



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 1

Tabla de contenido

INTRODUCCIÓN	5
OBJETIVO	5
ALCANCE	5
DESCRIPCIÓN	5
1. ESTRATEGIA DEL SERVICIO	6
1.1 Entendimiento del cliente	6
1.2 Gestión del portafolio de servicios	6
1.3 Políticas de prestación de servicios	7
1.3.1 Definiciones	7
1.3.2 Prerrequisitos para operar el servicio	8
1.3.3 Niveles de servicio	8
1.3.4 Servicios de soporte al cliente	8
1.3.5 Privacidad y confidencialidad	9
1.3.6 Propiedad intelectual	9
1.4 Activos del servicio	10
1.5 Proveedores	10
1.6 Gestión financiera	10
1.6.1 Valor de aprovisionamiento	10
1.6.2 Valor potencial del servicio	11
1.7 Gestión de demanda	11
2. DISEÑO DEL SERVICIO	12
2.1 Proceso del servicio	12
2.2 Gestión del catálogo de servicios (SCM)	14
2.2.1 Catálogo de servicios técnicos	14
2.2.2 Catálogo de servicios de negocio	14
2.3 Gestión del nivel del servicio (SLM)	14
2.3.1 Acuerdos a nivel de servicio (SLA)	14
2.3.2 Modelo RACI (Responsible- Accountable – Consulted - Informed)	14



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 2

2.4	4Ps del diseño	15
2.5	Gestión de la disponibilidad	16
2.6	Gestión de la capacidad	16
2.7	Gestión de proveedores	16
2.8	Gestión de la seguridad de la información	17
2.8.1	Políticas para la gestión de la seguridad de la información	17
2.8.2	Informes de seguridad de T.I	18
2.8.3	Estrategia de seguridad	18
2.8.3.1	Seguridad de la información	18
2.8.3.2	Gestión de cuentas de usuario, de contraseñas y recomendaciones.....	19
2.8.3.3	Gestión de actualización de software	21
2.8.3.4	Gestión de copias de respaldo	22
2.8.3.5	Políticas ante riesgos naturales.....	22
2.8.3.6	Fallas eléctricas	23
2.8.3.7	Soporte técnico	23
2.8.3.8	Contemplación de ataques	23
2.8.3.9	Políticas de gestión de las telecomunicaciones y operaciones.....	23
2.8.3.10	Mantenimiento de políticas	24
2.8.3.11	Seguridad del personal.....	24
2.8.3.12	Políticas para el cumplimiento y normatividad legal	24
2.8.4	Advertencias de seguridad	25
2.8.5	Alerta de seguridad.....	25
2.9	Gestión de la continuidad de los servicios T.I.....	25
2.9.1	Inicio.....	25
2.9.2	Requisitos y estrategia	28
2.9.3	Implementación	28
2.9.4	Operaciones continuadas	28
3.	TRANSICIÓN DEL SERVICIO.....	29
3.1	Plan de transición y soporte	29
3.2	Gestión del cambio	30



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 3

3.3	Gestión de activos del servicio y configuración (SACM)	32
3.4	Sistema de gestión de la configuración (CMS)	32
3.5	Gestión de entregas y despliegues	32
3.6	Validación y pruebas del servicio	34
3.7	Evaluación del cambio	36
3.8	Gestión del conocimiento	38
3.8.1	Sistema de gestión del conocimiento del servicio (SKMS)	38
3.8.2	Biblioteca definitiva de medios (DML)	38
4.	OPERACIÓN DEL SERVICIO	39
4.1	Gestión de eventos	40
4.2	Gestión de incidentes	42
4.3	Cumplimiento de solicitudes	44
4.4	Gestión de problemas	46
4.4.1	Base de datos de errores conocidos (KEDB)	48
4.5	Gestión de acceso	48
4.6	Funciones	50
a.	Service Desk	50
b.	Gestión Técnica	50
c.	Gestión de Aplicaciones	50
d.	Gestión de operaciones de T.I.	51
5.	MEJORA CONTINUA DEL SERVICIO	51
5.1	Planificar, Hacer, Verificar y Actuar (PDCA)	51
5.2	Proceso de mejora	52
5.3	Medición del servicio	52
5.3.1	Retorno de la inversión	53
5.4	Preguntas de negocio	53
5.5	Requerimientos de nivel de servicio (SLR)	54
5.5.1	Plan de mejora del servicio	54
6.	Referencias	56



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 4

Listado de Figuras

Figura 1. Portafolio del servicio y su contenido [1]	7
Figura 2. Modelo funcional de servicio (ejemplo).....	12
Figura 3. Diagrama módulos que componen el servicio (ejemplo).....	13
Figura 4. Diagrama de relaciones entre los servicios y las dependencias.....	13
Figura 5. Proceso gestión de la continuidad	27
Figura 6. Proceso de gestión de cambio [6]	30
Figura 7. Proceso de gestión de entregas y despliegues [2]	33
Figura 8. Modelo V [6]	34
Figura 9. Flujo de validación y pruebas del servicio (Sugerido por: [2])	35
Figura 10. Ejemplo de pruebas y validación	36
Figura 11. Proceso para la evaluación de un cambio [5] [2]	37
Figura 12. Estructura DML [2].....	38
Figura 13. Procesos operación del servicio [2].	40
Figura 14. Proceso gestión de eventos (Sugerido por: [8])	41
Figura 15. Proceso de gestión de incidentes (modificado [8])	43
Figura 16. Proceso para el cumplimiento de solicitudes (modificado [8]).....	45
Figura 17. Proceso para la gestión de problemas (modificado [8]).	47
Figura 18. Proceso para la gestión de acceso [8]	49

Listado de Tablas

Tabla 1. Formato de valoración de servicio (Sugerido por: [1])	11
Tabla 2. Estructura matriz RACI	15
Tabla 3. Categorización de riesgos (Sugerido por:[1]	31
Tabla 4. Requisitos de nivel de servicio (sugerido por:[1])	54
Tabla 5. Formato 1 para iniciativas de mejora (Sugerido por: [1])	55
Tabla 6. Formato 2 para iniciativas de mejora (Sugerido por: [1])	56



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 5

POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA DE PRODUCTOS Y SERVICIOS TENIENDO COMO BASE EL MARCO DE REFERENCIA ITIL

INTRODUCCIÓN:

El área de desarrollo y proyectos T.I de la empresa Interlink S.A establece la política de entregables con el propósito de establecer pautas y modelos que se deben seguir y aplicar para un adecuado manejo de las cinco fases que conforman el ciclo de vida de los servicios T.I.

OBJETIVO:

La presente política tiene por objeto integrar todas las políticas que deben ser incorporadas en la división de desarrollo y proyectos T.I de la empresa INTERLINK S.A, con el fin de que se convierta en una herramienta de apropiación del sistema de gestión de los productos, servicios T.I e infraestructura mediante el debido proceso de divulgación y concientización.

ALCANCE:

Establecer los lineamientos y buenas prácticas de ITIL para la definición de las políticas debido a su orientación a la mejora de la gestión, prestación y administración de servicios T.I a través de las cinco fases del ciclo de vida del servicio:

1. Estrategia del servicio.
2. Gestión del servicio.
3. Transición del servicio.
4. Operación del servicio.
5. Mejora continua del servicio.

DESCRIPCIÓN:

Se establecen las siguientes políticas de acuerdo a su propósito en cada una de las fases del ciclo de vida del servicio, proporcionando el marco de lineamientos planteados en el alcance a fin de dar cumplimiento al objetivo propuesto:



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 6

1. ESTRATEGIA DEL SERVICIO [1]

1.1 Entendimiento del cliente:

- 1.1.1 Misión, visión y objetivos: Es necesario tener constituidos, de forma clara y a disposición de los Stakeholders la misión, visión y objetivos a nivel empresarial.
- 1.1.2 Organigrama estructural y funcional: Antes de entrar en el detalle del o de los servicios, a nivel empresa se debe dejar establecido los organigramas estructural y funcional esto para su fácil comprensión por parte de los Stakeholders

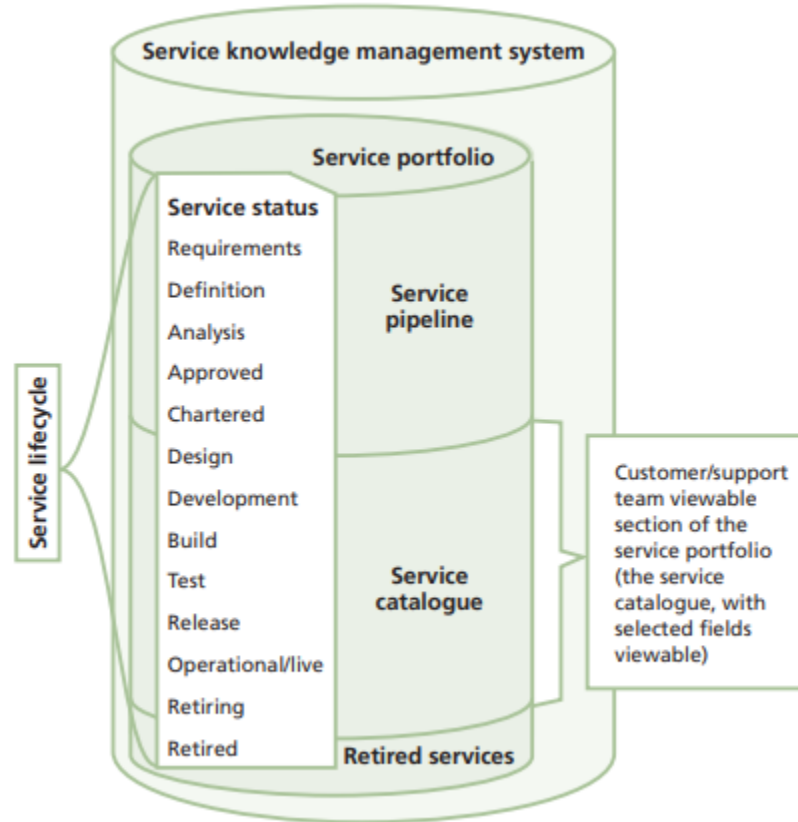
1.2 Gestión del portafolio de servicios:

