ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

MODELO DE GESTIÓN PARA OPTIMIZAR LOS SERVICIOS TECNOLÓGICOS AGREGADORES DE VALOR ENTREGADOS POR LA DITSI DE LA SENPLADES

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGÍSTER EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

ING. SANDRA PAULINA PAREDES ULLOA
paredessand@gmail.com

ING. LUIS ROBERTO TASINTUÑA CONDOY
luis.lrtc@gmail.com

DIRECTORA: ING. NIDIA LILIÁN DEL ROSARIO GUAYAQUIL JURADO MSc.
nidia.guayaquil@epn.edu.ec

Quito, diciembre 2013

DECLARACIÓN

Nosotros, **SANDRA PAULINA PAREDES ULLOA** y **LUIS ROBERTO TASINTUÑA CONDOY**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

ING. SANDRA PAREDES

ING. LUIS TASINTUÑA

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por **SANDRA PAULINA PAREDES ULLOA** y **LUIS ROBERTO TASINTUÑA CONDOY**, bajo mi supervisión.

ING. NIDIA GUAYAQUIL MSc.

DIRECTORA DE PROYECTO

AGRADECIMIENTOS

Cuando se finaliza un trabajo de alto nivel, solo queda la satisfacción personal de haber culminado una meta más. Sin embargo, para cada paso que he dado en mi vida y cada logro que he alcanzado, y sabiendo con mucho orgullo que todo ha sido esfuerzo propio, con un infinito gracias, que éstas palabras no alcanzan a reflejar, agradezco a Dios, a mi familia que siempre me ha apoyado, y a mi esposo que es el amor de mi vida y que siempre me acompaña y me apoya en cada pedacito de cielo que construimos juntos.

De igual forma agradezco a los profesores de la maestría y a mis compañeros, con quienes compartí gratas experiencias y enriquecí mi aprendizaje, y de manera muy especial a la Ing. Nidia Guayaquil, que a pesar de cualquier adversidad, ha guiado con sabiduría, paciencia y amistad la culminación de este trabajo.

Sandra Paredes

AGRADECIMIENTOS

Sin duda todo gran trabajo conlleva mucha responsabilidad y sacrificio, por ende este pequeño espacio no se puede desaprovechar para agradecer a Dios por permitirme tener una vida de logros junto a mi esposa y bella princesa con salud y felicidad. A mis padres, hermanos, familia política por ser siempre el apoyo y el buen consejo oportuno. A la Ingeniera Nidia por la apertura, profesionalismo y esfuerzo puesto en este trabajo. Por ultimo a todos mis amigos y compañeros que forman parte activa de mi vida.

Luis Tasintuña

DEDICATORIA

A mis padres y la hermosa familia que Dios me ha regalado y que sigue creciendo.

Sandra

DEDICATORIA

A las bellas princesas, mi esposa por su compresión, dedicación y amor; a mi ratona por la dicha y felicidad de tenerla junto a mi lado. A mis padres, hermanos, mis suegros y mis cuñados por la alegría de tenerlos en mi vida y ser mi inspiración.

Luis

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPÍTULO 1: DIAGNÓSTICO INICIAL DE SERVICIOS TECNOLÓGICOS EN LA DITSI

CAPÍTULO 2: DESARROLLO DEL MODELO DE GESTIÓN BASADO EN EL MAPEO Y/O COMBINACIÓN ENTRE EL MARCO DE REFERENCIA ITIL V3 Y EL ESTÁNDAR DE SEGURIDADES ISO 27005

CAPÍTULO 3: APLICACIÓN DEL MODELO DE GESTIÓN EN LA DITSI Y PRESENTACIÓN DE RESULTADOS

ÍNDICE DE TABLAS

CAPÍTULO 1: DIAGNÓSTICO INICIAL DE SERVICIOS TECNOLÓGICOS EN LA DITSI

CAPÍTULO 2: DESARROLLO DEL MODELO DE GESTIÓN BASADO EN EL MAPEO Y/O COMBINACIÓN ENTRE EL MARCO DE REFERENCIA ITIL V3 Y EL ESTÁNDAR DE SEGURIDADES ISO 27005

CAPÍTULO 3: APLICACIÓN DEL MODELO DE GESTIÓN EN LA DITSI Y PRESENTACIÓN DE RESULTADOS

RESUMEN

El presente proyecto de tesis, establece un Modelo de Gestión para Optimizar los Servicios Tecnológicos agregadores de valor entregados por la DITSI de la SENPLADES, basado en el mapeo del estándar ISO 27005 y el marco de referencia ITIL v3.

Este modelo denominado M_OPTIMIZA, fue estructurado en base al mapeo de procesos entre la ISO 27005 e ITIL, y provee 11 procesos, que pueden ser aplicados en empresas de cualquier tamaño y tipo de industria.

La generación de valor del M_OPTIMIZA es verificada con los formularios de aplicación, en los que a través de métricas, es posible obtener el estado actual de la organización en estudio respecto a los indicadores del modelo, en este caso puntual, se realizó la aplicación en la Dirección de Innovación Tecnológica de Sistemas de Información de la SENPLADES.

Esta aplicación finaliza con los resultados que permiten establecer el nivel actual de la organización en relación al M_OPTIMIZA, y las directrices que se debe seguir para llegar a un proceso de mejora continua.

Por último una de las metas por abordar con M_OPTIMIZA, es convertirse en una de herramienta de uso periódico, que permita proponer acciones correctivas, proactivas y preventivas para una mejora continua de los servicios de Tecnologías de la Información.

PRESENTACIÓN

Las empresas privadas y organizaciones de gobierno, reconocen hoy en día a la tecnología, como un componente esencial para establecer y desarrollar nuevas estrategias, que les permitan alcanzar sus objetivos.

El rápido crecimiento de la tecnología, establece la necesidad de contar con estándares, modelos y marcos de referencia que apoyen a la gestión efectiva de recursos.

De igual forma, se requiere la implantación de estándares para gestionar los riesgos a los que están expuestos los activos de soporte, de manera que los servicios que funcionan sobre éstos, no se vean afectados por la materialización de amenazas internas y/o externas.

El modelo de referencia ITIL v3, proporciona directrices para gestionar los servicios de TI, describiéndolos su ciclo de vida en cinco fases. Por otro lado, el estándar ISO/IEC 27005, es una guía para gestionar los riesgos a los que están expuestos los activos de TI.

Bajo este escenario, la necesidad de contar con un modelo que gestione los procesos de TI e incluya los riesgos a los que están expuestos, es fundamental hoy en día, y consecuentemente, un modelo que permita gestionar los activos de TI y sus riesgos, de tal forma identificar claramente las acciones que se deben seguir para administrar las tecnologías de información y comunicación con un enfoque de seguridades de la información.

CAPÍTULO 1: DIAGNÓSTICO INICIAL DE SERVICIOS TECNOLÓGICOS EN LA DITSI

1.1 CARACTERIZACIÓN DE LA SECRETARIA NACIONAL DE PLANIFICACIÓN Y DESARROLLO – SENPLADES

1.1.1 RESEÑA HISTÓRICA[1]

En Ecuador la planificación se inició con la Junta Nacional de Planificación y Coordinación Económica (Junapla), creada mediante Decreto Ley de Emergencia número 19, del 28 de mayo de 1954. En 1979, fue remplazada por el Consejo Nacional de Desarrollo (CONADE), con entidades adscritas, como, el Instituto Nacional de Estadísticas y Censos (INEC), el Fondo Nacional de Pre inversión, y el Consejo Nacional de Ciencia y Tecnología (CONACYT). En 1998, en lugar del CONADE, se creó la Oficina de Planificación (ODEPLAN).

En el 2004, mediante Decreto Ejecutivo No. 1372, se creó la Secretaría Nacional de Planificación y Desarrollo, SENPLADES, la cual en el 2007 mediante Decreto Ejecutivo No.103 del 8 de febrero, se fusionó el Consejo Nacional de Modernización del Estado, CONAM; y la Secretaría Nacional de los Objetivos de Desarrollo del Milenio, SODEM; a la Secretaría Nacional de Planificación y Desarrollo, SENPLADES.

En el artículo 255 de la Constitución Política de la República señala que el Sistema Nacional de Planificación estará a cargo de un organismo técnico dependiente de la Presidencia de la República, con la participación de los gobiernos seccionales autónomos y de las organizaciones sociales que determine la Ley, siendo delegada esta tarea a la SENPLADES.

[1] Fuente: www.planificacion.gob.ec

1.1.2 MISIÓN

"Administrar y coordinar el Sistema Nacional Descentralizado de Planificación Participativa como un medio de desarrollo integral del país a nivel sectorial y territorial, estableciendo objetivos y políticas estratégicas, sustentadas en procesos de información, investigación, capacitación, seguimiento y evaluación; orientando la inversión pública; y, promoviendo la democratización del Estado, a través de una activa participación ciudadana, que contribuya a una gestión pública transparente y eficiente"[2].

1.1.3 VISIÓN

"Ser el referente latinoamericano en términos de planificación nacional, visionando el Ecuador del futuro para las y los ecuatorianos"[3].

1.1.4 VALORES INSTITUCIONALES[4]

- Lealtad y compromiso
- Trabajo en equipo
- Honestidad y transparencia
- Eficiencia y Eficacia
- Responsabilidad
- Actitud de servicio, calidez y buen trato

1.1.5 TIPO DE ESTRUCTURA ORGANIZACIONAL

La Secretaría Nacional de Planificación y Desarrollo, SENPLADES, define la Misión, Objetivos Estratégicos y Estructura Organizacional por procesos que le permiten fundamentar, direccionar y posicionar el desarrollo institucional dentro de un marco de integración, participación, descentralización, desconcentración, transparencia y eficiencia en el contexto nacional.

La estructura organizacional corresponde a un esquema jerárquico en el cual los procesos de acuerdo a las competencias de cada subsecretarias son gestionadas

[2] Fuente: www.planificacion.gob.ec
[3] Fuente: www.planificacion.gob.ec
[4] Fuente: www.planificacion.gob.ec

desde Unidades, Coordinaciones, Direcciones y las mismas Subsecretarias, las cuales reportan a las Coordinaciones Generales y a su vez a la Secretaria Nacional (Despacho); definiendo de esta manera el modelo jerárquico.

La SENPLADES está liderada por la Secretaría Nacional, con unidades coordinadoras que son asesoras y tres ejes principales que trabajan en el cumplimiento de su misión que son la Subsecretaría General de Planificación para el Buen Vivir, la Subsecretaría General de Descentralización del Estado y las Subsecretarías Zonales.

El organigrama descrito corresponde al proyecto de reforma al estatuto orgánico de gestión organizacional por procesos de la SENPLADES aprobado en agosto de 2012. Empezando su implementación y transición de funciones el primero de enero de 2013. El Acuerdo No. 639-2012 Reformas al Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES a través del que se aprobó el nuevo estatuto vigente, establece la conformación de dos coordinaciones adicionales bajo la Secretaria Nacional: Coordinación General de Empresas Públicas y Coordinación General de Gestión Estratégica, con sus respectivos productos, servicios y actividades, unidad administrativa que tiene ahora a su cargo la Dirección de Tecnologías de Información y Comunicación, que cumple con las atribuciones y responsabilidades de la DITSI.

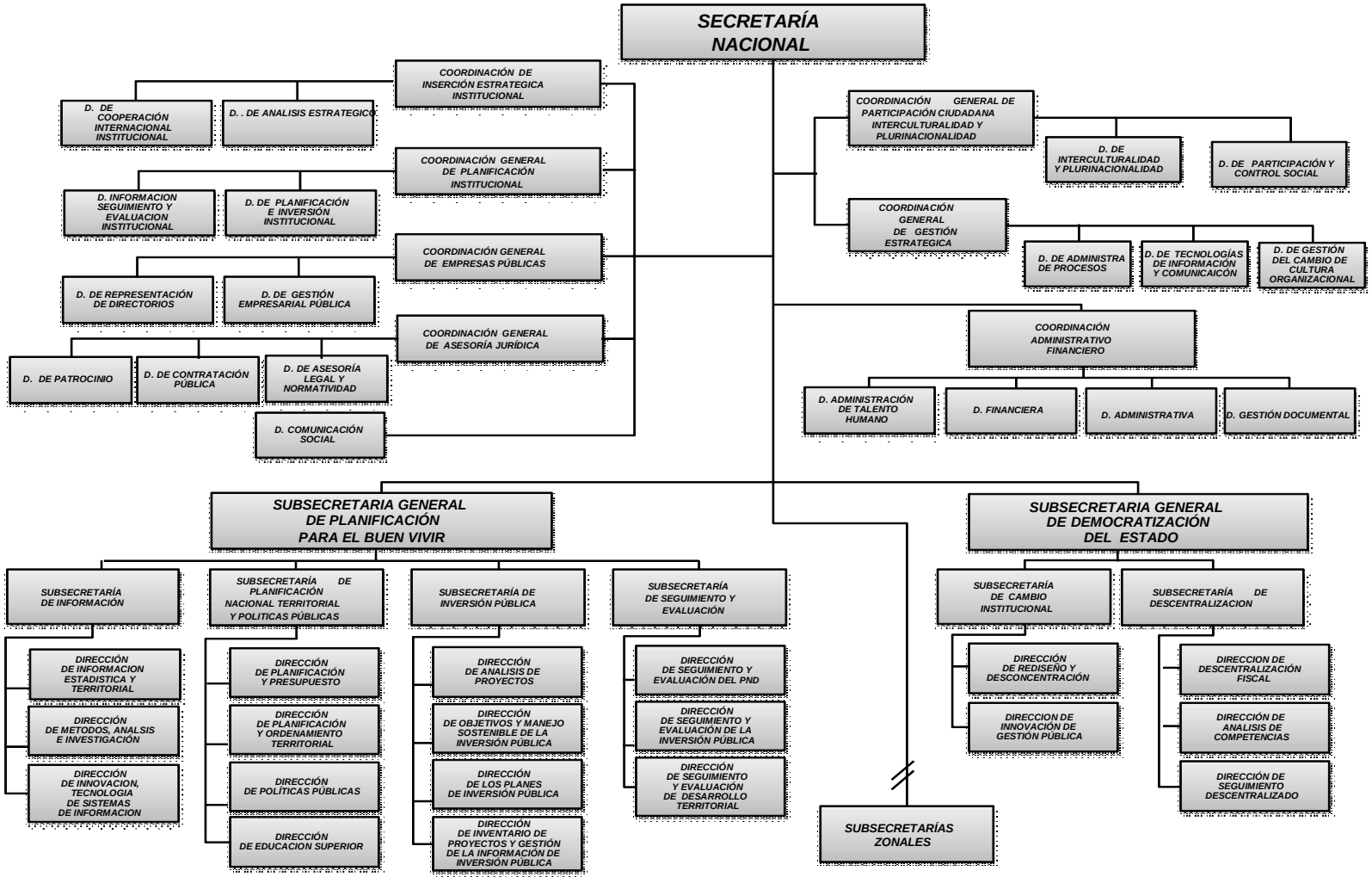


Figura 1.1 *Organigrama de la SENPLADES por unidades organizacionales y niveles jerárquicos*
(Acuerdo No. 639-2012 Reformas al Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES, 2012)

1.1.6 CULTURA ORGANIZACIONAL

La SENPLADES actualmente no ha posicionado totalmente una cultura organizacional entre sus servidores, en parte por la ausencia de implementación de procesos formalizados, haciendo relación a que el éxito de su implementación depende del compromiso y cultura organizacional adoptada en la Institución.

Con el nuevo proyecto de reforma como parte de la nueva Coordinación General de Gestión Estratégica, se forma la Dirección de Gestión de Cambio de Cultura Organizacional, que tiene como misión visualizar, administrar, implementar y supervisar las mejores prácticas de procesos de transformación transversales dentro y fuera de la Institución, a través de la gestión institucional y empoderamiento a los servidores públicos, orientando a un desarrollo continuo de la cultura organizacional y/o madurez institucional; siendo responsable de cambiar las condiciones evidenciadas actualmente:

- Motivación: no existe la motivación adecuada porque no se ha realizado un análisis de sensibilidad de los funcionarios que identifique la razón principal que los motiva a trabajar en la institución.
- Pasividad: las personas hacen lo necesario, falta motivación ejercida directamente por la cultura organizacional.
- Desconocimiento: la mayoría de los funcionarios desconocen la misión y visión de la institución.
- Confusión conceptual: se sabe que hay que hacer, y no necesariamente por que es importante hacerlo.
- Rutina: las actividades se realizan rutinariamente no se toma un criterio profesional para discrepar y para defender una idea.
- Impulsividad, reacción: poca pro actividad, las personas están dispuestas a solucionar asuntos, y no se soluciona desde la raíz, no hay cultura de la previsión y del mejoramiento.
- Enfoque a lo operativo: hay más actividades rutinarias, que realizar mejoras en los procesos se mide más por la cantidad de asuntos realizados que por la calidad de los mismos.

En relación a los esfuerzos realizados por la DITSI[5], desde el 2007 ha permitido la adopción en particular del framework de ITIL (Biblioteca de Infraestructura de Tecnologías de Información), específicamente de la Mesa de Servicios de TI y gestión de incidentes, por lo cual se ha llevado a cabo campañas de socialización de la forma de operación de este proceso, generando cierta cultura organizacional a través de un único punto de contacto.

A pesar de que en la mayor parte de la Institución está posicionada la Mesa de Servicios de TI, existe incumplimiento de esta forma de trabajo especialmente de requerimientos generados internamente por la unidad de tecnología y provenientes de mandos altos, puesto que son solicitados directamente a los involucrados y no se realizan a través del punto único de contacto.

1.2 DIAGNÓSTICO ACTUAL DE LA DIRECCIÓN DE INNOVACIÓN TECNOLÓGICO DE SISTEMAS DE INFORMACIÓN - DITSI

1.2.1 MISIÓN ACTUAL DE DITSI

"Planear y ejecutar proyectos y procesos de Tecnologías de la Información (TI) para la aplicación de políticas públicas y mejora de la gestión institucional y de los servicios a la ciudadanía, así como garantizar la operación de los sistemas y servicios informáticos, gestionar la seguridad informática, brindar soporte técnico en herramientas, aplicaciones, sistemas y servicios informáticos de la institución, e implementar la interoperabilidad con otras entidades"[6].

1.2.2 VISIÓN ACTUAL

"Ser la dirección que permita un acercamiento al usuario final, proporcionando siempre la mejor solución mediante el establecimiento de acuerdos de servicio y evaluando las mejores alternativas tecnológicas"[7].

[5] A pesar que la DITSI en el nuevo organigrama cambia de nombre a Dirección de Tecnologías de la Información y Comunicación (DTIC), en el desarrollo del proyecto de titulación se seguirá haciendo referencia a DITSI, debido a que la información se levantó previo al cambio mencionado, el 1 de enero de 2013.
[6] Fuente: proyecto de reforma al estatuto orgánico 2010.
[7] Fuente: Taller de marco estratégico de Subsecretaria de Información 2009.

La visión de la Dirección no es consistente con la misión y no muestra lo que se pretende lograr en un tiempo determinado.

1.2.3 ESTRUCTURA ORGANIZACIONAL

La estructura definida en la DITSI, establece siete unidades, alineadas a las funciones descritas en los procesos de ITIL (Ver figura 2).

Con el proyecto de reforma el estatuto el organigrama cambia a una gestión por procesos, definiendo seis productos y servicios como parte de la responsabilidad en la Dirección:

- Planificación TICs.
- Desarrollo de sistemas informáticos.
- Gestión de infraestructura y operaciones.
- Gestión de la seguridad de la información.
- Gestión de soporte técnico.
- Gestión de la interoperabilidad.

Sin embargo, esta estructura no ha sido implementada en su totalidad, ya que a la fecha actual, se encuentra en proceso de aprobación la nueva reforma al Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES, que implicará nuevos cambios en las atribuciones y responsabilidades de esta Dirección, como la separación de independización de las funciones de Seguridades de la Información, que actualmente trabaja como un proceso independiente de tecnología y transversal a la institución, en la Coordinación General de Planificación Institucional.

De esta manera para el presente estudio, se considera la estructura mostrada a continuación:

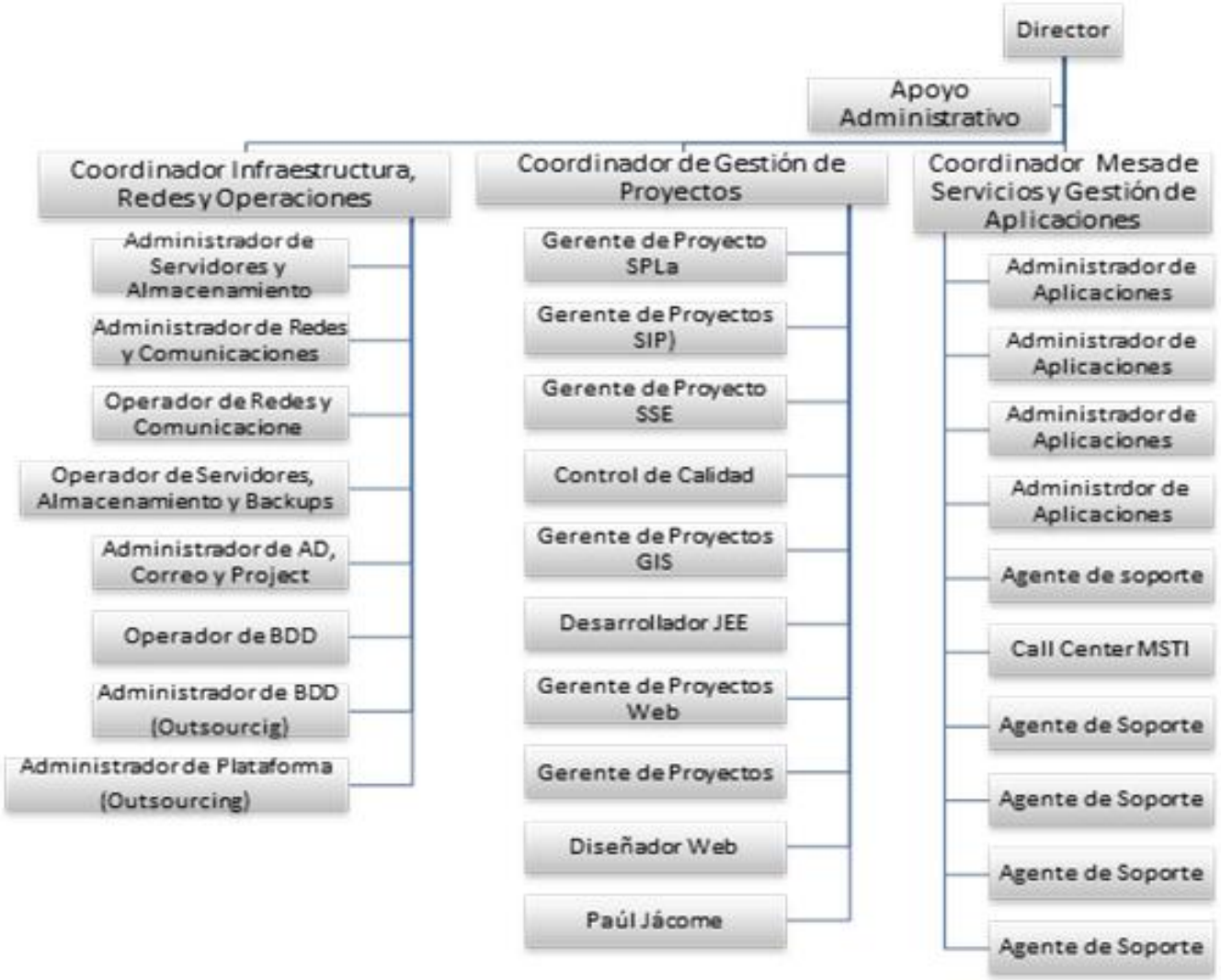


Figura 1.2. *Estructura organizacional actual de la Dirección de Tecnología*
(Plan Estratégico de Tecnología de información (PETI), 2012)

1.2.4 FUNCIONES Y RESPONSABILIDADES DE LA UNIDAD DE TI

A continuación se expone un comparativo de las atribuciones y responsabilidades de la Dirección de Tecnología, tomando como referencia el tiempo del proyecto de reforma al estatuto orgánico del 2010:

Atribuciones y responsabilidades – Estatuto Orgánico 2010	Atribuciones y responsabilidades – Proyecto de reforma al Estatuto Orgánico 2010
• Gestionar los proyectos que involucran componentes de tecnologías de información y comunicaciones para la prestación de servicios internos y externos alineados al rol de la SENPLADES. • Coordinar las actividades de integración e intercambio de información generada y procesada por los sistemas informáticos utilizados por las instituciones del Gobierno Central. • Promover el uso de alternativas tecnológicas para el intercambio de información con otras entidades del Estado. • Administrar y proveer los servicios de visualización de información disponible en el Sistema Nacional de Información. • Promover el uso racional de tecnología para los sistemas de información de la SENPLADES. • Apoyar la priorización de proyectos de inversión pública que tienen componentes tecnológicos. • Brindar asistencia técnica a otras entidades del Estado sobre implementación e innovación de sistemas de Información	• Formular y ejecutar los planes estratégico y operativo de las Tecnologías de la Información (TI), alineados al plan estratégico institucional y a las políticas que dicte el Gobierno en esta materia; • Dirigir, coordinar y controlar los procesos y proyectos de TI, así como los recursos humanos, físicos, de infraestructura tecnológica y financieros; • Gestionar la aprobación de la ejecución de Proyectos de TI, de acuerdo a la normativa vigente establecida por la Subsecretaría de Tecnologías de la Información de la Secretaría Nacional de la Administración Pública; • Proponer, implementar y controlar la aplicación de políticas y normativas para el uso de las TI alineadas a las políticas de dicte la Secretaría Nacional de la Administración Pública en esta materia; • Ejecutar y participar de manera activa para el desarrollo de la interoperabilidad gubernamental; • Implementar el Sistema de Seguridad de la Información en la institución, basado en las Normas Técnicas Ecuatorianas emitidas por las instituciones competentes y en los lineamientos de seguridad informática emitidos por la Secretaría Nacional de la Administración Pública; • Gestionar el ciclo de vida de las aplicaciones y sistemas informáticos para automatizar y mejorar procesos institucionales y trámites ciudadanos; • Asegurar el soporte técnico, capacidad, disponibilidad y continuidad de los aplicativos, sistemas y servicios informáticos, así como la eficiencia de los recursos tecnológicos: físicos, hardware, software y humanos, suficientes para el funcionamiento de la Unidad; • Conformar y dirigir el Comité de Gestión de las TI, con los Directores y Asesores de la entidad, para analizar los requerimientos de implementación de aplicativos, sistemas y servicios informáticos; • Medir los indicadores de los procesos, de la ejecución de los proyectos y los acuerdos de niveles de servicios informáticos establecidos; • Generar informes de gestión y rendición de cuentas respecto de las actividades del área; • Analizar periódicamente los procesos, procedimientos y metodologías de trabajo, a fin de consolidarlos, estandarizarlos, optimizarlos y actualizarlos; • Brindar asesoramiento en materia de TI a las autoridades, funcionarios y servidores de la institución; y, • Y demás actividades y responsabilidades emitidas por la Secretaría Nacional de la Administración Pública.

Tabla 1.1 Atribuciones y responsabilidades
(Estatuto orgánico, 2008 y 2010)

Del análisis de la Tabla 1.1 se evidencia que el actual estatuto permite un involucramiento directo de la Dirección de Tecnología, con los altos mandos de la SENPLADES debido a que ésta es parte de la Coordinación General de Gestión Estratégica.

Las actividades se realizan, pero no existe un modelo de gestión de TI que permita enfocar todo los esfuerzos en la consecución de los objetivos de la Dirección, optimizando recursos y velando por la mejora continua de los procesos. Adicionalmente no existen indicadores para evaluar la calidad y avance de las actividades encomendadas.

La misión y descripción de puestos de las actuales áreas definidas en la Dirección de Tecnología son:

Coordinación de Gestión de Proyectos

Misión:

Administrar el portafolio de proyectos de software incluyendo el análisis, identificación, priorización de actividades, gestión y control de proyectos, programas y otros trabajos relacionados para apoyar a conseguir los objetivos estratégicos de la institución con calidad, oportunidad y eficiencia aplicando tecnología.

Funciones:

- Dirigir la gestión de la ejecución de desarrollo del portafolio de proyectos de software usando las mejores prácticas internacionales.
- Coordinar y/o analizar los requerimientos, diseñar, desarrollar, poner en marcha y la gestión de cambios de los sistemas informáticos de apoyo a la gestión de la institución.
- Establecer y ejecutar un plan de gestión del análisis, diseño, desarrollo, pruebas, control de calidad, implantación y mantenimiento de los proyectos informáticos.
- Establecer y ejecutar programas de capacitación técnica de herramientas dirigida al personal técnico y funcional de la institución para la entrega de

los productos de software, en coordinación con las áreas administrativas pertinentes.

- Incubar y efectuar la transferencia tecnológica de proyectos informáticos enfocados a solucionar requerimientos específicos de las áreas de la institución.
- Elaborar manuales de procesos, procedimientos, instructivos y registros concernientes a su área de gestión.
- Realizar otras funciones afines que le sean asignadas por la Dirección de Innovación Tecnológica en Sistemas de Información.

Coordinación de Mesa de Servicios y de Gestión de Aplicaciones

Misión:

Facilitar la restauración de la operación normal de los servicios proporcionados por la Dirección de Tecnológica en el menor tiempo posible con la finalidad de minimizar el impacto que pueda causar a la SENPLADES y ser responsable del soporte y mantenimiento de las aplicaciones que la Dirección de Tecnológica pone a disposición como apoyo a la cadena de valor de la SENPLADES.

Funciones:

- Recibir y registrar requerimientos de servicios informáticos vía telefónica o correo electrónico como primer punto de contacto para los usuarios finales, así como también realizar la asignación de dichos requerimientos a los diferentes agentes de soporte.
- Atender los requerimientos asignados con el fin de brindar un soporte de primer nivel y mantener informado al usuario sobre el avance de solución de los mismos.
- Atender los requerimientos asignados con el fin de brindar un soporte de primer nivel en cada una de las zonales.
- Administrar, mantener y dar soporte técnico a las aplicaciones generadas por la Dirección de Tecnología y en funcionamiento en la SENPLADES.

Gestión de Infraestructura y Operaciones

Misión:

Realizar la administración de todo el software de base que permite el funcionamiento de la infraestructura física del Centro de Datos como de la red de datos y comunicaciones de la SENPLADES y realizar la administración de toda la infraestructura física del Centro de Datos como de la red de datos y comunicaciones de la SENPLADES.

Funciones:

- Administrar el Directorio Activo, Correo Electrónico y MS Project Server de la SENPLADES
- Administrar la plataforma de aplicaciones y brindar asesoramiento técnico al arquitecto de software en esta materia
- Administrar la base de datos
- Ejecutar procedimientos y tareas operativas sobre la base de datos
- Administrar, gestionar, asesorar y ejecutar proyectos de innovación de la infraestructura de servidores y almacenamiento.
- Administrar, gestionar, asesorar y ejecutar proyectos de innovación de la infraestructura de redes y comunicaciones
- Ejecutar el plan de respaldos de todos los sistemas informáticos además de ejecutar tareas, procedimientos, monitoreo, etc., establecidos para la operación y mantenimiento de servidores
- Administrar el sistema telefónico integral de la SENPLADES.
- Ejecutar los procedimientos para el mantenimiento de todos los elementos del centro de datos.
- Realizar el monitoreo integral de la infraestructura de red y
- Solucionar incidentes de segundo nivel en relación a componentes de infraestructura y operaciones.

Gestión de Seguridades de la Información[8]

Misión:

Gestionar la disponibilidad, integridad y confidencialidad de los activos de información y soporte de la SENPLADES.

Funciones:

- Elaborar el plan de implementación de un Sistema de Gestión de Seguridad de Información (SGSI) en la SENPLADES.
- Evaluar y realizar el seguimiento del cumplimiento de las configuraciones de los entornos de preproducción y producción, orientados a institucionalizar ambientes estables, disponibles y seguros sobre los cuales opera el Sistema Nacional de Información y el resto de sistemas y aplicaciones de la SENPLADES.
- Elaborar indicadores de gestión relacionados al seguimiento del cumplimiento de las políticas de seguridad para garantizar la continuidad de las aplicaciones que se encuentran desplegadas en la infraestructura de SENPLADES, estableciendo lineamientos que aseguren una recuperación inmediata de los sistemas y aplicaciones ante eventuales contingencias o desastres.
- Analizar, proponer y promover soluciones tecnológicas que coadyuven al mejoramiento continuo de las seguridades informáticas que conforman el Sistema Nacional de Información y que operan sobre la infraestructura de la SENPLADES.
- Analizar los riesgos que afecten la continuidad, disponibilidad e integridad de las aplicaciones que conforman el Sistema Nacional de Información con el objetivo de identificar los riesgos y tomar las acciones necesarias para minimizar el impacto de los mismos.
- Supervisar la correcta operación de los planes de seguridad y de versionamiento organizacional y disponibilidad de las aplicaciones para asegurar que la infraestructura tecnológica pueda ser recuperada dentro

[8] El 15 de abril de 2013, se establecieron dos ámbitos de acción: Gestión de Seguridad de la Información y Gestión de Seguridad informática, la primera a cargo de la Coordinación de Gestión de Planificación Institucional y la segunda como parte de la DITSI..

de los tiempos establecidos y verificar que éstos se encuentren alineados a los ciclos de la organización, con la finalidad de identificar los requerimientos de capacidad.

- Supervisar la correcta operación de los servicios de infraestructura de comunicaciones de datos inclusive cuando éstos sean proporcionados por terceros para garantizar la disponibilidad de la Aplicaciones de Internet, intranet y extranet del Sistema Nacional de Información.
- Coordinar y supervisar el cumplimiento de los Acuerdos de Nivel Servicio firmados con los proveedores y fabricantes con los cuales la institución mantiene relaciones contractuales en temas relacionados con seguridad, para garantizar el cumplimiento de los servicios adquiridos.

1.2.5 POSICIÓN EN LA TOMA DE DECISIONES

Debido a la estructura orgánica institucional, la Dirección de Tecnología no es una unidad asesora a pesar de que en la misión lo señala como tal, el principal inconveniente para no ejecutar el papel de unidad asesora es debido a que no tiene una línea de reporte directo hacia la máxima autoridad.

El rol desempeñado actualmente es de unidad ejecutora, que cumple con desplegar los servicios que requieran el resto de unidades administrativas de la Institución.

1.2.6 CATÁLOGO DE SERVICIOS

La Dirección de Tecnología no cuenta con un catálogo de servicios formalizado, por ende no se ha establecido los acuerdos de nivel de servicio para cada uno de ellos. A continuación se describen los servicios informáticos prestados por la Dirección.

