecnológica, Administración del desempeño de TIC, Cumplimiento regulatorio, Administración de riesgos de TIC, Administración de portafolio de proyectos de TIC, Administración de proyectos de TIC, Operación del sistema de gestión y mejora de procesos de la UTIC, Administración financiera de TIC, Administración de proveedores, Adquisiciones de TIC, Administración de portafolio de servicios de TIC, Diseño de servicios de TIC, Administración técnica de adquisiciones, Desarrollo de soluciones tecnológicas, Calidad de soluciones tecnológicas, Administración de cambios, Liberación y entrega, Transición y habilitación de la operación, Administración de la configuración, Operación de la mesa de servicios, Administración de servicios de terceros, Administración de niveles de servicio, Administración de la seguridad de la información, Administración de dominios tecnológicos, Administración del conocimiento, Integración y desarrollo del personal, Administración de la operación, Administración de ambiente físico, Mantenimiento de infraestructura.

[1.7] PETIC: Plan Estratégico de Tecnologías de Información y Comunicación

[1.8] CMMI: Capability Maturity Model Integration

[1.9] TOGAF: The Open Group Architecture Framework

[1.10] PMBOK: Project Management Body of Knowledge

[1.11] RISKIT: Riesgos TI

[1.12] COBIT: Control Objectives for Information and Related Technology

[1.13] ITIL: Information Technology Infrastructure Library

[1.14] BSC: Balanced Scorecard

[1.15] ISO 9001: La Norma especifica los requisitos para un Sistema de gestión de la calidad.

[1.16] ISO 27001: Es un estándar para la seguridad de la información.

[1.17] Hammer 1994

[1.18] Manganelli, 1995

[3.1]UTIC. MAAGTIC-SI V3 29-10-2011

[3.2]RACI. MAAGTIC-SI V3 29-10-2011

[3.3]Top-Down: Modelo usado generalmente en el diseño de sistemas que busca establecer la división de funcionalidades de cada módulo específico e ir escalando al sistema total.

[3.4]APP-Administración del Portafolio de Proyectos de TIC

[3.5]APS-Administración del Portafolio de Servicios de TIC

[3.6]PETIC-Planeación Estratégica de TIC

[3.7]Cuadro de mando integral de la UTIC: La herramienta mediante la cual se obtiene el grado de cumplimento de la planeación estratégica de TIC, representado por el valor de los indicadores definidos para los objetivos estratégicos que se pretenden alcanzar. MAAGTIC-SI V3 29-10-2011

[3.8]SGSI: El Sistema de Gestión de Seguridad de la Información que por medio del análisis de riesgos y de la definición de controles, implementa, opera, monitorea, revisa y mejora de manera continua la seguridad de la información. MAAGTIC-SI V3 29-10-2011

[3.9]Gobierno Digital: Las políticas, acciones y criterios para el uso y aprovechamiento de las TIC, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las instituciones. MAAGTIC-SI V3 29-10-2011

[3.10]FODA: Fortalezas, oportunidades, debilidades y amenazas.

[3.11]Mapa estratégico de la UTIC: La representación visual que integra los Objetivos estratégicos de la UTIC e ilustra cómo interactúan las perspectivas de presupuesto, de usuarios, de procesos internos y de crecimiento o aprendizaje de los servidores públicos de la UTIC. MAAGTIC-SI V3 29-10-2011

[3.12]Portafolio de proyectos: Es un proceso administrativo designado a ayudar a un organización a adquirir y ver información acerca de todos sus proyectos y programas, luego priorizar cada proyecto de acuerdo a ciertos criterios tales como valor estratégico, impacto en recursos, costos, etc.

http://es.wikipedia.org/wiki/Portafolio_de_proyectos

[3.13]DAS-IT: Digital Alignment Strategy-IT.
http://148.244.137.4/downloads/itpm/sfp/guia_petic.pdf

[3.14]UGD: Unidad de Gobierno Digital

IMPLANTACIÓN DE MAAGTIC EN LOS PROCESOS DEL SECTOR GOBIERNO BASADO EN LAS MEJORES PRÁCTICAS

ANEXOS

Para consultas amplias sobre el tema:

http://www.normateca.gob.mx/Archivos/67_D_2934_05-12-2011.pdf 1/10/2013, 14:24