Tiene como finalidad dar a conocer a los Stakeholders los servicios que se están ofertando y los servicios en los que se está trabajando y que están próximos a salir al mercado, es por ello que:

- 1.2.1 Se debe establecer el listado de servicios que alimenten la página de la empresa como parte del portafolio de servicios del área de desarrollo y proyectos T.I, esto teniendo como base el formato previamente establecido de **productos en explotación**.
- 1.2.2 Se debe incluir un apartado dedicado a los productos en desarrollo teniendo como base el formato **de inventario de proyectos**.
- 1.2.3 La gestión del portafolio de servicios debe contar con una adecuada clasificación de los diferentes servicios publicados, a fin de brindar orientación a los interesados sobre cuál es el servicio que se acomoda a sus respectivas necesidades. (eje: servicio de soporte y operaciones, servicios complementarios, servicios para la administración entre otros.).
- 1.2.4 Se debe incluir un formato en el cual se listen los servicios que por algún motivo estén fuera de operación o haya sido cancelado durante el proceso de desarrollo, junto con la debida justificación, evidenciando los motivos que llevar a tomar la decisión de cancelar el servicio. Lo anterior como política preventiva.

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 7

Figura 1. Portafolio del servicio y su contenido [1]



1.3 Políticas de prestación de servicios:

La empresa Interlink S.A y su división de desarrollo de software y proyectos T.I conforme a su responsabilidad, se compromete a brindar de forma integral los servicios que hayan sido contratados por terceros bajo los acuerdos de prestación de servicio o servicio que sean establecidos de forma individual.

1.3.1 Definiciones:

- **Servicio:** funcionalidad que es aprovechada por el cliente mediante plataformas software y móviles suministradas por la empresa proveedora.
- **Pago por el servicio:** pago establecido de forma periódica por el proveedor y en común acuerdo con el cliente por concepto del uso del servicio o en específico de las plataformas puestas a disposición.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 8

- **Licencias:** Contrato entre el proveedor del servicio sometido a propiedad intelectual y derechos de autos y el cliente, en donde se definen los derechos y deberes de ambas partes y adicionalmente se otorgan los correspondientes derechos de explotación ya sea de forma unilateral o en asociación.
- **Cuentas de usuario:** Hace referencia al conjunto “Usuario” y “Contraseña” otorgada a cada usuario mediante el cual podrá tener acceso al uso del servicio y plataformas (la asignación de credenciales depende del tipo de servicio y será realizado por medio de un registro individual ya sea mediante un tercero o directamente con la empresa).
- **Datos del cliente:** refiere a los datos personales del cliente que se almacenan en la plataforma de registro desde el primer acercamiento entre cliente y proveedor.

1.3.2 Prerrequisitos para operar el servicio:

Hacen referencia al listado de prerrequisitos que se debe entregar al cliente en el acuerdo de prestación de servicio para que el servicio adquirido opere de forma adecuada y optima. El listado de los prerrequisitos es individual para cada servicio, uno de los prerrequisitos que se podría llegar a tener es:

- **Acceso a conexión a internet:** el cliente debe contar con acceso a conexión a internet para poder disfrutar del servicio.

1.3.3 Niveles de servicio:

Durante la prestación del o los servicios, la empresa Interlink S.A y el área de desarrollo en su papel de proveedor se compromete:

- **Disponibilidad:** Se garantiza la disponibilidad del servicio 24/7 si el cliente por su parte cumple con todos los ítems del listado de los prerrequisitos establecidos.
- **Mantenimiento:** Como proveedores del servicio se garantiza el mantenimiento de las diversas plataformas periódicamente (como se establezca en el acuerdo o contrato) sin afectar la continuidad y disponibilidad del servicio.
- **Actualizaciones:** Se garantiza la actualización de los diversos servicios siempre y cuando involucren mejoras o funcionalidades adicionales que sean contratadas por el cliente o que sean autorizadas directamente por el proveedor a fin de mejorar la calidad en la prestación del servicio.

1.3.4 Servicios de soporte al cliente:

- **Aula virtual:** como parte de algunos servicios, el proveedor facilita al cliente el acceso a un aula virtual dedicada en donde encontrará el material necesario



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 9

(documentación y videos instructivos) para la capacitación sobre el uso de las plataformas.

- **Soporte telefónico:** el proveedor pone a disposición del cliente su servicio de soporte telefónico a cargo del área de atención al cliente para las diversas inquietudes, desde consulta por servicios ofertados hasta consultas por eventos específicos en servicios adquiridos.
- **Soporte presencial:** el proveedor pone a disposición del cliente su oficina y específicamente su centro de atención al cliente para consultas, dudas, resolución de problemas entre otros, por personal especializado.

1.3.5 Privacidad y confidencialidad:

La política de privacidad y confidencialidad se podrá encontrar en el siguiente enlace:

<http://www.gestion-ph.com/privacidad/>

1.3.6 Propiedad intelectual:

- El cliente reconoce que los productos, servicios, y sus derivados (plataformas web, aplicativos móviles, documentación, videos de capacitación, entre otros) se encuentran bajo la propiedad intelectual de la empresa **Interlink S.A.** El cliente se compromete a cuidar que los derechos de autor del proveedor sobre los productos, servicios y derivados mencionados, o sean violados por el cliente, su personal o terceros relacionados con la operación y manipulación.
- El cliente se compromete a comunicar al proveedor de forma inmediata si llegan a existir violaciones a los derechos de autor y sobre las cuales se tenga conocimiento.
- **Interlink S.A** tiene la potestad sobre los derechos de comercialización y distribución de los productos, servicios y sus derivados. El cliente no podrá de ninguna forma: 1. Transferir, vender, arrendar, syndicar, prestar, ni utilizar para alianzas de marca, actividades compartidas, entre otras, los productos, servicios y sus derivados sin la autorización de **Interlink S.A.** 2. Modificar, adaptar, traducir, preparar trabajos derivados, descompilar, realizar ingeniería inversa, desmontar o intentar obtener de algún modo el código fuente de alguno de los productos, servicios y sus derivados sin la autorización de **Interlink S.A.** 3. Eliminar, desconfigurar, ocultar o modificar las políticas o avisos de privacidad, confidencialidad y derechos de autor.
- **Interlink S.A** tiene bajo su potestad y se compromete a realizar una adecuada custodia de las bases de datos necesarias para el funcionamiento y operatividad de los diversos productos, servicios y sus derivados.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 10

- El cliente no podrá adquirir ningún derecho, título o interés contenido que exceptúe alguno o los derechos de propiedad intelectual que se expresan en la presente política.
- **Interlink S.A** mantendrá propiedad y derechos de propiedad intelectual de los productos, servicios y derivados, así como cualquier trabajo o mejora derivados de este. No obstante, el proveedor no es propietario de los Datos personales del cliente.
- Se establece que el equipo de desarrollo de la empresa Interlink S.A (programadores internos o externos) no son dueños del código fuente que sea producido.

1.4 Activos del servicio:

Para cada servicio o producto propio del área de desarrollo se debe realizar el diligenciamiento de los entregables de recursos y capacidades como parte de los activos del servicio, las características de los mismos se definen:

Entregable Recursos: Se debe realizar la definición de la infraestructura, información, aplicaciones, capital financiero y personal T.I necesario.

Entregable Capacidades: Se debe realizar la definición de la gestión, organización, procesos, conocimiento y personal T.I necesario.

1.5 Proveedores:

Definición de terceros responsables del suministro de bienes o servicios necesarios para lograr proporcionar el o los servicios T.I.

Entregable Proveedores: Se debe realizar una adecuada clasificación de los tipos de proveedores de servicios, es necesario hacer evidente en el entregable si se es proveedores de tipo 1 - servicio interno, tipo 2 - unidad de servicios compartidos o tipo 3- proveedores externos.