No	Responsable	Código	Nombre de Servicio	Descripción	Punto de contacto	SLA
1	Gestión de soporte técnico	CS-ST-001	Antivirus	La dirección suministra el sistema de antivirus para máquinas institucionales al igual que el soporte técnico a través de un equipo de técnicos calificados lo cual incluye la instalación y actualización del sistema.	Mesa de Servicio de TI	No

2	Gestión de Infraestructura y Operaciones	CS-ST-002	Autenticación	Se provee el servicio de autenticación para el ingreso a aplicaciones y recursos tecnológicos disponibles en la Institución	Mesa de Servicio de TI	No
3	Gestión de Infraestructura y Operaciones	CS-ST-003	Correo electrónico Institucional	La dirección provee el servicio de correo electrónico institucional para todos los funcionarios de la SENPLADES	Mesa de Servicio de TI	No
4	Gestión de Infraestructura y Operaciones	CS-ST-004	Respaldos de información	La dirección provee el servicio de respaldos de información de la institución en medios digitales y magnéticos	Gestión de Infraestructura y Operaciones	No
5	Gestión de Infraestructura y Operaciones	CS-IO-001	Puntos de datos y energía eléctrica	La dirección suministra el servicio de diagnóstico, mantenimiento correctivo y gestión para la implementación de nuevos puntos eléctricos.	Mesa de Servicio de TI	No
7	Gestión de Infraestructura y Operaciones	CS-IO-003	Telefonía	La dirección provee el servicio de telefonía IP para los funcionarios de la SENPLADES permitiendo la comunicación externa e interna (incluyendo llamadas directas con las zonales)	Mesa de Servicio de TI	No
8	Gestión de Infraestructura y Operaciones	CS-IO-004	Telefonía remota	La dirección provee el servicio de telefonía remota permitiendo disponer de las bondades de la telefonía Institucional en una portátil o smartphone mediante el uso de Skype	Unidad de infraestructura Operaciones	No
9	Gestión de Infraestructura y Operaciones	CS-IO-005	Videoconferencia	La dirección provee el servicio de videoconferencia para una comunicación interactiva con la zonales de la SENPLADES y puntos remotos compatibles con la tecnología adoptada	Mesa de Servicio de TI	No
10	Gestión de Infraestructura y Operaciones	CS-IO-006	Red Inalámbrica	La dirección provee el servicio red inalámbrica personalizada de acuerdo a un perfil de acceso a la red, asegurando el acceso a la red inalámbrica	Mesa de Servicio de TI	No
11	Gestión de Infraestructura y Operaciones	CS-IO-007	Filtrado Web	La dirección proporciona accesos personalizados para la navegación web en internet de acuerdo a formularios establecidos para este requerimiento, mediante mecanismo de seguridad para resguardar el buen uso de recursos institucionales	Mesa de Servicio de TI	No
12	Gestión de Infraestructura y Operaciones	CS-IO-008	Asesoramiento para adecuación de cableado estructurado y eléctrico	La dirección proporciona asesoramiento y apoyo técnico para la elaboración de pliegos e implementación de adecuación de cableado estructurado y eléctrico para nuevos oficinas y zonales de la SENPLADES	Mesa de Servicio de TI	No
13	Gestión de Infraestructura y Operaciones	CS-IO-009	Correo de voz	La dirección provee con cada extensión telefónica un casillero de voz que se sincroniza con el cliente de correo institucional, permitiendo escuchar los mensajes de voz desde la bandeja de entrada del correo.	Mesa de Servicio de TI	No
14	Gestión de Infraestructura y Operaciones	CS-IO-010	Almacenamiento de información sensible de la Institución	La dirección mediante equipos de alto rendimiento permite almacenar información sensible de la Institución, de manera segura y eficiente.	Mesa de Servicio de TI	No

15	Gestión de desarrollo de sistemas informáticos	CS-PRY-001	Diseño e implementación de portales WEB	La dirección proporciona a través de un trabajo conjunto con las Subsecretarías el diseño y puesta en marcha de portales WEB para la Institución	Dirección de TI	No
16	Gestión de desarrollo de sistemas informáticos	CS-PRY-002	Gestión de proyectos	La dirección ofrece a través de personal altamente calificado la gestión de proyectos asignando talento humano para cada uno de las áreas requirentes	Dirección de TI	No
17	Gestión de desarrollo de sistemas informáticos	CS-PRY-003	Gestión de cambio en sistemas informáticos en producción	La dirección ofrece a través de personal altamente calificado la gestión de cambios en aplicaciones institucionales en producción	Dirección de TI	No
18	Gestión de Soporte Técnico	CS-GA-001	Soporte informático de aplicaciones	La dirección a través de personal altamente calificado proporciona soporte técnico de las aplicaciones informáticas Institucionales, para usuarios internos y externos	Mesa de Servicio de TI	No
19	Gestión de Soporte Técnico	CS-ST-002	Mantenimiento correctivo de computadoras Institucionales	La dirección ofrece el servicio de mantenimiento correctivo de computadoras institucionales, mediante técnicos calificado	Mesa de Servicio de TI	No
20	Gestión de Soporte Técnico	CS-ST-003	Soporte técnico de ofimática	La dirección mediante personal capacitado ofrece asistencia técnica para las herramientas ofimáticas empleadas en la Institución.	Mesa de Servicio de TI	No
21	Gestión de Seguridades de la Información	CS-SI-001	Acceso al repositorio de código	La dirección administra y gestiona el acceso al repositorio de código de todas las aplicaciones	Mesa de Servicio de TI	No
22	Gestión de accesos a servicios	CS-SI-002	Gestión y custodia de contraseñas para sistemas sensibles	La dirección proporciona acceso a servicios sensibles como las bases de datos custodiando y autorizando los permisos otorgados	Mesa de Servicio de TI	No

Tabla 1.2. Catálogo de servicios
(Elaborado por: Los Autores)

1.3 CARACTERIZACIÓN DE LA CAPACIDAD INSTALADA

1.3.1 INFRAESTRUCTURA

En la figura 3, se aprecia la topología jerárquica en estrella adoptada en la red de datos de la SENPLADES, definiendo claramente la capa de distribución (switch de core) y de acceso. La velocidad de transmisión para la capa de acceso corresponde a 10/100 Mbps y 10/100/1000 Mbps para la conmutación en el Centro de Datos.

La red de datos proporciona las funcionalidades de Redes Basadas en Identidad (IBNS) permitiendo aplicar diferentes perfiles de acceso a la red, basados en un sistema de Autentificación, Autorización y Auditoria (AAA)

El Centro de Datos cuenta con todos los elementos para garantizar la operación de quipos activos de TI, tales como: climatización, energía regulada, control de acceso, sistema de detección y extinción de incendios, piso falso, tomadas como referencia de diseño la norma EIA/TIA 942.

La seguridad informática es controlada y monitoreada por equipos de prevención y detección de intrusos, firewalls, filtros web y controlador de ancho de banda de tal forma de asegurar los segmentos de red donde operan los servicios críticos de la Institución.

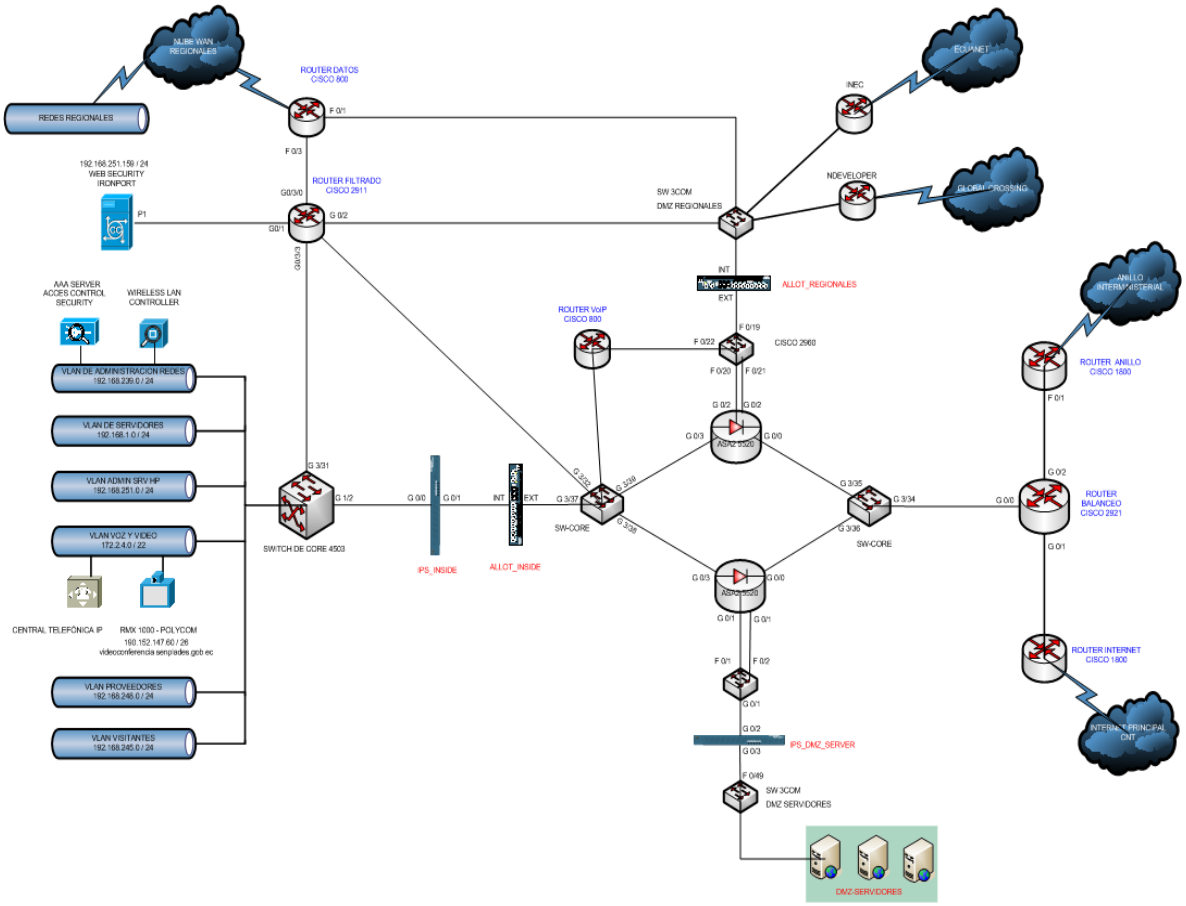


Figura 1.3. Arquitectura de red
(Unidad de infraestructura de la DITSI, 2012)

En relación a la plataforma de servidores, la SENPLADES cuenta con una arquitectura blade y sistema de almacenamiento externo, definiendo dos plataformas de operación: servidores físicos y servidores virtuales.

De acuerdo al decreto 1014, el cual por decreto presidencial se promueve el uso de software libre en las instituciones públicas, el 60% de sistemas operativos en la Institución corresponde a una distribución Linux (Red Hat Enterprise Linux) y la mayor parte de sus sistemas es open source.

1.3.2 TALENTO HUMANO

La dirección cuenta con 33 personas organizados de acuerdo al organigrama, 98% poseen título de tercer nivel, 40% estudiando maestrías y 2% con título de cuarto nivel. La Figura 4 muestra la distribución del personal de acuerdo al organigrama de la Dirección.

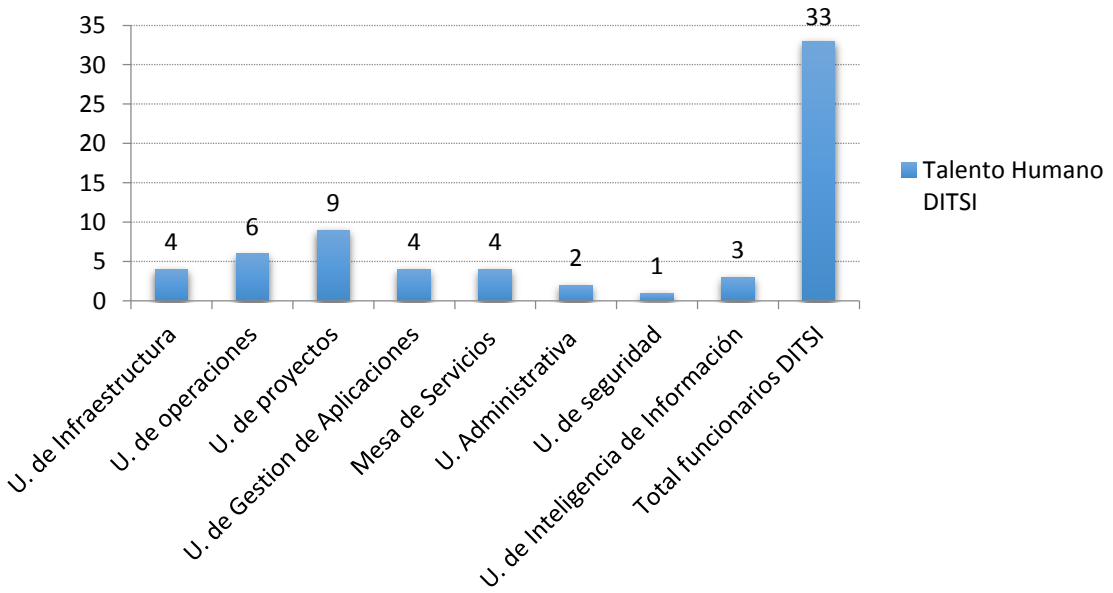


Figura 1.4 Número de personal de la Dirección de Tecnología
(Levantamiento de Información DITSI, 2012)

Debido a la estrategia de capacitación a personal de la dirección, ha permitido difundir los principales conceptos de la gestión de servicios, especialmente con el framework de ITIL. A pesar de este posicionamiento aún no se han formalizado los procesos relacionados con la gestión de servicios. Los avances presentados en este aspecto corresponden a iniciativas y disposiciones realizadas.

1.3.3 APLICACIONES

Principalmente existen dos tipos de aplicaciones, las desarrolladas internamente y propietarias, las cuales son clasificadas de acuerdo a la criticidad definida en base al siguiente cuadro:

CRITICIDAD	DESCRIPCIÓN	DOWNTIME
Alta	Pérdida o afectación de la producción, detiene la operación y no existe workaround.	1-2 HORAS
Media	Funciona pero en forma reducida, hay impacto pero no existe pérdida de datos críticos. El negocio continúa funcionando y tiene workaround. En ambientes de desarrollo previene al proyecto de continuar o de pasar a producción.	2-4 HORAS
Baja	Es un error de bajo impacto para el negocio, el rendimiento o la funcionalidad del sistema. En ambientes de desarrollo el negocio continúa funcionando y se puede aplicar un workaround.	>4 HORAS

Tabla 1.3. Definición de criticidad de aplicaciones/servicios
(Levantamiento de Información DITSI, 2012)

El objetivo de la tabla anterior es sentar la base para la definición de Acuerdos de Nivel de Servicios (SLA), pero a pesar de que se ha realizado el levantamiento de información de la correlación de aplicaciones y recursos de TI asociados a ellas, no existe un responsable para mantener y actualizar esta información. Adicionalmente este documento no forma parte de ningún proceso.

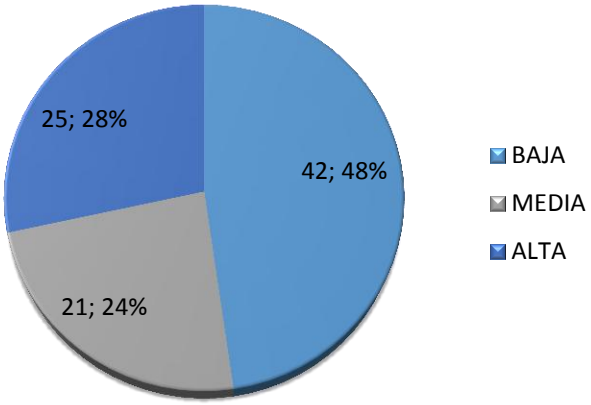


Figura 1.5. Número de aplicaciones/servicios por nivel de criticidad
(Levantamiento de Información DITSI, 2012)

La Figura 1.5 muestra el número de aplicaciones y servicios disponibles en al SENPLADES en un periodo anual, en base a la criticidad definida para cada una de ellas. Esta información es cambiante debido a la dinámica de la Institución, puesto que compromisos de la alta gerencia obligan a crear servicio o

aplicaciones sin el respaldo técnico y funcional requerido para un ambiente de producción, provocando el aumento de aplicaciones y por ende soporte y administración.

1.3.4 INFORMACIÓN

La información generada, mantenida, transferida y administrada por la institución, es un activo primario e importante para realizar las actividades diarias de la institución. Parte de esta información se encuentra desplegada en sistemas como: el Sistema Nacional de Información (SNI) y el Sistema Integrado de Planificación e Inversión Pública (SIPeIP).

Estos sistemas se encuentran alineados a estándares de interoperabilidad gubernamental y se alinearán a la política pública emitida para este fin. Los sistemas implementados en la SENPLADES buscan apoyar la gestión adecuada de la inversión pública y la publicación de información necesaria para la planificación nacional. El resto de información es tratada, generada y publicada por aplicaciones, sistemas y servicios adicionales institucionales, que alimentan y apoyan a los procesos críticos de la institución.

1.4ANÁLISIS DE ACUERDO A ETAPAS DE ITIL

Se realiza un análisis general de los principales procesos de ITIL que intervienen de alguna forma en la gestión de servicios de TI, proporcionados por la DITSI.

A través de entrevistas realizadas al Coordinador de Infraestructura y Coordinador de Soporte técnico se identificaron los siguientes procesos críticos, en base a la gestión de la DITSI.

Etapa	Proceso de ITIL
Estrategia de servicio	Gestión Financiera
Estrategia de servicio	Administración de niveles de servicio
Diseño del servicio	Catálogo de servicio
Diseño del servicio	Administración de la disponibilidad
Transición del servicio	Gestión de la configuración
Transición del servicio	Gestión de cambios
Función	Mesa de Servicio

Tabla 1.4 Procesos de ITIL analizados
(Levantamiento de Información DITSI, 2012)

A continuación se analiza cada uno de los procesos mencionados anteriormente:

Gestión financiera

Etapa: Estrategia del servicio

Proceso: Gestión Financiera

Objetivo: Administrar de manera eficaz y rentable los servicios y la organización TI.

Por regla general, a mayor calidad de los servicios, mayor es su coste, por lo que es necesario evaluar cuidadosamente las necesidades del cliente para que el balance entre ambos sea óptimo.

Las características de la gestión financiera de acuerdo a ITIL que debe cumplir son:

- Evaluar los costos asociados a la prestación de servicios.
- Llevar a contabilidad de los gastos asociados a los servicios de TI.
- Los gastos en servicios e infraestructura TI están alineados con los procesos de negocio.
- Evaluar conjuntamente con la Gestión de Portafolio de servicios, un análisis financiero para determinar el retorno de la inversión.
- Proporcionar toda la información financiera que la unidad de TI utilizará para la fijación de precios y toma de decisiones.

La institución cumple con lo siguiente:

- No se evalúa los costos asociados a la prestación de servicio.
- No lleva la contabilidad asociada a los servicios de TI.
- Se encuentran alineados los gastos de servicios e infraestructura de TI con los procesos de negocio.
- Se realiza muy rara vez el análisis del retorno de la inversión en los proyectos ejecutados.

- No se dispone de información financiera estructurada ni detallada que apoye la toma de decisiones en relaciona a los servicios de TI

La institución debe cumplir con lo siguiente:

- Establecer políticas donde se contemple en análisis de los costos relacionados con la prestación de servicios.
- Llevar la contabilidad asociada a los servicios de TI
- Realizar con cada nueva inversión en TI, el respectivo análisis de retorno de la inversión (ROI).
- Tabular y analizar la contabilidad asociada de los servicios de TI, de manera de proporcionar herramientas de BI, para la toma de decisiones.

Administración de niveles de servicio

Etapa: Estrategia del servicio

Proceso: Administración de niveles de servicio

Objetivo: Buscar un compromiso realista entre las necesidades y expectativas del cliente y los costes de los servicios asociados, de forma que estos sean asumibles tanto por el cliente como por la organización TI.

Las características de la gestión de nivele de servicio de acuerdo a ITIL que debe cumplir la institución son:

- Existir un responsable para la gestión de los niveles de servicio
- Elaboración y aceptación de acuerdos necesarios para la prestación de servicios
- Indicadores específicos de rendimiento
- Seguimiento del resultado y el grado de satisfacción de los clientes con el servicio prestado
- Propuestas para la mejora de los servicio de TI y el impacto en la calidad de servicio.
- Informes de rendimiento donde se detallen los SLAs, OLAs y UCs elaborados así como su cumplimiento, costos promedios, etc.

La Institución cumple con lo siguiente:

- No existe un responsable de la gestión de los niveles de servicio
- Se redactan SLA para servicios críticos de la Institución mas no se lo ha generalizado para todo el catálogo de servicio de la SENPLADES
- Se encuentra definido un procedimiento para dar seguimiento a los SLAs actualmente definidos.
- Existen propuestas para la mejora de los servicios de TI, en base a los indicadores clave utilizados para dar seguimiento a los SLA actualmente definidos; sin embargo no es parte de un proceso formal.
- No existe documentación formal de la recopilación de todos los SLAs realizados, así como su cumplimiento, costos promedios, multas, etc.

La institución debe cumplir con lo siguiente:

- Nombrar a un responsable de la gestión de niveles de servicio.
- Definir políticas donde se estipule la redacción de acuerdos de niveles de servicio para cada uno de los componentes del portafolio de servicio de TI, manejo de proveedores y operación internas.
- Establecer un proceso para analizar el cumplimiento de los niveles de servicio y proponer planes de mejora de servicios de TI.
- Documentar y consolidar la información relacionada con la elaboración de SLA, indicadores, cumplimiento, etc.

Catálogo de servicio

Etapa: Diseño del servicio

Proceso: Catálogo de servicio

Objetivo: Sintetizar toda la información referente a los servicios que los clientes deben conocer para asegurar un buen entendimiento entre éstos y la organización TI.

Las características de la gestión de catálogo de servicio de acuerdo a ITIL que debe cumplir la institución son:

- El catálogo de servicio sintetiza de forma gerencial el fin de los servicio de TI, de manera que incluso puede ser empleado como una herramienta de venta o promoción.
- Delimita las funciones y compromisos de la Dirección de TICs
- Registra los clientes actuales de cada servicio
- Discrimina periódicamente y conforme es requerido los servicios que ya no estén activos del portafolio de servicios.
- Revisiones y actualizaciones periódicas de los estados de los servicios, responsables, precios y demás aspectos directamente involucrados con el catálogo de servicios.

La Institución cumple con lo siguiente:

- No se encuentra definido correctamente el catálogo de servicios.
- No delimita las funciones y compromisos de la Dirección de TICs
- Tiene registrado los clientes actuales de cada servicio.
- No discrimina periódicamente del portafolio de servicios aquellos que ya no están activos.
- No realiza periódicamente actualizaciones al catálogo de servicio.

La institución debe cumplir con lo siguiente:

- Definir de manera sistemática y con lenguaje gerencial el catálogo de servicios.
- Establecer procedimientos para identificar y delimitar las funciones y compromisos de la Dirección de TICs.
- Establecer políticas para la periódica actualización del catálogo de servicio.

Administración de la disponibilidad

Etapa: Diseño del servicio

Proceso: Administración de la disponibilidad

Objetivo: Asegurar que los servicios TI estén disponibles y funcionen correctamente siempre que los clientes y usuarios deseen hacer uso de ellos en el marco de los SLAs.

Las características de la gestión de la disponibilidad de acuerdo a ITIL que debe cumplir la institución son:

- Desarrollar un plan de disponibilidad a corto y medio plazo.
- Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo.
- Determinar cuáles son los requisitos de disponibilidad reales del negocio.
- Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios.
- Evaluar la capacidad de servicio de los proveedores internos y externos.
- Monitorizar la disponibilidad de los servicios TI.
- Elaborar informes de seguimiento con la información recopilada sobre disponibilidad, fiabilidad, capacidad de mantenimiento y cumplimiento de OLAs y UCs.
- Evaluar el impacto de las políticas de seguridad en la disponibilidad.
- Asesorar a la Gestión de Cambios sobre el posible impacto de un cambio en la disponibilidad.

La Institución cumple con lo siguiente:

- No dispone un plan de disponibilidad.
- Se tiene definido procedimientos para la recuperación de los servicios ante fallas
- No se tiene identificado totalmente los requisitos de disponibilidad reales del negocio.
- No se realiza evaluaciones de la capacidad de servicio de los proveedores.
- Se tiene implementado sistemas de monitoreo de la Infraestructura de TI.
- No existe documentación formal de la recopilación de todos los SLAs realizados, así como su cumplimiento, costos promedios, multas, etc.
- La conexión con la gestión de cambios es informal.

- La institución debe cumplir con lo siguiente:
- Elaborar un plan de disponibilidad para corto y mediano plazo.
- Sistematiza en un documento los requisitos de disponibilidad reales de negocio utilizando como apoyo los SLA definidos.
- Establecer políticas que involucren evaluaciones de la capacidad de servicio de los proveedores.
- Establecer procedimientos formales para lograr la adecuada interrelación con la gestión de cambios, ante un posible impacto de un cambio en disponibilidad.

Proceso: Gestión de la configuración

Etapa: Transición del servicio

Proceso: Gestión de la configuración

Objetivo: Llevar el control de todos los elementos de configuración de la infraestructura TI con el adecuado nivel de detalle y gestionar dicha información a través de la Base de Datos de Configuración (CMDB).

Para cumplir su cometido, la Gestión de la Configuración desempeña las siguientes actividades:

- **Planificación:** determinar los objetivos y estrategias de la Gestión de Configuraciones.
- **Clasificación y Registro:** los Ítems de Configuración (CI) deben ser registrados conforme al alcance, nivel de profundidad y nomenclatura predefinidas.
- **Monitorización y Control:** monitorizar la CMDB para asegurar que todos los componentes autorizados estén correctamente registrados y se conoce su estado actual.
- **Realización de auditorías:** para asegurar que la información registrada en la CMDB coincide con la configuración real de la estructura TI de la organización.

- **Elaboración de informes:** para evaluar el rendimiento de la Gestión de Configuraciones y aportar información de vital importancia a otras áreas de la infraestructura TI.

La institución cumple con lo siguiente:

- Existen actividades levemente definidas de planificación, ejecución y control al interior del departamento de TI.

La institución debe cumplir con lo siguiente:

- Debe existir una adecuada gestión de la Base de datos de la gestión de configuraciones CMDB.
- Debe existir un adecuado levantamiento de información que incluya al menos todos los sistemas de HW y SW implicados en los servicios críticos.
- Deben determinarse los elementos de configuración CI que deben incluirse dependiendo del estado de su ciclo de vida.
- Se debe conocer el estado de cada componente de HW y SW en todo momento de su ciclo de vida.

Proceso: Gestión de cambios

Etapa: Transición del servicio

Proceso: Gestión de cambios

Objetivo: El objetivo primordial de la Gestión de Cambios es que se realicen e implementen adecuadamente todos los cambios necesarios en la infraestructura y servicios TI garantizando el seguimiento de procedimientos estándar.

Para cumplir su cometido, la Gestión de Cambios desempeña las siguientes actividades:

- Monitorizar y dirigir todo el proceso de cambio.
- Registrar, evaluar y aceptar o rechazar las RFCs recibidas.
- Convocar reuniones del CAB, excepto en el caso de cambios menores, para la aprobación de las RFCs y la elaboración del FSC.

- Coordinar el desarrollo e implementación del cambio.
- Evaluar los resultados del cambio y proceder a su cierre en caso de éxito.

La institución cumple con lo siguiente:

- Una razón para realizar un cambio en la infraestructura de TI es el desarrollo de nuevo servicios y la mejora de los servicios existentes.

La institución debe cumplir con lo siguiente:

- Seguir los procedimientos establecidos y, en particular, se actualiza correctamente la información sobre los CIs en la CMDB.
- Disponer de las herramientas adecuadas de software para monitorizar y documentar adecuadamente el proceso.
- Establecer una manera eficiente de control de cambios realizados, siguiendo procedimientos establecidos y asegurando en todo momento la calidad y la continuidad del servicio de TI.

Función: Mesa de Servicios

Etapa: Operación del servicio

Función: Mesa de servicios

Objetivo: Representar la interfaz para clientes y usuarios de todos los servicios TI ofrecidos por la organización con un enfoque centrado en los procesos de negocio.

Para cumplir su cometido, la mesa de servicios desempeña las siguientes actividades:

- Monitorizar el entorno de IT para el cumplimiento de estos niveles predeterminados de servicio y escalar las incidencias en la entrega de servicios de la manera adecuada cuando surjan.
- Supervisión de los contratos de mantenimiento y niveles de servicio.
- Canalización de las Peticiones de Servicio de los clientes.
- Gestión de las licencias de software.
- Centralización de todos los procesos asociados a la Gestión TI.

La institución cumple con lo siguiente:

- Tiene un responsable de mesa de servicios.
- La mesa de ayuda gestiona la primera línea de soporte de Gestión de Incidentes.
- Las encuestas de las realiza esporádicamente.
- No se tiene implementado ni estructurado una base de conocimiento ni errores.
- Si se dispone de una herramienta para la gestión de la información de la mesa de servicio, OTRS.

La institución debe cumplir con lo siguiente:

- Establecer políticas para supervisar la calidad del servicio ofertado.
- Establecer políticas para realizar encuestas periódicamente, para conocer y tomar accionas correcticas respecto del grado de satisfacción del cliente.
- Estructurar y hacer parte del proceso de resolución de incidentes la alimentación de la base de conocimiento y de errores.

1.5ANÁLISIS DE ACUERDO A LA NORMA TÉCNICA ISO/IEC 27005

La ISO/IEC 27005 es una norma de apoyo para la implantación de la ISO/IEC 27001, proporcionando a través de la ISO/IEC 27005 lineamientos para la gestión de seguridad basada en un enfoque de riesgo. Esta norma no proporciona la metodología específica, ya que esta debe ser establecida por la organización.

En este marco se analizará el estado de la Gestión del Riesgo de Seguridad de la Información en la SENPLADES de acuerdo a la estructura de esta norma que contempla las siguientes actividades:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo

- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Todas las actividades están estructuradas con la siguiente información:[9]

Entrada: explica los insumos requeridos para cumplir con la actividad

Acciones: pasos para desarrollar la actividad

Guía de Implementación: describe los pasos para cumplir con la actividad, Estos lineamientos no son rígidos en su aplicación y dependen de la realidad de cada organización.

Salida: es la información que debe obtenida como producto de realizar la actividad.

A inicios de este capítulo se presentó la información que permite describir a la SENPLADES. En este ítem, se procederá a describir el Estudio de la Organización propuesto por la norma ISO/IEC 27005 desde el punto de vista de Gestión del Riesgo de la Seguridad de la Información.

1.5.1 ESTUDIO DE LA ORGANIZACIÓN

1.5.1.1 Establecimiento del contexto

La Secretaría Nacional de Planificación y Desarrollo (SENPLADES) tiene como propósito principal la planificación del Buen Vivir para el estado ecuatoriano.

Al momento no existe participación del nivel jerárquico superior, incluyendo en éste a la máxima autoridad de la SENPLADES en la gestión de seguridades de la información ya que ésta reporta a la Dirección de Información, Seguimiento y Evaluación Institucional.

La Gestión de Seguridades de la Información, es un proceso nuevo en la Secretaría, por lo que no existe a nivel del servidor/a y el funcionario/a pública una conciencia establecida para proteger la información institucional. Es decir, la cultura organizacional actual no posee directrices organizacionales, legales y de tecnología que reflejen una gestión de seguridades de la información implantada.

[9] De acuerdo a la Norma Técnica NTE ISO/IEC 27005, Estructura de la Norma

La Secretaría Nacional de Planificación y Desarrollo posee una estructura por áreas (está dividida en áreas) y una estructura funcional (existen procesos establecidos por la naturaleza de sus actividades), por lo que al tener las dos de manera simultánea estaría conformada por una estructura matricial[10].

1.5.1.2 Restricciones que afectan a la organización

Las restricciones se analizan en función de las que apliquen tomando como referencia las mencionadas en la norma NTC-ISO/IEC 27005. Las mismas determinan la orientación de la SENPLADES sobre seguridades de la información. Entre las principales se tienen:

Restricciones de naturaleza política

La SENPLADES es una entidad del gobierno central que se cumple con las decisiones y lineamientos dados por la Presidencia de la República y por la Secretaría Nacional de la Administración Pública (SNAP).

Restricciones de naturaleza estratégica

La planeación estratégica y operativa de la SENPLADES tiene riesgos establecidos por proporcionar información para la planificación a nivel nacional y a nivel internacional por los acuerdos de cooperación estratégica que mantiene con organismos de otros países.

Restricciones territoriales

La SENPLADES abarca todo el territorio nacional, a través de ocho zonales autónomas distribuidas de acuerdo a la zonificación territorial establecida.

Restricciones que se originan en el clima político y económico

Por ser una institución del gobierno central, la SENPLADES está expuesta a riesgos producidos por aquellos cambios relevantes en la política nacional que produzcan interrupciones en sus actividades diarias como huelgas, intentos de desestabilización del gobierno, etc.

Restricciones funcionales

[10] De acuerdo a lo indicado en la norma técnica NTE-ISO/IEC 27005, Anexo A (Definición del alcance y los límites de los procesos de la gestión del riesgo en la seguridad de la información)

La SENPLADES cuenta con sistemas que apoyan a la planificación en el país, los cuales no cuenta con una definición clara y formal que indique los acuerdos de nivel de servicio requeridos por la Institución.

Restricciones de presupuesto

La SENPLADES cuenta con un Plan Anual de Contratación, el mismo que especifica el presupuesto anual de cada área. Por esta razón, el presupuesto relacionado a seguridades de la información deben estar reflejados en Plan Operativo Anual o Proyecto de Inversión correspondiente, en base a los metas y objetivos a alcanzar.

1.5.1.3 Listado de referencias legislativas y reglamentarias que se aplican a la SENPLADES

La institución debe cumplir con la siguiente normativa legal y reglamentaria, tanto interna como externa:

- Constitución de la República del Ecuador.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley del Sistema Nacional de Registro de Datos Públicos.
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.
- Ley Orgánica y Normas de Control de la Contraloría General del Estado.
- Leyes y normas de control del sistema financiero.
- Leyes y normas de control de empresas públicas.
- Ley del Sistema Nacional de Archivos.
- Decreto ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública.
- Acuerdo No. 166, sobre el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000, para la Gestión de la Seguridad de la Información.
- Acuerdo No. SNPD-084-2013, que contiene las Políticas de Seguridad de la Información de la SENPLADES.

- Acuerdo No. SNPD-039-2013, que contiene el Reglamento para la Asignación, Uso y Control de los Servicios y Activos de Tecnología de Información y Comunicaciones y sus Derivados de la SENPLADES.
- Otras normas cuya materia trate sobre la gestión de los activos de información en las entidades de la Administración Pública.

1.5.1.4 Restricciones originadas en procesos

La SENPLADES al momento tiene una reestructuración en su organigrama que origina cambio y establecimiento de nuevos procesos.

Restricciones técnicas

Se refiere especialmente a la normativa y base legal generada por la Secretaría Nacional de la Administración Pública (SNAP).[11]

Restricciones de tiempo

Por el cambio continuo que existe en las amenazas, los controles establecidos por Seguridades de la Información deben ser ejecutados en un periodo de tiempo adecuado antes de que los riesgos identificados cambien.

A continuación se establece un comparativo entre la estructura de cada actividad de la norma con el estado actual de la dirección.

1.5.2 COMPARATIVO BASADO EN LA INFORMACIÓN DE CADA ACTIVIDAD

1.5.2.1 Establecimiento del Contexto

Fases	Actividades ISO/IEC 27005	La institución debe cumplir con
Entrada	Toda la información para gestionar el riesgo.	Contar con el establecimiento de recursos necesarios, procedimientos y políticas internas para gestionar el riesgo.
Acción	Establecimiento de contexto con criterios básicos como alcance, límite y la organización adecuada para gestionar el riesgo.	Establecer criterios para evaluación de riesgo, criterios de impacto y de aceptación de riesgo, como por ejemplo: • Valorar el riesgo y establecer un plan de tratamiento. • Establecer políticas y

[11] Fuente: http://sge.administracionpublica.gob.ec/sbs/bl

		procedimientos para gestión del riesgo. • Establecer controles y su proceso de monitoreo. • Definir la criticidad de los activos de información involucrados. • Definir los requisitos legales y reglamentarios.
Guía para la Implementación	Determinar el propósito de la Gestión del Riesgo.	Se encuentra definido como soporte para el SGSI, sin embargo este alcance se puede ampliar para el Plan de Recuperación de Desastres y para solución de incidentes.
Salida	Especificación de los criterios básicos, alcances y límites y organización del proceso del Gestión del Riesgo en la Seguridad de la Información.	Establecer los criterios básicos, alcances y límites y organización del proceso del Gestión del Riesgo en la Seguridad de la Información.

Tabla 1.5. Diagnóstico, Establecimiento del Contexto
(Levantamiento de Información DITSI, 2012)

1.5.2.2 Valoración del Riesgo en la Seguridad de la Información

Fases	Actividades ISO/IEC 27005	La institución debe cumplir con
Entrada	Criterios básicos, alcance y límites establecidos en el contexto.	Se debe definir acorde a la documentación resultado del Establecimiento del Contexto.
Acción	Identificación de riesgos con su descripción cualitativa o cuantitativa, priorización.	Identificación documentada de los riesgos, descripción o cuantificación de los riesgos.
Guía para la Implementación	• Análisis del riesgo. • Identificación del riesgo. • Estimación del riesgo. • Evaluación del riesgo.	• Determinar el valor de activos de información. • Identificar amenazas y vulnerabilidades. • Determinar controles. • Determinar consecuencias potenciales. • Priorizar y clasificar riesgos. • Estimación cualitativa y/o cuantitativa del riesgo. • Tratamiento de riesgos de acuerdo a sus prioridades.
Salida	Salidas por acción que se requiera implementar de acuerdo al enfoque dado por la organización.	Establecer los riesgos valorados con prioridad de acuerdo a los criterios de evaluación.

Tabla 1.6 Diagnóstico, Valoración del Riesgo
(Levantamiento de Información DITSI, 2012)

1.5.2.3 Tratamiento del Riesgo en la Seguridad de la Información

Fases	Actividades ISO/IEC 27005	La institución debe cumplir con
Entrada	Lista de los riesgos con prioridad de acuerdo a los criterios de evaluación y relacionado a los escenarios de	Establecer los riesgos valorados con prioridad de acuerdo a los criterios de evaluación.

	incidentes que llevan a tales riesgos	
Acción	Selección de controles para reducir, retener, evitar o transferir los riesgos y definir el plan para tratar los mismos	Desarrollar el plan que permita tratar los riesgos.
Guía para la Implementación	La norma ofrece cuatro opciones: • Reducción del riesgo • Retención del riesgo • Evitación del riesgo • Transferencia del riesgo	Establecer el plan para tratar el riesgo. Este tratamiento deberá ser seleccionado dependiendo de la valoración, el costo asociado y los requisitos legales y reglamentarios con que debe cumplir la SENPLADES.
Salida	Plan de tratamiento del riesgo	Desarrollar el plan que permita tratar los riesgos.