1.6 Gestión financiera:

Se establecen los lineamientos que permitan realizar una cuantificación exacta del valor de cada uno de los servicios que se ofertan actualmente, al igual que el valor de los activos que son demandados para la presentación de dichos servicios. Lo anterior con el fin de evaluar el rendimiento de los servicios en cuestión de costos y rentabilidad en cuanto a dos perspectivas:

1.6.1 Valor de aprovisionamiento:

Se debe realizar el adecuado diligenciamiento de los formatos: formato inventario



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 11

de licencias y servicios, formato inventario recursos físicos, hojas de especificación y formato inventario servidores privados virtuales para su posterior registro en las plataformas dedicadas. A partir de lo anterior se obtiene un valor promedio de consumo por cada servicio.

1.6.2 Valor potencial del servicio:

En la presentación del portafolio de servicio se debe hacer evidente el valor agregado de cada uno de los servicios ofertados al igual que en el valor monetario en la valoración del servicio.

A partir de lo anterior se debe obtener los datos necesarios para el diligenciamiento del siguiente formato (sugerido por [2]):

Tabla 1. Formato de valoración de servicio (Sugerido por: [2])

Servicio	Aprovisionamiento		Potencial	
	Concepto	Costo Mensual	Valor agregado	Monetización
S1	E1	CM1	VA1	VM1
	E2	CM2	VA1	VM2
Total: A+B		A= total suma CM		B= total suma VM
S2	E1	CM1	VA1	VM1
	E2	CM2	VA1	VM2
Total: A+B		A= total suma CM		B= total suma VM

1.7 Gestión de demanda:

Se debe realizar una adecuada evaluación y medición del cubrimiento de la demanda que tiene la división de desarrollo y proyectos TI con el fin de que no se presenten excesos o insuficiencia de capacidad para la atención de la demanda.

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 12

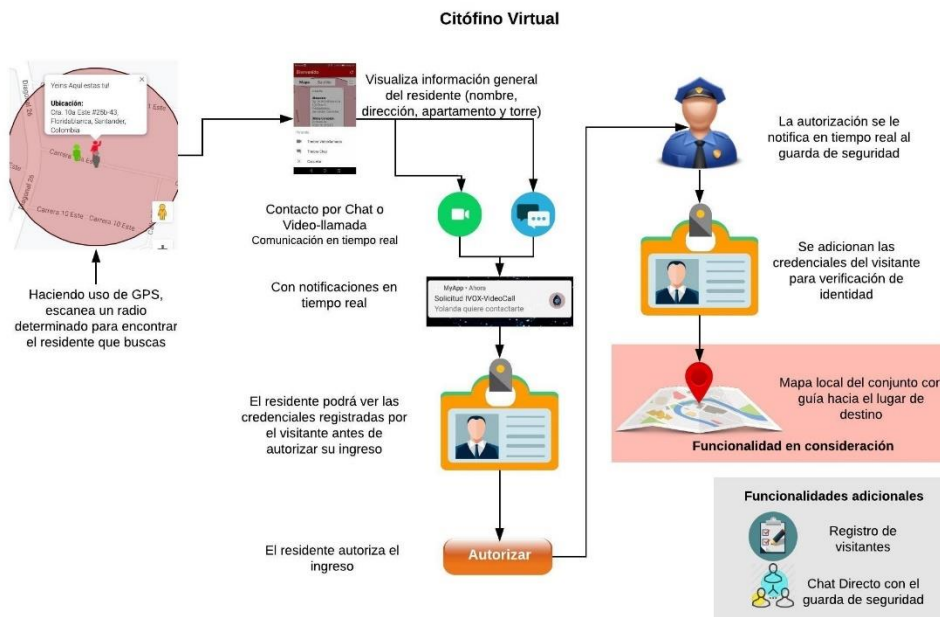
2. DISEÑO DEL SERVICIO [3]

Para el diseño de cualquier servicio que se pretenda ofertar se debe tener en cuenta la ejecución de los siguientes procesos:

2.1 Proceso del servicio:

Para cada servicio que se desee desarrollar una vez se diligencie el formato de inventario de proyecto junto con sus correspondientes requisitos, se debe realizar el diagrama de flujo del modelo funcional de la plataforma de forma gráfica, incluyendo el diagrama con los módulos que lo componen. Lo anterior para la identificación de aspectos críticos, actores que pueden llegar a intervenir en el desarrollo, trazabilidad del desarrollo, identificación de posibles inconvenientes de forma que en el proceso se presenten afectaciones en la calidad y disponibilidad (ejemplo *Figura 1* y *Figura 2*).

Figura 2. Modelo funcional de servicio (ejemplo)



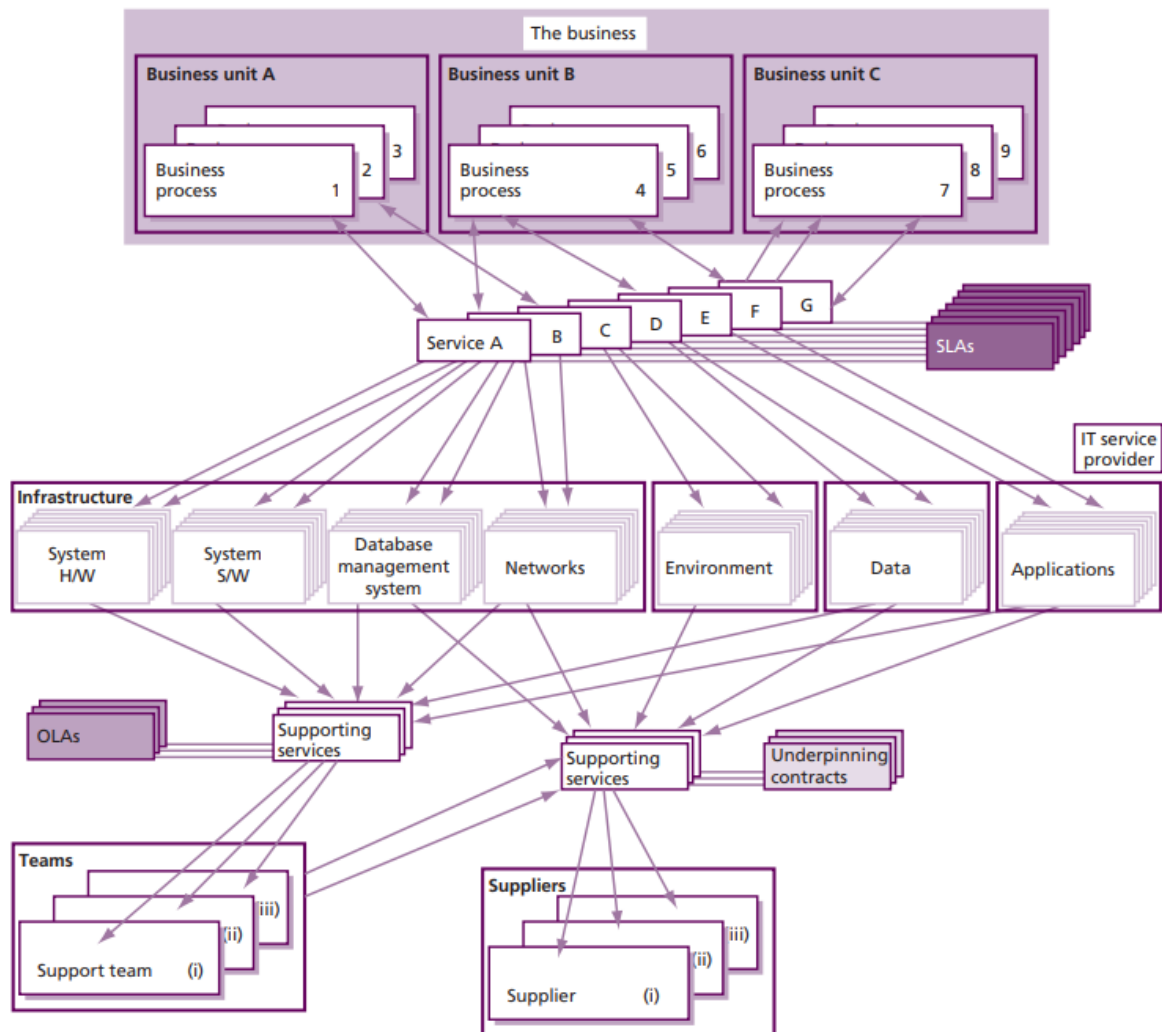
	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 13

Figura 3. Diagrama módulos que componen el servicio (ejemplo).



Se adiciona a modo de orientación el diagrama de relaciones del servicio y sus dependencias:

Figura 4. Diagrama de relaciones entre los servicios y las dependencias





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 14

2.2 Gestión del catálogo de servicios (SCM):

Se debe realizar el diligenciamiento del formato correspondiente al SCM en el cual se consiga la información relevante de todos los servicios que se están ofertando. Dicho formato se compone del catálogo de servicio a nivel técnico y el catálogo de servicios a nivel de negocio, cada uno se compone:

- 2.2.1 Catálogo de servicios técnicos: se consignan las especificaciones técnicas de cada uno de los servicios ofertados (formato inventario de proyectos y formato hojas de especificación).
- 2.2.2 Catálogo de servicios de negocio: Contiene los servicios en que se encuentran en explotación (se especifican dependencias de cada uno – formato de servicios en explotación).