Tabla 1.7 Diagnóstico, Tratamiento del Riesgo
(Levantamiento de Información DITSI, 2012)

1.5.2.4 Comunicación de los Riesgos en la Seguridad de la Información

Fases	Actividades ISO/IEC 27005	La institución debe cumplir con
Entrada	Toda la información sobre el o los riesgos obtenidas de las actividades anteriores	Consolidar toda la información generada por las actividades de gestión de riesgo.
Acción	Intercambiar información del riesgo entre persona que toma la decisión y las partes involucradas.	Intercambiar información del riesgo entre persona que toma la decisión y las partes involucradas.
Guía para la Implementación	La comunicación logra un acuerdo para tratar los riesgos y/o compartir información entre quienes toman las decisiones y el resto de partes involucradas	Desarrollar el plan de comunicación para gestionar riesgos en la SENPLADES.
Salida	Comprensión continua del proceso y de resultados en la gestión de riesgo	Establecer los mecanismos para una adecuada comunicación en la gestión de riesgos.

Tabla 1.8 Diagnóstico, Comunicación del Riesgo
(Levantamiento de Información DITSI, 2012)

1.5.2.5 Monitoreo y Revisión del Riesgo en la Seguridad de la Información

Fases	Actividades ISO/IEC 27005	La institución debe cumplir con
Entrada	• Monitoreo y Revisión de los Factores de Riesgo • Monitoreo, Revisión y Mejora de la Gestión del Riesgo	Consolidar la información sobre riesgos para su monitoreo, revisión y mejora.
Acción	Monitorear riesgos y sus factores	Monitorear y revisar con el fin de identificar todo cambio en el contexto de la SENPLADES.
Guía para la Implementación	Monitoreo de riesgos que son dinámicos a través de vulnerabilidades, amenazas, impacto, incidentes de seguridad de información, etc.; a través de los	Garantizar el monitoreo continuo de los riesgos identificados.

	que se obtendrá la mejora continua de su gestión.	
Salida	Alineación permanente de la gestión de riesgos con los objetivos del negocio y con los criterios de aceptación del riesgo.	Establecer mecanismos para dar relevancia continua al proceso de gestión del riesgo en la seguridad de la información

Tabla 1.9 Diagnóstico, Monitoreo del Riesgo
(Levantamiento de Información DITSI, 2012)

CAPÍTULO 2: DESARROLLO DEL MODELO DE GESTIÓN BASADO EN EL MAPEO Y/O COMBINACIÓN ENTRE EL MARCO DE REFERENCIA ITIL V3 Y EL ESTÁNDAR DE SEGURIDADES ISO 27005

2.1 MAPEO ENTRE ITIL V3 Y EL ESTÁNDAR DE SEGURIDADES ISO 27005

2.1.1 ELEMENTOS PARA EL MAPEO ITIL V3 - NTE INEN-ISO/IEC 27005:2008

2.1.1.1 Análisis de grupos de interés

Los grupos de interés corresponden a las personas o grupos de la organización, que pueden ser afectados por las decisiones tomadas en una empresa o institución en pro de alcanzar sus objetivos.

La definición de estos grupos es importante por su rol de aprobación, para los planes, proyectos y modelos a ser aplicados en una organización. Esto es trascendental para modelos de gestión de riesgos, donde se debe tener el compromiso de todo el personal, y a manera de ejemplo desde el más alto nivel de la organización, hacia las áreas operativas, asegurando de esta forma el éxito del modelo de gestión.

El modelo de gestión planteado en este proyecto de tesis, busca optimizar los procesos de Tecnología de la Información y Comunicaciones (TIC's), de manera que las áreas de TIC's, generen valor en la organización de la siguiente manera:

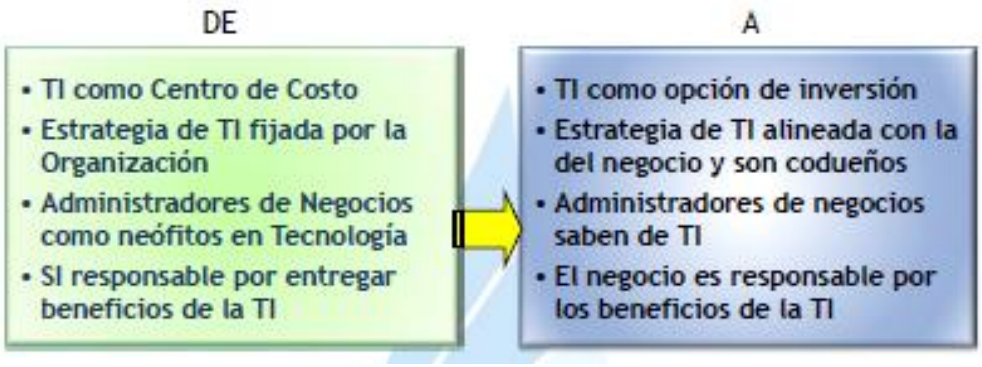


Figura 2.1 Generación de valor en las áreas de TI
(CIO 2.0, Deloitte, 2008)

Con un enfoque que le permita a TI, incluir en sus procesos la gestión de riesgos presentes en los activos de seguridades de la información bajo su cargo, como son ‘hardware’ y ‘software’.

Por esta razón, es necesario identificar los grupos de mayor interés de la organización, en mejorar la gestión de TI y que adicionalmente busquen establecer mecanismos adecuados para gestionar el riesgo de los activos que son soporte para los servicios, sistemas y aplicaciones sobre los que trabaja el personal de la empresa o institución, y además que son utilizados por sus clientes y/o usuarios finales.

2.1.1.2 Esquema de ITIL V3

ITIL es un marco de referencia utilizado en TIC’s, estructurado con cinco etapas: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio.

Cada etapa contiene procesos de TI utilizados para gestionar de manera efectiva el ciclo de vida de los servicios. Estos procesos permiten gestionar las áreas de TIC’s de una organización, de manera independiente al tipo de industria donde se apliquen.

A excepción de la etapa de Estrategia del Servicio que no tiene procesos definidos, los procesos definidos para cada etapa son:

Etapa	Procesos
Diseño del Servicio	Gestión del Catálogo del Servicio
	Gestión del Nivel del Servicio
	Gestión de la Capacidad
	Gestión de la Disponibilidad
	Gestión de la Continuidad del Servicio de TI
	Gestión de la Seguridad de la Información
	Gestión de Proveedores
Transición del Servicio	Planificación y soporte de la transición
	Gestión del cambio
	Gestión y configuración de activos
	Gestión de liberación y despliegue
	Validación y pruebas del servicio
	Evaluación
	Gestión del conocimiento
Operación del Servicio	Gestión de eventos
	Gestión de incidentes
	Solicitud de requerimientos
	Gestión de problemas
	Gestión de accesos
	Actividades operativas de los procesos cubiertas en otras fases del ciclo de vida
Mejora Continua del Servicio	Servicio de reporte
	Medida del servicio
	Retorno de la inversión de la mejora continua
	Preguntas del negocio para la mejora continua
	Gestión del Nivel del Servicio

Tabla 2.1 Procesos por etapa de ITIL V3
(Libros de ITIL v3, 2007)

2.1.1.3 Esquema de la norma NTE INEN-ISO/IEC 27005:2008

La familia de normas NTE INEN-ISO/IEC 27000:2012, hacen referencia al Sistema de Gestión de Seguridades de la Información (SGSI), y están estructuradas en un grupo de estándares normativos con los requisitos para implementar un SGSI en cualquier tipo de organización.

En este grupo se encuentran directrices generales para la Gestión del Riesgo, los mismos que han sido plasmados en la norma NTE INEN-ISO/IEC 27005:2008.

El estándar NTE INEN-ISO/IEC 27005:2008, es utilizado por directores y personal involucrado en la gestión del riesgo de seguridad de la información, y puede ser

aplicada a toda la organización, una parte de la misma como una unidad administrativa, una ubicación geográfica o un servicio específico.

El estándar contiene seis procesos, que son:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Este estándar proporciona las directrices de implementación de cada proceso, identificando entradas, acciones que se deben realizar, guía de implementación y la salida esperada de cada proceso.

2.1.2 CONSTRUCCIÓN DEL MODELO DE GESTIÓN

2.1.2.1 Nombre del modelo

La selección del nombre del modelo de gestión es trascendente, ya que debe expresar directamente lo que hace el modelo y prácticamente se convierte en la carta de presentación del mismo.

De esta forma, el nombre del modelo debe ser seleccionado cuidadosamente, para influir en su posicionamiento posterior.

En base al objetivo del modelo construido y ya que su fin principal es proporcionar las directrices necesarias para optimizar los procesos de TI con un enfoque en riesgos de seguridades de la información, se estableció el nombre del modelo en **M_OPTIMIZA**.

2.1.2.2 Nomenclatura de los procesos

En el desarrollo del modelo se estableció una nomenclatura que permita identificar a los procesos del marco de referencia ITIL V3 y del estándar NTE

INEN-ISO/IEC 27000:2012. La estructura de la nomenclatura se muestra a continuación.

2.1.2.2.1 ITIL V3

- La primera letra corresponde al nombre del proceso, con la siguiente asignación:
  Diseño del Servicio – D
  Transición del Servicio – T
  Operación del Servicio - O
  Mejora Continua del Servicio – MC

- La segunda letra corresponde a un número asignado ascendentemente, para cada proceso de las diferentes etapas.
  Ejemplo:
  En la etapa de Diseño del Servicio, existe el proceso de Gestión del Catálogo del Servicio, por lo que la nomenclatura asignada será D.01.

2.1.2.2.2 NTE INEN-ISO/IEC 27005:2008

- La primera letra corresponde al nombre del proceso, con la siguiente asignación:

  Establecimiento del contexto - A
  Valoración del riesgo - B
  Tratamiento del riesgo - C
  Aceptación del riesgo - DR
  Comunicación del riesgo - E
  Monitoreo y revisión del riesgo - F
- La segunda letra corresponde a un número asignado ascendentemente, para cada proceso.
  Ejemplo:

Para el proceso de Establecimiento del Contexto, la nomenclatura asignada es A.01.

2.1.2.2.3 Matriz resumen de nomenclatura

De esta forma, los códigos establecidos para los procesos de ITIL v3 y del estándar NTE INEN-ISO/IEC 27005:2008, son:

Etapa	Procesos	Código
Diseño del Servicio	Gestión del Catálogo del Servicio	D.01
	Gestión del Nivel del Servicio	D.02
	Gestión de la Capacidad	D.03
	Gestión de la Disponibilidad	D.04
	Gestión de la Continuidad del Servicio de TI	D.05
	Gestión de la Seguridad de la Información	D.06
	Gestión de Proveedores	D.07
Transición del Servicio	Planificación y soporte de la transición	T.01
	Gestión del cambio	T.02
	Gestión y configuración de activos	T.03
	Gestión de liberación y despliegue	T.04
	Validación y pruebas del servicio	T.05
	Evaluación	T.06
	Gestión del conocimiento	T.07
Operación del Servicio	Gestión de eventos	O.01
	Gestión de incidentes	O.02
	Solicitud de requerimientos	O.03
	Gestión de problemas	O.04
	Gestión de accesos	O.05
	Actividades operativas de los procesos cubiertas en otras fases del ciclo de vida	O.06
Mejora Continua del Servicio	Servicio de reporte	MC.01
	Medida del servicio	MC.02
	Retorno de la inversión de la mejora continua	MC.03
	Preguntas del negocio para la mejora continua	MC.04
	Gestión del Nivel del Servicio	MC.05

Tabla 2.2 Nomenclatura de procesos por etapa de ITIL V3
(Elaborado por: Los Autores**)**

Proceso	Subproceso		Código
Establecimiento del contexto	Consideraciones Generales		A.01
Valoración del riesgo en Seguridad de la Información	Análisis de riesgo	Descripción General de la Valoración del riesgo en la seguridad de la información	B.01
		Identificación de los activos	B.02
		Identificación de las amenazas	B.03
		Identificación de los controles existentes	B.04
		Identificación de las vulnerabilidades	B.05
		Identificación de las consecuencias	B.06
	Estimación del riesgo	Valoración de las consecuencias	B.07
		Valoración de los incidentes	B.08
		Nivel de estimación del riesgo	B.09
	Evaluación del riesgo	Evaluación del riesgo	B.10
Tratamiento del riesgo en la Seguridad de la Información	Descripción General del tratamiento del riesgo		C.01
	Reducción del riesgo		C.02
	Retención del riesgo		C.03
	Evitación del riesgo		C.04
	Transferencia del riesgo		C.05
Aceptación del riesgo en Seguridad de la Información	Aceptación del riesgo en la seguridad de la información		DR.01
Comunicación de los riesgos de la Seguridad de la Información	Comunicación de los riesgos de la seguridad de la información		E.01
Monitoreo y revisión del riesgo en Seguridad de la Información	Monitoreo y revisión de los factores de riesgo		F.01
	Monitoreo, revisión y mejora de la gestión del riesgo		F.02

Tabla 2.3 Nomenclatura de procesos de la NTE INEN-ISO/IEC 27005:2008
(Elaborado por: Los Autores)

2.1.3 FASES DEL MAPEO ENTRE ITIL V3 Y NTE INEN-ISO/IEC 27005:2008

Una vez realizado el análisis de la estructura del marco de referencia ITIL V3 y del estándar NTE INEN-ISO/IEC 27005:2008, se establecen los elementos comunes, para generar los procesos, actividades e indicadores del nuevo modelo M_OPTIMIZA.

En este contexto, y por la extensión de ITIL V3, así como de la ISO, el mapeo fue realizado en tres fases que son detalladas a continuación y que sirvieron para determinar los 11 procesos que conforman el nuevo modelo de gestión.

2.1.3.1 Primera fase

La primera fase de mapeo implanta el estándar NTE INEN-ISO/IEC 27005:2008, como base para determinar las relaciones existentes entre los procesos de ITIL V3 y el estándar en estudio.

M_OPTIMIZA toma como puntos principales, la gestión del riesgo en la seguridad de la información y la entrega de los servicios de TI, estableciendo 25 procesos para la ITIL v3 – excluyendo a la fase de Estrategia de Servicio que no cuenta con procesos estructuraos - y 20 procesos de la NTE ISO/IEC 27005; realizando en primera instancia un mapeo entre todos los procesos, considerando la influencia de cada proceso de ITIL en los objetivos de los proceso de la NTE ISO/IEC 27005, de acuerdo a la siguiente codificación y códigos de colores

Fases del ciclo de vida del servicio ITIL	Código de colores
Diseño del Servicio	
Transición del Servicio	
Operación del Servicio	
Mejora Continua del Servicio	

Figura 2.2 Código de colores

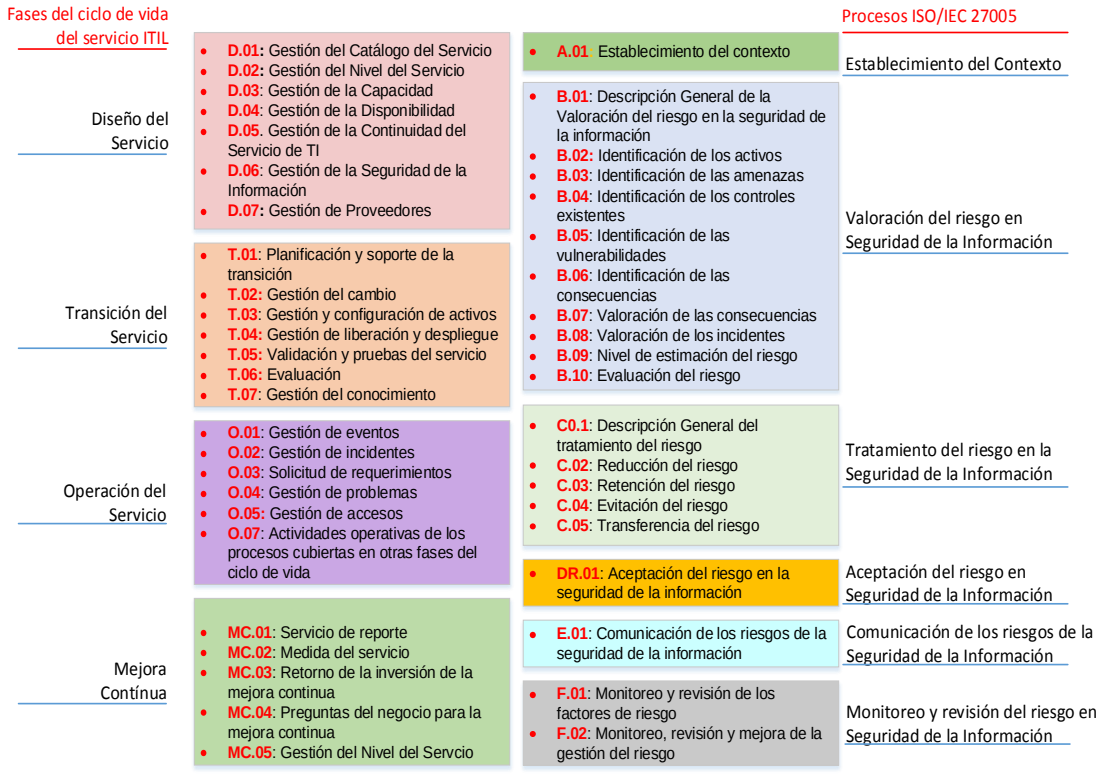


Figura 2.3 Procesos mapeados ITIL – ISO/IEC 27005

Es importante señalar, que en esta fase todavía participan todos los procesos a ser mapeados, aunque su producto final ya distingue únicamente los que son comunes. El esquema de esta fase se muestra a continuación.

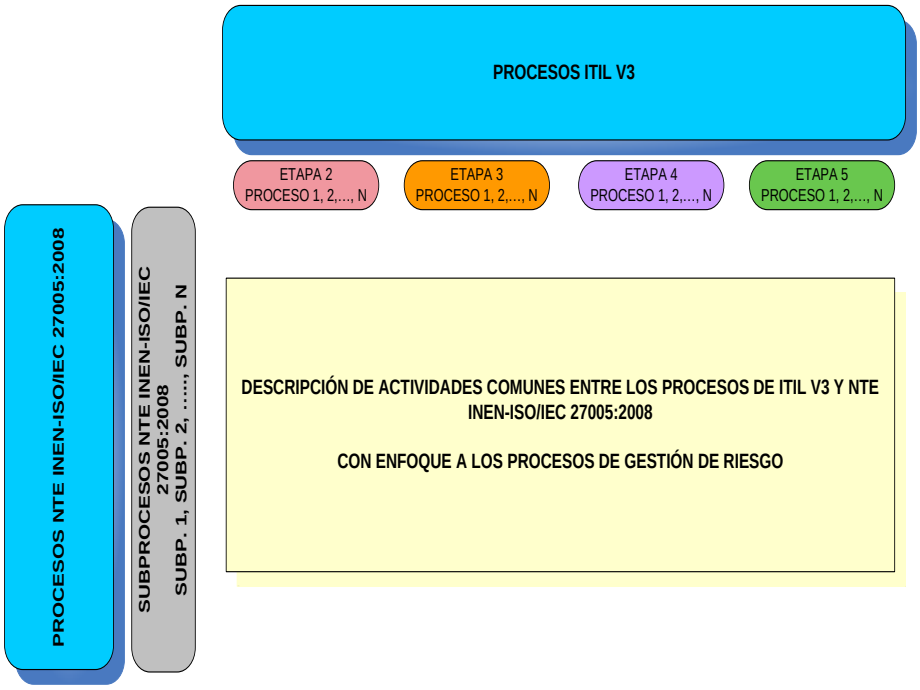


Figura 2.4 Primer nivel de construcción del modelo M_OPTIMIZA
(Elaborado por: Los Autores)

La siguiente tabla expone los criterios de relación entre los procesos de ITIL y la NTE ISO/IEC 27005.

Proceso NTE ISO/IEC 27005	ETAPA: DISEÑO DEL SERVICIO						
	Gestión del Catálogo del Servicio	Gestión del Nivel del Servicio	Gestión de la Capacidad	Gestión de la Disponibilidad	Gestión de la Continuidad del Servicio de TI	Gestión de la Seguridad de la Información	Gestión de Proveedores
Consideraciones Generales	Provee la información para establecer el alcance y límite de la gestión de riesgo de la seguridad de información (GRSI)		Proporciona y mantiene un plan adecuado que reflejas las capacidades actuales y futuras enfocados en el negocio				
Descripción General de la Valoración del riesgo en la seguridad de la información.							
Identificación de los activos.	Provee la información para la identificación de los activos						
Identificación de las amenazas.							
Identificación de los controles existentes.	Provee los controles asignados al catálogo de servicio						
Identificación de las vulnerabilidades.							
Identificación de las consecuencias.							
Valoración de las consecuencias.							
Valoración de los incidentes.							
Nivel de estimación del riesgo.							
Evaluación del riesgo.				Provee asistencia con la evaluación del riesgo y gestión de actividades			
Descripción General del tratamiento del riesgo.							
Reducción del riesgo.				Proporciona el plan de disponibilidad, el cual contiene información del estado de operación del servicio y propuestas para mejorar la disponibilidad.			Gestionar los requisitos de contratación, evaluación, selección, rendimiento de proveedores, proporcionando información relevante para realizar el tratamiento del riesgo mediante terceros.
Retención del riesgo.							
Evitación del riesgo.							
Transferencia del riesgo.							Provee reportes e información de contratos y proveedores para administrar la calidad del servicio compartidos donde esto sea apropiado
Aceptación del riesgo en la seguridad de la información.							
Comunicación de los riesgos de la seguridad de la información.							
Monitoreo y revisión de los factores de riesgo.							
Monitoreo, revisión y mejora de la gestión del riesgo.		Provee el plan de mejora continua para la gestión del riesgo en todos los servicios			Establecer políticas y procedimientos que eviten, en la medida de lo posible, la paralización de los servicios por desastres del tipo informático		

Proceso NTE ISO/IEC 27005	ETAPA: TRANSICIÓN DEL SERVICIO						
	Planificación y soporte de la transición	Gestión del cambio	Gestión y configuración de activos	Gestión de liberación y despliegue	Validación y pruebas del servicio	Evaluación	Gestión del conocimiento
Consideraciones Generales							
Descripción General de la Valoración del riesgo en la seguridad de la información.				Provee el plan de liberación y despliegue de los servicio de TI, que contiene la evaluación de riesgos en la entrega de servicio			
Identificación de los activos.			Provee la base de datos de gestión de configuración para realizar la identificación de activos				
Identificación de las amenazas.					Provee el análisis de resultados de las pruebas con la identificación de riesgos		
Identificación de los controles existentes.							
Identificación de las vulnerabilidades.							
Identificación de las consecuencias.							
Valoración de las consecuencias.		Provee los criterios de impacto a través del RFC para la valoración de las consecuencias					
Valoración de los incidentes.							
Nivel de estimación del riesgo.							
Evaluación del riesgo.							
Descripción General del tratamiento del riesgo.	Identifica, administra y controla los riesgos de falla y degradación a través del plan de transición del servicio				Provee la política de riesgo de la validación y pruebas de servicio con los controles respectivos, útiles para el tratamiento del riesgo durante la transición del servicio		
Reducción del riesgo.							
Retención del riesgo.							
Evitación del riesgo.							
Transferencia del riesgo.							
Aceptación del riesgo en la seguridad de la información.		Provee información a través del RFC para la evaluación del riesgo				Provee el reporte de evaluación con el perfil del riesgo residual, después de la implementación de cambios y contramedidas	Provee la base de datos de conocimientos que pueden ser utilizados para los criterios de aceptación del riesgo.
Comunicación de los riesgos de la seguridad de la información.							
Monitoreo y revisión de los factores de riesgo.							
Monitoreo, revisión y mejora de la gestión del riesgo.							

Proceso NTE ISO/IEC 27005	ETAPA: OPERACIÓN DEL SERVICIO					
	Gestión de eventos	**Gestión de incidentes**	**Solicitud de requerimientos**	**Gestión de problemas**	**Gestión de accesos**	**Actividades operativas de los procesos cubiertas en otras fases del ciclo de vida**
Consideraciones Generales					Provee las restricciones técnicas de acceso para los servicios	
Descripción General de la Valoración del riesgo en la seguridad de la información.						
Identificación de los activos.					Provee el acceso controlado, los niveles de acceso a los servicios y los usuarios autorizados	
Identificación de las amenazas.	Provee los eventos que han iniciado un incidente, problema o cambio y que pueden representar una amenaza	Provee el mecanismo de gestión de incidentes para la identificación de amenazas				
Identificación de los controles existentes.	Provee los eventos que se catalogan como informacionales, de advertencia o excepción que pueden implicar el estado o uso de los controles implementados				Proporciona información en relación a los controles establecidos para la gestión de accesos	
Identificación de las vulnerabilidades.			Provee la información sobre los requerimientos de los usuarios que permitan evaluar los riesgos relacionados al uso de los activos			
Identificación de las consecuencias.				Provee la información para minimizar el impacto en el tiempo de los incidentes que no pueden ser prevenidos		
Valoración de las consecuencias.	Provee la gestión de eventos que sirven para la medición del impacto a través de modelado de resultados de eventos	Provee la identificación, el registro, categorización y priorización del incidente				
Valoración de los incidentes.		Provee todo el proceso de gestión de incidentes para su valoración		Provee la información para llegar a la causa raíz, el workaround y la resolución de un incidente		
Nivel de estimación del riesgo.		Provee los escenarios de incidentes y los activos relacionados		Provee la probabilidad de ocurrencia de un incidente cuando se trata de manera proactiva		
Evaluación del riesgo.						
Descripción General del tratamiento del riesgo.						
Reducción del riesgo.		Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.	Provee actividades para mejorar el control de accesos a los servicios de manera centralizada, de tal forma que se puede establecer mecanismos para tratar el riesgo ante una eventualidad	Provee el mecanismo de para analizar las cusas raíces de los problemas, además de elaborar RFC para reestablecer el servicio. Estas actividades proporcionan información relevante para tratar el riesgo	Provee en conjunto con seguridades de la información, los perfiles de os usuarios para acceder a los servicio publicados en el respectivo catálogo, proporcionando iniciativas e información para tratar el riesgo.	
Retención del riesgo.						
Evitación del riesgo.						
Transferencia del riesgo.						
Aceptación del riesgo en la seguridad de la información.						
Comunicación de los riesgos de la seguridad de la información.						
Monitoreo y revisión de los factores de riesgo.						
Monitoreo, revisión y mejora de la gestión del riesgo.						

Proceso NTE ISO/IEC 27005	ETAPA: MEJORA CONTINUA DEL SERVICIO					
	Proceso de mejora de 7 pasos	Servicio de reporte	Medida del servicio	Retorno de la inversión de la mejora continua	Preguntas del negocio para la mejora continua	Gestión del Nivel del Servicio
Consideraciones Generales	La gestión del riesgo provee la información para estructurar los siete pasos de mejora continua del servicio		Esta información es proporcionada en los procesos del diseño del servicio		Provee información del estado actual y deseado de TI y del negocio	
Descripción General de la Valoración del riesgo en la seguridad de la información.						
Identificación de los activos.						
Identificación de las amenazas.						
Identificación de los controles existentes.						
Identificación de las vulnerabilidades.						
Identificación de las consecuencias.						
Valoración de las consecuencias.						
Valoración de los incidentes.						
Nivel de estimación del riesgo.						
Evaluación del riesgo.						
Descripción General del tratamiento del riesgo.				Provee el caso de negocio para establecer los controles		
Reducción del riesgo.						
Retención del riesgo.						Provee la información como entrenamiento necesario, pruebas y documentación para retener el riesgo que se establece en el plan de mejora del servicio
Evitación del riesgo.						
Transferencia del riesgo.						
Aceptación del riesgo en la seguridad de la información.						
Comunicación de los riesgos de la seguridad de la información.		Provee reportes con un análisis del rendimiento de los servicios, considerando eventos e información relevante para identificar y adquirir nuevos conocimientos en seguridad de la información				
Monitoreo y revisión de los factores de riesgo.			Provee el marco de referencia o procedimiento para el monitoreo de los servicios de TI, considerando criterios de disponibilidad, SLA, priorización, seguridad y responsables. Adicionalmente recopila la información de la gestión de incidencias, problemas, continuidad y disponibilidad del servicio.			
Monitoreo, revisión y mejora de la gestión del riesgo.						

Tabla 2.4 Mapeo primer nivel
(Elaborado por: Los Autores)

2.1.3.2 Segunda fase

La segunda fase, agrupa los elementos comunes de ITIL V3 y NTE INEN-ISO/IEC 27005:2008 en una matriz que integra la codificación de los procesos de ITIL V3. El esquema de esta fase se muestra a continuación.

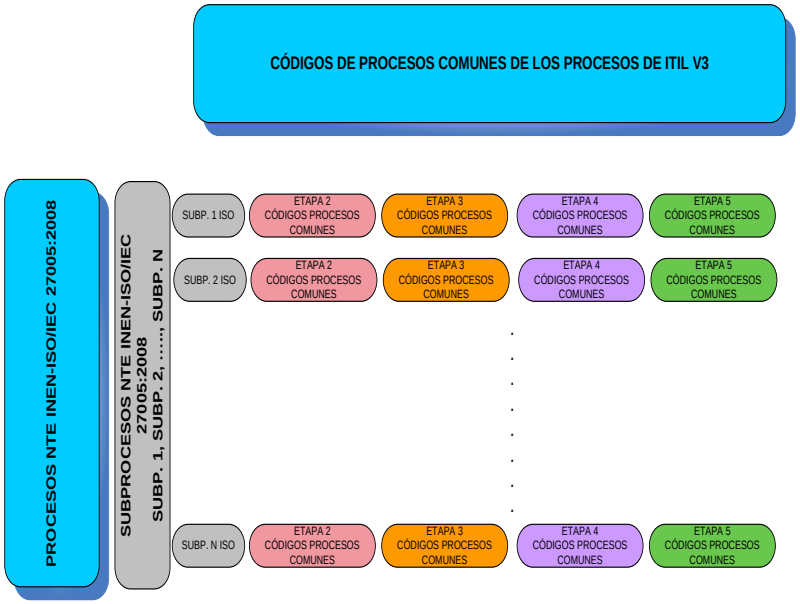


Figura 2.5 Segundo nivel de construcción del modelo M_OPTIMIZA (Elaborado por: Los Autores)

Como resultado se obtiene, se realiza una codificación general y se sistematiza los procesos de ITIL en función de los procesos de la ISO/IEC 27005

Procesos de la gestión de riesgo de la seguridad de la información	**Procesos de ITIL relacionados**					
Consideraciones Generales	D.01	D.03	D.06	O.05	MC.02	MC.04
Descripción General de la Valoración del riesgo en la seguridad de la información.	T.04					
Identificación de los activos.	D.01	T.03	O.05			
Identificación de las amenazas.	T.05	O.01	O.02			
Identificación de los controles existentes.	D.01	O.01	O.05			
Identificación de las vulnerabilidades.	O.03					
Identificación de las consecuencias.	O.04					
Valoración de las consecuencias.	T.02	O.01	O.02			
Valoración de los incidentes.	O.02	O.04				
Nivel de estimación del riesgo.	O.02	O.04				
Evaluación del riesgo.	D.04					
Descripción General del tratamiento del riesgo.	T.01	T.05	MC.03			
Reducción del riesgo.	D.04	D.07	O.02	O.03	O.04	O.05
Retención del riesgo.	O.02	O.03	O.04	O.05	MC.05	

Evitación del riesgo.	O.02	O.03	O.04	O.05		
Transferencia del riesgo.	D.07	O.02	O.03	O.04	O.05	
Aceptación del riesgo en la seguridad de la información.	T.02	T.06	T.07			
Comunicación de los riesgos de la seguridad de la información.	MC.01					
Monitoreo y revisión de los factores de riesgo.	MC.02					
Monitoreo, revisión y mejora de la gestión del riesgo.	D.02	D.05	MC.01			

Tabla 2.5 Mapeo nivel 2
(Elaborado por: Los Autores)

2.1.3.3 Tercera fase

Esta es la fase final del modelo M_OPTIMIZA, en la que se consolidan los procesos, subprocesos y códigos del estándar NTE INEN-ISO/IEC 27005:2008, con los procesos de ITIL V3 definidos en la fase anterior.

Con la visión completa de los elementos comunes, se definen los nuevos procesos que conformarán M_OPTIMIZA.

Los procesos son agrupados, dependiendo de las variables comunes que permitan generar indicadores. De esta manera se crean nuevos códigos y nombres en función de la base sobre la que mapearon anteriormente. El esquema final se muestra a continuación.

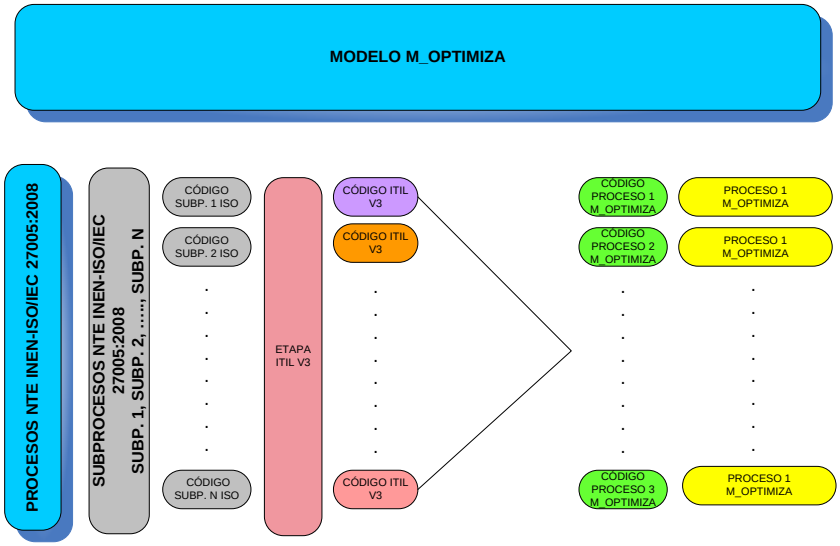


Figura 2.6 Tercera fase del modelo M_OPTIMIZA
(Elaborado por: Los Autores)

Procesos ISO/IEC 27005	Código ISO 27005	Nombre de proceso ITIL	Código ITIL	Códigos fase 3	Procesos M_OPTIMIZA
Consideraciones Generales	A.01	Gestión del Catálogo del Servicio	D.01	P01_M_OPTIMIZA	*Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios*
	A.01	Gestión de la Capacidad	D.03		
	A.01	Gestión de la Seguridad de la Información	D.06		
	A.01	Gestión de accesos	O.05		
	A.01	Medida del servicio	MC.02		
	A.01	Preguntas del negocio para la mejora continua	MC.04		
Descripción General de la Valoración del riesgo en la seguridad de la información	B.01	Gestión de liberación y despliegue	T.04	P02_M_OPTIMIZA	*Definición de los activos por catálogo de servicios y accesos definidos*
Identificación de los activos	B.02	Gestión del Catálogo del Servicio	D.01		
	B.02	Gestión y configuración de activos	T.03		
	B.02	Gestión de accesos	O.05		
Identificación de las amenazas	B.03	Validación y pruebas del servicio	T.05	P03_M_OPTIMIZA	*Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios*
	B.03	Gestión de eventos	O.01		
	B.03	Gestión de incidentes	O.02		
Identificación de los controles existentes	B.04	Gestión del Catálogo del Servicio	D.01		
	B.04	Gestión de eventos	O.01		
	B.04	Gestión de accesos	O.05		
Identificación de las vulnerabilidades	B.05	Solicitud de requerimientos	O.03	P04_M_OPTIMIZA	*Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas*
Identificación de las consecuencias	B.06	Gestión de problemas	O.04		
Valoración de las consecuencias	B.07	Gestión del cambio	T.02		
	B.07	Gestión de eventos	O.01		
	B.07	Gestión de incidentes	O.02		
Valoración de los incidentes	B.08	Gestión de incidentes	O.02		
	B.08	Gestión de problemas	O.04		
Nivel de estimación del riesgo	B.09	Gestión de incidentes	O.02	P05_M_OPTIMIZA	*Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad*
	B.09	Gestión de problemas	O.04		
Evaluación del riesgo	B.10	Gestión de la Disponibilidad	D.04		
Descripción General del tratamiento del riesgo	C.01	Planificación y soporte de la transición	T.01	P06_M_OPTIMIZA	*Reducción del riesgo basado en la gestión de servicios*
	C.01	Validación y pruebas del servicio	T.05		
	C.01	Retorno de la inversión de la mejora continua	MC.03		
Reducción del riesgo	C.02	Gestión de la Disponibilidad	D.04		
	C.02	Gestión de Proveedores	D.07		
	C.02	Gestión de incidentes	O.02		
	C.02	Solicitud de requerimientos	O.03		
	C.02	Gestión de problemas	O.04		
	C.02	Gestión de accesos	O.05		
Retención del riesgo	C.03	Gestión de incidentes	O.02	P07_M_OPTIMIZA	*Retención del riesgo basado en la gestión de servicios*
	C.03	Solicitud de requerimientos	O.03		
	C.03	Gestión de problemas	O.04		
	C.03	Gestión de accesos	O.05		
	C.03	Gestión del Nivel del Servicio	MC.05		
Evitación del riesgo	C.04	Gestión de incidentes	O.02	P08_M_OPTIMIZA	*Evitación del riesgo basado en la gestión de servicios*
	C.04	Solicitud de requerimientos	O.03		
	C.04	Gestión de problemas	O.04		
	C.04	Gestión de accesos	O.05		
Transferencia del riesgo	C.05	Gestión de Proveedores	D.07	P09_M_OPTIMIZA	*Transferencia del riesgo basado en la gestión de servicios*
	C.05	Gestión de incidentes	O.02		
	C.05	Solicitud de requerimientos	O.03		
	C.05	Gestión de problemas	O.04		
	C.05	Gestión de accesos	O.05		
Aceptación del riesgo en la seguridad de la información	DR.01	Gestión del cambio	T.02	P10_M_OPTIMIZA	*Aceptación del riesgo basado en la transición del servicio*
	DR.01	Evaluación	T.06		
	DR.01	Gestión del conocimiento	T.07		
Comunicación de los riesgos de la seguridad de la información	E.01	Servicio de reporte	MC.01	P11_M_OPTIMIZA	*Comunicación y monitoreo del riesgo en base a la gestión del servicio*
Monitoreo y revisión de los factores de riesgo	F.01	Medida del servicio	MC.02		
	F.01	Gestión del Nivel del Servicio	D.02		
Monitoreo, revisión y mejora de la gestión del riesgo	F.02	Gestión de la Continuidad del Servicio de TI	D.05		

Tabla 2.6 Mapeo tercer nivel
(Elaborado Por: Los Autores)

La tabla anterior expone el mapeo nivel 3, detallando las agrupaciones respectivas para formar los 11 procesos del modelo M_OPTIMIZA.