2.3 Gestión del nivel del servicio (SLM):

2.3.1 Acuerdos a nivel de servicio (SLA):

los acuerdos a nivel de servicio entre Interlink S. A y el cliente se especifican, grosso modo, en las políticas de prestación de servicio en donde se definen las responsabilidades de ambas partes. Adicionalmente y con el objetivo de realizar aclaraciones y complementar la información presentada, se lista los componentes básicos del acuerdo:

- Propósito y objetivos
- Fechas
- Definiciones
- Prerrequisitos para operar el servicio
- Niveles de servicio
- Servicio de soporte al cliente final
- Política de privacidad y confidencialidad
- Periodo de vigencia
- Causales de cancelación de contrato
- penalidades
- Propiedad intelectual
- Limitación de responsabilidad
- Mora y no pago
- Resolución de reclamaciones
- Clausulas y otros compromisos
- Firmas

2.3.2 Modelo RACI (Responsible- Accountable – Consulted - Informed):



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 15

Matriz de asignación de responsabilidades para la organización y asignación de roles y responsabilidades en cada uno de los procesos ITIL. En la matriz de deben incluir el listado de los diversos procesos ITIL (listado que debe dirigir en cada Item a la descripción de cada proceso) por cada producto o servicios en el que se esté trabajando a fin de definir la participación del recurso humano en el mismo. Con el diligenciamiento del modelo RACI se espera poder establecer roles y responsabilidades, definir el equipo de trabajo que debe rendir cuenta por las tareas asignadas a producto o servicios, equilibrar las cargas de trabajo y controlar la ejecución de actividades.

NOTA: El modelo RACI debe ser diligenciado una vez el estado del proyecto esté en aprobado y asignado, el formato debe afrontar los roles y las actividades (*Ver tabla 2*).

Tabla 2. Estructura matriz RACI

Roles	Rol 1	Rol 2	Rol 3
Actividad			
A1	R		C
A2		I	R
A3	C	A	I

2.4 4Ps del diseño:

Teniendo como base las buenas prácticas de ITIL se establece la preparación y la planificación de los elementos conocidos como las 4Ps para una correcta implementación de la gestión de servicios:

- Personas: Se debe contar con el estudio de personas, habilidades y competencias involucradas en el suministro de los servicios ofertados.
- Procesos: Se debe tener conocimiento de los procesos, asignación de roles, actividades involucradas en la prestación de los servicios ofertados.
- Productos: Inventario de la tecnología y los sistemas de gestión usados en la prestación de los servicios T.I.
- Partners o Asociados: Se debe tener conocimiento de los Stakeholders o interesados, vendedores, fabricantes y proveedores con los que se cuenta para asistir y dar soporte a los servicios.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 16

2.5 Gestión de la disponibilidad:

Se debe evaluar, medir, monitorear y analizar los servicios definidos en el formato de productos en explotación con el fin de establecer y garantizar su estado en cuanto al nivel de disponibilidad requerido por el cliente de forma eficiente. Para generar el reporte correspondiente a la gestión según ITIL se debe seguir las siguientes actividades [2]:

- Análisis y evaluación de tiempos de incidencias y afectación a la disponibilidad.
- Planificar y diseñar nuevos servicios o realizar modificaciones a servicios existentes.
- Implementar medidas eficientes en cuestión de costos.
- Garantizar los niveles de disponibilidad y garantizar lo acordado con el cliente en este ámbito.
- Revisar las actividades proactivas junto al proceso de gestión de la capacidad con el objetivo de analizar los niveles de riesgo.
- Analizar y determinar los impactos en caso de fallos (diligenciar formato de fallos).
- Monitorizar, medir, analizar y generar informe de disponibilidad, archivar en plataforma dedicada.

2.6 Gestión de la capacidad:

Se debe evaluar la capacidad de cada uno de los servicios puestos en el formato de productos en explotación, de tal forma se pueda garantizar el cumplimiento de las necesidades actuales y futuras de los clientes. Para la realización de dicha valoración se debe tener en cuenta los requisitos establecidos en el SLA (Acuerdo de nivel de servicio) se deben seguir las siguientes actividades [2]:

- Análisis y planteamiento de ajustes, optimizaciones y mejoras de los servicios.
- Analizar el uso de los componentes actuales y estimar requisitos futuros.
- Análisis de la monitorización del servicio.
- Modelar y predecir el impacto de los cambios en los servicios ofertados.
- Explotación de nuevas tecnologías.
- Diseño de la capacidad.
- Gestión de la demanda.
- Medir, informa y revisar el rendimiento de los servicio y componentes.

2.7 Gestión de proveedores:

Se debe realizar una adecuada gestión y seguimiento de los contratos realizados con los diversos proveedores de servicios que se encuentran en el formato inventario de licencias y servicios, asegurando que por su parte los proveedores cumplan con los



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 17

debidos compromisos contractuales. Se debe monitorizar la relación calidad-precio en todos los contratos con proveedores. El proceso de gestión de proveedores según ITIL debe incluir [2]:

- Implementación de políticas para proveedores.
- Alimentación de base de datos con datos de proveedores.
- Categorización de proveedores (tener en cuenta el apartado de proveedores de la fase diseño del servicio).
- Evaluación de contratos.
- Negociación de contratos.
- Revisión, renovación y terminación de contratos.

Se establecen las siguientes fases como sugerencia de ITIL para el manejo del ciclo de vida del contrato con proveedores:

- Identificación de la necesidad de proveedor: Plantear los requisitos o pliego de oferta, preparar un caso de negocio inicial (Establecer los requisitos según la necesidad).
- Evaluación de proveedores: Establecer criterios de evaluación, seleccionar, evaluar, negociar, acordar y adjudicar contrato.
- Categorizar al proveedor
- Gestión de rendimiento de proveedor: gestionar y monitorear la operación y entrega del servicio.
- Terminación o renovación del contrato.

2.8 Gestión de la seguridad de la información:

Se establecen las siguientes prácticas a fin de garantizar la disponibilidad, integridad y confidencialidad de la información, para el manejo de una buena gestión de seguridad de la información ITIL:

2.8.1 Políticas para la gestión de la seguridad de la información: Se listan las políticas para la gestión de la seguridad de la información y adicionalmente se listan las políticas de seguridad correspondientes a otras áreas de interés. En el apartado de estrategias de seguridad se orienta sobre su correspondiente implementación:

- Seguridad de la información: Confidencialidad, integridad, disponibilidad, uso legítimo.
- Gestión de cuentas de usuario, de contraseñas y recomendaciones.
- Gestión de actualización de software.
- Gestión de copias de respaldo.
- Caracterización de la red.
- Acceso físico.
- Responsabilidades.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 18

- Gestión de cambios.
- Políticas ante riesgos naturales.
- Gestión de cambios.
- Mantenimiento de políticas.
- Contemplación de ataques.
- Mecanismos de seguridad (prevención, detección y recuperación).

2.8.2 Informes de seguridad de T.I: se debe seguir la guía de documentación para la realización de informes de seguridad los cuales deben proveer información sobre asuntos de la seguridad mediante la siguiente estructura:

- Responsable
- Inspección
- Diagnostico
- Condiciones y comprobación de los sistemas y servicios T.I
- Observaciones

2.8.3 Estrategia de seguridad:

Las políticas de seguridad tienen como objetivo, proporcionar directrices que soportan y orienten el proceso de seguridad T.I. en el área de desarrollo de la empresa, estas incluyen:

2.8.3.1 Seguridad de la información: Se debe garantizar la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por personal autorizado. Los tipos de acceso según el nivel de confidencialidad son:

Tipo público: Información que puede ser conocida y utilizada por cualquier tipo de persona, sea personal de la empresa o externo.

Tipo reservada – uso interno: Información que puede ser conocida y utilizada por todo el personal de Interlink y entidades autorizadas. La divulgación sin autorización de este tipo de información puede ocasionar riesgos o pérdidas de nivel bajo para la empresa.

Tipo reservada – confidencial: Información que solo puede ser conocida y de uso expreso por la división de desarrollo y proyectos TI, y sus respectivas unidades para la ejecución de su trabajo. Su divulgación o uso no autorizado puede ocasionar pérdidas significativas a la empresa o inclusive a terceros.