De esta forma se tiene como resultado de la construcción del modeló los siguientes procesos, que permiten optimizar los Servicios de Tecnologías de la Información, considerando aspectos relevantes de ITIL v3 e NTE ISO/IEC 27005 (Gestión de Riesgos en la Seguridad de la Información).

Figura 2.7 Procesos del modelo M_OPTIMIZA
(Elaborado por: Los Autores)

2.2PRESENTACIÓN DEL MODELO

Para la presentación del modelo M_OPTIMIZA, se utilizará un documento desprendible, que es una adaptación del estándar IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications, el cual puede ser usado de forma independiente para el análisis y mejora de los procesos de la Organización.

M_OPTIMIZA
OPTIMIZACIÓN DE SERVICIOS DE TI

MODELO DE GESTIÓN DE TI COMBINADO M_OPTIMIZA

ISO/IEC 27005 e ITIL v3

Autores:
Sandra Paulina Paredes Ulloa
Luis Roberto Tasintuña Condoy

2013
Quito - Ecuador

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Conscientes de que las tecnologías de la información y comunicación, actualmente son un factor crítico para la innovación y modernización de los procesos de las empresas, el presente modelo impulsa el aprovechamiento de las Tecnologías de la Información (TI) mediante el manejo adecuado de la información, de tal forma que se convierta en un agente de cambio para facilitar la transformación de la organización o negocio.

Los servicios de TI proveen los activos de soporte (hardware y software) para la operación de procesos importantes del negocio. Sin embargo, los recursos de TI a menudo se pasan por alto o se gestionan superficialmente dentro de muchas organizaciones.

La construcción del modelo es una combinación entre el marco de referencia de gestión de servicio ITIL v3 y la norma de gestión del riesgo de la seguridad de la información ISO/IEC 27005, permitiendo gestionar el riesgo de la información en base al ciclo de vida de los servicios.

1.1 PROPÓSITO

El modelo es una herramienta de gestión, que proporciona una guía de implementación y mecanismos de medición relacionados con el ciclo de vida del servicio y gestión del riesgo de la seguridad de la información.

Las organizaciones deben gestionar los riesgos a los que están expuestos sus activos para alcanzar sus objetivos. El modelo de gestión M_OPTIMIZA, establece los procesos, actividades, roles y responsabilidades para identificar, tratar, monitorear y comunicar los riesgos de TI, considerando el ciclo de vida de los servicios.

Los indicadores planteados en el modelo, identifican las variables que se quieren medir en cada proceso, entregando información estratégica para la toma de decisiones a los usuarios y/o clientes, con el fin de mejorar la calidad de los servicios de TI.

Las organizaciones entienden la importancia de la gestión de los servicios y riesgos, y los beneficios proporcionados por las Tecnologías de la Información para controlarlos, de forma que:

- Se defina el contexto de la gestión del riesgo de la seguridad de la información en la organización.
- El ciclo de vida de los servicios de TI se alinee a la administración del riesgo.
- La satisfacción de los clientes y usuarios se incremente.
- Exista información de calidad para tomar decisiones con conocimiento de los riesgos.
- Se mida el desempeño de TI.
- Existan medios de comunicación acerca del riesgo a las partes interesadas del negocio.

1.2 AUDIENCIA OBJETIVO

El documento está dirigido para los directores y personal involucrado en la gestión del riesgo de la seguridad de la información y de servicios de TI, tales como:

Director de Informática (CIO): El CIO se asegura de llevar a cabo procesos de planificación estratégica para que los requisitos de información, sistemas de soporte y la infraestructura, estén alineado con los requisitos legislativos y los objetivos estratégicos. El CIO se encarga de la planificación, diseño, ejecución y monitoreo de los recursos de TI, para la entrega efectiva de servicios tecnológicos.

Gerente de Seguridad de la Información (CISO): El CISO es responsable de la gestión, diseño, evaluación, planificación de la gestión de la seguridad de la Información en la Organización.

Gerente General financiero (CFO): Responsables de la gestión y asignación de recursos financieros.

Director General de Riesgos (CRO): responsable de todos los riesgos de la Organización, incluido el riesgo de la seguridad de la información.

Coordinadores/supervisores de TI: son responsables de supervisar la operación de los componentes y sistemas tecnológicos.

Oficial de Seguridad (OSI): forman parte de la implementación y mantenimiento de la gestión de la seguridad de la información.

1.3 ALCANCE

El modelo se puede aplicar a organizaciones de cualquier tamaño y en todo tipo de industria, que tengan implementado su modelo de gestión de servicios de TI en base a ITIL y que busquen gestionar los riesgos de seguridad de la información.

El Modelo de Gestión M_OPTIMIZA, proporciona formularios para determinar el estado actual de las unidades de Tecnologías de la Información y Comunicación, independientemente de su estructura y tecnología implementada, obteniendo una línea base que permita mejorar los resultados con la aplicación de los procesos generados en el modelo.

1.3.1 GESTIÓN DE SERVICIOS DE TI

ITIL es un marco de referencia que describe las mejores prácticas en la gestión del servicio de TI, considerando la mejora continua para entregar servicios de calidad tanto para el negocio como para los clientes.

Las fases del ciclo de vida de servicios, está reflejado en cinco libros, desde la definición inicial y análisis de requerimientos de negocio en la Estrategia de Servicio y Diseño de Servicio, continuando a una migración a un ambiente de producción en la Transición de Servicio, a una operación y mejora en la Operación del Servicio y Mejora Continua del Servicio. Estas fases están descritas en la figura 1.

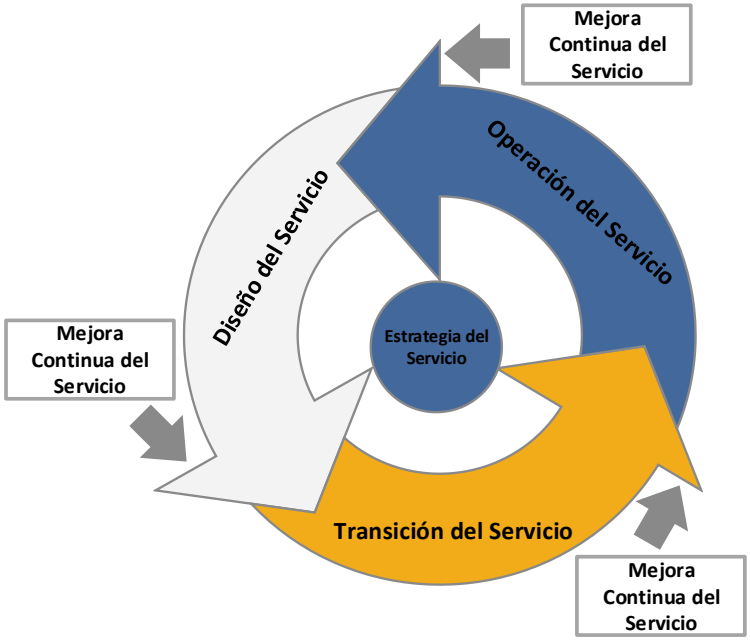


Figura 8. Ciclo de vida del servicio
(Libros de ITIL v3, 2007)

Es importante indicar que los servicios y actividades relacionadas, deben ser alineados a los requerimientos y necesidades del negocio.

1.3.2 GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN (ISO 27005)

Es un estándar que proporciona lineamientos, directrices y descripción de los procesos para la gestión del riesgo en la seguridad de la información, complementando los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI).

Este estándar fue desarrollado con el fin de ayudar en la implementación exitosa de la seguridad de la información desde un enfoque de gestión de riesgos. Adicionalmente no describe ni sugiere un método en específico para el análisis del riesgo, pero si especifica una estructura sistemática y procesos para analizar el riesgo, con el fin de obtener el plan de tratamiento del riesgo, siendo aplicable a cualquier tipo de organización como: empresas comerciales, organismos gubernamentales, organismos sin fines de lucros, entidades financieras, entre otras.

La Figura 9. P, muestra el proceso de la gestión del riesgo en la seguridad de la información definida en la ISO/IEC 27005.

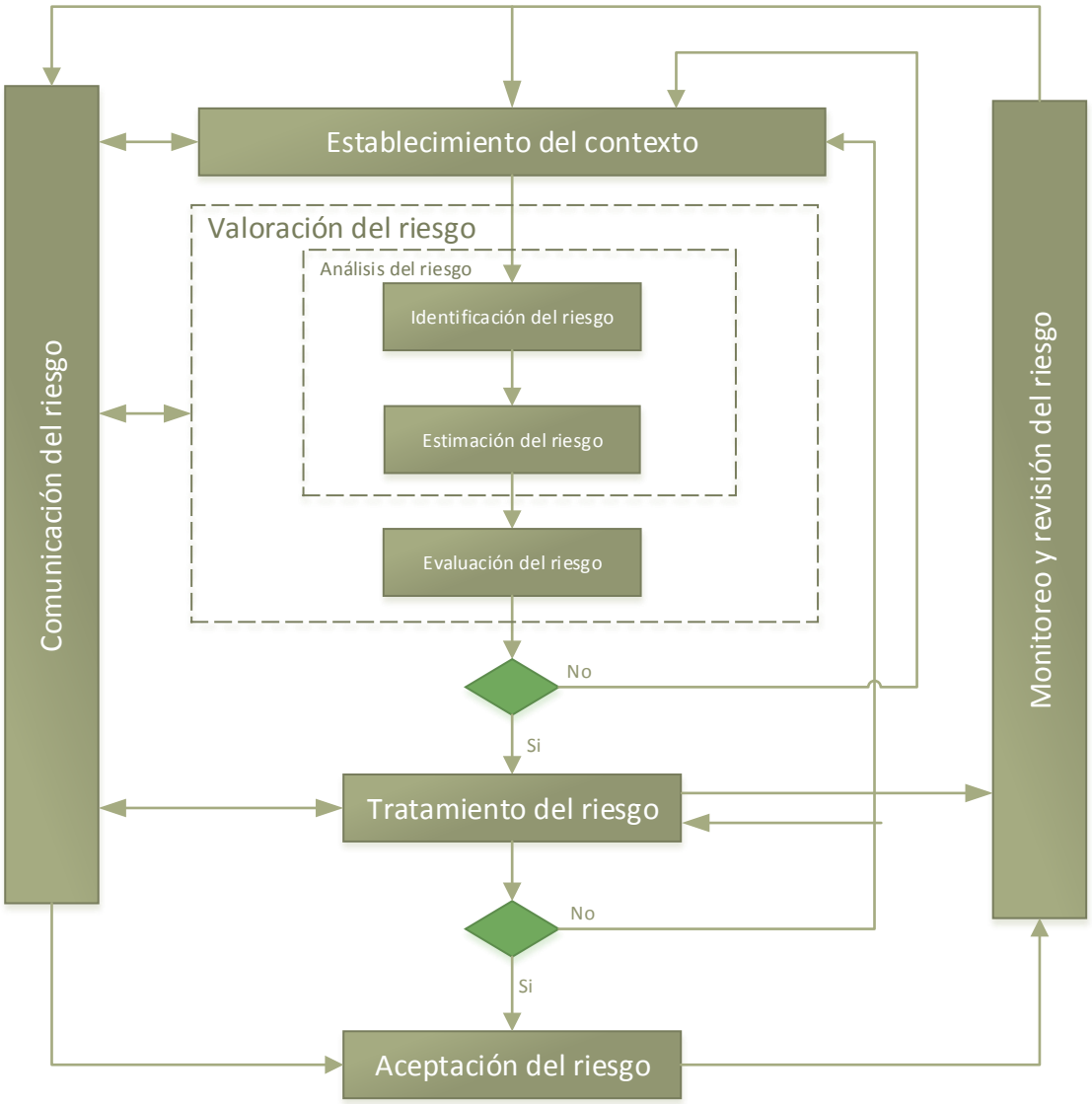


Figura 9. Proceso de gestión del riesgo en la seguridad de la información
(Norma técnica NTE ISO/IEC 27005:2008, 2012)

Este proceso, establece como primer paso el contexto, en el cual se definirá un enfoque y alcance en base a los requerimientos del negocio, factores internos (tecnología, recurso económico, etc.) y externos (sociales, legales, etc.) que inciden en los criterios para la gestión del riesgo. Posteriormente se identifica el riesgo, llevando a cabo una metodología para valorar los riesgos, identificando vulnerabilidades y amenazas, además de los controles existentes y

consecuencias potenciales, obteniendo una priorización para el tratamiento del riesgo clasificados de acuerdo a los criterios establecidos en el contexto.

Si la valoración del riesgo es aceptable se procede con el tratamiento del riesgo a través de controles para reducir, retener, evitar o transferir el riesgo, sustentados y apoyados en el Plan de Tratamiento del Riesgo establecido, considerando las restricciones tales como: de tiempo, financieras, técnicas operativas, legales entre otras, durante su implementación.

Luego que se aceptan los riesgos y se ha dado una valoración y tratamiento, se puede tener riesgos residuales, siendo necesario hacer nuevamente un procedimiento de estimación y tratamiento adecuado.

La comunicación del riesgo se realiza en todo el proceso de gestión de riesgo para todos los involucrados e integrantes del mismo, al igual que el seguimiento, monitoreo y revisión continúa de todo el proceso.

1.3.3 MODELO DE GESTIÓN M_OPTIMIZA – ISO/IEC 27005 E ITIL V3

Actualmente la importancia de un efectivo enfoque en la gestión de la seguridad de la información en el negocio, hacen evidentes escenarios que pueden suceder en ausencia de su debido tratamiento, considerando que los controles implementados dentro del alcance de los límites y el contexto del sistema de seguridad, se deben basar en el riesgo.

Por ende M_OPTIMIZA, permite optimizar los servicios de tecnologías de la información considerando la gestión del riesgo asociados a los activos de TI, detallando elementos, actividades, procesos e indicadores para la creación de un modelo de gestión eficiente y una implementación exitosa.

1.3.4 ESTRUCTURA DEL MODELO

El modelo de gestión M_OPTIMIZA está divido en 5 fases de acuerdo a la gestión de riesgo, de los cuales se realiza una agrupación con los procesos de gestión de servicios de TI, dando como resultado 11 procesos.

Fase 1. Establecimiento del Contexto basado en la Gestión del Servicio.- El objetivo es establecer los criterios básicos, alcance y límites, y organización de la

gestión del riesgo en la seguridad de la información, haciendo uso de las definiciones y actividades descritas en el proceso de ITIL: Diseño del Servicio, Gestión de la Seguridad de la Información y Mejora Continua.

Fase 2. Valoración del Riesgo basado en la Gestión del Servicio.- Se obtienen cuatro procesos basados en el Diseño, Transición y Operación del Servicios que permiten contar con una lista de riesgos valorados, con prioridad en base a los criterios de evaluación del riesgo.

Fase 3. Tratamiento del Riesgo basado en la Gestión del Servicio.- A través de la Gestión del Servicio se cuenta con información y actividades claras para seleccionar controles para reducir, retener, evitar o transferir los riesgos, todo esto definido en un plan de tratamiento de riesgo. Se establecen cuatro procesos en cada uno de ellos se emplea mecanismos para tratar el riesgo a través de las guías de implementación.

Fase 4. Aceptación del riesgo basado en la Gestión del Servicio.-Posterior a los servicios definidos en la fase de Diseño del Servicio, es necesario garantizar su correcto despliegue en los ambientes de producción, de tal forma que cumplan los requerimientos de calidad, soporte debido y se minimice el riesgo en controles de cambios solicitados. Por tanto, en base a la Transición del Servicio se obtiene una lista de riesgos que se aceptan y aquellos que no satisfacen los criterios de aceptación del riesgo de la organización.

Fase 5. Comunicación, Monitoreo y Revisión del riesgo basado en la Gestión del Servicio.- Las fases de comunicación y, monitoreo y revisión, para todo el proceso de gestión de riesgo en la seguridad de la información es necesaria para que la información relacionada con el riesgo se intercambie y/o compartir con las personas involucradas. De igual forma es importante monitorear que el control e implementación de los procesos se encuentren alineados a los intereses del negocio, considerando la mejora continua del proceso. Para cumplir con estas actividades se hace uso de procesos de las fases de mejora continua y diseño de gestión del servicio.

Para la aplicación del modelo M_OPTIMIZA utiliza formularios para obtener una fotografía de los procesos implementados. Posteriormente a través de la adopción

de las guías de implementación de los procesos de M_OPTIMIZA proporciona los medios para llegar alcanzar los niveles de gestión esperados. Resultados que son contrastados con una nueva aplicación de los formularios para determina el “to be” de las organizaciones.

Como parte complementaria, para cada proceso de M_OPTIMIZA, se dispone de indicadores que proporcionan información para realizar cambios en las unidades de gestión y buscar oportunidades de mejoramiento.

La siguiente figura muestra los 11 procesos que forman parte del modelo de gestión combinado M_OPTIMIZA.

Figura 10. Procesos de M_OPTIMIZA
(Elaborado por: Los Autores)

1.4 DEFINICIONES, ABREVIATURAS

1.4.1 DEFINICIONES

Término	Definición
ITIL	Es un marco de referencia y define un conjunto de buenas prácticas en la gestión del servicio.
ISO/IEC 27005	Es una norma que proporciona directrices generales para la gestión del riesgo en la seguridad de la información.
*Impacto**	Cambio adverso en el nivel de los objetivos del negocio.
*Evitación del riesgo**	Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
*Riesgo en la seguridad de la información**	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos.
*Estimación del riesgo**	Procesos para asignar valores a la probabilidad y las consecuencias de un riesgo.
*Identificación del riesgo**	Proceso para encontrar, enumerar y caracterizar los elementos del riesgo.
*Reducción del riesgo**	Acciones que se toma para disminuir la probabilidad de las consecuencias negativas asociadas a un riesgo.
*Retención del riesgo**	Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
*Transferencia del riesgo**	Compartir con otras partes la pérdida o la ganancia de un riesgo.
Business Impact Analysis	Una actividad en la gestión de continuidad del negocio que identifica las funciones vitales del negocio y sus dependencias.
Unidad de Negocio	Un segmento del negocio que tiene sus propios planes, métricas, los ingresos y los gastos. Cada unidad de negocio tiene activos y las utiliza para crear valor para los clientes en forma de bienes y servicios.
Capacidad	El máximo rendimiento que un elemento de configuración o servicio puede ofrecer.
Elemento de Configuración (CI)	Cualquier componente u otro activo de servicio que necesita ser manejado con el fin de ofrecer un servicio de TI.
Servicio de usuario final	Por lo general apoyan los procesos de negocio y facilitan uno o más resultados deseados por el cliente.
El tiempo de inactividad	El momento en que un servicio de TI u otro elemento de configuración no están disponibles durante su tiempo de servicio acordado.
Impacto	Medida del efecto de un incidente, problema o cambio en los procesos de negocio.
Prioridad	Una categoría utilizada para identificar la importancia relativa de algo.
Proceso	Un conjunto estructurado de actividades diseñadas para lograr un objetivo específico.
Solicitud de Cambio (RFC)	Propuesta formal para un cambio que se hizo.
Rol	Un conjunto de responsabilidades, actividades y autoridades asignadas a una persona o equipo.
Catálogo de Servicios	Una base de datos o documento estructurado con información sobre todo el ciclo de vida de los servicios de TI, incluyendo los que están disponibles para su despliegue. El catálogo de servicios es parte del portafolio servicios y contiene información sobre dos tipos de servicios de TI: de usuario final (los servicios que son visibles para el negocio), y servicios de apoyo que son requeridos por el proveedor de servicios para ofrecer servicios de cara al cliente o usuario final.
Contrato de servicio	Contrato para entregar uno o más servicios de TI.
Horario de servicio	Plazo acordado cuando un servicio TI en particular debe estar disponible.

Acuerdo de Nivel de Servicio (SLA)	Un acuerdo entre un proveedor de servicios de TI y un cliente. Un acuerdo de nivel de servicio se describe el servicio, objetivos y especifica las responsabilidades del proveedor de servicios de TI y el cliente. Un solo acuerdo puede abarcar múltiples servicios de TI o varios clientes.
Dueño del servicio	Responsable de la gestión de uno o más servicios en todo su ciclo de vida.
Servicio de soporte	Un servicio de TI que no se utiliza directamente por la empresa, pero que requiere el proveedor de servicios de TI para ofrecer servicios de cara al cliente, pueden incluir servicios de TI sólo utilizados por el proveedor de servicios de TI.

Tabla 7. Definiciones
(Norma técnica NTE SO/IEC 27005, 2012)

1.4.2 ABREVIATURAS

ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
SLA	Service level agreement
TI	Tecnologías de Información

1.5 REFERENCIAS

Referencias normativas

- NTC - ISO/IEC 27005, Tecnologías de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.

Publicaciones

- Publicaciones de ITIL: Service Strategy, Service Design, Service Transition, Service Operation, Continua Service Improvement

Internet

- http://wiki.es.it-processmaps.com/index.php/Portada Wiki de ITIL

- http://itilv3.osiatis.es/ Curso en línea de ITIL

2. DESCRIPCIÓN DEL MODELO

2.1 ESTRUCTURA DE LOS PROCESOS

Las fichas técnicas de los procesos contienen la guía para implementarlos dentro de la organización, estructurados con los siguientes campos

NOMBRE DEL PROCESO **CÓDIGO DEL PROCESO**

DESCRIPCIÓN DEL PROCESO

La descripción del proceso indica su contenido y las actividades que desarrolla para su implementación, así como su finalidad, el detalle de los elementos base que utilizan en su desarrollo y que forman parte del proceso, y finalmente cómo se desarrolla el mismo.

Si el proceso tiene fases, se expone de manera general cada una en el orden de las operaciones que se ejecutan.

Valor para el negocio

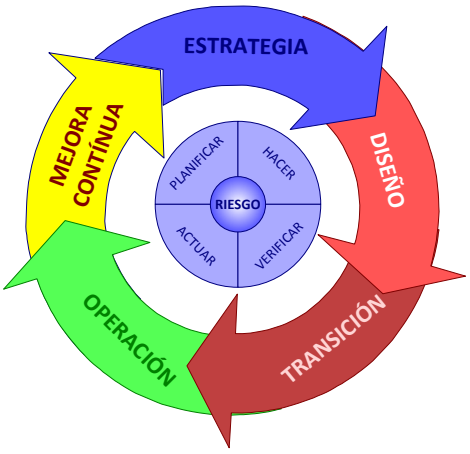


Figura 11. Ciclo M_OPTIMIZA

(Elaborado por: Los Autores)

La implantación de cualquier proceso en función de las etapas del ciclo de vida de los servicios, debe tener como objetivo principal el de ayudar a la parte de negocio a conseguir sus objetivos.

El valor para el negocio explica cómo el proceso ayuda a cumplir la misión de la organización, cómo este proceso aporta valor agregado a las operaciones.

DIRECTRICES GENERALES

Proceso

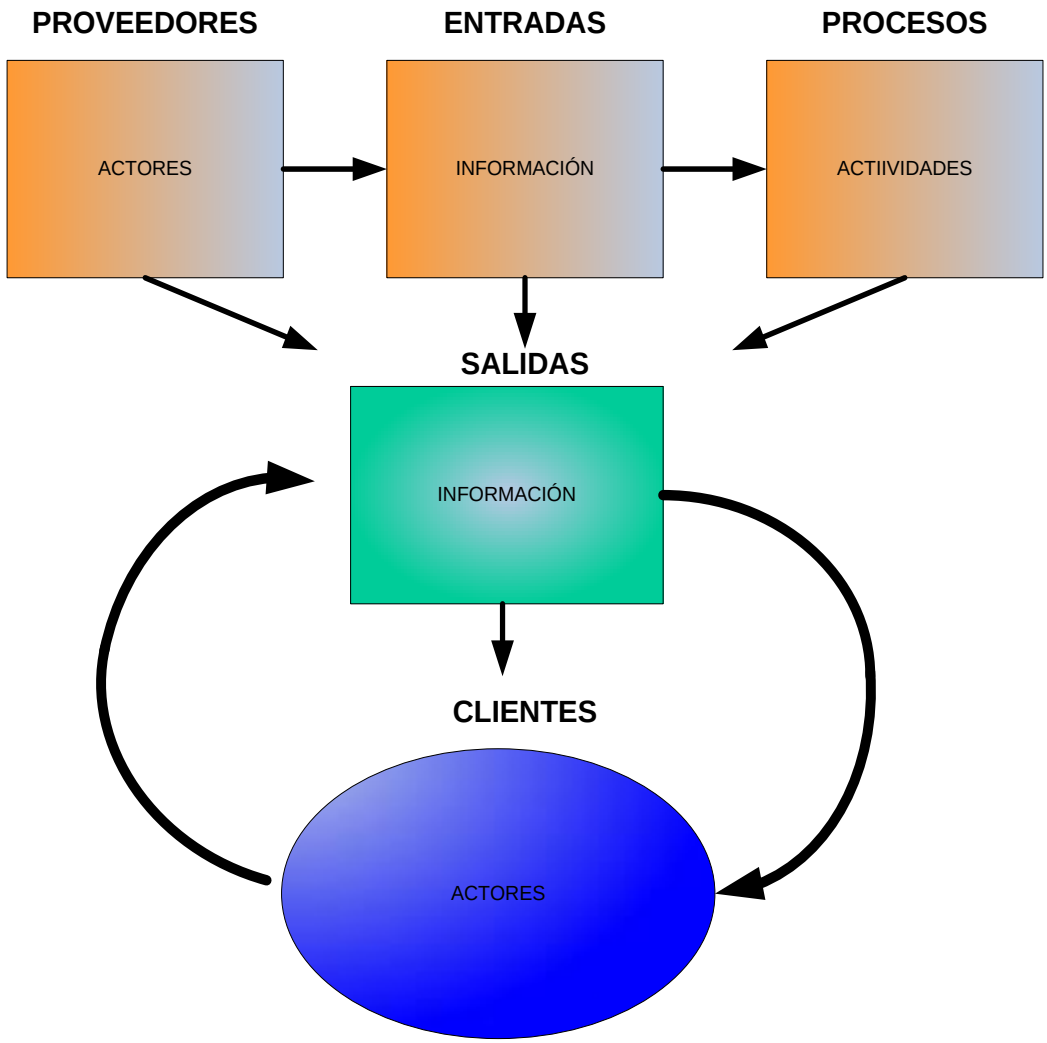


Figura 12. Proceso
(Elaborado por: Los Autores)

En las directrices generales se detalla en forma gráfica los proveedores del proceso (internos o externos), la información que se requiere para realizar las actividades, el listado de actividades que transformarán las entradas en resultados, los resultados que se obtiene una vez que se aplica el proceso y los actores que consumen esta información.

Guía de Implementación

La guía de implementación contiene la información para aplicar el proceso. La misma se compone de varios pasos en función de las actividades que se deben realizar, el momento y responsables de cada una, y el detalle a nivel de las tareas que se ejecutarán.

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1	A través de un correo		
PASO 2			
PASO 3			
PASO 4			

Tabla 8. Guía de implementación
(Elaborado por: Los Autores)

Indicadores

Los indicadores expresan en a través de fórmulas matemáticas lo que se espera medir para evaluar los procesos. De esta forma, se presentan con su método de cálculo y la unidad de medición.

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN

Tabla 9. Presentación de indicadores
(Elaborado por: Los Autores)

Escala de Evaluación

La escala de evaluación permitirá medir el nivel de implementación del proceso en la organización, de manera que se pueda mejorar hasta que se encuentre totalmente gestionado.

Para esto, se definieron tres niveles con la siguiente descripción:

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

Tabla 10. Escala de evaluación
(Elaborado por: Los Autores)

En síntesis, el modelo M_OPTIMIZA, propone para la optimización de los servicios de TI, 11 procesos agrupados en 5 fases, desarrollando fichas técnicas para cada uno de ellos con la siguiente estructura:

- Descripción del proceso.
- Etapas de ITIL relacionadas.
- Valor para el negocio.
- Directrices generales.
- Guía de implementación.
- Indicadores.
- Escala de evaluación.

Adicionalmente, se describe una serie de actividades y formularios para aplicar de manera práctica el modelo, de tal forma que en primera instancia se identifique el estado actual en el cual se encuentra la organización a través de la utilización de formularios. Obtenida la línea base se procede a la implementación de los

procesos de M_OPTIMIZA de acuerdo a las “guías de Implementación “para cada uno de ellos.

Finalmente, el control y seguimiento se lo realiza a través de la gestión de indicadores que junto con el procedimiento de análisis e interpretación de resultados, hará posible tomar acciones proactivas para optimizar o corregir las actividades ejecutadas por los involucrados de los procesos de acuerdo a los requerimientos y lineamientos del negocio.

2.2 NOMENCLATURA

Cada uno de los procesos tiene asignada la nomenclatura, con su correspondiente formulario de aplicación, para una fácil y compresible implementación, de acuerdo al siguiente detalle:

Proceso M_OPTIMIZA	Código de proceso	Código de formulario
Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios	P01_M_OPTIMIZA	F01_M_OPTIMIZA
Definición de los activos por catálogo de servicios y accesos definidos	P02_M_OPTIMIZA	F02_M_OPTIMIZA
Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios	P03_M_OPTIMIZA	F03_M_OPTIMIZA
Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas	P04_M_OPTIMIZA	F04_M_OPTIMIZA
Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad	P05_M_OPTIMIZA	F05_M_OPTIMIZA
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P06_M_OPTIMIZA	F06_M_OPTIMIZA
Retención del riesgo basado en la gestión de servicios	P07_M_OPTIMIZA	F07_M_OPTIMIZA
Evitación del riesgo basado en la gestión de servicios	P08_M_OPTIMIZA	F08_M_OPTIMIZA
Transferencia del riesgo basado en la gestión de servicios	P09_M_OPTIMIZA	F09_M_OPTIMIZA
Aceptación del riesgo basado en la transición del servicio	P10_M_OPTIMIZA	F10_M_OPTIMIZA
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P11_M_OPTIMIZA	F11_M_OPTIMIZA

Tabla 11. Códigos de procesos y formularios de aplicación de M_OPTIMIZA
Realizado por. Los Autores

M_OPTIMIZA
OPTIMIZACIÓN DE SERVICIOS DE TI

MODELO DE GESTIÓN DE TI COMBINADO M_OPTIMIZA ISO/IEC 27005 e ITIL v3

2.3 PROCESOS

FORMULACIÓN DEL CONTEXTO BASADO EN EL DISEÑO, REQUISITOS DE SEGURIDADES DE LA INFORMACIÓN Y MEJORA CONTINUA DE SERVICIOS

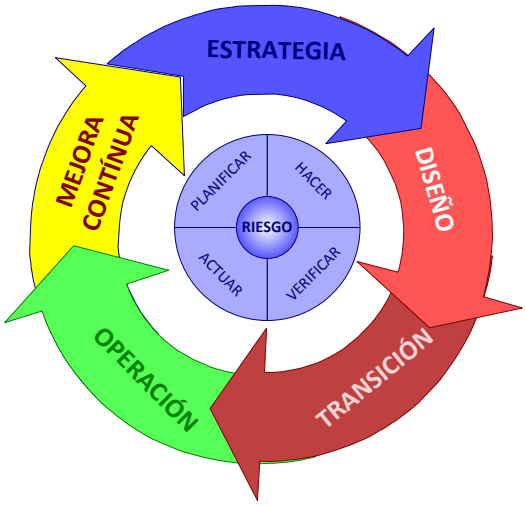
P01_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Este proceso contiene las consideraciones generales para establecer el contexto, además del alcance, los límites y la organización para operar el riesgo en Seguridades de la Información, a través de actividades diseñadas en etapas de ITIL como el diseño del servicio, la asignación adecuada de accesos a los activos y la medida y mejora continua que se espera obtener en el servicio.

ETAPAS DE ITIL RELACIONADAS	
Gestión del Catálogo del Servicios	Proporciona información sobre el estado y requerimientos de los servicios en operación y aquellos en transición para salir a producción.
Gestión de la Capacidad	Proporciona y mantiene un plan de la capacidad utilizada por los servicios y los eventos relacionados
Gestión de la Seguridades de la Información	Provee la Política de Seguridades de la Información
Gestión de Accesos	Provee los accesos autorizados a los activos de información
Medida del Servicio	Define las métricas que influyen en los criterios de impacto que se deben establecer
Preguntas del Negocio para la Mejora Continua	Proporciona las expectativas y percepciones de las partes involucradas

VALOR PARA EL NEGOCIO

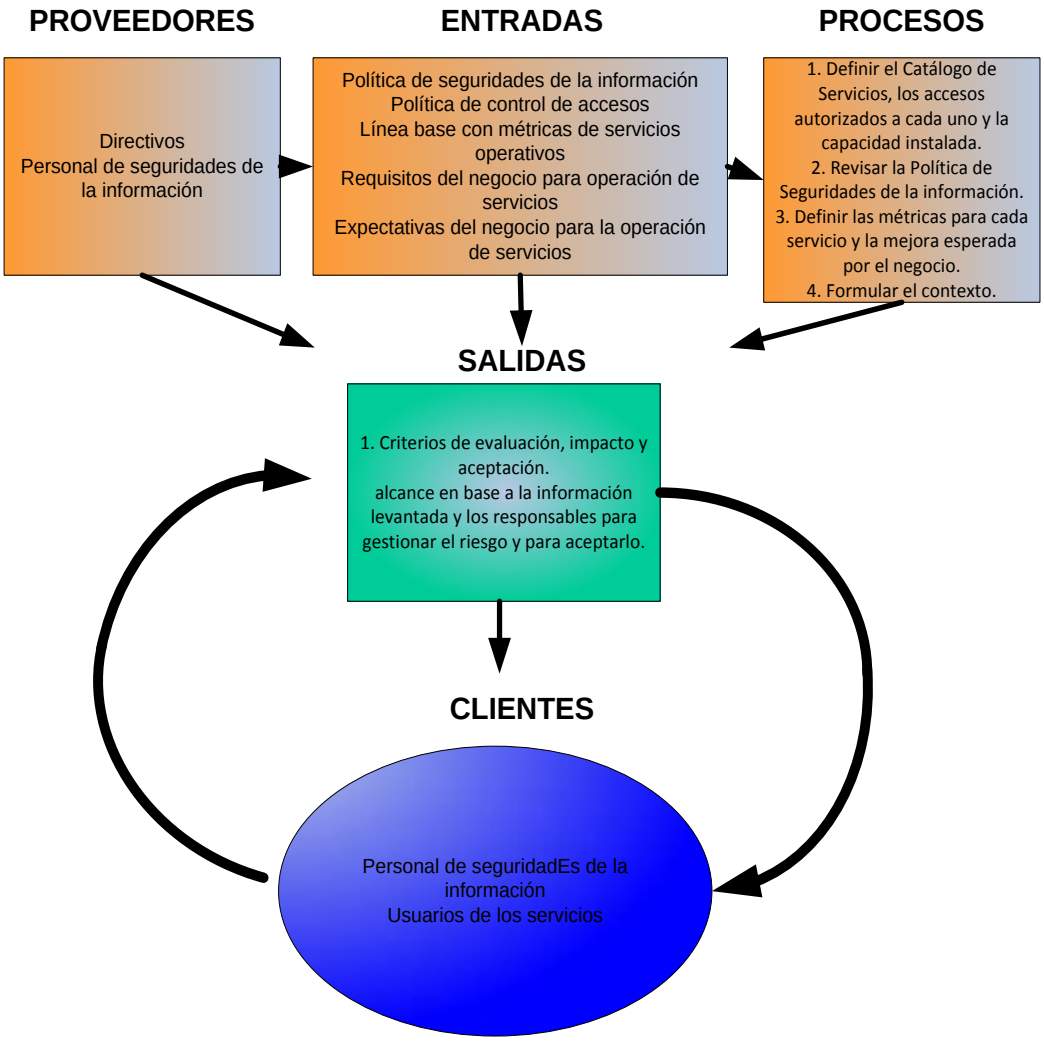


Define el contexto adecuado para gestionar el riesgo, tomando como insumo la información de servicios de tecnología en operación, controles existentes y las necesidades de la organización.