Tipo reservada -secreta: Información que solo puede ser conocida y utilizada por un equipo con permiso especial de la división de desarrollo y proyectos T.I y ejecutivos de la alta dirección de la empresa. Su divulgación o uso no autorizado puede ocasionar pérdidas graves a la empresa.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 19

- **Integridad:** Los activos de información no debe presentar alteración y debe estar completa. Las modificaciones que se realicen deben contar con su adecuado registro y firmas del personal que lo manipuló. Si la integridad se ve afectada los tipos de afectaciones pueden ser:
Nivel de afectación bajo: Información cuya modificación no autorizada puede ser reparada fácilmente y no afecta la continuidad de operaciones.
Nivel de afectación medio: Información que al ser modificada de forma no autorizada puede repararse, aunque puede ocasionar perdidas leves para la empresa.
Nivel de afectación alto: La información que se modificó de forma no autorizada es difícil de reparar y puede ocasionar pérdidas significativas para la empresa y para terceros.
Nivel de afectación grave: Información que al ser modificada de forma no autorizada no puede repararse, ocasionado pérdidas graves a la empresa y a terceros.
- **Disponibilidad:** Se debe garantizar el acceso a los activos de información tanto a personal autorizado como a terceros, según sea su nivel de acceso y sus permisos asignados. Si no se garantiza el acceso a la información se pueden presentar los siguientes casos teniendo en cuenta el análisis temporal:
Nivel de afectación bajo: información que al no estar disponible no afecta la continuidad de las operaciones y servicios de la empresa.
Nivel de afectación media: Información que al no estar disponible durante una semana puede ocasionar pérdidas significativas para la empresa.
Nivel de afectación alta: información que al no estar disponible permanentemente durante un día puede ocasionar pérdidas significativas a la empresa y a terceros.
Nivel de afectación grave: Información que al no estar disponible permanentemente durante una hora puede ocasionar pérdidas significativas a la empresa y a terceros.
- **Clasificación:** Se debe asignar a los activos de la información una clasificación que especifique su nivel de criticidad según el nivel de afectación que puedan llegar a presentar:
 - Criticidad Baja
 - Criticidad Media
 - Criticidad Alta

2.8.3.2 Gestión de cuentas de usuario, de contraseñas y recomendaciones:



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 20

- **Perfiles de usuario:** Se debe realizar la respectiva creación y clasificación de usuarios, asignado privilegios de acuerdo al nivel de responsabilidad, actividades o dependencia, unidad o área a la que pertenezca. La creación debe incluir: abreviatura del área a la que pertenece, abreviatura de la unidad a la que pertenece, abreviatura de nombre y categoría de nivel de acceso o permisos.
- **Administración de cuentas de usuario:** Se debe designar a una persona encargada de realizar la administración de cuentas de usuario en la división. El administrador de cuentas de usuario es el encargado de designar las cuentas de usuarios con identificadores únicos (evitando la existencia de múltiples perfiles de acceso para el mismo empleado).
Debe verificar que el usuario cuente con la respectiva autorización para el uso de los sistemas de la división, dar a conocer en detalle los derechos de cada usuario con su perfil (el usuario debe aceptar las condiciones que le sean presentadas).
El administrador debe mantener un registro formal de todas las personas internas y externas que usen los servicios.
Cancelar de forma inmediata los derechos de acceso a personal designado a otras tareas o a usuarios que cambiaron los servicios, también a aquellos que se les revoca el acceso o se desvincularon de la empresa. Las cuentas se inhabilitan y llevan más de 30 días inactivas.
Las excepciones deben ser justificadas y aprobadas.
Se deben incluir cláusulas en contratos de personal y de servicios que incumplan con los protocolos de acceso.
- **Administración de privilegios:** los privilegios deben ser limitados y controlados, en este contexto los privilegios deben:
Ser identificados en asociación a los componentes del sistema tanto de la división como del servicio.
Asignar privilegios sobre la base de la necesidad de uso y evento.
Los privilegios asignados deben contar con autorización y registro.
- **Cuentas de usuarios especiales para administrador de servidores:** Se deben crear cuentas de usuario específicas y con permisos especiales para personal que manipule los servidores.
- **Nombres de cuentas de usuario:** La asignación de cuentas no debe ser arbitraria y debe reflejar el cargo o dependencia a la que pertenece.
- **Asignación de contraseñas:** Se deben asignar contraseñas a cada usuario y luego éste la debe cambiar y dejar constancia de ello en una bitácora personal.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 21

- Responsabilidad de las credenciales de acceso: Se designa a cada usuario como responsable del usuario y contraseña asignada y de las operaciones que con ellas se realicen.
- Confidencialidad de las credenciales de acceso: Las credenciales de acceso son personales e intransferibles.
- Confiabilidad de las contraseñas: se establece una longitud mínima de ocho caracteres y adicionalmente deben contar con una letra mayúscula, y un número o grupo de números.

El almacenamiento de contraseñas y general de credenciales, deben estar almacenadas en sistemas protegidos.

Se suspende o se bloquea permanentemente al usuario luego de tres intentos de entrar con una contraseña incorrecta, posteriormente debe pedir el restablecimiento de contraseñas.

Impedir la reutilización de contraseñas.

- Responsabilidades de usuario:
Los usuarios son responsables de usar de forma adecuada sus credenciales de usuario y de seleccionar la contraseña según los parámetros establecidos (fáciles de recordar y no puedan ser deducidas fácilmente).
Notificar ante cualquier incidente de violación a la seguridad de los activos.
- Cambio de contraseñas: se establece una frecuencia mensual para el cambio de contraseñas, se solicita cambio de contraseña cuando existan indicios de violaciones por terceros.
- Cifrado simétrico: Las claves son almacenadas con cifrado simétrico garantizando confidencialidad y autenticación segura.
- Sistemas: Se recomienda la implementación de sistemas de IDS (sistema de detección de intrusiones SNORT) y sistemas de no repudio para proteger que cualquiera de las entidades que participen en una comunicación nieguen que el intercambio ha ocurrido, se protege a los usuarios de la comunicación contra amenazas de un usuario legítimo más que de atacantes (repudio de origen y de destino).

2.8.3.3 Gestión de actualización de software:

- Licencias: se deben adquirir las licencias con el debido proceso legal y actualizarlas cada vez que el proveedor lo disponga.
- Actualizaciones de componentes: Se debe realizar las actualizaciones de los componentes de servidores y demás componentes que lo requiera cada vez que sea necesario y el proveedor lo disponga.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 22

- Actualizaciones de seguridad: Aplicar los parches de seguridad a los sistemas a los sistemas operativos, servidores y demás componentes que lo requieran programados en calendario por el personal designado.
- Disponibilidad de servicios e información: Verificar y deshabilitar aquellos servicios que no se requieren, determinar una ubicación central para archivos de configuración del sistema.
- Archivos de configuración: Restringir el acceso a algunos archivos de configuración y restringir el acceso a IP que se detecten como sospechosas.
- Otras determinaciones: Instalación de Firewalls, detectores de troyanos, virus, spam y phishing.

2.8.3.4 Gestión de copias de respaldo:

- Copias de respaldo: El equipo perteneciente a la unidad de copias de seguridad son los responsables de realizar dicha tarea sobre los diversos recursos y bases de datos. Se deben realizar pruebas periódicas de la integridad de los backups. Las copias de seguridad copias de seguridad del sistema deben ser completas y para mayor seguridad, almacenadas de forma externalizada.
- Recuperación de información: en caso de presentarse algún problema o incidente extraordinario que comprometa los activos de información, la unidad a la que pertenezca el recurso o activo, debe realizar su correspondiente recuperación dentro de las siguientes 24 horas como máximo (durante el proceso de recuperación se deben implementar los planes de contingencia necesarios).

2.8.3.5 Políticas ante riesgos naturales:

- Se debe contar con el equipo de protección contra incendios. Mantenimiento de políticas.
- Tener duplicidad de los principales equipos que sostienen el funcionamiento y operación de los servicios, además de instaladores de software.
- Instalar sistemas de detección y extinción de incendios que cumplan con la normatividad de protección.
- En caso de que el riesgo ante calamidades naturales sea alto, se debe considerar construir o adaptar una sala de servidores como habitación segura, utilizando un diseño de Federal Emergency Management Agency. La publicación de FEMA "Tomar refugio de la tormenta: edificio un seguro habitación para su inicio o Small Business" proporciona las especificaciones y planos de construcción. Esto no sólo proteger sus servidores, sino proporcionar un lugar seguro para los empleados cuando amenazan peligros naturales.
- Se debe establecer un plan de seguridad en el que se incluya tiempo y recursos, topología de la red y servicios, especificación de funciones.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 23

2.8.3.6 Fallas eléctricas:

- Se debe usar protectores de sobretensión, baterías u otras fuentes de energía de reserva.
- Evitar supresores transitorios de sobretensión, ya que pueden dañar los servidores.
- Elegir protección de baja tensión de paso y evitar frecuencias de sobretensión.

2.8.3.7 Soporte técnico:

Asignar un equipo de ingenieros encargados de realizar con cierta frecuencia (programada en calendario), el soporte técnico de los elementos hardware de la red (reemplazo de partes defectuosas, hacer efectivas las garantías). Se debe realizar la debida instalación configuración, actualización y mantenimiento de los equipos hardware (se debe dejar registro de las operaciones realizadas y control de inventario).

2.8.3.8 Contemplación de ataques:

- Determinar causas de inseguridad.
- Clasificar ataques.
- Identificación de ataques pasivos y activos.
- Identificar tipos de atacantes, software malwares, virus y otros.

2.8.3.9 Políticas de gestión de las telecomunicaciones y operaciones [4]:

Adicionalmente de los servicios y la información, se establecen controles para garantizar la seguridad y el correcto funcionamiento operativo de los equipos o dispositivos de tratamiento de la información.

- Se debe contar con la adecuada documentación de procedimientos y responsabilidades en cada ambiente tecnológico. Dicha documentación debe incluir información detallada de instrucciones para la ejecución del procesamiento y manejo de la información, requerimientos de programación de procesos, instrucciones para el manejo de errores y excepciones, restricciones en el uso de equipos o programas, reinicios del sistema y recuperación ante fallas del sistema.
- Se deben documentar procesos de instalación y mantenimiento de equipos, plataformas de procesamiento, gestión de servicios, resguardo de la información, gestión de incidentes, reemplazo y cambios de equipos, entre otros.
- Se deben establecer mecanismos de protección contra software malicioso, mantenimiento y administración de la red, y seguridad de los medios de almacenamiento e intercambio de la información.
- Reporte de incidentes:
- Los incidentes relacionados con la vulnerabilidad de la seguridad de la información deben ser reportados a la unidad de soporte correspondiente. Si



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 24

existe vulnerabilidad, el reporte debe ser socializado ante los involucrados directamente y posteriormente deben ser informados sobre el manejo que se le está dando al incidente.

- Los incidentes pueden ser clasificados en las siguientes categorías [4]: Acceso no autorizado, Modificación de recursos no autorizado (plagio, base de datos), uso inapropiado de recursos (divulgación) y no disponibilidad (DOS).
- Se debe establecer la prioridad del incidente.
- Tratamiento de incidentes: Una vez el incidente se reporte es necesario recolectar y presentar evidencias para la clasificación y priorización del mismo, se debe proceder a tomar decisiones y ejecutar acciones sobre el incidente, se debe documentar el proceso correspondiente y archivar en lecciones aprendidas, si es necesario se debe realizar contención del incidentes para evitar daños potenciales en la información o arquitectura T.I, se debe verificar la erradicación total del incidente, finalmente se documenta la evaluación del manejo del incidente y el cierre del mismo.

2.8.3.10 Mantenimiento de políticas:

- Auditorías internas: Se deben establecer la frecuencia con la que se deben llevar a cabo la evaluación de las políticas de seguridad y determinar su grado de cumplimiento.
- Auditorías externas: se debe llevar a cabo al menos una auditoría externa anual basada en riesgos, se deben tomar decisiones y adoptar medidas pertinentes y actualizaciones de las políticas de seguridad.

2.8.3.11 Seguridad del personal:

- Formación en materia de seguridad: Dar lecciones al personal en torno a temas de seguridad de manejo de activos y la infraestructura.
- Cláusulas de confidencialidad: Imponer al personal que lo requiera, la cláusula de confidencialidad para garantizar la no divulgación de información concerniente a la red de la empresa.
- Reporte de incidentes: Se debe dar a conocer la plataforma para registro de cualquier tipo de incidentes que ocurra en cualquier bloque del servicio o de la infraestructura, para su correspondiente análisis y acción.
- Monitorización del personal: tener vigilancia, control y evaluación de las actividades desarrolladas por el personal.
- Capacitaciones: Se deben realizar capacitaciones a personal de la empresa sobre aspectos de seguridad de los activos y de la infraestructura.

2.8.3.12 Políticas para el cumplimiento y normatividad legal: Se deben realizar los adecuados controles para prevenir incumplimiento de normativas o leyes penales o



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 25

civiles, de las obligaciones reglamentarias o contractuales. Se debe garantizar el cumplimiento explícito de la normatividad vigente en cuanto a derechos de propiedad intelectual, privacidad y confidencialidad de información, uso inadecuado de recursos, entre otros.

2.8.4 Advertencias de seguridad:

Para cada uno de los servicios expuestos en el inventario de productos en explotación, se debe listar las posibles vulnerabilidades con el fin de que se establezcan medidas preventivas.

2.8.5 Alerta de seguridad:

Se debe realizar un análisis periódico en el cual se logren conocer aquellos sitios inseguros o personal que pueda poner en riesgo la política de seguridad de la información.

2.9 Gestión de la continuidad de los servicios T.I:

Con el fin de garantizar la continuidad y llegado al caso la recuperación del servicio (sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, entornos, soporte técnico, centros de servicios, entre otros) se debe realizar la implementación del siguiente ciclo:

2.9.1 Inicio:

Definición de la política

Se definen los lineamientos que se deben seguir, antes, durante y después de una interrupción en las operación de los servicios, sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, entornos entre otros, de tal forma que respondan de forma adecuada y oportuna ante los diversos eventos que se puedan llegar a presentar en la empresa, así como gestionar de forma adecuada la continuidad y restauración de sus correspondientes procesos afectando de forma mínima las operaciones.

Para la implementación de la presente política es necesario tener la adecuada documentación de cada uno de los apartados presentes en cada una de las fases del ciclo de vida del servicio, por ejemplo, es necesario contar con detalles de la arquitectura T.I, diagrama funcional del servicio y sus módulos, documento en donde se especifiquen las funciones y responsabilidades, los diagramas de flujo para el manejo de incidentes y problemas, registro de incidentes, la base de datos de incidentes registrados, entre otros.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 26

Para el mantenimiento de la continuidad de los servicios se deben tener en cuenta los siguientes planes:

- Respuesta inicial: plan en donde se evalúan los daños, establecer el impacto y se determina en que punto del servicio se presenta la interrupción, el incidente o problema.
- Recuperación del servicio: Se efectúan los planes de ejecución en donde se pretende recuperar el servicio en el menor tiempo posible.
- Prestación de servicio en circunstancias anormales: Se establecen medidas provisionales para garantizar la continuidad del servicio, se evalúa la posibilidad de reubicar los servicios o utilizar equipos de repuesto según sea el caso. Esta es una medida temporal para proporcionar un servicio limitado hasta que se pueda reanudar el servicio normal.
- Reanudación normal del servicio: volver al servicio habitual, recuperación tras ejecutar las acciones de recuperación del servicio y tras la entrega anormal del servicio.

Principios para la gestión de la continuidad del servicio:

- Proteger: Aplicar las políticas de seguridad de la información de eventualidades como incidentes, fallas, problemas e interrupciones al proteger o mantener seguros los servicios de forma que se pueda mejorar los niveles deseados de disponibilidad.
- Detectar: Detectar los incidentes lo más pronto posible para minimizar el impacto de dichas eventualidades en el servicio.
- Reaccionar: Tener la capacidad de reaccionar de la forma más adecuada de tal forma se pueda conducir a una recuperación eficiente y reducir el tiempo de la inactividad, evitando que la eventualidad se convierta en un problema mayor.
- Recuperar: Identificar e implementar una estrategia de recuperación adecuada, garantizando de forma oportuna la reanudación del servicio. Se deben establecer prioridades para recuperar los servicios más críticos.
- Operar: Se ejecutan los planes de recuperación.
- Restaurar: Diseñar una estrategia que permita después de implementar los planes de recuperación volver a la prestación de servicios con normalidad.

Elementos clave de los servicios que se pueden ver afectados o involucrados al mantener la continuidad del servicio:

- Personal
- Entorno físico
- Tecnología: incluyen servidores, dispositivos de almacenamiento, equipos de cómputo, equipos de red, conexiones de red, servicio de voz, enrutadores y los diferentes softwares. Para definir estrategias se debe considerar el acceso



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 27

remoto a los sistemas, requisitos de enfriamiento, requerimientos de energía, conectividad y enrutamiento redundante, niveles de automatización y la conectividad de proveedor subcontratado u otros enlaces externos ante eventualidades.

- Datos: Se debe tener como base la política de seguridad de la información teniendo en cuenta el almacenamiento de los datos, respaldos apropiados, mecanismos seguros de restauración, medios de transmisión seguros, entre otros. Externalización de información.
- Procesos
- Proveedores de servicios

Figura 5. Proceso gestión de la continuidad



Diligenciamiento de formatos: Como parte del proceso de acciones preventivas para el mantenimiento de la continuidad del servicio, se realizar el diligenciamiento de los siguientes formatos:

- Matriz de riesgos.
- Lecciones aprendidas
- Matriz de vulnerabilidades
- Formato de efectos de interrupción de servicio (primeras 24 horas, entre 24 y 48 horas, una semana, más de dos semanas).



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 28

- Requisitos de recursos para la recuperación (tiempos analizados en el formato anterior, personal requerido, relocalización necesaria si-no, recursos requeridos, información requerida).
- Formato de funciones críticas (unidad o módulo, personas a cargo, funciones críticas, tiempo objetivo de interrupción, necesita escalamiento, tiempo estimado de reanudación de funciones sin afectación).
- Formato de clasificación de eventualidad (menor, significativa y mayor).

Después de la recuperación del servicio: Cuando se restaure el servicio con normalidad, se debe documentar todo el proceso bajo la guía de documentación establecida y se debe almacenar en la KEBD para el manejo de futuras interrupciones similares.

2.9.2 Requisitos y estrategia: los requisitos y estrategias van ligados a las políticas de seguridad establecidos en el inciso anterior siguiendo el siguiente proceso:

- a. Análisis de impacto: se debe realizar un adecuado estudio, de tal forma que se pueda determinar el impacto que una interrupción de los servicios T.I, sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, entornos y otros, puedan tener sobre la empresa. En el caso del servicio se deben analizar factores como: 1. Pérdida de rentabilidad, 2. Pérdida de cuota del mercado, 3. Mala imagen de marca, 4. Otros.
- b. Identificación y estimación de riesgos.
- c. Identificación de amenazas.
- d. Acciones mitigadoras.