La formulación inicial identifica las condiciones internas reales y del entorno, así como las esperadas por el negocio.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Definir el Catálogo de Servicios, los accesos autorizados a cada uno y la capacidad instalada	A través del levantamiento de información, en caso que estas entradas no existan. Solicitudes de información a las áreas de tecnología y seguridad.	Personal de tecnología. Usuarios de los servicios. Otras partes implicadas (proveedores, instituciones, etc.).	Registro de los servicios operativos y en transición y de la documentación asociada a los mismos. Mantenimiento y actualización del Catálogo de Servicios. Entrega del plan de capacidad con el monitoreo de los recursos y su supervisión. Revisión de accesos a los servicios, que incluye la petición, verificación, registro, retirada y monitoreo.
PASO 2 Revisar la Política de Seguridades de la Información	Solicitud de la Política de Seguridades de la Información.	Personal de seguridades de la información.	Establecimiento o revisión de la Política de Seguridades de la Información. Revisión del plan de seguridad y de las medidas aplicadas. Evaluación del cumplimiento de las políticas.
PASO 3 Definir las métricas para cada servicio y la mejora esperada por el negocio	Encuestas y levantamiento de estado actual.	Personal de tecnología. Usuarios de los servicios. Otras partes implicadas (proveedores, instituciones, etc.). Áreas de auditoría y control.	Analizar a detalle la calidad y rendimiento de los servicios operativos. Detectar oportunidades de mejora. Proponer acciones correctivas. Supervisar su implementación.
PASO 4 Formular el contexto	Con toda la información levantada, documentada y revisada.	Personal de seguridades de la información.	Definir los criterios de evaluación, impacto y aceptación. Definir el alcance en base a la información levantada y los responsables para gestionar el riesgo y para aceptarlo.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de criterios de evaluación del riesgo aprobados	Número de criterios de evaluación propuestos/ Número de criterios aprobados	Porcentaje
Porcentaje de servicios cubiertos en el contexto	Número de servicios establecidos en el contexto/Número total de servicios del catalogo	Porcentaje

ESTADOS

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

DEFINICIÓN DE LOS ACTIVOS POR CATÁLOGO DE SERVICIOS Y ACCESOS DEFINIDOS

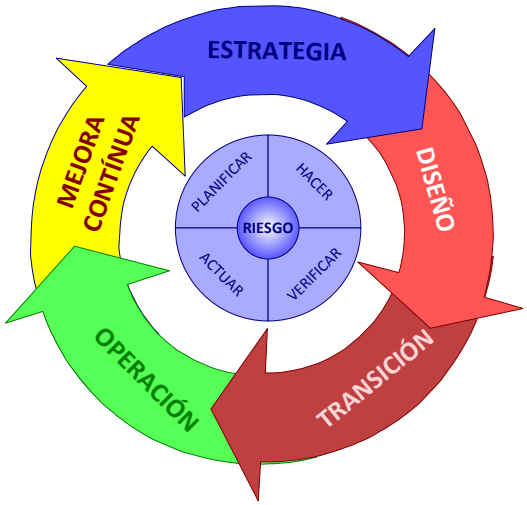
P02_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Este proceso se basa en que un activo es todo lo que tiene valor para la organización, generando de esta forma las actividades para establecer una lista de activos para valorar el riesgo, en función del catálogo de servicios, el control de calidad de todo el software y hardware instalado para los servicios en producción, la configuración de los activos involucrados en los servicios y sus accesos autorizados.

ETAPAS DE ITIL RELACIONADAS	
Gestión de Liberación y Despliegue	Proporciona las pruebas de control de calidad para todo el software y hardware instalado en el entorno de producción.
Gestión del Catálogo de Servicios	Suministra los servicios en producción o transición.
Gestión y Configuración de Activos	Proporciona el control de todos los elementos de tecnología que proporcionan un servicio, y la base de datos que gestiona esta información.
Gestión de Accesos	Proporciona los permisos de acceso autorizados para los usuarios de los servicios.

VALOR PARA EL NEGOCIO

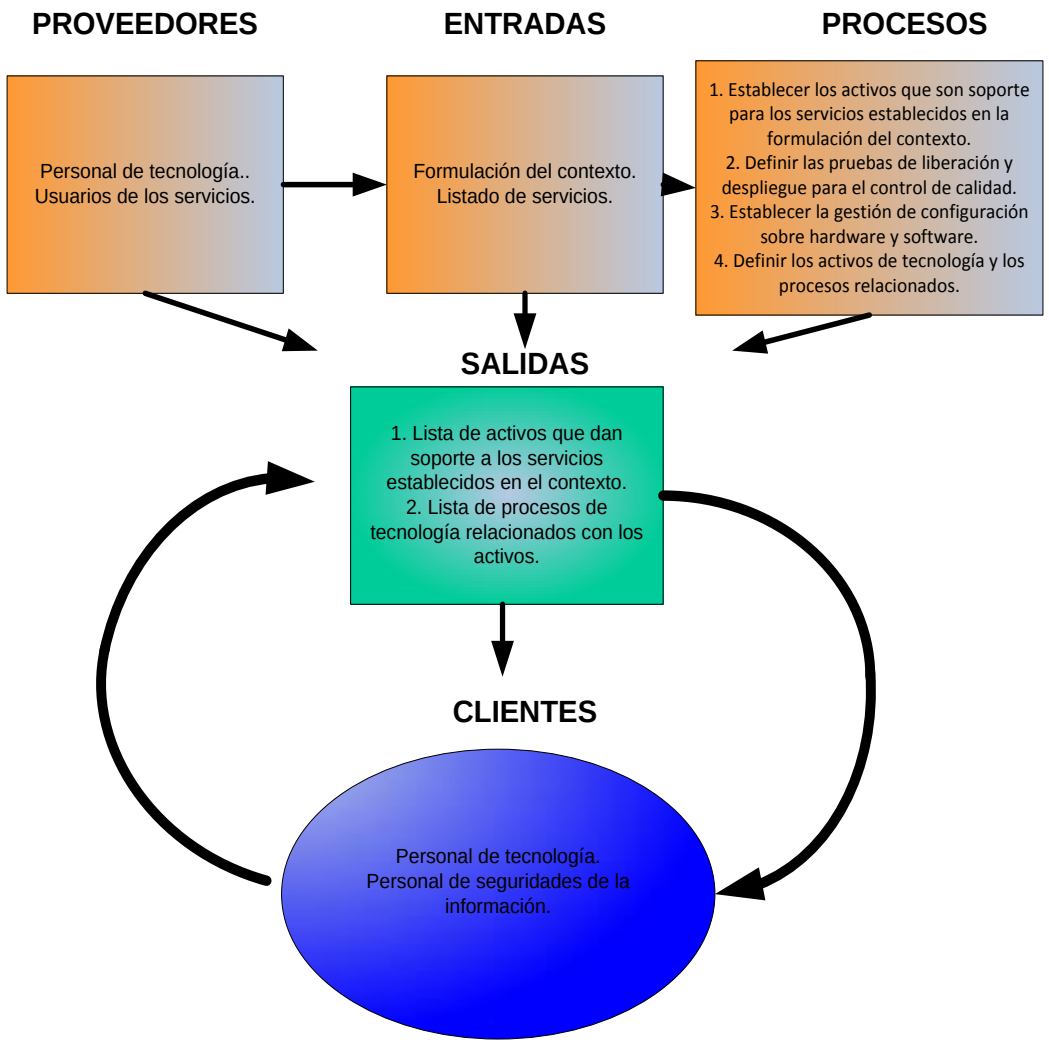


En el contexto se limita el alcance sobre el que se valorará el riesgo. Los activos están compuestos por el hardware, software, información y procesos de tecnologías de información que permiten brindar un servicio a la empresa.

La definición de activos basada en el catálogo de servicios, permite limitar las iteraciones con una lista de componentes de tecnología, sus propietarios, ubicación y funciones.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Establecer los activos que son soporte para los servicios establecidos en la formulación del contexto.	Luego de la formulación del contexto	Personal de tecnología. Personal de seguridades de la información.	Registro del hardware que sirve de soporte para los servicios operativos y en transición. Registrar el software utilizado por cada activo.
PASO 2 Definir las pruebas de liberación y despliegue para el control de calidad.	Una vez que se definen los activos se deben establecer las pruebas de hardware y software, a través de planes de control de calidad.	Responsables de tecnología.	Establecer una política de planificación para liberar nuevas versiones de software relacionadas con los activos. Desarrollar planes de roll-back en caso que las nuevas versiones en producción afecten la disponibilidad de los servicios. Actualizar la biblioteca de medios definitivos, los repuestos definitivos y la base de datos de gestión de configuraciones. Comunicar a los usuarios sobre las nuevas versiones de hardware y software liberadas y cómo se afecta los servicios.
PASO 3 Establecer la gestión de configuración sobre hardware y software.	Luego del control de calidad, a través de documentación generada por los responsables de los activos y aprobada por los propietarios.	Responsables de tecnología.	Definir las estrategias para gestionar los activos de tecnología y su configuración. Clasificar y registra los componentes de la CMDB. Monitorizar la CMDB. Auditar la CMDB para que la información ingresada coincida con la infraestructura instalada en la organización.
PASO 4 Definir los activos de tecnología y los procesos relacionados.	Una vez que se han identificado los activos, las condiciones de calidad y su registro en la CMDB.	Responsables de seguridades de la información.	Registrar los servicios y los activos que dan soporte a cada uno. Desarrollar el plan de calidad para los activos de hardware y software. Ingresar la información en la CMDB. Verificar la información ingresada en la CMDB. Obtener el listado de activos de hardware y software con los responsables. Mantener actualizada y monitoreada la CMDB.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de registro de activos	Número de activos registrados en la CMDB/Número total de activos	Porcentaje
Porcentaje de cumplimiento de pruebas de control de calidad	Número de activos que cumplen las pruebas de control de calidad/Número total de activos	Porcentaje
Cumplimiento de ítems ingresados en la CMDB	Número de ítems que registrados que han sido revisados	Número

ESTADOS

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

IDENTIFICACIÓN DE AMENAZAS BASADOS EN LAS PRUEBAS, EVENTOS E INCIDENTES DEL CATÁLOGO DE SERVICIOS

P03_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Una amenaza se define como la causa potencial de un incidente no deseado. Típicamente las amenazas dañan un sistema u organización.

Este proceso contiene los pasos para identifica las amenazas en base a varios insumos, de forma que su prevención sea efectiva. La validación y pruebas del servicio antes de salir a producción, la gestión de eventos e incidentes registrados en cada servicio, permiten definir con mayor claridad las amenazas, su tipo y origen.

ETAPAS DE ITIL RELACIONADAS	
Validación y Pruebas del Servicio	Garantiza que las nuevas versiones cumplen con los requisitos de calidad que incluyen los riesgos.
Gestión de Eventos	Proporciona todos los sucesos importantes de un servicio, entre los que están los eventos de operación normal, los eventos que indican una excepción y los eventos que indican operaciones inusuales y requieren un monitoreo exhaustivo.
Gestión de Incidentes	Facilita la información de los incidentes resueltos, que ayudan a identificar las amenazas que han sido materializadas.
Gestión del Catálogo de Servicios	Proporciona los controles implementados en los servicios en operación
Gestión de Accesos	Provee los controles de acceso para los activos

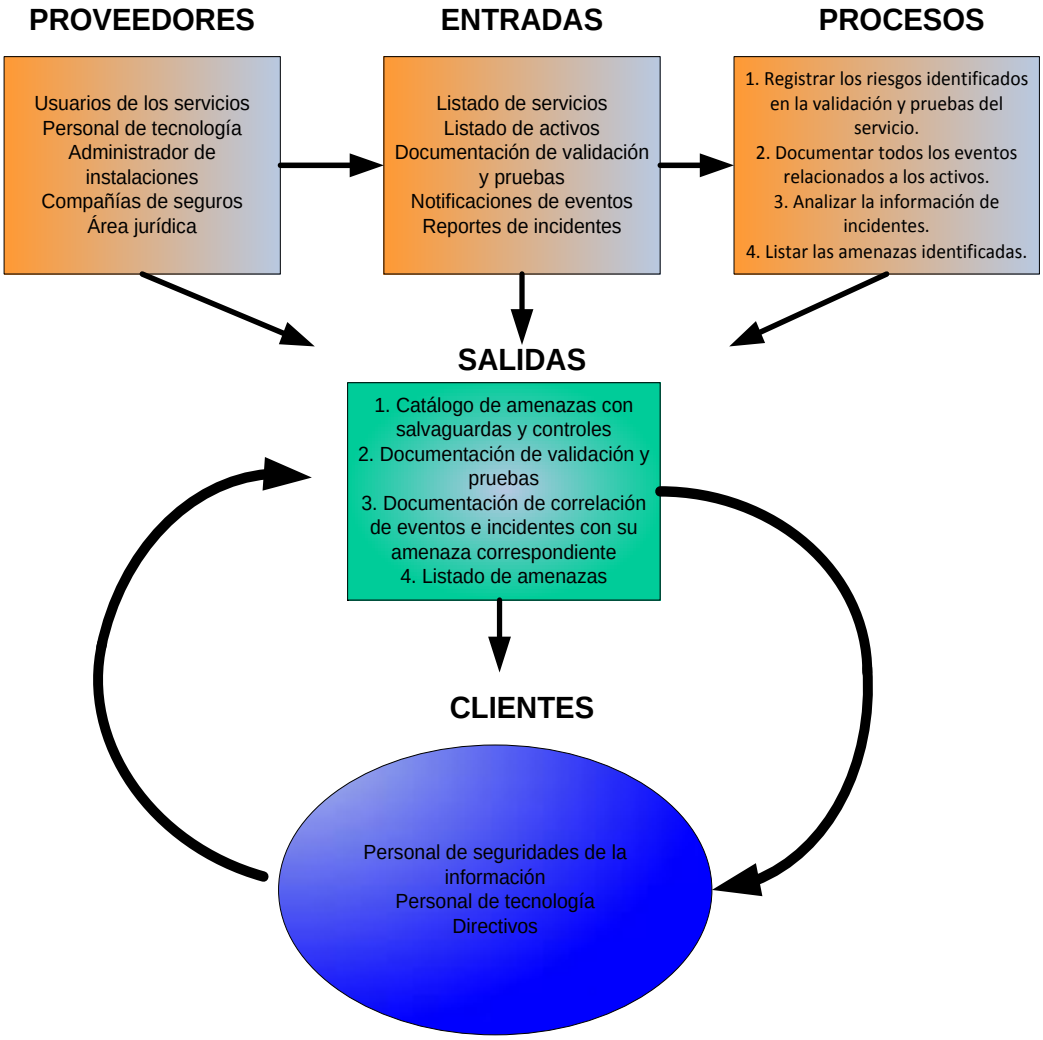
VALOR PARA EL NEGOCIO

Las amenazas pueden dañar activos de tecnología como hardware y software que son base de los servicios ofrecidos por la organización.

La identificación apropiada de amenazas ayuda a la definición eficiente de las consecuencias y los controles que se deben implementar.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Registrar los riesgos identificados en la validación y pruebas del servicio	Luego de identificar los activos involucrados en cada servicio	Personal de tecnología. Personal de seguridades de la información.	Revisar la documentación de validación y pruebas del servicio. Validar la presencia de los riesgos identificados en la validación para cada servicio.
PASO 2 Documentar todos los eventos relacionados a los activos	A través de los correos, alertas, notificaciones enviadas. Esta actividad se debe realizar luego de la validación y pruebas del servicio.	Usuarios de los servicios. Personal de tecnológica. Personal de seguridades de la información.	Implementar herramientas de detección, filtrado y notificación de eventos. Registrar los activos identificados en las herramientas de monitoreo. Clasificar los eventos de operación normal, operación excepcional y los de operación inusual. Listar los eventos de operación inusual por cada activo. Identificar y registrar las fechas, horas y solución dada a los eventos de operación inusual.
PASO 3 Analizar la información de incidentes	Una vez revisados los eventos relacionados con los activos	Usuarios de los servicios. Personal de seguridades de la información.	Registrar los incidentes. Clasificar los incidentes incluyendo la categorización, prioridad, recursos, monitoreo del estado y tiempo de resolución. Registrar los incidentes resueltos con su solución.
PASO 4 Listar las amenazas identificadas	Con formularios levantados con toda la información relacionada al activo	Personal de seguridades de la información.	Desarrollar el catálogo de amenazas con las salvaguardas y controles. Relacionar la validación y pruebas del servicio a las amenazas del catálogo. Correlacionar los eventos a una de las amenazas del catálogo. Correlacionar los incidentes a las amenazas del catálogo. Registrar los activos y sus amenazas. Registrar los controles implementados por activo incluyendo los de gestión de accesos. Registrar los controles que han fallado produciendo eventos inusuales. Listar los controles que se deben reemplazar, eliminar y mantener.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de amenazas que tienen salvaguardas	Número de amenazas con salvaguarda/Número total de amenazas del catálogo	Porcentaje
Porcentaje de activos con amenazas identificadas	Número de activos con amenazas identificadas/Número total de activos	Porcentaje
Porcentaje de activos con controles implementados	Número de activos con controles/Número total de activos	Porcentaje
Porcentaje de controles que se deben mantener	Número de controles que se mantendrán/Número total de controles	Porcentaje

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

IDENTIFICACIÓN DE VULNERABILIDADES Y VALORACIÓN DE CONSECUENCIAS EN BASE A LOS REQUERIMIENTOS, GESTIÓN DE CAMBIOS Y EL ANÁLISIS DE INCIDENTES Y PROBLEMAS

P04_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Este proceso contiene los pasos para identificar las vulnerabilidades que existen en la organización, en los procesos y procedimientos, en el personal, ambiente físico, activos de soporte y partes externas que interactúan con la organización. Estas vulnerabilidades pueden ser explotadas por amenazas externas o internas, con consecuencias como pérdida de tiempo en las operaciones, costos financieros en actividades para reparar el daño, pérdida de imagen, reputación y buen nombre, entre otras que se pueden mencionar.

Adicionalmente, el proceso ayuda a definir los requerimientos de los usuarios y la gestión de problemas que proporcionan las vulnerabilidades que han sido explotadas y los requerimientos que deben ser atendidos durante la operación de los servicios.

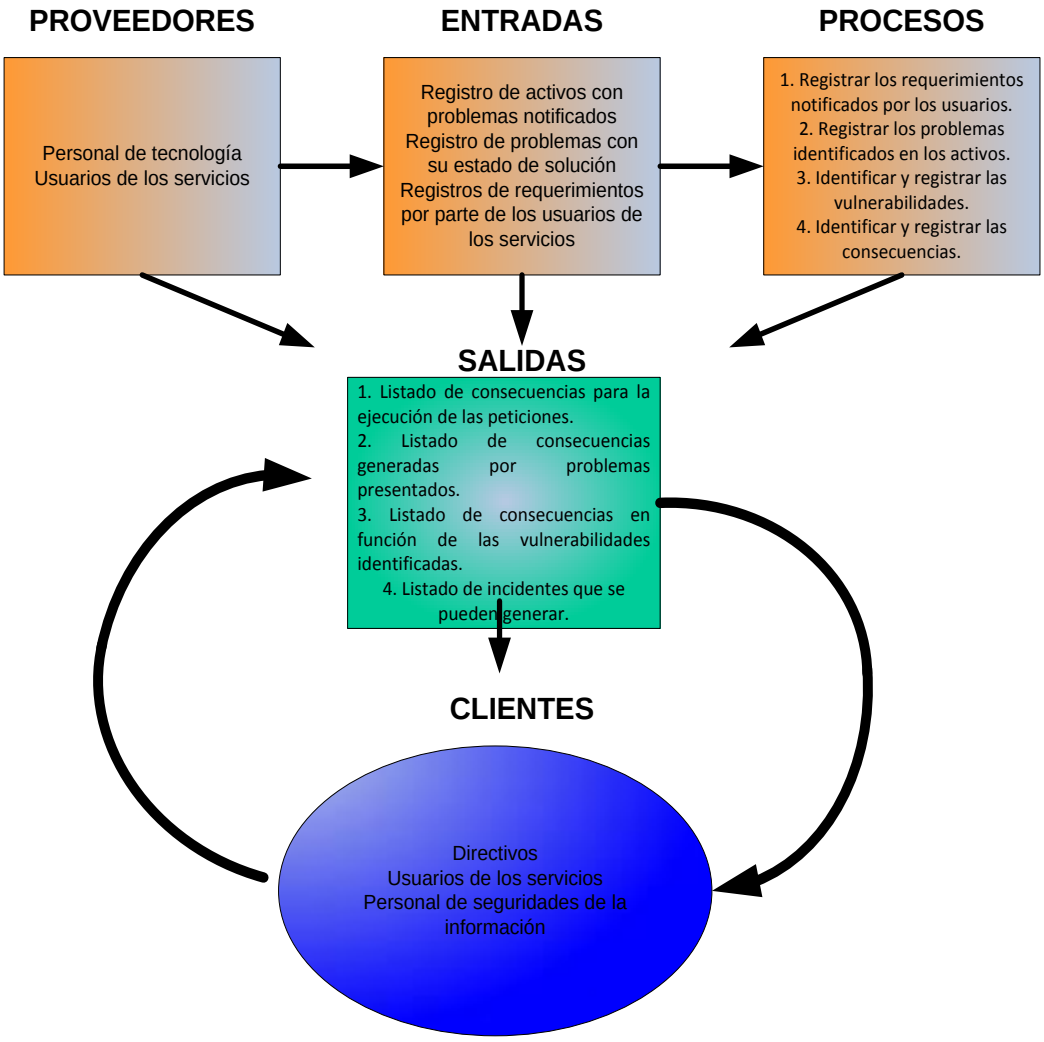
ETAPAS DE ITIL RELACIONADAS	
Solicitud de Requerimientos	Proporciona los riesgos relacionados ante la ausencia de atención de los requerimientos de los usuarios de los servicios.
Gestión de Problemas	Proporciona los incidentes ocurridos y el análisis de la causa raíz que los produjo, y de manera proactiva monitorea la infraestructura tecnológica para prevenir incidentes.
Gestión del Cambio	Proporciona las acciones que deben ser ejecutadas para disminuir el valor de las consecuencias y la probabilidad de escenarios de incidentes.
Gestión de Eventos	Aporta información sobre los eventos que han generado interrupción del servicio y con eso aumentan la probabilidad de escenarios de incidentes.
Gestión de Incidentes	Provee información sobre los activos involucrados en los incidentes para valorar las consecuencias.

VALOR PARA EL NEGOCIO

Las vulnerabilidades que pueden ser explotadas deben ser de tema de análisis en la organización, antes que las consecuencias de su explotación por parte de una amenaza se materialicen.

La identificación temprana de estos dos aspectos con base a los problemas detectados ayuda a en la prevención oportuna de las consecuencias que pueden tener para una organización.

DIRECTRICES GENERALES PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Registrar los requerimientos notificados por los usuarios	Con la definición del catálogo de amenazas	Personal de tecnología. Personal de seguridades de la información.	Registrar las solicitudes de los usuarios incluyendo peticiones de cambios y de accesos.
PASO 2 Registrar los problemas identificados en los activos	Cuando exista una CMDB con el detalle de los activos y registro de sus incidentes	Usuarios de los servicios. Personal de seguridades de la información.	Identificación y registro de problemas por activo. Analizar si los problemas se deben a la falta de capacidad. Registrar los servicios afectados. Registrar el diagnóstico de los problemas y las soluciones temporales.
PASO 3 Identificar y registrar las vulnerabilidades	Con la información de requerimientos de los usuarios y de problemas registrados por activo	Usuarios de los servicios. Personal de seguridades de la información.	Identificar las vulnerabilidades explotadas que derivaron en un problema. Registrar las vulnerabilidades que no han sido explotadas. Relacionar las vulnerabilidades identificadas con las amenazas.
PASO 4 Identificar y registrar las consecuencias	Al contar con la información de servicios, amenazas, vulnerabilidades	Personal de seguridades de la información.	Establecer las consecuencias para la ejecución de las peticiones. Establecer las consecuencias generadas por problemas presentados. Detallar las consecuencias en función de las vulnerabilidades identificadas. Listar los incidentes que se pueden generar. Determinar el valor de reemplazo para cada activo en cada caso de incidentes. Valorar el costo de recuperar un servicio.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de problemas no resueltos	Número de problemas sin resolver/Número total de problemas registrados	Porcentaje
Porcentaje de peticiones que impactan negativamente las operaciones	Número de peticiones con cambios significativos/Número total de peticiones	Porcentaje
Número de escenarios de incidentes con consecuencias para el negocio	Número de escenarios de incidente	Número
Valor promedio de recuperación de un activo	Cálculo del valor	USD

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

ESTIMACIÓN Y EVALUACIÓN DEL RIESGO EN BASE A LOS INCIDENTES, PROBABILIDAD DE OCURRENCIA Y GESTIÓN DE DISPONIBILIDAD

P05_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

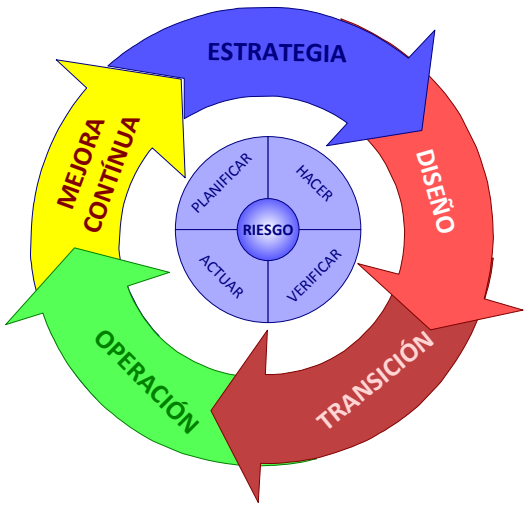
DESCRIPCIÓN DEL PROCESO

El tratamiento de riesgos está relacionado con la estimación y evaluación. Este proceso ayuda a realizar una estimación adecuada del riesgo, tomando como base los incidentes y problemas, que proveen los escenarios de afectación de los servicios y las probabilidades de ocurrencia de estos escenarios.

De esta forma, el proceso proporciona las actividades para evaluar el riesgo y determinar la prioridad para tratar los riesgos en función de la disponibilidad con la que debe cumplir el servicio.

ETAPAS DE ITIL RELACIONADAS	
Gestión de Incidentes	Proporciona los escenarios de incidentes que son pertinentes para estimar los riesgos
Gestión de Problemas	Provee la información de los incidentes cuyas causas no han sido determinadas y que una vez que se han escalado como problemas ayudan a determinar las consecuencias
Gestión de la Disponibilidad	Proporciona la garantía de los servicios brindados de acuerdo a los contratos previamente establecidos

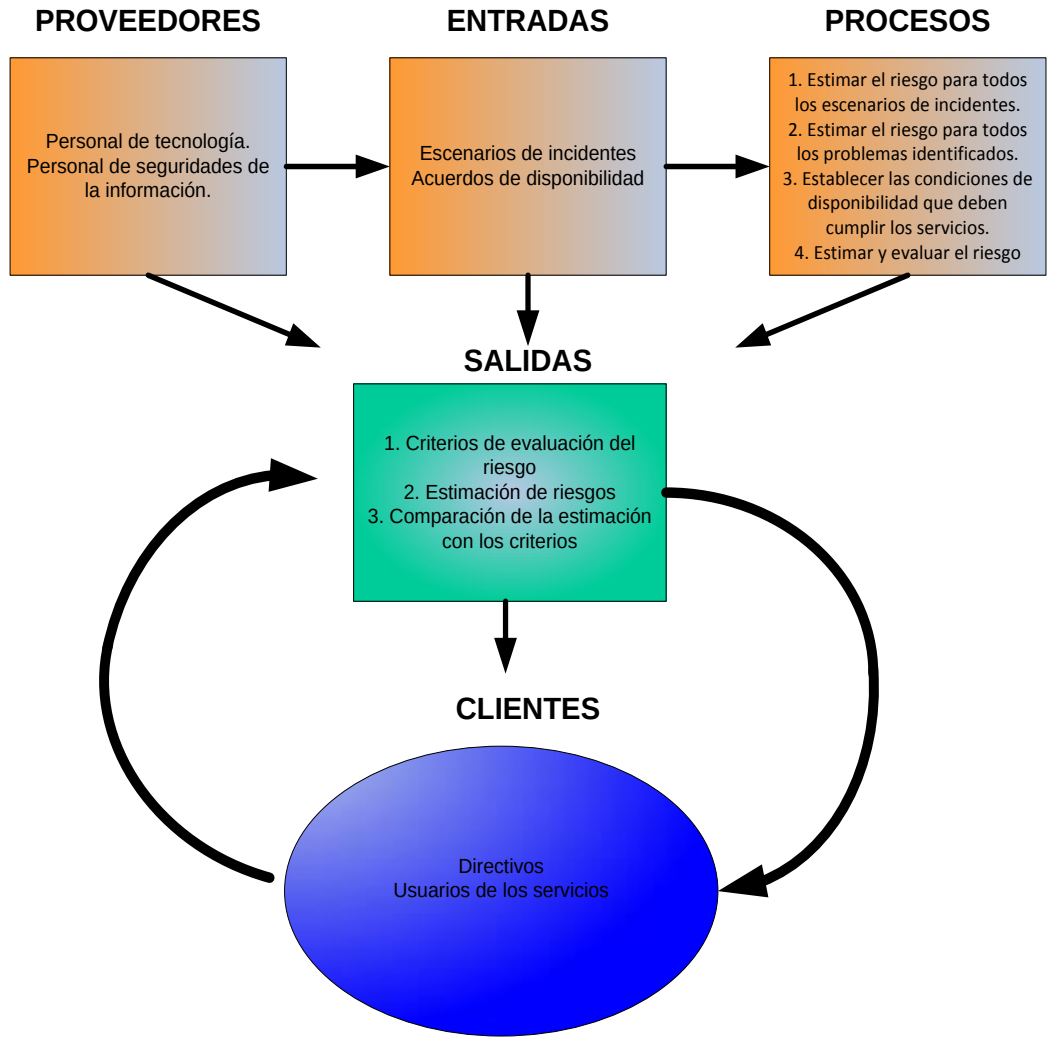
VALOR PARA EL NEGOCIO



La estimación y evaluación del riesgo en función de los incidentes, problemas y la disponibilidad que se debe proporcionar a los usuarios, permite obtener entradas realistas para tratar los riesgos adecuadamente, evitando re procesos y nuevas iteraciones en el proceso inicial de identificación y análisis.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Estimar el riesgo para todos los escenarios de incidentes	Una vez que se cuenta con toda la información de los incidentes y sus consecuencias	Personal de seguridades de la información.	Listar los escenarios de incidentes. Establecer la probabilidad de ocurrencia de los incidentes. Identificar las consecuencias de los incidentes.
PASO 2 Estimar el riesgo para todos los problemas identificados	Una vez que se han identificado los problemas y sus consecuencias	Personal de seguridades de la información.	Listar los escenarios de problemas. Establecer la probabilidad de ocurrencia de problemas. Identificar las consecuencias de los problemas.
PASO 3 Establecer las condiciones de disponibilidad que deben cumplir los servicios	Cuando se han determinado los incidentes y problemas que afectan a los servicios	Personal de tecnología. Personal de seguridades de la información.	Registrar los escenarios de incidentes y problemas que afectan la disponibilidad de servicios.
PASO 4 Estimar y evaluar el riesgo	Con toda la información sobre incidentes, problemas y la disponibilidad que deben cumplir los servicios	Personal de seguridades de la información.	Establecer criterios de evaluación de riesgos. Estimar el riesgo para los escenarios de pérdida de disponibilidad de servicios por incidentes y problemas. Comparar los riesgos estimados con los criterios de evaluación. Priorizar los riesgos.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Cantidad de riesgos priorizados	Número de riesgos priorizados/Número total de riesgos	Porcentaje
Porcentaje de riesgos estimados adecuadamente	Número de riesgos estimados aprobados para tratamiento/Número total de riesgos	Porcentaje

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

REDUCCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

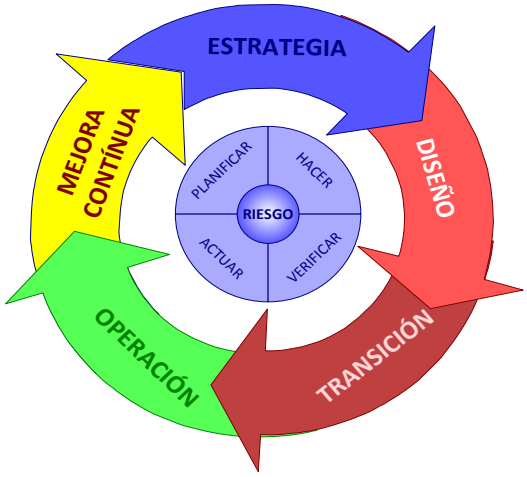
P06_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Este proceso proporciona las actividades para aceptar el riesgo residual que mediante la evaluación respectiva sea definido como aceptable. Esto se logra mediante la reducción y selección de controles durante el ciclo de vida de los servicios de TI, de tal forma de satisfacer los requerimientos identificados en la valoración y tratamiento del riesgo.

ETAPAS DE ITIL RELACIONADAS	
Planificación y soporte de la transición	Identifica, administra y controla los riesgos de falla y degradación a través del plan de transición del servicio
Validación y Pruebas del Servicio	Provee la política de riesgo de la validación y pruebas de servicio con los controles respectivos, útiles para el tratamiento del riesgo durante la transición del servicio
Retorno de la Inversión de la Mejora Continua	Provee el caso de negocio para establecer los controles
Gestión de la Disponibilidad	Proporciona el plan de disponibilidad, el cual contiene información del estado de operación del servicio y propuestas para mejorar la disponibilidad.
Gestión de Proveedores	Gestionar los requisitos de contratación, evaluación, selección, rendimiento de proveedores, proporcionando información relevante para realizar el tratamiento del riesgo mediante terceros.
Gestión de Incidentes	Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.
Solicitud de Requerimientos	Provee actividades para mejorar el control de accesos a los servicios de manera centralizada, de tal forma que se puede establecer mecanismos para tratar el riesgo ante una eventualidad
Gestión de Problemas	Provee el mecanismo de para analizar las cusas raíces de los problemas, además de elaborar RFC para reestablecer el servicio. Estas actividades proporcionan información relevante para tratar el riesgo.
Gestión de Accesos	Provee en conjunto con seguridades de la información, los perfiles de os usuarios para acceder a los servicio publicados en el respectivo catálogo, proporcionando iniciativas e información para tratar el riesgo.

VALOR PARA EL NEGOCIO

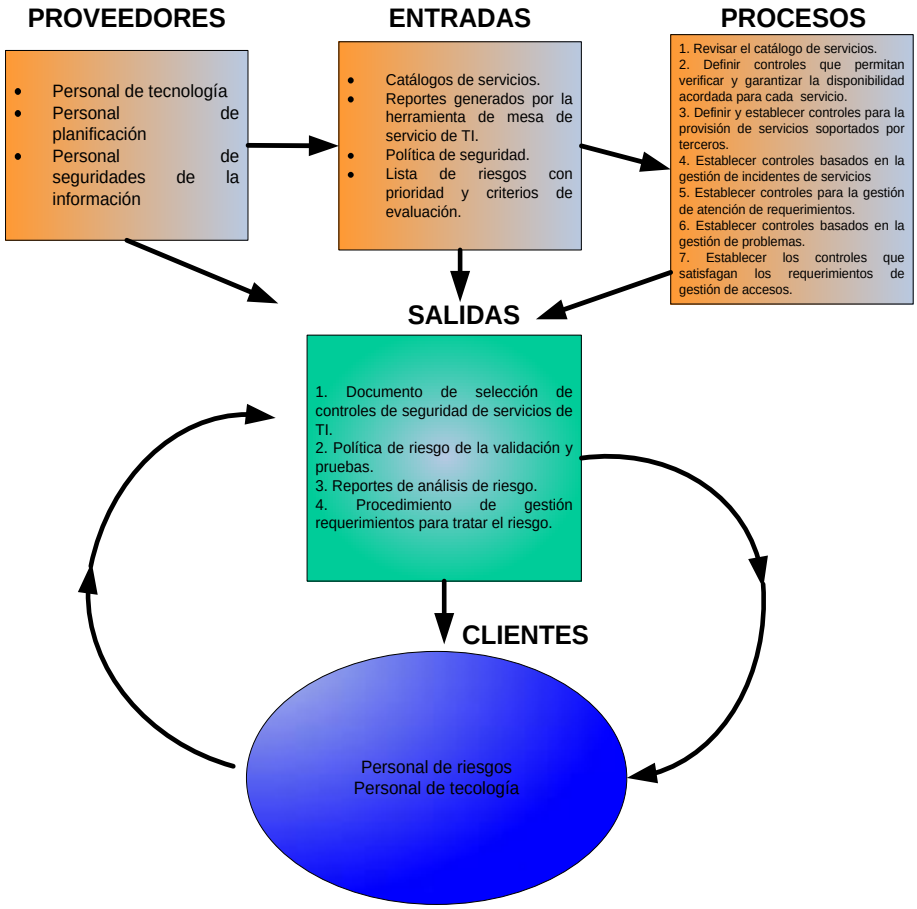


De acuerdo a la lista de riesgos priorizados y con criterio de evaluación, se logra identificar los beneficios, costos e prioridad de los controles a ser implementados para la gestión de los servicios de TI.

Proporciona los controles de seguridad o cambios en la infraestructura tecnológica contrastados con la información presupuestaria y por orden de prelación al negocio, para analizar su posible factibilidad de implementación.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Revisar el catálogo del servicios de TI, desde el punto de vista de riesgo de la seguridad de la información	Es una actividad periódica que se establece de acuerdo a la frecuencia de revisión del catálogo de servicio, política de seguridad y documento de establecimiento de contexto	Responsable de la Mesa de Servicio. Responsables de la seguridad de la información	Identificar del catálogo de servicios, aquellos que se relacionan con la lista de riesgos indicados en el establecimiento de contexto del riesgo (Servicios de TI filtrados), sobre los cuales se enfocarán los respectivos controles
PASO 2 Definir controles que permitan verificar y garantizar la disponibilidad acordada para cada servicio	Es una actividad periódica que se establece de acuerdo a la frecuencia de revisión del catálogo de servicio, política de seguridad y documento de establecimiento de contexto	Responsable de la Mesa de Servicio. Responsables de la seguridad de la información	De los Servicios de TI filtrados obtener: - El periodo de tiempo establecido por el negocio para operar. - Establecer los mecanismos de mantenimiento. - Revisión de la documentación de los procedimientos de operación
PASO 3 Definir y establecer controles para la provisión de servicios soportados por terceros.	Se lo debe realizar en la planificación, ejecución y cierre de proyectos o actividades, que sean ejecutadas por proveedores	Gerentes de proyectos Responsables de la seguridad de la información	De los Servicios de TI filtrados obtener: - Las actividades, responsabilidades y obligación a exigir a los proveedores - Supervisar los servicios prestados por proveedores. - Supervisar los controles de cambio realizados por los proveedores
PASO 4 Establecer controles basados en la gestión de incidentes de servicios	Es una actividad que se realiza cuando se tiene un incidente registrado a través de la Mesa de Servicio	Responsable de la Mesa de Servicio	De los Servicios de TI filtrados considerar, - El procedimiento para tratar los incidentes y las actividades relacionadas: registro, clasificación, diagnóstico y resolución. - Notificar los incidentes de seguridad de la información - Identificar si el incidente provoca una debilidad en la

			seguridad
PASO 5 Establecer controles para la gestión de atención de requerimientos	Es una actividad que se realiza cuando se atiende un requerimiento registrado a través de la Mesa de Servicio	Responsable de la Mesa de Servicio	De los Servicios de TI filtrados realizar - La plantilla de peticiones que el usuario podrá realizar y el tratamiento de cada uno de ellos. - Supervisar la implementación y revisión de la política de control de accesos, registros de usuarios y perfiles.
PASO 6 Establecer controles basados en la gestión de problemas	Es una actividad que se realiza cuando se tiene un problema registrado a través de la Mesa de Servicio, en el caso de que se escale un incidente recurrente o de afectación considerable en la infraestructura de TI	Responsable de la Mesa de Servicio Responsable de seguridad de la información	De los Servicios de TI filtrados realizar: - El procedimiento para el control de problemas (convertir los problemas en errores conocidos) y control de errores (registrar los errores conocidos y realizar RFC[12]) - Supervisar la gestión de cambios
PASO 7 Establecer los controles que satisfagan los requerimientos de gestión de accesos.	Es una actividad que se realiza cuando se tiene un requerimiento de acceso o reporte no autorizado registrado a través de la Mesa de Servicio o sistema de monitoreo, respectivamente.	Responsable de la Mesa de Servicio Unidad de tecnología Responsable de seguridad de la información	De los Servicios de TI filtrados identificar los perfiles de acceso, mecanismos de verificación y mecanismo de registro. Supervisar la implementación y cumplimiento de la política de control de accesos.

[12] RFC: Requerimiento para el cambio

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Número de controles implementados	Número de controles implementados/Número de controles propuestos	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

RETENCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

P07_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

Este proceso establece las actividades para monitorear los riesgos identificados en el establecimiento del contexto mediante la gestión del ciclo de vida de los servicios de TI, de tal forma de verificar si cumple con los criterios de aceptación del riesgo y por ende no sea necesario implementar controles adicionales y el riesgo se pueda retener.

ETAPAS DE ITIL RELACIONADAS	
Gestión de Incidentes	Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.
Solicitud de Requerimientos	Provee actividades para mejorar el control de accesos a los servicios de manera centralizada, de tal forma que se puede establecer mecanismos para tratar el riesgo ante una eventualidad
Gestión de Problemas	Provee el mecanismo de para analizar las cusas raíces de los problemas, además de elaborar RFC para reestablecer el servicio. Estas actividades proporcionan información relevante para tratar el riesgo.
Gestión de Accesos	Provee en conjunto con seguridades de la información, los perfiles de los usuarios para acceder a los servicios publicados en el respectivo catálogo, proporcionando iniciativas e información para tratar el riesgo.
Gestión del Nivel del Servicio	Provee la información como entrenamiento necesario, pruebas y documentación para retener el riesgo que se establece en el plan de mejora del servicio

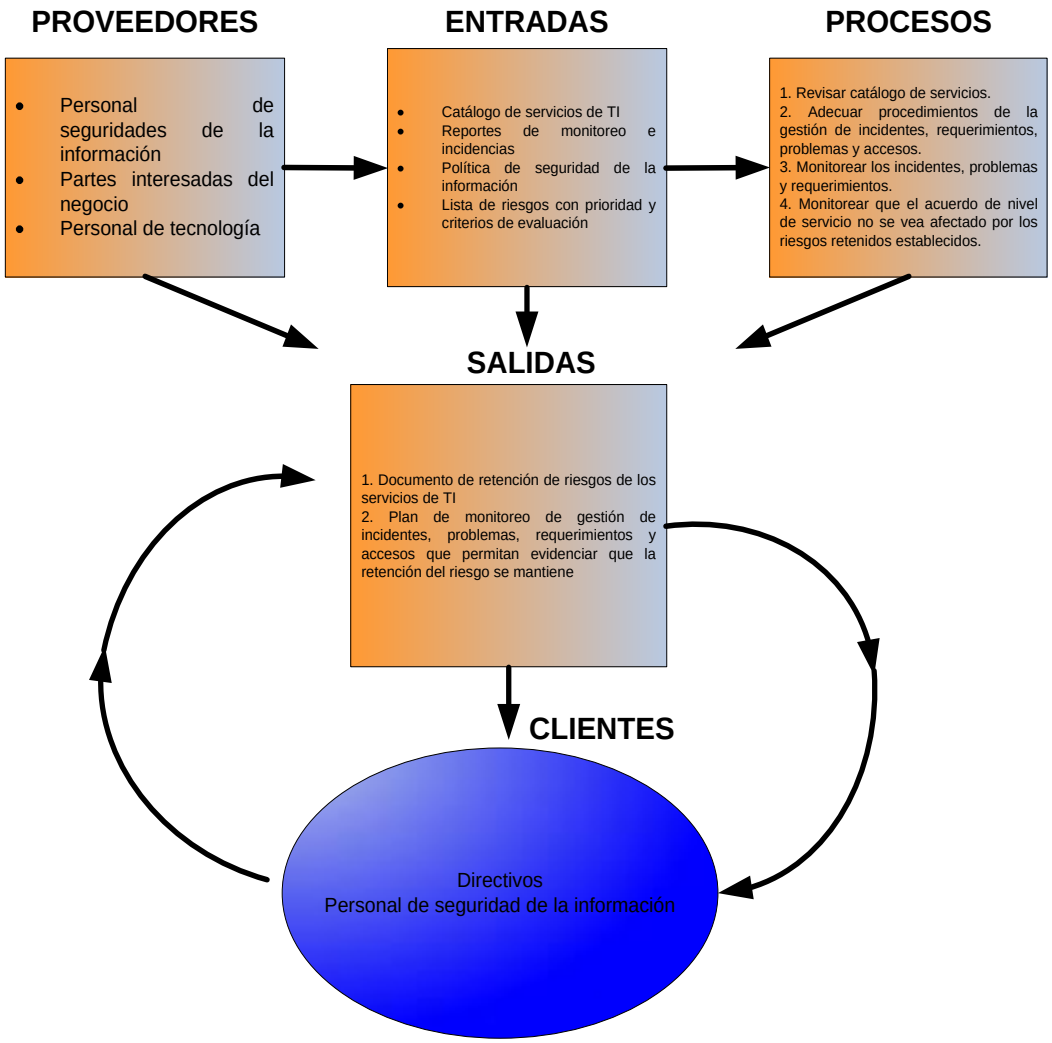
VALOR PARA EL NEGOCIO

Permite adoptar una estrategia al negocio para la aceptación del riesgo, permitiendo cuantificar las pérdidas en el escenario de que se efectivizará. De igual manera para aceptar los riesgos asociados a los servicios de TI que no han sido identificados.

El negocio retendrá el riesgo en base a los criterios de aceptación establecidos.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Revisar el catálogo de servicios de TI, desde el punto de vista de riesgo de la seguridad de la información.	Es una actividad periódica que se establece de acuerdo a la frecuencia de revisión del catálogo de servicio, política de seguridad y documento de establecimiento de contexto	Responsable de la Mesa de Servicio. Responsables de la seguridad de la información	Identificar del catálogo de servicios, aquellos que de acuerdo a los criterios de evaluación se hayan retenido el riesgo.
PASO 2 Adecuar los procedimientos de la gestión de incidentes, requerimientos, problemas y accesos para establecer mecanismos que permitan mantener el riesgo residual.	Actividad continua, de acuerdo a la operación propia de cada servicio	Responsable de Mesa de Servicio	En la atención y registro a través de la Mesa de Servicio, se debe establecer mecanismos diferentes para trabajar conjuntamente con seguridad de la información relacionados con la operación del servicio identificado en el paso 1.
PASO 3 Monitorear los incidentes, problemas y requerimientos que se relacionan con los riegos retenidos de los servicios de TI.	Es una actividad que se realiza cuando se tiene un incidente, problema o requerimiento registrado a través de la Mesa de Servicio	Responsable de la Mesa de Servicio Responsables de seguridad informática	En los incidentes, problemas y requerimientos de los servicios de TI considerar: - Definir las actividades relacionadas: registro, clasificación, diagnóstico y resolución. - Monitorear que las consecuencias provocadas por los incidentes, problema o requerimiento permanezca dentro del riesgo retenido acordado.
PASO 4 Monitorear que el acuerdo de nivel de servicio no se vea afectado por los riesgos retenidos establecidos.	Es una actividad que se realiza cuando se tiene un requerimiento de acceso o reporte no autorizado registrado a través de la Mesa de Servicio o sistema de monitoreo, respectivamente.	Responsable de la Mesa de Servicio Unidad de tecnología Responsable de seguridad de la información	- Supervisar y revisar el rendimiento de los servicios. - Notificar al personal de seguridades de la información cuando el riesgo retenido se encuentre fuera de los parámetros de evaluación y aceptación del establecimiento del contexto.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de servicios y componente de TI relacionados con el riesgo retenido monitoreados	Número de servicios monitoreados con riesgo retenido/ Número de servicios totales definidos	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

EVITACIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

P08_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

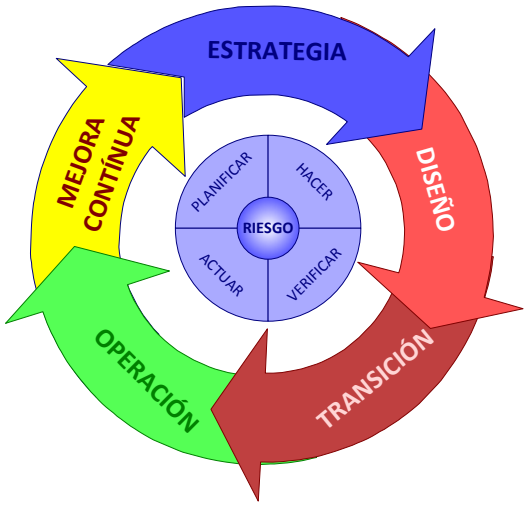
DESCRIPCIÓN DEL PROCESO

El proceso contiene las actividades para implementar los controles requeridos en la gestión de servicios de TI que permitan evitar el riesgo, de acuerdo a los criterios y evaluación del mismo, de tal forma de identificar las actividades o conjunto de actividades que deben ser tratadas.

Las actividades de la gestión de incidentes, requerimientos, problemas y acceso, proporcionaran controles que permitan identificar el origen de los riesgos a evitar. Adicionalmente estas actividades se tendrán que adaptar nuevamente con los procedimientos de operación requeridos por los servicios de TI.

ETAPAS DE ITIL RELACIONADAS	
Gestión de Incidentes	Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.
Solicitud de Requerimientos	Provee actividades para mejorar el control de accesos a los servicios de manera centralizada, de tal forma que se puede establecer mecanismos para tratar el riesgo ante una eventualidad
Gestión de Problemas	Provee el mecanismo de para analizar las cusas raíces de los problemas, además de elaborar RFC para reestablecer el servicio. Estas actividades proporcionan información relevante para tratar el riesgo.
Gestión de Accesos	Provee en conjunto con seguridades de la información, los perfiles de os usuarios para acceder a los servicio publicados en el respectivo catálogo, proporcionando iniciativas e información para tratar el riesgo.

Valor para el negocio

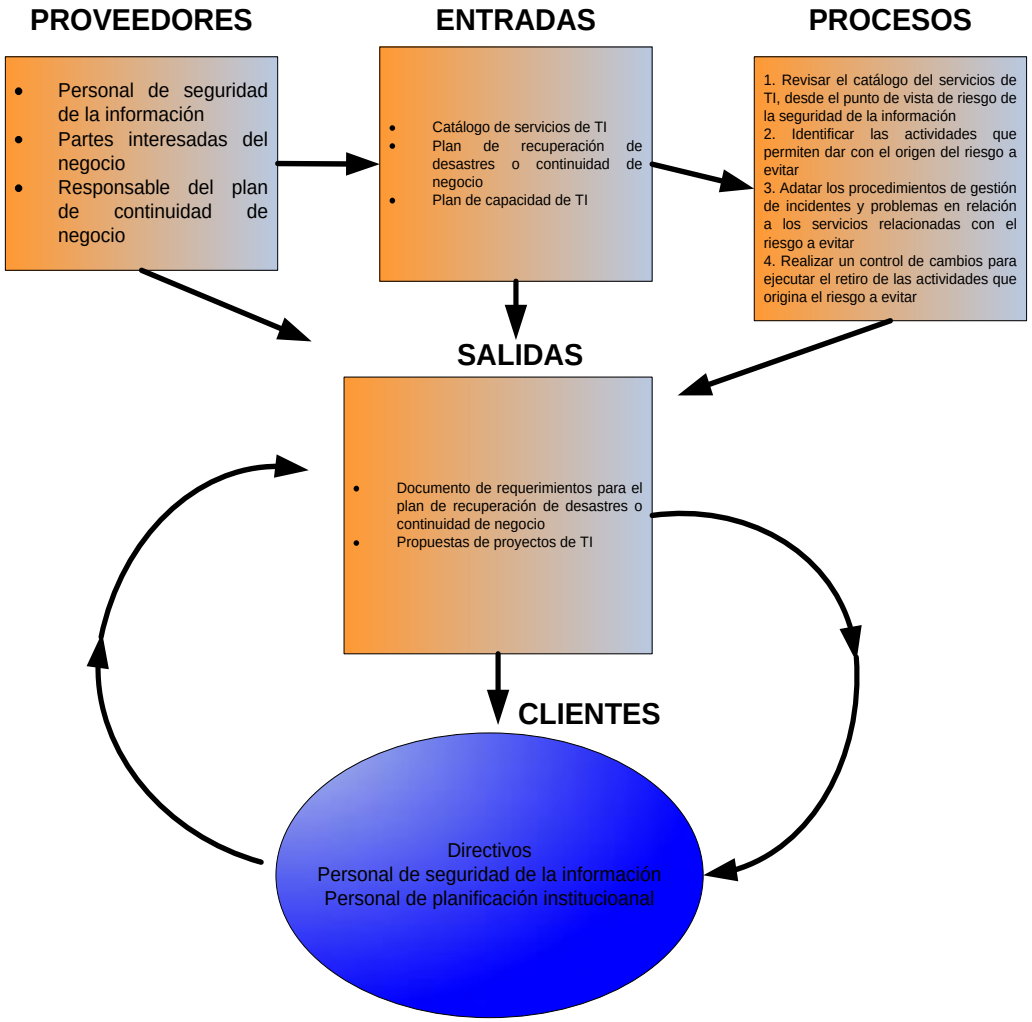


Cuando lo riesgos en la gestión de los servicios es alta y el costo de implementar controles no justifica su beneficio. El negocio podrá decidir por evitar el riesgo respectivo tratando las actividades que dan origen al riesgo.

De esta forma se podrá reevaluar el riesgo en la gestión de servicios de TI para determinar si se encuentra dentro de los parámetros de aceptación

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Revisar el catálogo del servicios de TI, desde el punto de vista de riesgo de la seguridad de la información.	Es una actividad periódica que se establece de acuerdo a la frecuencia de revisión del catálogo de servicio, política de seguridad y documento de establecimiento de contexto	Responsable de la Mesa de Servicio. Responsables de la seguridad de la información	Identificar del catálogo de servicios, aquellos que de acuerdo a los criterios de evaluación sea necesario tratarlos con el fin de obtener las actividades que den origen el riesgo a ser evitado.
PASO 2 Identificar las actividades que permiten dar con el origen del riesgo a evitar.	Se tiene un incidente, problema o requerimiento registrado a través de la Mesa de Servicio o en el sistema de monitoreo de la plataforma tecnológica.	Responsable de la Mesa de Servicio Responsables de seguridad informática	- En las actividades de diagnóstico y resolución de un incidente o problema, registrar aquellos relacionadas con los riesgos a evitar. - Notificar al responsable de seguridad para la respectiva evaluación.
PASO 3 Adatar los procedimientos de gestión de incidentes y problemas en relación a los servicios relacionadas con el riesgo a evitar	Se ejecuta el debido mecanismo para retirar las actividades que origina el riesgo a evitar	Responsable de mesa de servicios Responsable de seguridad de la información	- Actualizar los procedimientos de gestión de incidentes y problemas de los servicios de TI relacionados. - Realizar la respectiva socialización, de ser el caso.
PASO 4 Realizar un control de cambios para ejecutar el retiro de las actividades que origina el riesgo a evitar.	Aprobación de la implementación de un control de evitación de riesgo	Responsable de tecnología Responsable de seguridad de la información	- Realizar RFC. - Aprobar y dar seguimiento de cumplimiento del RFC. - En el caso de que signifique un proyecto realizarlo de acuerdo a la metodología establecida en la organización.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Proyectos o actividades ejecutadas para evitar el riesgo	Actividades ejecutadas/actividades propuestas	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

TRANSFERENCIA DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

P09_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

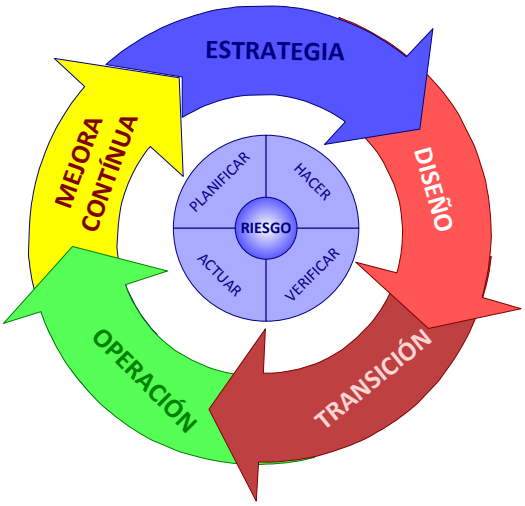
DESCRIPCIÓN DEL PROCESO

Las actividades que permiten establecer controles para transferir algún o algunos riesgos hacia un tercero que garantice una gestión eficaz, son explicadas en este proceso, para lo cual la fase de operación de los servicios de TI tendrá que acoplarse a la entrega de los mismos de forma transparente para los usuarios finales.

A pesar de que la gestión se encuentra en un tercero, el punto único de contacto para reportar o requerir de los servicio de TI afectados por la transferencia de riesgo, seguirá siendo la mesa de servicios de la organización. Es decir la responsabilidad de la gestión del riesgo se la transfiere a un tercero pero la responsabilidad del impacto es atribuible a la organización.

ETAPAS DE ITIL RELACIONADAS	
Gestión de Proveedores	Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.
Gestión de Incidentes	Se centra en restablecer de manera ágil y rápida cualquier incidente que comprometa la disponibilidad del servicio, proveedor información o actividades que permitan tratar el riesgo derivado del incidente.
Solicitud de Requerimientos	Provee actividades para mejorar el control de accesos a los servicios de manera centralizada, de tal forma que se puede establecer mecanismos para tratar el riesgo ante una eventualidad
Gestión de Problemas	Provee el mecanismo de para analizar las cusas raíces de los problemas, además de elaborar RFC para reestablecer el servicio. Estas actividades proporcionan información relevante para tratar el riesgo
Gestión de Accesos	Provee en conjunto con seguridades de la información, los perfiles de os usuarios para acceder a los servicio publicados en el respectivo catálogo, proporcionando iniciativas e información para tratar el riesgo.

VALOR PARA EL NEGOCIO

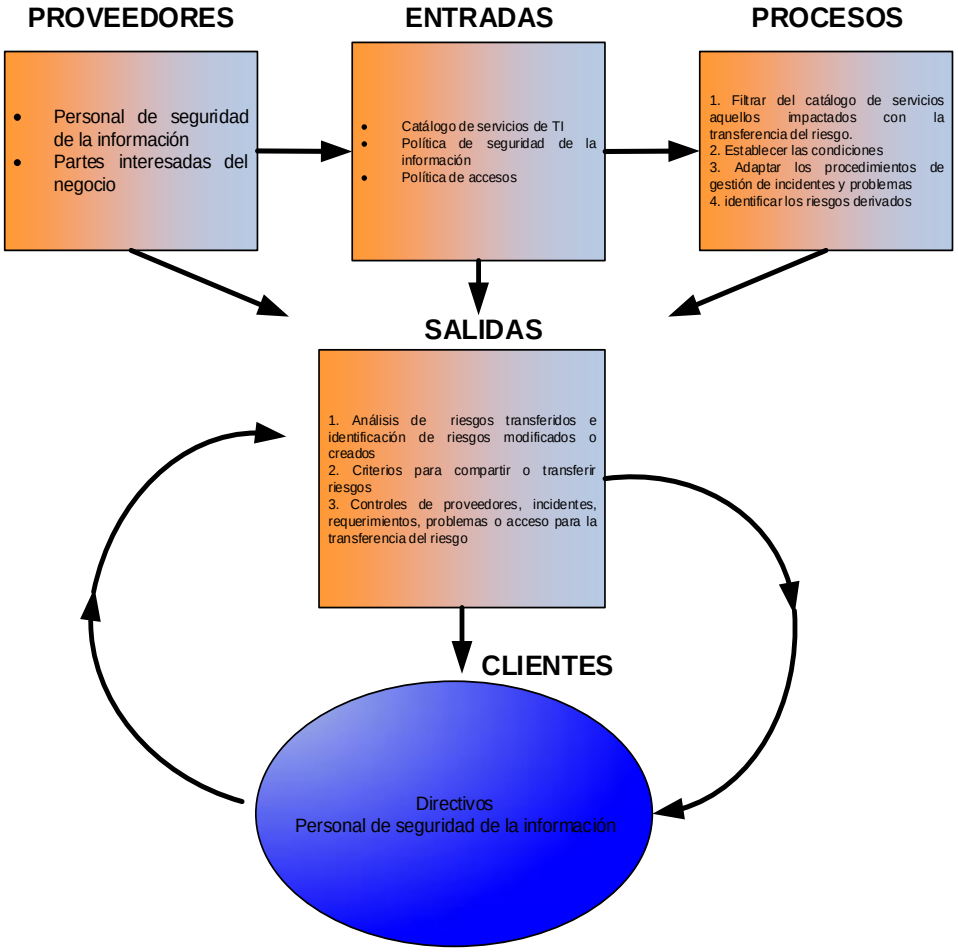


De acuerdo a los criterios de evaluación y aceptación del riesgo, es posible analizar el transferir su gestión a un tercero.

De esta forma el riesgo se podrá posteriormente evaluar como aceptable y el negocio a través de la modificación de los procesos de la operación (gestión de proveedores, incidentes, requerimientos, problemas y acceso) podrá garantizar el acceso y calidad de los servicios de TI relacionados.

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Filtrar del catálogo del servicios de TI, los servicios impactados con la transferencia del riesgo, de acuerdo al documento de establecimiento del contexto del riesgo de la seguridad de la información.	Es una actividad periódica que se establece de acuerdo a la frecuencia de revisión del catálogo de servicio, política de seguridad y documento de establecimiento de contexto	Responsable de la Mesa de Servicio. Responsables de la seguridad de la información	Identificar del catálogo de servicios, aquellos que de acuerdo a los criterios de evaluación sea necesario colocar controles para transferir el riesgo. Adaptar los procedimientos de gestión de servicios de TI asociados.
PASO 2 Establecer las condiciones, responsabilidades y obligaciones del proveedor o parte a la cual se le transfiere el riesgo.	Ejecución de un proyecto, RFC o actividad por un proveedor o parte a la cual se le transfiere el riesgo	Responsable de la Mesa de Servicio Responsables de seguridad informática	- Evaluar el cumplimiento de los requisitos establecidos en la trasferencia del riesgo. - Dar criterios del rendimiento de las partes que se les transfiere el riesgo. - Dar criterios de renovación o terminación de la transferencia de riesgo en base a la respetiva evaluación. - Notificar al responsable de seguridad para la respectiva evaluación.
PASO 3 Adatar los procedimientos de gestiones de incidentes y problemas en relación a los servicios relacionadas con la transferencia del riesgo.	El riesgo se transfiere a un tercero o parte que lo va a gestionar	Responsable de mesa de servicios Responsable de seguridad de la información	- Actualizar los procedimientos de gestión de incidentes y problemas de los servicios de TI relacionados. - Realizar la respectiva socialización, de ser el caso.
PASO 4 Identificar riesgos derivados de la gestión de terceros o partes externa.	Cuando la parte externa ejecuta las acciones respectivas para gestionar el riesgo transferido	Directivos Personal de seguridad de la información	- Revisa el cumplimiento de la política de acceso. - Identificar riesgos asociados por el acceso de terceros. - Cumplimiento del acuerdo de confidencialidad. - Implementar controles para el tratamiento de acceso de terceros, los cuales deber aprobados y establecido en el contexto del riesgo.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de riesgos derivados identificados y tratados	Riesgos derivados tratados/riesgos derivados identificados	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

ACEPTACIÓN DEL RIESGO BASADO EN LA TRANSICIÓN DEL SERVICIO

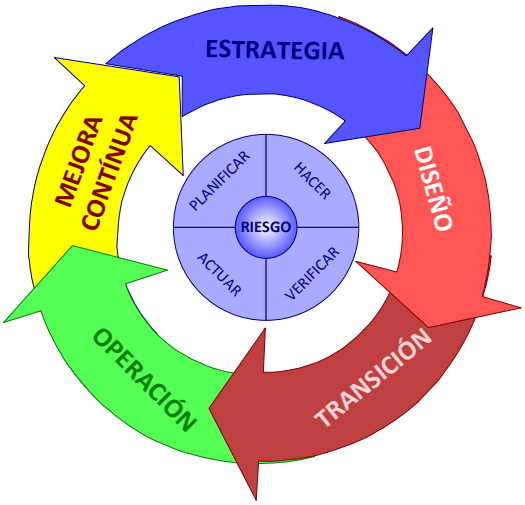
P10_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

DESCRIPCIÓN DEL PROCESO

El proceso permite analizar los riesgos residuales y el plan de tratamiento de los riesgos mediante la gestión de servicio de TI. Estas actividades apoyadas en la gestión de cambio, evaluación y conocimiento proporcionan información relevante que servirá de insumo para que los directivos tomen la decisión de aceptar el riesgo o determinar si los riesgos residuales no cumplen las expectativas y criterios de aceptación.

ETAPAS DE ITIL RELACIONADAS	
Gestión del Cambio	Provee información a través del RFC para la evaluación del riesgo
Evaluación	Provee el reporte de evaluación con el perfil del riesgo residual, después de la implementación de cambios y contramedidas
Gestión del Conocimiento	Provee la base de datos de conocimientos que pueden ser utilizados para los criterios de aceptación del riesgo.

VALOR PARA EL NEGOCIO

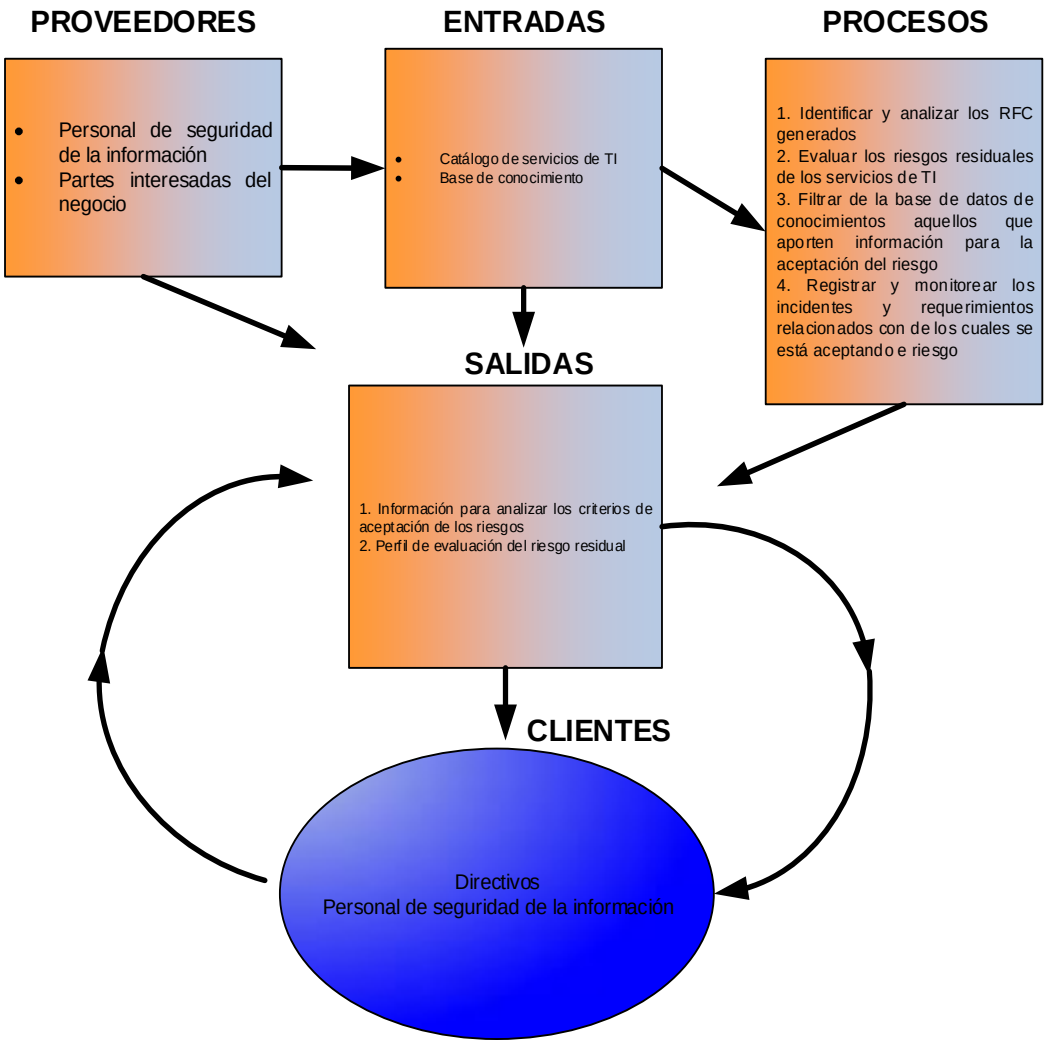


De acuerdo a los criterios de aceptación es necesario evaluar el plan de tratamiento y los riesgos residuales identificados.

Por tanto la gestión del servicio permite al negocio obtener información relevante para la toma de decisión, de tal forma que el negocio obtendrá una lista de riesgos aceptados considerando aspectos de transición del servicio previo su despliegue (operación).

DIRECTRICES GENERALES

PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Identificar y analizar los RFC generados para el tratamiento de los riesgos a ser analizados bajo los criterios de aceptación.	Actividad periódica cuando se requiere implementar un cambio en los servicios en operación	Personal de tecnología. Responsables de la seguridad de la información	- Establecer criterios en relación al control de cambio de los servicios involucrados con los riesgos a aceptar.
PASO 2 Evaluar los riesgos residuales de los servicios de TI	Cuando se ejecute un control de cambio en los servicios de TI	Responsable de la Mesa de Servicio Responsables de seguridad informática	- Identificar del catálogo de servicio, aquellos que presentan riesgos residuales basados en el plan de tratamiento. - Evaluar el rendimiento del servicio de TI asociado al riesgo a analizar, después de implementar los controles respectivos.
PASO 3 Filtrar de la base de datos de conocimientos aquellos que aporten información para la aceptación del riesgo.	Se revise los criterios de aceptación de riesgos y riesgos residuales	Directivos Responsable de seguridad de la información	- Proporcionar los mecanismos para disponibilizar la información requerida a todas las personas de la organización. - Establecer mecanismo para garantizar su calidad. - Obtener reportes de la información generada en el plan de tratamiento de riesgos.
PASO 4 Registrar y monitorear los incidentes y requerimientos relacionados con de los cuales se está aceptando e riesgo.	Actividad continua propia de la operación de los servicios de TI	Responsable de Mesa de Servicio	- Con la información recopilada, analizarla y elaborar informes técnicos para evidenciar la pertinencia del riesgo aceptado.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de riesgos que no satisfacen los criterios de aceptación	Riesgos aceptados/riesgos identificados totales	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

COMUNICACIÓN Y MONITOREO DEL RIESGO EN BASE A LA GESTIÓN DEL SERVICIO

P11_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

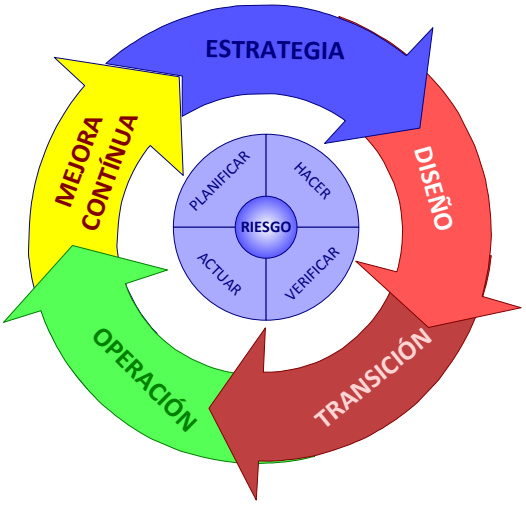
DESCRIPCIÓN DEL PROCESO

Este proceso contiene las actividades para desarrollar planes de comunicación del riesgo y nuevo conocimiento sobre seguridad de la información, mediante la gestión de reporte que parte de la mejora continua del servicio.

Los riesgos no son estáticos debido a que pueden variar de forma abrupta, por lo cual se debe monitorear continuamente con el fin de que estén alineados a los objetivos del negocio y criterios de aceptación, impulsando la relevancia del proceso de riesgo de la seguridad de la información, considerado como base la gestión del nivel de servicio.