2.9.3 Implementación: Se deben realizar controles periódicamente con el fin de reducir los efectos de las interrupciones y de forma paralela proteger los procesos esenciales contra averías o siniestros mayores. De igual forma los procesos van ligados a las políticas de seguridad en referencia a los planes de prevención de riesgos, gestión de emergencias y planes de recuperación.

2.9.4 Operaciones continuadas:

- a. Formación: Se debe brindar una formación adecuada del personal involucrado en cuanto a los planes de prevención y recuperación. Se deben realizar simulacros a fin de capacitar al personal ante diferentes tipos de desastres. Adicionalmente se debe facilitar la documentación necesaria de políticas de seguridad en la página oficial de la empresa.
- b. Actualización y auditorías: Periódicamente se debe actualizar políticas, estrategias y planes. Llegado el caso, si se realizan cambios en la

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 29

infraestructura T.I o planes de negocio y comercialización, es necesario realizar las correspondientes auditorias para evaluar las nuevas situaciones.

3. TRANSICIÓN DEL SERVICIO [5]

Es necesario asegurar que se tenga claridad en cuestión de administración y expectativas de negocio sobre todos los proyectos, servicios y sus derivados tanto nuevos, como modificados, cancelados o diferidos. Para ello se definen según ITIL los siguientes procesos:

3.1 Plan de transición y soporte:

Se debe definir para cada servicio T.I del área de desarrollo su correspondiente clasificación según sea el tipo de **liberación**, con el fin de garantizar que los problemas, riesgos y desviaciones que se presenten en la transición del servicio sean reportados de forma oportuna a los interesados y se tomen a tiempo las decisiones sobre los mismos. Para ello se tienen los siguientes tipos de liberaciones:

- a. Liberación mayor: Se asigna cuando el producto, servicio o derivados contienen gran cantidad de nuevas funcionalidades. En este caso se puede orientar por el sistema de versiones establecido en el formato de inventario haciendo referencia a la versión mayor que como el tipo de liberación mayor, reemplaza liberaciones menores o de emergencias.
- b. Liberación menor: Se asigna cuando el producto, servicio o derivados contiene mejoras o arreglos más pequeños. En el formato de inventario se encuentra como versión menor.
- c. Liberación de emergencia: Se asigna cuando se realizan correcciones sobre errores o mejoras de alta prioridad. En el formato de inventario se asocia con la versión de revisión.

Adicionalmente para cada producto, servicio y derivados, se debe aplicar la siguiente estructura para el manejo de la transición en el formato correspondiente orientado por la guía de documentación:

1. Estrategia de la transición: Se define el enfoque de la transición, se asignan recursos y se clasifica según el tipo de liberación (objeto de la transición, contexto e interesado).
2. Preparación para la transición: Se definen las actividades de revisión y se establecen criterios de aceptación (revisar y aceptar entradas, criterios de aceptación y se realiza la revisión).
3. Planeación y coordinación de la transición: Se describen las tareas y actividades para la implementación del tipo de liberación.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

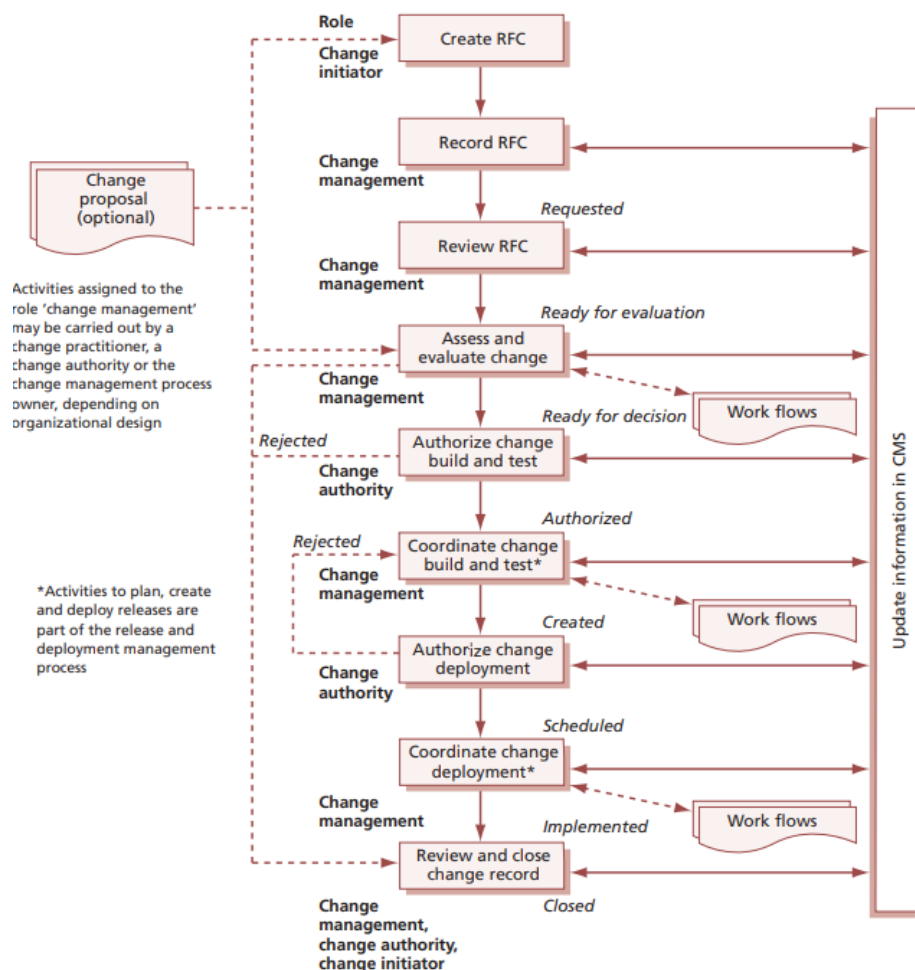
Página: 30

3.2 Gestión del cambio:

Para gestionar los cambios (modificaciones, adiciones, eliminaciones, entre otras) de los productos, servicios y sus derivados, siguiendo las recomendaciones de ITIL se debe tomar como referencia el siguiente diagrama de flujo para la ejecución de actividades que enmarcan la gestión y facilitan el seguimiento y proceso del ciclo de vida del cambio (Ver Figura 4). El proceso de documentación del ciclo que se muestra en el diagrama se debe hacer bajo la **guía de documentación** ya conocida, teniendo una adecuada trazabilidad de todos los cambios que se realicen.

NOTA: RFC hace referencia a las solicitudes de cambio, pueden ser realizadas individualmente o por unidad de trabajo y deben quedar registradas con el formato de solicitudes de cambio con identificador único que a su vez refiera a la documentación del ciclo.

Figura 6. Proceso de gestión de cambio [6]



En la creación de la RFC se debe especificar quién solicita el cambio, cuál es la razón de ser del cambio, que retorno o utilidad se espera que tenga, se deben identificar los posibles riesgos, se deben listar los recursos necesarios y se debe asignar el recurso humano que requiera. Los riesgos a los que se hagan referencia deben ser categorizados para su posterior estudio mediante la siguiente matriz de riesgos:

Tabla 3. Categorización de riesgos (Sugerido por: [6])

Categorización de Riesgos		
Impacto	Categoría 2	Categoría 1
	Alto Impacto	Alto Impacto
	Baja Probabilidad	Alta Probabilidad
	Categoría 4	Categoría 3
	Bajo Impacto	Bajo Impacto
	Baja Probabilidad	Alta Probabilidad
Probabilidad		

Posterior a ello en la documentación se deben categorizar los RFC por tipo de prioridad a partir de su impacto y su nivel de urgencia en cuanto a tiempo, estas pueden ser:

1. Prioridad inmediata: requiere intervención inmediata pues tiene impacto directo en la continuidad y prestación del servicio.
2. Prioridad alta: Cambio relacionado con la corrección de algún tipo de falla que afecta la continuidad y el correcto funcionamiento del servicio.
3. Prioridad media: Cambio en donde su impacto no es de gran magnitud pero que se debe dar solución en un periodo máximo de 15 días.
4. Prioridad baja: es un cambio que se puede manejar en largo periodo de tiempo pues no es de gran relevancia.