ETAPAS DE ITIL RELACIONADAS	
Reporte del Servicio	Provee reportes con un análisis del rendimiento de los servicios, considerando eventos e información relevante para identificar y adquirir nuevos conocimientos en seguridad de la información.
Medida del Servicio	Provee el marco de referencia o procedimiento para el monitoreo de los servicios de TI, considerando criterios de disponibilidad, SLA, priorización, seguridad y responsables. Adicionalmente recopila la información de la gestión de incidencias, problemas, continuidad y disponibilidad del servicio.
Gestión del Nivel de Servicio	Provee el plan de mejora continua para la gestión del riesgo en todos los servicios
Gestión de la Continuidad del Servicio de TI	Establecer políticas y procedimientos que eviten, en la medida de lo posible, la paralización de los servicios por desastres del tipo informático

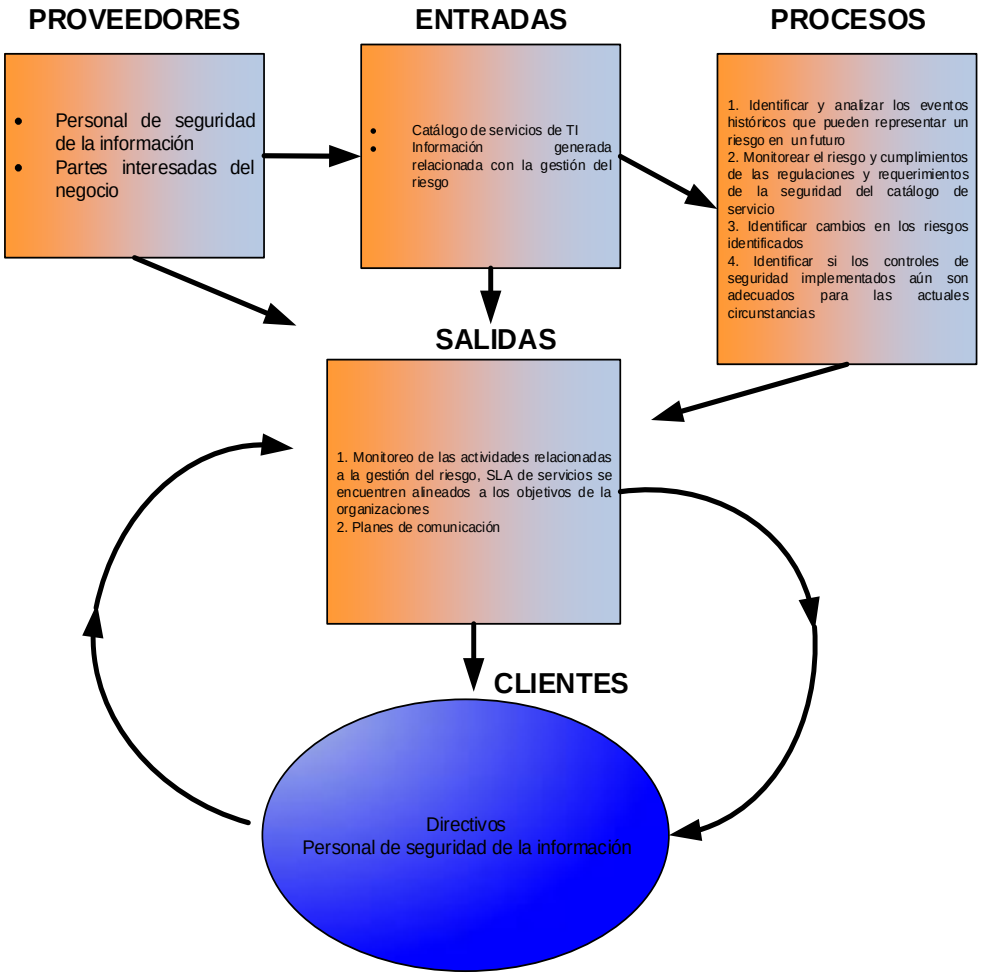
VALOR PARA EL NEGOCIO



Durante el proceso de gestión del riesgo de la seguridad de la información, de forma paralela a todas sus fases, la comunicación del riesgo permite al negocio recolectar información del riesgo, obtener nuevos conocimientos y desarrollar planes de comunicación del riesgo, basado en procesos de mejora continua del servicio.

Adicionalmente evidencia de forma continua el cumplimiento las metas y objetivos del proceso de gestión del riesgo en la seguridad de la información, lo cual permite establecer controles para la planificación, implementación, monitorización y revisión como parte de las actividades de la gestión del nivel y continuidad del servicio.

DIRECTRICES GENERALES PROCESO



GUÍA DE IMPLEMENTACIÓN

GUÍA DE IMPLEMENTACIÓN			
QUÉ?	**CUÁNDO?**	**QUIÉN?**	**CÓMO?**
PASO 1 Identificar y analizar los eventos históricos que pueden representar un riesgo en un futuro.	Actividad periódica propia de la operación de los servicios y cuando se requiera comunicar información que puede tener impacto en la gestión del riesgo	Personal de tecnología. Personal de seguridad de la información	- Identificar de los eventos históricos y amenazas que pueden representar en un futuro un potencial riesgo.
PASO 2 Monitorear el riesgo y cumplimientos de las regulaciones y requerimientos de la seguridad del catálogo de servicio.	Actividad periódica y definida en base a las prioridades, disponibilidad de los servicios de TI y establecimiento del contexto del riesgo de la información.	Personal de tecnología. Personal de la seguridad de la información	- Identificar del catálogo de servicio, aquellos que necesitan ser monitoreados de manera particular. - Elaborar informes que proporcionen información para reducir el riesgo en el ciclo de vida de los servicios monitoreados.
PASO 3 Identificar cambios en los riesgos identificados.	Actividad periódica durante el ciclo de vida del servicio y proceso de gestión del riesgo de la seguridad de la información	Personal de tecnología. Personal de la seguridad de la información	- Monitorear constantemente so existe cambios en los riesgos. - Definir, establecer acuerdos, y monitorear constantemente los servicios de TI ofrecidos.
PASO 4 Identificar si los controles de seguridad implementados aún son adecuados para las actuales circunstancias.	Actividad periódica y definida en base a las prioridades, disponibilidad de los servicios de TI y establecimiento del contexto del riesgo de la información.	Personal de tecnología	- Revisar que los criterios empleados para medir el riesgo son válidos y consistentes con el negocio. - Revisión continua de la calidad de los servicios ofrecidos.

INDICADORES

INDICADOR	FÓRMULA	UNIDAD DE MEDICIÓN
Porcentaje de riesgos identificados alineados al negocio	Porcentaje de riesgos aprobados de acuerdo a la gestión de riesgos/ porcentaje de riesgos totales identificados	**%**

ESCALA DE EVALUACIÓN

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

M_OPTIMIZA
OPTIMIZACIÓN DE SERVICIOS DE TI

MODELO DE GESTIÓN DE TI COMBINADO M_OPTIMIZA ISO/IEC 27005 e ITIL v3

2.4 FORMULARIOS DE APLICACIÓN

Existen 11 formularios de aplicación, que levantan la información a través de entrevistas a las personas que ejecutan los roles descritos para cada proceso, o de una autoevaluación realizada por el responsable de cada proceso.

La evaluación se realiza en base a los porcentajes que se ingresen en cada componente, de acuerdo a la persona que registre estos datos, la misma que debe conocer el modelo y aplicarlo con información real y de calidad de manera que permita establecer el estado actual de cada proceso en la organización.

Los formularios de aplicación contienen los siguientes campos:

- El "*Detalle del proceso*" muestra la información referente al proceso al cual se relaciona el respectivo formulario, además de los datos del entrevistado y el responsable de levantar la información.

- En "*Roles y responsabilidades*", debido a que la aplicación del formulario generalmente abarca más de un rol, la persona entrevistada deberá facilitar los nombres de las personas que desempeñan esos roles, de tal forma de realizar sesiones independientes para determinar el porcentaje de cumplimiento del mismo.

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
						100/número de ítems	0.00
Total							

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Tabla 12. Roles y Responsabilidades
(Elaborado por: Los Autores)

- La "*Medición de Directrices Generales*" reflejan las variables más relevantes requeridas para tener una gestión adecuada del proceso evaluado.

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
	Variable del proceso a ser medida		100/No. ítems	
Total				

Tabla 13. Medición de Directrices Generales
(Elaborado por: Los Autores)

- Los "*Indicadores*" y su resultado, muestran parte fundamental del estado del proceso, de acuerdo a las actividades descritas en las guías de aplicación de los procesos M_OPTIMIZA. Es necesario solicitar al entrevistado información relacionada con la frecuencia de medición, si existe una meta establecida y si existe mecanismo de monitoreo y control del indicador, de acuerdo a la siguiente tabla.

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
	A S M Q N			100/No. de ítems	
Total					

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Tabla 14. Medición de indicadores
(Elaborado por: Los Autores)

- En la "Ponderación", se tabula los valores de cada "*parte*" del formulario, y se calcula el puntaje final de evaluación para cada proceso.

Parte 4: Ponderaciónñ

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.34	
3	Indicadores		33.33	
Totales			**100,00**	

Tabla 15. Ponderación

- Finalmente debido que los procesos son dinámicos y requieren obedecer a los requerimientos de negocio, posiblemente se utilizarán los formularios periódicamente para establecer el "*Estado*" del proceso. Los niveles identificados para los "Estados" de los procesos, se realizará de acuerdo al siguiente detalle:

Parte 5: Estados

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

Tabla 16. Medición del estado

Donde se procede a resaltar el nivel que ha obtenido en el proceso la organización, utilizando el valor total de la ponderación.

FORMULACIÓN DEL CONTEXTO BASADO EN EL DISEÑO, REQUISITOS DE SEGURIDADES DE LA INFORMACIÓN Y MEJORA CONTINUA DE SERVICIOS

F01_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F01_M_OPTIMIZA**
Proceso:	**FORMULACIÓN DEL CONTEXTO BASADO EN EL DISEÑO, REQUISITOS DE SEGURIDADES DE LA INFORMACIÓN Y MEJORA CONTINUA DE SERVICIOS**
Descripción:	Este proceso contiene las consideraciones generales para establecer el contexto, además del alcance, los límites y la organización para operar el riesgo en Seguridades de la Información, a través de actividades diseñadas en etapas de ITIL como el diseño del servicio, la asignación adecuada de accesos a los activos y la medida y mejora continua que se espera obtener en el servicio.
Aplicable a:	Directivos, Máximas Autoridades de la Organización
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor del Catálogo de Servicios					33.33	
1.2	Gestor de Capacidad					33.33	
1.3	Gestor de Seguridades de la Información					33.34	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Existe un Catálogo de Servicios establecido y que incorpore nuevos servicios o aquellos que están en transición		10	
2.2	Los accesos a los servicios son entregados de acuerdo a normativas establecidas		10	
2.3	Se tiene establecido un Plan de Capacidad para los servicios de TI		10	
2.4	La organización tiene implementado un sistema de monitoreo de los activos de TI		10	
2.5	Se cuenta con una Política de		10	

	Seguridades de la Información aprobada y socializada			
2.6	El plan de seguridad se encuentra en proceso de ejecución		10	
2.7	Existen controles y auditorías periódicos para evaluar el nivel de cumplimiento de las Políticas de Seguridades de la Información		10	
2.8	Las oportunidades de mejora de los servicios de TI en base al análisis de calidad y rendimiento han sido identificadas		10	
2.9	Existen procesos e indicadores que midan la implementación de los procesos		10	
2.10	Los criterios de evaluación, impacto y aceptación han sido identificados, así como la formulación del alcance establecida		10	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de criterios de evaluación del riesgo aprobados	A S M Q N			50.0	
Porcentaje de servicios cubiertos en el contexto	A S M Q N			50.0	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

DEFINICIÓN DE LOS ACTIVOS POR CATÁLOGO DE SERVICIOS Y ACCESOS DEFINIDOS

F02_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F02_M_OPTIMIZA**
Proceso:	**DEFINICIÓN DE LOS ACTIVOS POR CATÁLOGO DE SERVICIOS Y ACCESOS DEFINIDOS**
Descripción:	Este proceso se basa en que un activo es todo lo que tiene valor para la organización, generando de esta forma las actividades para establecer una lista de activos para valorar el riesgo, en función del catálogo de servicios, el control de calidad de todo el software y hardware instalado para los servicios en producción, la configuración de los activos involucrados en los servicios y sus accesos autorizados.
Aplicable a:	Personal de tecnología, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de CMDB					20.00	
1.2	Custodio de software					20.00	
1.3	Gestor de Control de Calidad					20.00	
1.4	Gestor de Configuraciones					20.00	
1.5	Gestor de Seguridades de la Información					20.00	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Existe una CMDB administrada y actualizada constantemente		20.00	
2.2	La política de planificación de liberación de nuevas versiones ha sido aprobada y comunicada		20.00	

2.3	La liberación de nuevas versiones contiene el plan de roll-back		20.00	
2.4	Se cuenta con una base de gestión de configuraciones actualizada		20.00	
2.5	Los usuarios de los servicios están notificados de las liberaciones de nuevas versiones y la afectación en un servicio		20.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de registro de activos	A S M Q N			33.33	
Porcentaje de cumplimiento de pruebas de control de calidad	A S M Q N			33.33	
Cumplimiento de ítems ingresados en la CMDB	A S M Q N			33.34	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

IDENTIFICACIÓN DE AMENAZAS BASADOS EN LAS PRUEBAS, EVENTOS E INCIDENTES DEL CATÁLOGO DE SERVICIOS

F03_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F03_M_OPTIMIZA**
Proceso:	**IDENTIFICACIÓN DE AMENAZAS BASADOS EN LAS PRUEBAS, EVENTOS E INCIDENTES DEL CATÁLOGO DE SERVICIOS**
Descripción:	Una amenaza se define como la causa potencial de un incidente no deseado. Típicamente las amenazas dañan un sistema u organización. Este proceso contiene los pasos para identifica las amenazas en base a varios insumos, de forma que su prevención sea efectiva. La validación y pruebas del servicio antes de salir a producción, la gestión de eventos e incidentes registrados en cada servicio, permiten definir con mayor claridad las amenazas, su tipo y origen.
Aplicable a:	Personal de tecnología, usuarios de los servicios, Administradores de instalaciones, Aseguradora de la empresa, Responsable del área jurídica
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de CMDB					14.28	
1.2	Custodio de Software					14.28	
1.3	Gestor de Control de Calidad					14.28	
1.4	Gestor de Configuraciones					14.29	
1.5	Gestor de Incidentes					14.29	
1.6	Gestor de Problemas					14.29	
1.7	Gestor de Seguridades de la Información					14.29	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento	Peso (%)	Valor

		(%)		
2.1	Existe documentación con los cambios en los servicios		10.00	
2.2	Se han identificado los riesgos para los servicios del Catálogo		10.00	
2.3	Se tiene un sistema que registre los logs y notifique los eventos		10.00	
2.4	Los eventos de operación inusual tienen seguimiento hasta su cierre		10.00	
2.5	Existen bitácoras de las acciones realizadas		10.00	
2.6	Los incidentes se cierran con el reporte correspondiente		10.00	
2.7	Existe una gestión de incidentes con tiempos de respuesta, niveles de escalamiento y clasificación de los eventos		10.00	
2.8	Se cuenta con un catálogo de amenazas definido		10.00	
2.9	Los eventos, incidentes y controles son correlacionados con amenazas identificadas		10.00	
2.10	Existe un listado con los controles a implementar, reemplazar, eliminar y mantener		10.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	**Frecuencia**	**Monitoreo meta (Si/No)**	**Cumplimiento (%)**	**Peso (%)**	**Resultado**
Porcentaje de amenazas que tienen salvaguardas	A S M Q N			25.00	
Porcentaje de activos con amenazas identificadas	A S M Q N			25.00	
Porcentaje de activos con controles implementados	A S M Q N			25.00	
Porcentaje de controles que se deben mantener	A S M Q N			25.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	**Componente**	**Valor**	**Porcentaje de cumplimiento (%)**	**Valor ponderado**
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

IDENTIFICACIÓN DE VULNERABILIDADES Y VALORACIÓN DE CONSECUENCIAS EN BASE A LOS REQUERIMIENTOS, GESTIÓN DE CAMBIOS Y EL ANÁLISIS DE INCIDENTES Y PROBLEMAS

F04_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F04_M_OPTIMIZA**
Proceso:	**IDENTIFICACIÓN DE VULNERABILIDADES Y VALORACIÓN DE CONSECUENCIAS EN BASE A LOS REQUERIMIENTOS, GESTIÓN DE CAMBIOS Y EL ANÁLISIS DE INCIDENTES Y PROBLEMAS**
Descripción:	Este proceso contiene los pasos para identificar las vulnerabilidades que existen en la organización, en los procesos y procedimientos, en el personal, ambiente físico, activos de soporte y partes externas que interactúan con la organización. Estas vulnerabilidades pueden ser explotadas por amenazas externas o internas, con consecuencias como pérdida de tiempo en las operaciones, costos financieros en actividades para reparar el daño, pérdida de imagen, reputación y buen nombre, entre otras que se pueden mencionar. Adicionalmente, el proceso ayuda a definir los requerimientos de los usuarios y la gestión de problemas que proporcionan las vulnerabilidades que han sido explotadas y los requerimientos que deben ser atendidos durante la operación de los servicios.
Aplicable a:	Personal de tecnología, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Responsable del punto único de contacto para usuarios					16.66	
1.2	Gestor de Incidentes					16.66	
1.3	Gestor de Problemas					16.67	
1.4	Gestor de Configuraciones					16.67	
1.5	Gestor de CMDB					16.67	
1.6	Gestor de Seguridades de la Información					16.67	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor

2.1	Se tiene un sistema automatizado para el registro de requerimientos de usuarios		10.00	
2.2	Los requerimientos son analizados y clasificados de acuerdo a su impacto en los servicios de TI		10.00	
2.3	Se registra en la CMDB los problemas por cada activo		10.00	
2.4	Se realizan análisis de capacidad en los servicios		10.00	
2.5	Se establecen workarounds para los incidentes y las causas raíz para los problemas		10.00	
2.6	Las vulnerabilidades de cada activo están identificadas		10.00	
2.7	Se registra y clasifica las vulnerabilidades por activo		10.00	
2.8	Existe un mapa que correlacione las vulnerabilidades con las amenazas		10.00	
2.9	Los incidentes y consecuencias están claramente identificados de acuerdo al tipo de requerimientos		10.00	
2.10	Se ha determinado el valor de reemplazo de cada activo		10.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	**Frecuencia**	**Monitoreo meta (Si/No)**	**Cumplimiento (%)**	**Peso (%)**	**Resultado**
Porcentaje de problemas no resueltos	A S M Q N			25.00	
Porcentaje de peticiones que impactan negativamente las operaciones	A S M Q N			25.00	
Número de escenarios de incidentes con consecuencias para el negocio	A S M Q N			25.00	
Valor promedio de recuperación de un activo	A S M Q N			25.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	**Componente**	**Valor**	**Porcentaje de cumplimiento (%)**	**Valor ponderado**
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

ESTIMACIÓN Y EVALUACIÓN DEL RIESGO EN BASE A LOS INCIDENTES, PROBABILIDAD DE OCURRENCIA Y GESTIÓN DE DISPONIBILIDAD

F05_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F05_M_OPTIMIZA**
Proceso:	**ESTIMACIÓN Y EVALUACIÓN DEL RIESGO EN BASE A LOS INCIDENTES, PROBABILIDAD DE OCURRENCIA Y GESTIÓN DE DISPONIBILIDAD**
Descripción:	El tratamiento de riesgos está relacionado con la estimación y evaluación. Este proceso ayuda a realizar una estimación adecuada del riesgo, tomando como base los incidentes y problemas, que proveen los escenarios de afectación de los servicios y las probabilidades de ocurrencia de estos escenarios. De esta forma, el proceso proporciona las actividades para evaluar el riesgo y determinar la prioridad para tratar los riesgos en función de la disponibilidad con la que debe cumplir el servicio.
Aplicable a:	Personal de tecnología, Personal de seguridades de la información
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de Incidentes					33.33	
1.2	Gestor de Problemas					33.33	
1.3	Gestor de Seguridades de la Información					33.34	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Existe una gestión de incidentes hasta su cierre		10.00	
2.2	La probabilidad de ocurrencia de los incidentes y problemas, así como sus consecuencias está documentada		10.00	
2.3	Los escenarios de problemas se encuentran documentados		10.00	
2.4	Los criterios de evaluación de		10.00	

	riesgos están definidos			
2.5	Se ha estimado los riesgos para cada servicio		10.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Cantidad de riesgos priorizados	A S M Q N			25.00	
Porcentaje de riesgos estimados adecuadamente	A S M Q N			25.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

REDUCCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

F06_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F06_M_OPTIMIZA**
Proceso:	**REDUCCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO**
Descripción:	Este proceso proporciona las actividades para aceptar el riesgo residual que mediante la evaluación respectiva sea definido como aceptable. Esto se logra mediante la reducción y selección de controles durante el ciclo de vida de los servicios de TI, de tal forma de satisfacer los requerimientos identificados en la valoración y tratamiento del riesgo.
Aplicable a:	Personal de tecnología, personal de planificación, personal de seguridades de la información
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor del Catálogo de Servicios					14.28	
1.2	Gestor de Seguridades de la Información					14.28	
1.3	Gerente de Proyecto					14.28	
1.4	Gestor de Incidentes					14.29	
1.5	Gestor de Problemas					14.29	
1.6	Gestor de Cambios					14.29	
1.7	Gestor de requerimientos					14.29	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Se cuenta con un listado de riesgos de acuerdo al contexto establecido		10.00	
2.2	Existe un plan de mantenimiento preventivo y correctivo para los		10.00	

	servicios de TI			
2.3	Los requerimientos de seguridad han sido incorporados en los Acuerdos de Nivel de Servicio		10.00	
2.4	Se realizan controles periódicos de los reportes presentados por los proveedores		10.00	
2.5	Los controles de cambios de personal interno, así como de proveedores es supervisado por personal de la organización		10.00	
2.6	Existe un proceso y procedimiento establecido para el tratamiento de incidentes		10,00	
2.7	Se cuenta con una política de control de accesos aprobada e implementada		10.00	
2.8	Se ha definido un procedimiento aprobado para control de problemas		10.00	
2.9	Se cuenta con un procedimiento aprobado para control de errores		10.00	
2.10	El cumplimiento de políticas es verificado con auditorías periódicas		10.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Número de controles implementados	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

RETENCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

F07_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F07_M_OPTIMIZA**
Proceso:	**RETENCIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO**
Descripción:	Este proceso establece las actividades para monitorear los riesgos identificados en el establecimiento del contexto mediante la gestión del ciclo de vida de los servicios de TI, de tal forma de verificar si cumple con los criterios de aceptación del riesgo y por ende no sea necesario implementar controles adicionales y el riesgo se pueda retener.
Aplicable a:	Personal de seguridades de la información, usuarios de los servicios, personal de tecnología
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor del Catálogo de Servicios					20.00	
1.2	Gestor de Seguridades de la Información					20.00	
1.3	Gestor de Incidentes					20.00	
1.4	Gestor de Problemas					20.00	
1.5	Gestor de Acuerdos de Nivel de Servicio					20.00	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Se cuenta con un listado de riesgos retenidos y los servicios asociados		25.00	
2.2	Los procesos de gestión de requerimientos están alineados a las Políticas de Seguridad de la Información		25.00	
2.3	El proceso de gestión de incidentes		25.00	

	cuenta con un registro, documentación y gestión adecuada hasta su resolución			
2.4	Se realizan controles periódicos de los servicios y sus acuerdos, para identificar nuevos riesgos		25.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de servicios y componente de TI relacionados con el riesgo retenido monitoreados	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

EVITACIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

F08_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F08_M_OPTIMIZA**
Proceso:	**EVITACIÓN DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO**
Descripción:	El proceso contiene las actividades para implementar los controles requeridos en la gestión de servicios de TI que permitan evitar el riesgo, de acuerdo a los criterios y evaluación del mismo, de tal forma de identificar las actividades o conjunto de actividades que deben ser tratadas. Las actividades de la gestión de incidentes, requerimientos, problemas y acceso, proporcionaran controles que permitan identificar el origen de los riesgos a evitar. Adicionalmente estas actividades se tendrán que adaptar nuevamente con los procedimientos de operación requeridos por los servicios de TI.
Aplicable a:	Personal de seguridades de la información, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor del Catálogo de Servicios					20.00	
1.2	Gestor de Seguridades de la Información					20.00	
1.3	Gestor de Incidentes					20.00	
1.4	Gestor de Problemas					20.00	
1.5	Gestor de requerimientos					20.00	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	El tratamiento de riesgos incluye al Catálogo de Servicios		25.00	
2.2	Las actividades para resolución de		25.00	

	incidentes y problemas son notificadas previamente a su ejecución a Seguridades de la Información			
2.3	Los procesos de Gestión de Incidentes y Gestión de Problemas de TI son revisados periódicamente		25.00	
2.4	Existe documentación de los cambios realizados en los servicios de TI, la misma que es aprobada por Seguridades de la Información		25.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Proyectos o actividades ejecutadas para evitar el riesgo	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

TRANSFERENCIA DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO

F09_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F09_M_OPTIMIZA**
Proceso:	**TRANSFERENCIA DEL RIESGO BASADO EN LA GESTIÓN DEL SERVICIO**
Descripción:	Las actividades que permiten establecer controles para transferir algún o algunos riesgos hacia un tercero que garantice una gestión eficaz, son explicadas en este proceso, para lo cual la fase de operación de los servicios de TI tendrá que acoplarse a la entrega de los mismos de forma transparente para los usuarios finales. A pesar de que la gestión se encuentra en un tercero, el punto único de contacto para reportar o requerir de los servicio de TI afectados por la transferencia de riesgo, seguirá siendo la mesa de servicios de la organización. Es decir la responsabilidad de la gestión del riesgo se la transfiere a un tercero pero la responsabilidad del impacto es atribuible a la organización.
Aplicable a:	Personal de seguridades de la información, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de Proveedores					20.00	
1.2	Gestor de Seguridades de la Información					20.00	
1.3	Gestor de Incidentes					20.00	
1.4	Gestor de Problemas					20.00	
1.5	Gestor de requerimientos					20.00	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Se cuenta con un listado de los riesgos que se deben transferir		25.00	

2.2	Existen requerimientos definidos de seguridad con los que deben cumplir los proveedores de servicios externos		25.00	
2.3	Los procedimientos de Gestión de Incidentes y Gestión de Problemas son actualizados en función de las directrices de transferencia del riesgo		25.00	
2.4	Se cuenta con Acuerdos de Confidencialidad firmados por proveedores, terceras partes y usuarios externos de la organización		25.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de riesgos derivados identificados y tratados	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

ACEPTACIÓN DEL RIESGO BASADO EN LA TRANSICIÓN DEL SERVICIO

F10_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F10_M_OPTIMIZA**
Proceso:	**ACEPTACIÓN DEL RIESGO BASADO EN LA TRANSICIÓN DEL SERVICIO**
Descripción:	El proceso permite analizar los riesgos residuales y el plan de tratamiento de los riesgos mediante la gestión de servicio de TI. Estas actividades apoyadas en la gestión de cambio, evaluación y conocimiento proporcionan información relevante que servirá de insumo para que los directivos tomen la decisión de aceptar el riesgo o determinar si los riesgos residuales no cumplen las expectativas y criterios de aceptación.
Aplicable a:	Personal de seguridades de la información, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de Cambios					25.00	
1.2	Gestor de Seguridades de la Información					25.00	
1.3	Gestor de Conocimientos					25.00	
1.4	Gestor de Incidentes					25.00	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Existe documentación para realizar cambios necesarios para tratar el riesgo		20.00	
2.2	Los riesgos residuales de los servicios de TI son evaluados periódicamente		20.00	
2.3	Existe una base de datos para gestionar el conocimiento		20.00	
2.4	La base de datos de Gestión del Conocimiento es administrada y actualizada, registrando los cambios del negocio		20.00	
2.5	En la documentación de resolución de incidentes de incorporan los resultados del tratamiento de riesgos		20.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de riesgos que no satisfacen los criterios de aceptación	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

COMUNICACIÓN Y MONITOREO DEL RIESGO EN BASE A LA GESTIÓN DEL SERVICIO

F11_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F11_M_OPTIMIZA**
Proceso:	**COMUNICACIÓN Y MONITOREO DEL RIESGO EN BASE A LA GESTIÓN DEL SERVICIO**
Descripción:	Este proceso contiene las actividades para desarrollar planes de comunicación del riesgo y nuevo conocimiento sobre seguridad de la información, mediante la gestión de reporte que parte de la mejora continua del servicio. Los riesgos no son estáticos debido a que pueden variar de forma abrupta, por lo cual se debe monitorear continuamente con el fin de que estén alineados a los objetivos del negocio y criterios de aceptación, impulsando la relevancia del proceso de riesgo de la seguridad de la información, considerado como base la gestión del nivel de servicio.
Aplicable a:	Personal de seguridades de la información, usuarios de los servicios
Organización:	

Cargo:
Fecha: **Unidad/Departamento:**
Responsable:

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de Seguridades de la Información					33.33	
1.2	Gestor del Catálogo de Servicios					33.33	
1.3	Gestor de Requerimientos					33.34	
Total							Sumatoria

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Se realiza monitoreo de eventos para identificar aquellos que puedan representar nuevos riesgos para la organización		25.00	
2.2	Se actualiza el Catálogo de Servicios en función de los nuevos riesgos identificados		25.00	
2.3	Los servicios de TI son monitoreados periódicamente		25.00	
2.4	Los controles implementados son evaluados en función de los nuevos riesgos identificados		25.00	
Total				Sumatoria

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de riesgos identificados alineados al negocio	A S M Q N			100.00	
Total					Sumatoria

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza
Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**Sumatoria**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

M_OPTIMIZA
OPTIMIZACIÓN DE SERVICIOS DE TI

MODELO DE GESTIÓN DE TI COMBINADO M_OPTIMIZA ISO/IEC 27005 e ITIL v3

3. APLICACIÓN DEL MODELO DE GESTIÓN

3.1 POLÍTICAS DE APLICACIÓN

Para la aplicación del modelo M_OPTIMIZA, se establecen dos mecanismos de aplicación:

- Evaluación externa: levantamiento de información por medio de partes externas a la organización (consultores, auditores, reguladores, etc.).
- Autoevaluación: que se recomienda realizarla periódicamente para identificar los puntos de mejora que permitan mejorar los resultados de la evaluación. Se lo realiza por medio de pates internas a la Organización (oficial de seguridad, director de tecnologías, dueños de procesos, etc.).

A continuación se expone ejemplos de roles para las partes internas y externas más comunes:

Partes internas	Partes externas
Directores de Tecnologías	Consultores
Oficiales de Seguridad	Auditores externos
Auditores internos	Aliados de negocio
Responsables de la riesgos	
Responsables de seguridad de la información	
Gerentes de TI	
Dueño de procesos	

Tabla 17. Partes internas y externas
(Elaborado por: Los Autores)

De esta manera, a continuación se detallan las políticas generales que se debe observar, para la aplicación del modelo:

- En cualquier mecanismo de aplicación, se recomienda que los formularios sean levantados por cargos con responsabilidad directiva en la organización en áreas de riesgo, seguridad de la información y tecnología, como por ejemplo gerentes, directores, jefes de área. O su defecto por personal externo calificado.
- Si pudieren existir mejores resultados, se debe delegar a los dueños de los procesos para que ingresen la información en cada formulario.

- Un mismo formulario puede ser aplicado a varios roles. En este caso se promediará los resultados finales de la ponderación de los formularios aplicados para obtener el nivel de la organización en cada proceso.
- La información ingresada debe ser de calidad, con el estado real de los procesos en la organización, de forma que no se altere los resultados finales.
- La información de los formularios no debe contemplar el estado futuro de los procesos sino el actual.
- Los porcentajes de cumplimiento de cada componente de los formularios de aplicación, deben tomar de referencia los porcentajes de cumplimiento descritos a continuación:

Porcentaje de cumplimiento (%)	Descripción
0	No existe
10	Existe de manera incompleta y ad hoc
30	Se cumple o existe de manera regular con cierta documentación
50	Se cumple, la documentación es incompleta pero están comunicados
70	Se cumple y es aceptable,, es medido y monitoreado
100	Se cumple, es optimizado (mejora continua)

Tabla 18. Porcentajes de cumplimiento
(Elaborado por: Los Autores)

3.2 PROCEDIMIENTO DE APLICACIÓN

El modelo M_OPTIMIZA se aplica siguiendo los siguientes pasos:

1. *Caracterización de la empresa*: realizar la caracterización de la empresa, en base al marco de referencia ITIL v3 y de la ISO 27005.
2. *Mecanismo de evaluación*: determinar el mecanismo de aplicación del modelo en base a la caracterización y a los recursos disponibles (evaluación externa o autoevaluación)
3. *Selección de roles*: levantar un listado que contenga la selección de roles, con los que se podrá levantar la información, para cualquiera de los dos mecanismos de evaluación (evaluación externa o autoevaluación).

No.	Nombre	Cargo	Rol

Tabla 19 Listado de selección de roles
(Elaborado por: Los Autores)

A continuación una identificación comúnmente usada en la gestión de servicios de TI y gestión del riesgo de la seguridad de la información, y por ende en M_OPTIMIZA.

Roles/Unidad Gestión de Servicios	Roles/unidades Gestión de Riesgos de Seguridad de la información
Gestor del Catálogo de Servicios	Comité de gestión del riesgo
Gestor de Capacidad	Comité de gestión de la seguridad de la información.
Gestor de Seguridades de la Información	Auditores internos
Gestor de CMDB	Gerente de la Seguridad de la Información
Custodio de software	Oficiales de seguridad
Gestor de Control de Calidad	
Gestor de Configuraciones	
Gestor de Incidentes	
Gestor de Problemas	
Responsable del punto único de contacto para usuarios	
Gerente de Proyecto	

Tabla 20. Roles comunes de M_OPTIMIZA
(Elaborado por. Los Autores)

4. *Entrevistas*: realizar entrevistas con cada rol de la organización, definido en el punto anterior, si la aplicación es externa. En el caso de una autoevaluación se entrega los formularios a los roles de la organización definidos para levantar la información.
5. *Tabulación de resultados*: promediar la ponderación obtenida por proceso, en caso que se aplique un formulario a varios roles.

La evaluación se define de acuerdo a la calificación obtenida en los Formularios de Aplicación, numerados desde el F01_M_OPTIMIZA al F11_M_OPTIMIZA, correspondiente para cada proceso.

En la “Parte 4: Ponderación” de cada formulario de aplicación, se obtiene el valor evaluado para cada proceso del modelo M_OPTIMIZA en la organización.

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades		33.33	
2	Medición de Directrices Generales		33.33	
3	Indicadores		33.34	
Totales		**Sumatoria**	**100,00**	**VALOR DE EVALUACIÓN**

Tabla 21. Evaluación
(Elaborado por: Los Autores)

6. *Presentación de resultados*: presentar los resultados en una tabla consolidada de todos los procesos, la misma que servirá para que los directivos puedan tomar decisiones. Un ejemplo de este resumen se muestra a continuación.

Proceso M_OPTIMIZA	Código de proceso	Código de formulario	Calificación obtenida	Estado	
Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios	P01_M_OPTIMIZA	F01_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Definición de los activos por catálogo de servicios y accesos definidos	P02_M_OPTIMIZA	F02_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios	P03_M_OPTIMIZA	F03_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas	P04_M_OPTIMIZA	F04_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad	P05_M_OPTIMIZA	F05_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P06_M_OPTIMIZA	F06_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Retención del riesgo basado en la gestión de servicios	P07_M_OPTIMIZA	F07_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Evitación del riesgo basado en la gestión de servicios	P08_M_OPTIMIZA	F08_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Transferencia del riesgo basado en la gestión de servicios	P09_M_OPTIMIZA	F09_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Aceptación del riesgo basado en la transición del servicio	P10_M_OPTIMIZA	F10_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P11_M_OPTIMIZA	F11_M_OPTIMIZA	0<PONDERACIÓN<=49	NIVEL BAJO	
			50<PONDERACIÓN<=69	NIVEL MEDIO	
			70<PONDERACIÓN<=100	NIVEL ALTO	

Tabla 22. Resumen de Alto Nivel
(Elaborado por: Los Autores)

7. *Validación y análisis de resultados*: aplicar la siguientes recomendaciones de mejora, en base a los resultados obtenidos en la tabla consolidada:

   1.- Bajos o Medios: requieren la definición de roles y responsables de cada proceso, y efectuar las acciones de mejora en base a lo establecido en las Guías de Implementación, de las fichas P01_M_OPTIMIZA a la P11_M_OPTIMIZA del Modelo M_OPTIMIZA definidas en la sección 2.2.
   2.- Altos, se consideran aceptables y se recomienda, mantener o mejorar los puntajes aplicando las Guías de Implementación y evaluando continuamente los resultados con los Formularios de Aplicación desde el F01_M_OPTIMIZA al F11_M_OPTIMIZA.
   3.- Al inicio se debe realizar aplicaciones con periodicidad más frecuente hasta obtener resultados aceptables y aceptados por la organización, para mantener el equilibrio en el desempeño de los procesos del Modelo M_OPTIMIZA.

3.3 INTERPRETACIÓN

La interpretación, está definida en tres niveles, que establecen el ajuste a las bandas de calificación:

NIVEL	DESCRIPCIÓN
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.

Tabla 23. Interpretación
(Elaborado por: Los Autores)

3.4 ANÁLISIS DE RESULTADOS

El análisis de resultados establece la relación entre la evaluación e interpretación. De esta manera, se ubica el puntaje obtenido en la evaluación en la escala de interpretación, definiendo el estado de la organización para cada proceso.

CAPÍTULO 3: APLICACIÓN DEL MODELO DE GESTIÓN EN LA DITSI Y PRESENTACIÓN DE RESULTADOS

El modelo desarrollado M_OPTIMIZA, permitirá optimizar los servicios tecnológicos de las organizaciones, centrando su ámbito de acción en la gestión de servicios de TI y riesgo de la seguridad de la información. De esta forma es una herramienta de apoyo y puede ser utilizada dentro del programa de gestión del riesgo corporativo.

Una de las metas por abordar con M_OPTIMIZA, es convertirse en una herramienta de uso periódico, de tal forma proponer acciones correctivas y preventivas para una mejora continua de los servicios de TI.

El valor agregado de M_OPTIMIZA, se centra principalmente en la conceptualización de un modelo de servicio basado en riesgos, dando como resultando 11 procesos, que permiten adaptar controles en beneficio de la entrega de los servicios de TI. Adicionalmente contribuye y se alinea en una implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), debido que M_OPTIMIZA se basa en riesgo.

Es importante indicar que la generación de valor, se refleja parte por la efectividad de los controles establecidos, pero en mayor medida en que sea una necesidad de las Organizaciones y se potencialice los resultados esperados, de todas estas iniciativas.

3.1IDENTIFICANDO LAS FACTORES DE MOTIVACIÓN

Adicional a los inconvenientes y problemas percibidos en los servicios tecnológicos que interviene en la cadena de valor de la SENPLADES, es necesario que la directiva este consiente de los factores que impulsan el negocio, tales como:

- Obtener el mayor valor de las Tecnologías de la información y la importancia y éxito que tiene en la consecución de los objetivos de la Institución

- Lograr que las Tecnologías de la información sea una parte integral de la Institución.
- Establecer una relación o alineación de las Tecnologías de la Información con lo que la Institución requiere.
- Cumplir con el marco regulatorio.
- Ajustarse al entorno cambiante y dinámico de las Tecnologías de la Información.
- Gestionar el riesgo o los niveles establecidos y permitidos por la Institución.

El entendimiento de estas motivaciones, permitirán lograr un patrocinio a nivel directivo y por ende un compromiso directo, en la ejecución e implementación del modelo M_OPTIMIZA.

Es importante indicar que la aplicación del modelo, se centra en conocer el estado actual de la DITSI y proporcionar las guías y recomendaciones para su mejora continua a través de los 11 procesos establecidos. La implementación per se no forma parte de este proyecto de titulación.

3.2APLICACIÓN DEL MODELO M_OPTIMIZA

De acuerdo al procedimiento de aplicación descrito en la sección 3 del modelo M_OPTIMIZA, se desarrollaron los siguientes pasos:

3.2.1 RESUMEN CARACTERIZACIÓN DE LA EMPRESA

En el CAPÍTULO I “Diagnóstico Inicial de Servicios Tecnológicos en la DITSI”, se hizo un análisis a detalle de la situación actual de la DITSI, sin embargo se presenta un resumen de los aspectos relevantes encontrados:

3.2.1.1 Reseña histórica13

La planificación estatal en el Ecuador se inició con la Junta Nacional de Planificación y Coordinación Económica (Junapla), creada mediante Decreto Ley de Emergencia número 19, del 28 de mayo de 1954. En 1979, fue remplazada por el Consejo Nacional de Desarrollo (CONADE), con entidades adscritas, como, el

[13] Fuente: www.planificacion.gob.ec

Instituto Nacional de Estadísticas y Censos (INEC), el Fondo Nacional de Pre inversión, y el Consejo Nacional de Ciencia y Tecnología (CONACYT). En 1998, en lugar del CONADE, se creó la Oficina de Planificación (ODEPLAN). En el 2004, mediante Decreto Ejecutivo No. 1372, se creó la Secretaría Nacional de Planificación y Desarrollo, SENPLADES.

3.2.1.2 Misión, visión, atribuciones

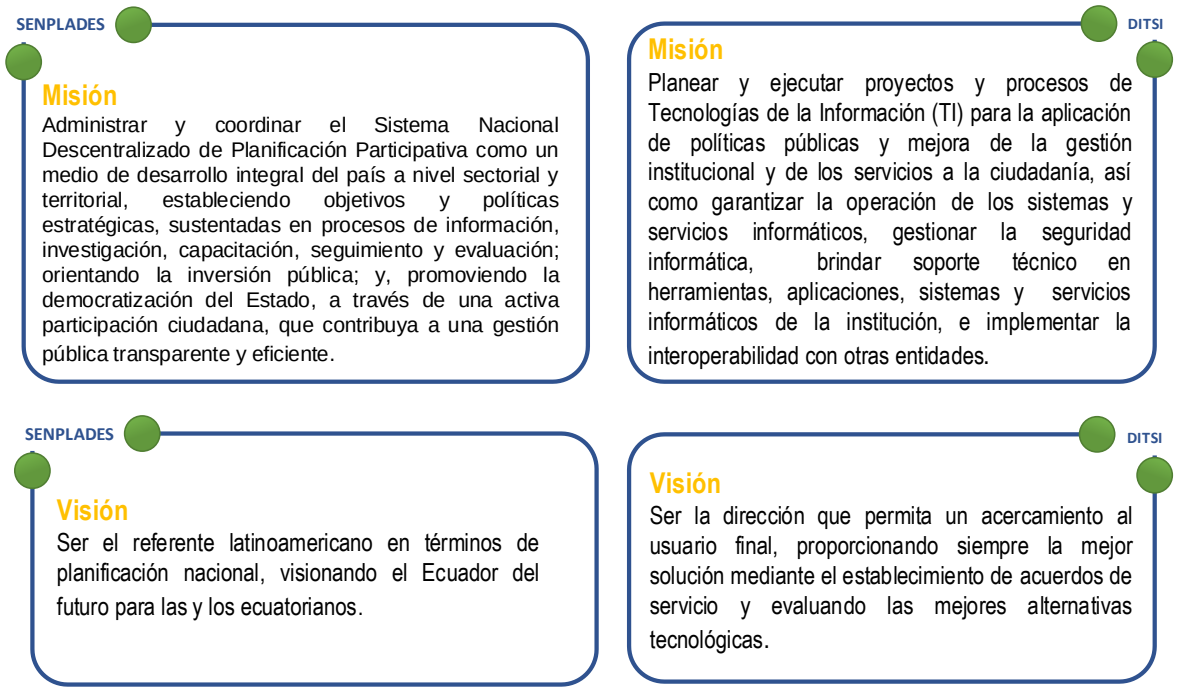


Figura 3.1 Misión y visión – SENPLADES y DITSI
(www.planificacion.gob.ec, 2012)

3.2.1.3 Posición respecto a la toma de decisiones

Como se mencionó en el primer capítulo, la DITSI a pesar de que pertenece a una Coordinación General de Gestión Estratégica, la cual reporta a la máxima autoridad, no interviene en la toma de decisión directamente. Lo cual ocasiona que realice actividades enfocadas a la operación, desatendiendo la alineación de las iniciativas y recursos con los objetivos estratégicos de la Institución.

Por esta situación, es importante el compromiso de la alta directiva y máxima autoridad para patrocinar iniciativas que cambien la estructura en la toma decisión

e incentiven la adopción de Gobierno Corporativo de Tecnologías de la Información.

3.2.2 MECANISMO DE APLICACIÓN DE FORMULARIOS

M_OPTIMIZA, permite aplicar el modelo a través de dos mecanismos: evaluación externa o autoevaluación. En este caso, los resultados y el respectivo análisis son obtenidos por medio de la evaluación externa, es decir los responsables del levantamiento de la información y entrevistas no pertenecen a la Institución.

3.2.3 SELECCIÓN DE ROLES

De acuerdo al organigrama de la unidad y al diagnóstico de la DITSI, se identificaron los siguientes roles, los cuales aportan en el levantamiento de información, y de igual forma aquellos que no están asignados.

Rol	Cargo asignado
Director de Tecnología	Asignado
Gestor del Catálogo de Servicios	Coordinador de Soporte Técnico
Gestor de Capacidad	Coordinador de Infraestructura
Gestor de Seguridades de la Información	Oficial de Seguridades de la Información
Gestor de CMDB	No está asignado
Custodio de software	Administrador de Directorio Activo
Gestor de Control de Calidad	Líder de equipo de Control de Calidad
Gestor de Configuraciones	Coordinador de Infraestructura
Gestor de Incidentes	Coordinador de Infraestructura
Gestor de Problemas	No está asignado
Responsable del punto único de contacto para usuarios	Coordinador de Soporte Técnico
Gerente de Proyecto	Existen varias asignaciones
Gestor de Cambios	No está asignado
Gestor de requerimientos	Coordinador de Soporte Técnico
Gestor de Acuerdos de Nivel de Servicio	No está asignado
Gestor de Proveedores	No está asignado
Gestor de Conocimientos	No está asignado

Tabla 3.1 Roles y funciones DITSI

3.2.4 ENTREVISTAS

Para la aplicación, se levantó la respectiva información a través de los formularios de M_OPTIMIZA, a cuatro funcionarios que desempeñan roles claves en la gestión de servicios de TI, descritas a continuación:

- Director de Tecnología, responsable de la gestión de la DITSI.
- Oficial de la Seguridades de la Información, responsable en las actuales condiciones del Sistema de Gestión de Seguridad (SGSI) de la Información.
- Coordinador de infraestructura, gestiona los recursos tecnológicos y la operación de los servicios de TI en producción.
- Coordinador de Soporte Técnico, responsable de la gestión de Mesa de Servicios de TI.

En este caso con el fin de reducir el nivel de subjetividad, se aplicaron todos los formularios (F01_M_OPTIMIZA al F11_M_OPTIMIZA) a las cuatro funcionaros, para obtener un promedio por cada proceso.

En cada entrevista, el evaluador externo quien conoce a detalle el modelo M_OPTIMIZA, proporciona información relacionado con el proceso evaluado y da las pautas adecuadas para obtener información precisa y objetiva de cada entrevistado.

Con esta información será posible continuar con la debida evaluación, tabulación de resultado y obtener una visión general del estado actual de la DITSI, en relación a los procesos establecidos en el modelo M_OPTIMIZA.

A continuación se adjunta un ejemplo de los formularios aplicados al Coordinador de Infraestructura, el resto de los formularios se adjuntan como parte del Anexo Digital A.

DEFINICIÓN DE LOS ACTIVOS POR CATÁLOGO DE SERVICIOS Y ACCESOS DEFINIDOS

F02_M_OPTIMIZA OPTIMIZACIÓN DE SERVICIOS DE TI

Nombre:	**F02_M_OPTIMIZA**
Proceso:	**DEFINICIÓN DE LOS ACTIVOS POR CATÁLOGO DE SERVICIOS Y ACCESOS DEFINIDOS**
Descripción:	Este proceso se basa en que un activo es todo lo que tiene valor para la organización, generando de esta forma las actividades para establecer una lista de activos para valorar el riesgo, en función del catálogo de servicios, el control de calidad de todo el software y hardware instalado para los servicios en producción, la configuración de los activos involucrados en los servicios y sus accesos autorizados.
Aplicable a:	Personal de tecnología, usuarios de los servicios
Organización:	Secretaría Nacional de Planificación y Desarrollo

Cargo: Coordinador de Infraestructura
Fecha: Diciembre de 2013 **Unidad/Departamento:** DITSI
Responsable: Evaluador externo

Parte 1: Roles y responsabilidades

No.	Rol	¿Asignado formalmente?	Reporta a	Cumplimiento (%)	Nombre del responsable	Peso (%)	Valor
1.1	Gestor de CMDB	No	-	0.00	-	20.00	0.00
1.2	Custodio de software	Si	Director de la DITSI	60.00	Verónica Parreño	20.00	12.00
1.3	Gestor de Control de Calidad	Si	Director de la DITSI	100.00	Lilia González	20.00	20.00
1.4	Gestor de Configuraciones	No	Director de la DITSI	60.00	Roberto Andrade	20.00	12.00
1.5	Gestor de Seguridades de la Información	Si	Coordinación de Planificación	100.00	Sandra Paredes	20.00	20.00
Total							64.00

Cumplimiento= Rol y responsable asignado (100%); rol asignado a un responsable que comparte otras funciones (60%); no existe el rol en la organización (0%)

Parte 2: Medición de Directrices Generales

No.	Pregunta	Porcentaje de cumplimiento (%)	Peso (%)	Valor
2.1	Existe una CMDB administrada y actualizada constantemente	0.00	20.00	0.00
2.2	La política de planificación de liberación de nuevas versiones ha sido aprobada y comunicada	50.00	20.00	10.00
2.3	La liberación de nuevas versiones contiene el plan de roll-back	10.00	20.00	2.00
2.4	Se cuenta con una base de gestión de configuraciones actualizada	0.00	20.00	0.00
2.5	Los usuarios de los servicios están notificados de las liberaciones de nuevas versiones y la afectación en un servicio	10.00	20.00	2.00
Total				12.00

Parte 3: Indicadores

Indicador	Frecuencia	Monitoreo meta (Si/No)	Cumplimiento (%)	Peso (%)	Resultado
Porcentaje de registro de activos	A S M Q N	No	0.00	33.33	0.00
Porcentaje de cumplimiento de pruebas de control de calidad	A S M Q N	Si	50.00	33.33	16.67
Cumplimiento de ítems ingresados en la CMDB	A S M Q N	No	0.00	33.34	0.00
Total					16.67

Frecuencia: A=anual; S=semestral; M=mensual; Q=Quincenal; N=no se realiza

Frecuencia y monitoreo (100%), solo frecuencia (50%), ninguna acción (0%)

Parte 4: Ponderación

No.	Componente	Valor	Porcentaje de cumplimiento (%)	Valor ponderado
1	Roles y responsabilidades	64.00	33.33	21.33
2	Medición de Directrices Generales	12.00	33.33	3.99
3	Indicadores	16.67	33.34	5.55
Totales		**56.67**	**100,00**	**30.87**

En base al valor total ponderado, indicar el nivel de la organización en este proceso:

NIVEL	DESCRIPCIÓN	PONDERACIÓN (%)
BAJO No logrado	El proceso no está implementado. No tiene nada ninguna actividad implementada ni indicadores. No existe evidencia de haber iniciado la guía de implementación.	0-49
MEDIO Parcialmente alcanzado	El proceso está parcialmente implementado. Existe evidencia de que se cumplen algunas actividades. Se registra interacción de los responsables y el proceso cumple en cierta medida con su propósito.	50-69
ALTO Logrado en gran medida	El proceso está casi o totalmente implementado y gestionado. Cumple con todas las actividades establecidas y alcanza los productos planteados.	70-100

3.2.5 TABULACIÓN DE RESULTADOS

La siguiente tabla muestra los resultados de los puntajes obtenidos para cada uno de los 11 procesos, relacionados con cada entrevistado.

Proceso M_OPTIMIZA	Código de proceso	Código de formulario	Coordinador de Infraestructura Puntaje	Coordinador de Soporte Técnico Puntaje	Oficial de Seguridades Puntaje	Directora de la DITSI (s) Puntaje
Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios	P01_M_OPTIMIZA	F01_M_OPTIMIZA	29.10	30.43	27.77	31.10
Definición de los activos por catálogo de servicios y accesos definidos	P02_M_OPTIMIZA	F02_M_OPTIMIZA	30.87	32.87	29.54	34.21
Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios	P03_M_OPTIMIZA	F03_M_OPTIMIZA	19.75	20.75	19.08	22.08
Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas	P04_M_OPTIMIZA	F04_M_OPTIMIZA	20.44	21.76	21.10	23.10
Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad	P05_M_OPTIMIZA	F05_M_OPTIMIZA	18.43	19.76	18.10	20.43
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P06_M_OPTIMIZA	F06_M_OPTIMIZA	17.56	18.89	16.89	19.56
Retención del riesgo basado en la gestión de servicios	P07_M_OPTIMIZA	F07_M_OPTIMIZA	15.49	16.32	16.32	17.99
Evitación del riesgo basado en la gestión de servicios	P08_M_OPTIMIZA	F08_M_OPTIMIZA	19.49	19.49	18.66	19.49
Transferencia del riesgo basado en la gestión de servicios	P09_M_OPTIMIZA	F09_M_OPTIMIZA	14.66	15.49	14.66	15.65
Aceptación del riesgo basado en la transición del servicio	P10_M_OPTIMIZA	F10_M_OPTIMIZA	14.00	14.66	14.67	14.66
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P11_M_OPTIMIZA	F11_M_OPTIMIZA	27.77	29.43	26.10	27.77

Tabla 3.2 Tabulación de resultados
(Elaborado por: Los Autores)

3.2.6 PRESENTACIÓN DE RESULTADOS

Del promedio de las puntaciones obtenidas, da como resultado la calificación de cada uno de los procesos de M_OPTIMIZA, los cuales reflejan la gestión de servicios de TI y gestión del riesgo de la seguridad de la información en la Institución de estudio, SENPLADES.

La Tabla 3.3, muestra el resultado de la evaluación obtenida.

Proceso M_OPTIMIZA	Código de proceso	Código de formulario	Promedio	Nivel	Semaforización
Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios	P01_M_OPTIMIZA	F01_M_OPTIMIZA	29.60	NIVEL BAJO	
Definición de los activos por catálogo de servicios y accesos definidos	P02_M_OPTIMIZA	F02_M_OPTIMIZA	31.87	NIVEL BAJO	
Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios	P03_M_OPTIMIZA	F03_M_OPTIMIZA	20.42	NIVEL BAJO	
Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas	P04_M_OPTIMIZA	F04_M_OPTIMIZA	21.60	NIVEL BAJO	
Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad	P05_M_OPTIMIZA	F05_M_OPTIMIZA	19.18	NIVEL BAJO	
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P06_M_OPTIMIZA	F06_M_OPTIMIZA	18.23	NIVEL BAJO	
Retención del riesgo basado en la gestión de servicios	P07_M_OPTIMIZA	F07_M_OPTIMIZA	16.53	NIVEL BAJO	
Evitación del riesgo basado en la gestión de servicios	P08_M_OPTIMIZA	F08_M_OPTIMIZA	19.28	NIVEL BAJO	
Transferencia del riesgo basado en la gestión de servicios	P09_M_OPTIMIZA	F09_M_OPTIMIZA	15.12	NIVEL BAJO	
Aceptación del riesgo basado en la transición del servicio	P10_M_OPTIMIZA	F10_M_OPTIMIZA	14.50	NIVEL BAJO	
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P11_M_OPTIMIZA	F11_M_OPTIMIZA	27.77	NIVEL BAJO	

Tabla 3.3 Resultados de evaluación
(Elaborado por: Los Autores)

Como conclusión podemos observar que los niveles de gestión para todos los procesos, se encentran en un “nivel bajo”, lo cual se contrasta con el inconvenientes presentados en la planificación y entrega de servicios TI, además de la falta de gestión de riesgos en la Institución.

3.2.7 VALIDACIÓN Y ANÁLISIS DE RESULTADOS

Con el fin de validar el puntaje obtenido se analizara cada proceso de M_OPTIMIZA y se realizará las debidas recomendaciones, en base a las fichas de los procesos establecidos en el modelo, de tal forma de obtener acciones a mediano y corto plazo.

No se trata o se sugiere acciones a largo plazo, debido a que el análisis se centra en contar con resultados rápidos y que permitan tratar los riesgos de mayor impacto, obtenido con esto una justificación práctica y valiosa ante la directiva para apalancar su implementación.

Proceso M_OPTIMIZA	Código de proceso	Código de formulario	Coordinador de Infraestructura Puntaje	Roles y responsabilidades	Medición de directrices generales	Indicadores	Ponderación
Formulación del contexto basado en el diseño, requisitos de seguridades de la información y mejora continua de servicios	P01_M_OPTIMIZA	F01_M_OPTIMIZA	Coordinador de Infraestructura	73.32	14.00	0.00	29.10
			Coordinador de Soporte	73.32	18.00	0.00	30.43
			Oficial de Seguridades	73.32	10.00	0.00	27.77
			Directora de la DITSI (s)	73.32	20.00	0.00	31.10
			Promedio	**73.32**	**15.50**	**0.00**	**29.60**
Definición de los activos por catálogo de servicios y accesos definidos	P02_M_OPTIMIZA	F02_M_OPTIMIZA	Coordinador de Infraestructura	64.00	12.00	16.67	30.87
			Coordinador de Soporte	64.00	18.00	16.67	32.87
			Oficial de Seguridades	64.00	8.00	16.67	29.54
			Directora de la DITSI (s)	64.00	22.00	16.67	34.21
			Promedio	**64.00**	**15.00**	**16.67**	**31.87**
Identificación de amenazas basados en las pruebas, eventos e incidentes del catálogo de servicios	P03_M_OPTIMIZA	F03_M_OPTIMIZA	Coordinador de Infraestructura	54.28	5.00	0.00	19.75
			Coordinador de Soporte	54.28	8.00	0.00	20.75
			Oficial de Seguridades	54.28	3.00	0.00	19.08
			Directora de la DITSI (s)	54.28	12.00	0.00	22.08
			Promedio	**54.28**	**7.00**	**0.00**	**20.42**
Identificación de vulnerabilidades y valoración de consecuencias en base a los requerimientos, gestión de cambios y el análisis de incidentes y problemas	P04_M_OPTIMIZA	F04_M_OPTIMIZA	Coordinador de Infraestructura	53.32	8.00	0.00	20.44
			Coordinador de Soporte	53.32	12.00	0.00	21.76
			Oficial de Seguridades	53.32	10.00	0.00	21.10
			Directora de la DITSI (s)	53.32	16.00	0.00	23.10
			Promedio	**53.32**	**11.50**	**0.00**	**21.60**
Estimación y evaluación del riesgo en base a los incidentes, probabilidad de ocurrencia y gestión de disponibilidad	P05_M_OPTIMIZA	F05_M_OPTIMIZA	Coordinador de Infraestructura	53.33	2.00	0.00	18.43
			Coordinador de Soporte	53.33	6.00	0.00	19.76
			Oficial de Seguridades	53.33	1.00	0.00	18.10
			Directora de la DITSI (s)	53.33	8.00	0.00	20.43
			Promedio	**53.33**	**4.25**	**0.00**	**19.18**
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P06_M_OPTIMIZA	F06_M_OPTIMIZA	Coordinador de Infraestructura	45.70	7.00	0.00	17.56
			Coordinador de Soporte	45.70	11.00	0.00	18.89
			Oficial de Seguridades	45.70	5.00	0.00	16.89
			Directora de la DITSI (s)	45.70	13.00	0.00	19.56
			Promedio	**45.70**	**9.00**	**0.00**	**18.23**
Retención del riesgo basado en la gestión de servicios	P07_M_OPTIMIZA	F07_M_OPTIMIZA	Coordinador de Infraestructura	44.00	2.50	0.00	15.49
			Coordinador de Soporte	44.00	5.00	0.00	16.32
			Oficial de Seguridades	44.00	5.00	0.00	16.32
			Directora de la DITSI (s)	44.00	10.00	0.00	17.99
			Promedio	**44.00**	**5.63**	**0.00**	**16.53**
Evitación del riesgo basado en la gestión de servicios	P08_M_OPTIMIZA	F08_M_OPTIMIZA	Coordinador de Infraestructura	56.00	2.50	0.00	19.49
			Coordinador de Soporte	56.00	2.50	0.00	19.49
			Oficial de Seguridades	56.00	0.00	0.00	18.66
			Directora de la DITSI (s)	56.00	2.50	0.00	19.49
			Promedio	**56.00**	**1.88**	**0.00**	**19.28**
Transferencia del riesgo basado en la gestión de servicios	P09_M_OPTIMIZA	F09_M_OPTIMIZA	Coordinador de Infraestructura	44.00	0.00	0.00	14.66
			Coordinador de Soporte	44.00	2.50	0.00	15.49
			Oficial de Seguridades	44.00	0.00	0.00	14.66
			Directora de la DITSI (s)	44.00	10.00	0.00	17.99
			Promedio	**44.00**	**3.13**	**0.00**	**15.70**
Aceptación del riesgo basado en la transición del servicio	P10_M_OPTIMIZA	F10_M_OPTIMIZA	Coordinador de Infraestructura	40.00	2.00	0.00	14.00
			Coordinador de Soporte	40.00	4.00	0.00	14.66
			Oficial de Seguridades	40.00	4.00	0.00	14.67
			Directora de la DITSI (s)	40.00	4.00	0.00	14.56
			Promedio	**40.00**	**3.50**	**0.00**	**14.47**
Comunicación y monitoreo del riesgo en base a la gestión del servicio	P11_M_OPTIMIZA	F11_M_OPTIMIZA	Coordinador de Infraestructura	73.32	10.00	0.00	27.77
			Coordinador de Soporte	73.32	15.00	0.00	29.43
			Oficial de Seguridades	73.32	5.00	0.00	26.10
			Directora de la DITSI (s)	73.32	10.00	0.00	27.77
			Promedio	**73.32**	**10.00**	**0.00**	**27.77**

Figura 3.2 Análisis de resultados por partes o componentes del formulario de aplicación
(Elaborado por: Los Autores)

La Figura 3.2, muestra los puntajes obtenidos por cada componente desarrollado en los formularios de aplicación, evidenciando que existe en todos los procesos un avance significante en la designación de “Roles y responsabilidades” en la mayoría de los procesos, lo cual ha permitido de cierta forma mantener la operación de los servicios de TI.

En este sentido las responsabilidades están definidas y se las ejecuta, pero en muchos de los casos son roles compartidos entre varios especialistas o en su defecto las actividades se las realiza de forma empírica, como parte de la operación propia de la los sistemas de información.

La siguiente figura corrobora lo antes mencionado y permite evidenciar el bajo nivel obtenido en los componentes de “Medición de Directrices Generales” e “Indicadores”. Este resultado tiene relación directa a la ausencia de la gestión de riesgo de la seguridad de la información en la Institución y por tanto de indicadores.

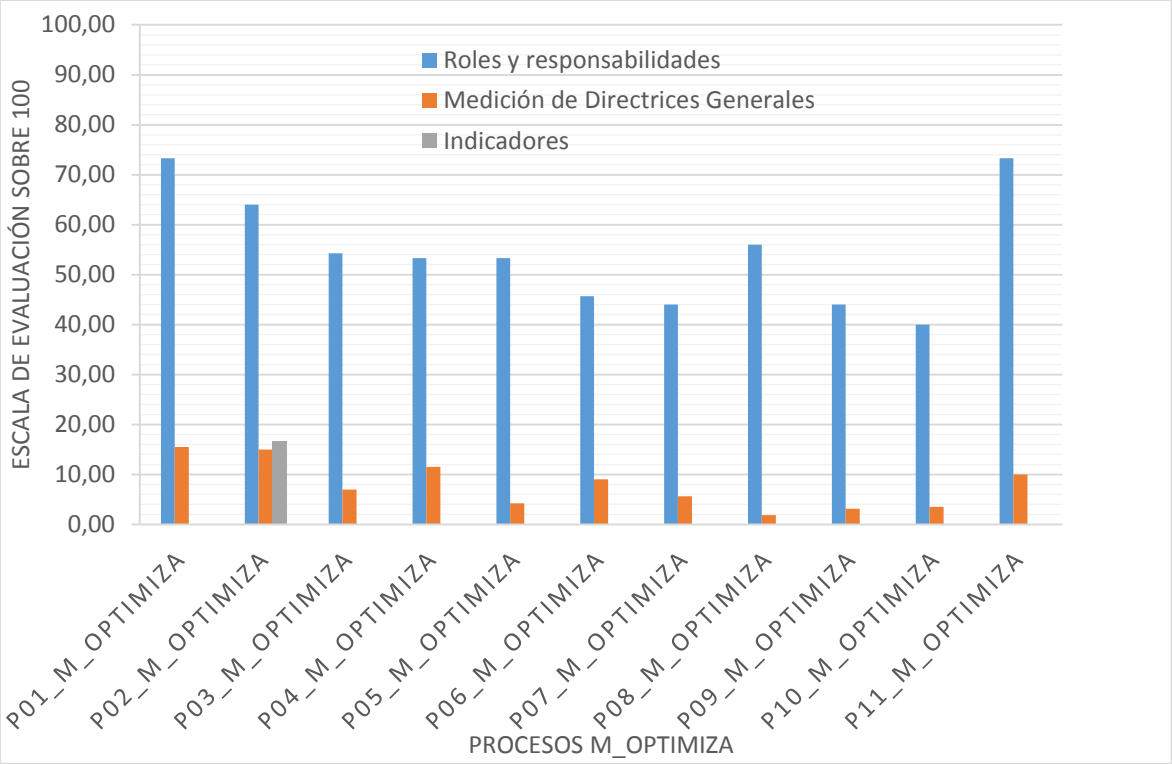


Figura 3.3 Resultados por componentes de cada formulario
(Elaborado por: Los Autores)

De forma general para todos los procesos de M_OPTIMIZA se tiene un *nivel bajo*, por lo cual se debe tomar las debidas acciones en base a las guías de implementación establecidas para cada proceso.

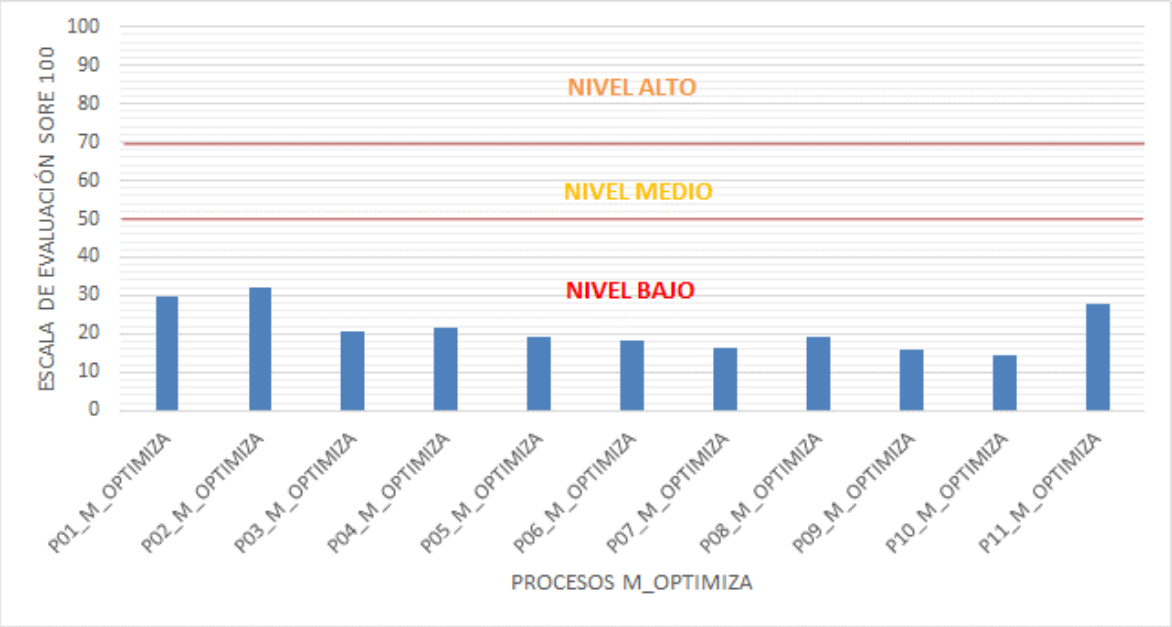


Figura 3.4 Resultados por proceso
(Elaborado por: Los Autores)

En base a los resultados presentados en la “Tabla 3.3 Resultados de evaluación” se sugiere aplicar las siguientes recomendaciones de mejora:

Niveles bajos o medios: requieren la definición de roles y responsables de cada proceso, trabajar en la Directrices Generales e Indicadores y efectuar las acciones de mejora en base a lo establecido en las Guías de Implementación, de las fichas P01_M_OPTIMIZA a la P11_M_OPTIMIZA del Modelo M_OPTIMIZA definidas en la sección 2.2 del modelo desprendible.

Altos, se consideran aceptables y se recomienda, mantener o mejorar los puntajes aplicando las Guías de Implementación y evaluando continuamente los resultados con los Formularios de Aplicación desde el F01_M_OPTIMIZA al F11_M_OPTIMIZA.

Al inicio se debe realizar aplicaciones con periodicidad más frecuente hasta obtener resultados aceptables y aceptados por la institución, para mantener el equilibrio en el desempeño de los procesos del Modelo M_OPTIMIZA.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1CONCLUSIONES

- El estándar ISO 27005 y el marco de referencia ITIL v3 son compatibles, ya que ambos contienen procesos en su estructura. Sin embargo, ITIL puede ser implantado de varias formas, mientras que la ISO 27005 es una guía de gestión de riesgos, que no proporciona una metodología y orden sugerido para su implementación.

- El método heurístico de ensayo-error, ha sido ejecutado en el mayor número de iteraciones necesarias, para definir el modelo óptimo de mapeo.

- La ISO 27005 fue la base para realizar el mapeo de servicios de ITIL, ya que estudia los activos de soporte o de tecnologías de la información, facilitando la relación entre las entradas, guías de implementación y salidas del mismo, con la estructura de procesos de ITIL.

- El mapeo entre la ISO 27005 e ITIL v3, ha sido realizado identificando los puntos comunes entre los procesos que los componen, y excluyendo del estudio al resto de sus componentes.

- La caracterización de los procesos del modelo M_OPTIMIZA, permitió identificar los elementos esenciales y necesarios para implementar el proceso y definir sus principales características, facilitando su entendimiento, gestión y control de interrelaciones en los formularios de aplicación.

- Los procesos han sido definidos con los subprocesos correspondientes o actividades, estableciendo los flujos que permitan a la organización implementar el modelo en la organización.

- La generación de indicadores, se ha realizado identificando las variables que se requerían medir en cada proceso y su frecuencia de medición.

- Como fase previa a la aplicación del modelo M_OPTIMIZA, se caracterizó la organización en estudio, para levantar sus características generales y particulares, específicamente en la organización y estructura de los procesos de TI.

- En la fase de aplicación, el ámbito se limitó inicialmente, así como la definición de los actores relevantes o dueños de los procesos, que permitieron obtener resultados confiables.

- Los tres niveles definidos para calificar el estado actual en el que se encuentre la organización en estudio, han sido establecidos para que en base a los estándares aceptados internacionalmente, la organización cuente con un puntaje aceptable cuando al menos alcance el 70%.

- El modelo de gestión M_OPTIMIZA, busca entregar una herramienta que garantice a las organizaciones, que al sacar el máximo provecho de su aplicación a través de mediciones continuas, mayor partido podrán obtener del mismo en cuando a los problemas tradicionales de la gestión de TI.

4.2 RECOMENDACIONES

- Es necesario que la organización cuente al menos con una estructura inicial de procesos, que aunque no tenga como base un marco de referencia de TI, tenga identificado los roles y responsabilidades en su estructura.

- La organización en la que se aplique el modelo M_OPTIMIZA, debe tener como meta la mejora continua de su capacidad y resultados, de forma que en cada medición periódicamente realizada, se identifique únicamente los puntos clave que se debe cambiar o mejorar.

- Es necesario que se identifique la estructura de las normas o marcos de referencia a ser mapeados, caso contrario, se puede llegar a varios ciclos de mapeo sin alcanzar los resultados deseados.

- Las organizaciones que apliquen el modelo M_OPTIMIZA, deben establecer una línea base que les permitirá partir para las siguientes mediciones.

- La aplicación debe obtener información útil para iniciar procesos de mejora continua, por lo que se recomienda que la información ingresada en los formularios de evaluación sea real y no pretenda ocultar el verdadero estado de la organización.

- Este estudio puede ser complementado con el desarrollo de herramientas de automatización de sus procesos y medición de los indicadores planteados.

- El modelo M_OPTIMIZA puede ser afinado, para lo que se recomienda su aplicación en empresas de diferentes tamaños y sectores, ya que inicialmente ha sido validado únicamente en una organización gubernamental.

- La gestión de riesgos en TI debe estar acompañada por los dueños de los procesos y de la información que se administra, ya que son ellos los que pueden determinar las amenazas reales a las que está expuesta su información.

- Se recomienda que en cada proceso se aplique el formulario a varios roles, en caso que se pueda realizar, ya que el promedio de resultados reflejará de mejor manera el estado real y diferentes puntos de vista de la organización.

- Es importante, que a más de establecer métricas, se logre definir metas que la organización busque alcanzar, para que se apliquen los procesos del modelo M_OPTIMIZA que estén directamente relacionados con las mismas.

REFERENCIAS BIBLIOGRÁFICAS

Internet:

Information Technology - Information Security – Information Assurance | ISACA. (n.d.). Retrieved from https://www.isaca.org/Pages/default.aspx

ITIL OFFICIAL WEBSITE. (n.d.). Retrieved from http://www.itil-officialsite.com/

ITIL® v3: Gestión de Servicios de TI. (n.d.). Retrieved from http://itilv3.osiatis.es/

NTE-INEN/ISO 27005:2005, INEN, 2012.

ITIL v3, "**Estrategia del Servicio**", "**Diseño del Servicio**", "**Transición del Servicio**", "**Operación delServicio**", "**Mejora Continua del Servicio**", ITIL.

Carl Young, "**Metrics and Methods for Security Risk Management**", Syngress Publishing, 2010.

ISACA, "**The Risk IT Framework**", ISACA, 2009.

Hayden Lance, "**IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data**", McGraw-Hill/Osborne, 2010.

Phillips Joseph, "**IT Project Management: On Track from Start to Finish, Third Edition**", McGraw-Hill/Osborne, 2010.