Posterior a la documentación requerida, las RFC deben contar con una adecuada revisión y aprobación formal (autorizada, denegada o incompleta) por parte del llamado CAB (comité Asesor de Cambio) que puede estar conformado por el líder de la unidad y el grupo encargado del producto o servicio; llegado al caso si la solicitud es rechazada se debe especificar el motivo de la decisión y se establecerá un periodo máximo de 15 días para la apelación. Finalmente, como se mencionó anteriormente, con el fin de llevar la trazabilidad de los cambios, se debe documentar en el formato de cambios la siguiente información:



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 32

- Id del cambio
- Nombre del cambio
- Fecha de aprobación formal
- Aprobación formal

3.3 Gestión de activos del servicio y configuración (SACM):

Se establece para cada producto, servicio y derivados a partir del formato de inventario de proyectos, VPS, hojas de especificación e infraestructura un modelo lógico de los mismos con sus respectivos activos (orientados por el diseño del servicio) y las relaciones que existen entre ellos (elementos de configuración, infraestructura, funcionalidades compartido(a)s de mayor relevancia). Para mayor claridad en el diseño de dicho modelo lógico se debe considerar la integración de los siguientes elementos de configuración (CIs):

- Ciclo de vida del servicio: Elementos de configuración que pueden ser orientados por los esquemas establecidos en el diseño del servicio.
- Servicio: Elementos que hacen referencia a las funcionalidades y capacidades del servicio.
- Organizativo: Elementos de configuración que se relacionan con aspectos específicos de documentación del servicio.
- Internos: Elementos asociados a proyectos individuales.
- Externos: Hace referencia a la documentación de requisitos y acuerdos con interesados externos (cliente).
- De interrelación: documentación si se llegase a entregar el servicio a través de externos.

3.4 Sistema de gestión de la configuración (CMS):

Se debe contar con una plataforma que cuente con las herramientas necesarias en donde se recompila, almacene actualice, analice, se gestione y se presenten los datos acerca de todos los elementos de configuración del área de desarrollo. Se debe adicionar apartados para el registro de información de incidentes, problemas, errores, cambios y liberaciones relacionados con cada servicio.

3.5 Gestión de entregas y despliegues:

La entrega hace referencia a los elementos de configuración de un servicio ya sean nuevos o modificados una vez son probados e implantados, dicha entrega está conformada por unidades de entregas (porciones o módulos del servicio).

Los diseños establecidos a la hora de desplegar las entregas según el caso pueden ser: tipo “*Big Bang*” en donde el servicio nuevo o modificado se ofrece al mismo tiempo para

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 33

todos los usuarios en una única operación y el tipo “*por fases*” en donde la entrega se hace de forma progresiva en cada fase y sobre los usuarios. Las mejores prácticas de ITIL sugieren el siguiente flujo de actividades para un correcto desarrollo de la gestión:

Figura 7. Proceso de gestión de entregas y despliegues [2]



Plan de contingencia ante fallas en la entrega y despliegue del servicio:

Adicional a la información anterior se debe orientar la construcción y testeo de los diferentes niveles de configuración del servicio mediante la herramienta del Modelo V, con el objetivo de llevar a cabo un balance entre lo planteado en el diseño del servicio y sus correspondientes especificaciones del servicio actual con CIs nuevas o modificadas y finalmente poder llegar a determinar riesgos o problemas relacionados con el servicio y sus elementos [7].

Figura 8. Modelo V [6]



buenas prácticas de ITIL se debe realizar el proceso que indica el siguiente diagrama de flujo de validación y pruebas de la mano de la información obtenida en la gestión de conocimiento y la correspondiente documentación.

Figura 9. Flujo de validación y pruebas del servicio (Sugerido por: [2])

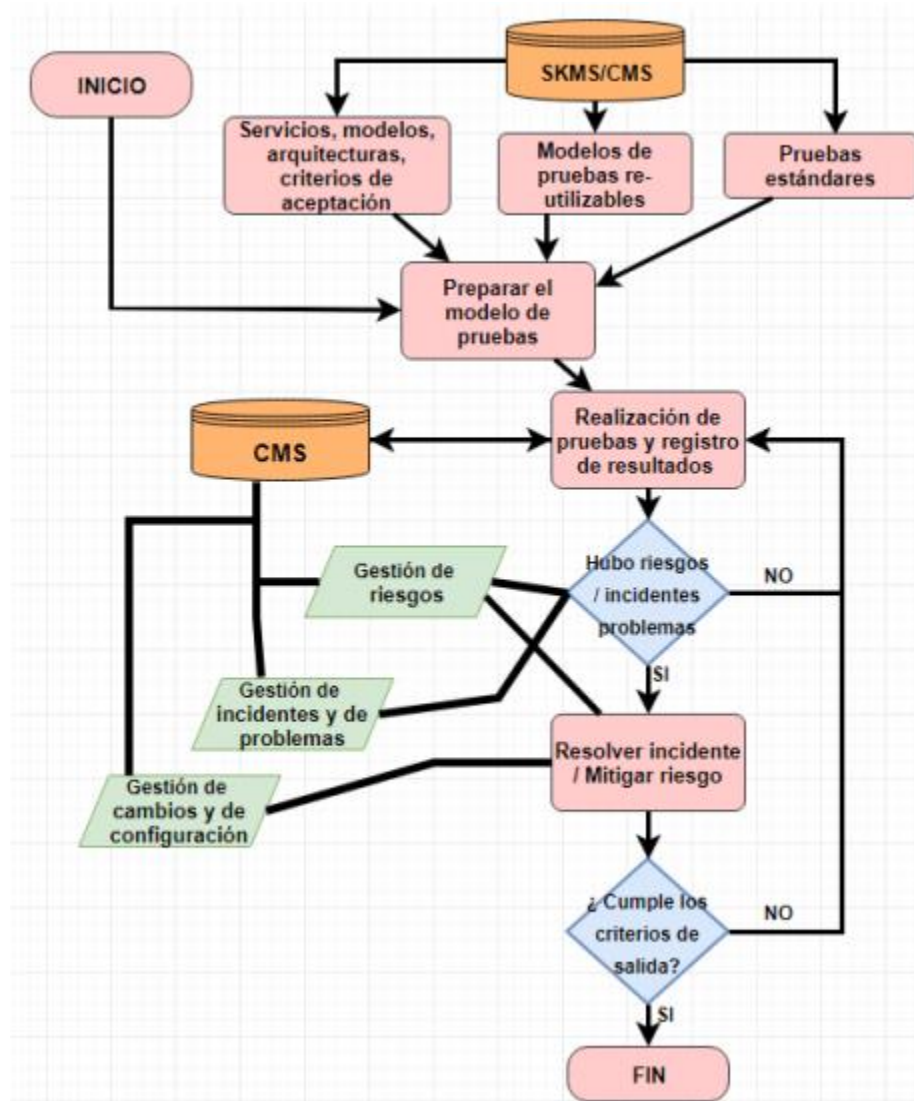
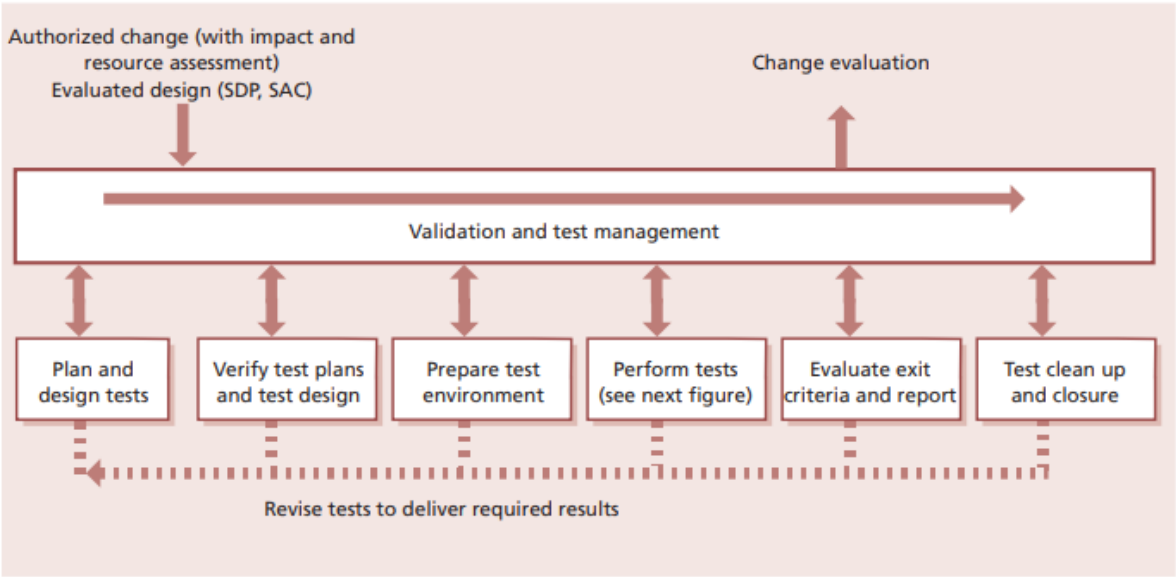


Figura 10. Ejemplo de pruebas y validación



3.7 Evaluación del cambio:

Se debe documentar el rendimiento del servicio con el cambio realizado (nuevo o modificación) teniendo como base los análisis realizados en los anteriores apartados, se evalúan efectos previstos e imprevistos, se debe responder a los criterios de aceptación previamente definidos y basados en los requerimientos del cliente, se debe mostrar la comparación de rendimiento entre lo previsto y lo real. Llegado al caso si la presente evaluación arroja niveles por debajo de lo aceptable, se debe generar un informe que posteriormente será revisado para replantear el cambio por el área de gestión del cambio. Si la aceptación del cambio es buena, se debe estar evaluando el rendimiento esperado una vez llegue al cliente final. Para tener claridad del presente proceso se muestra un diagrama de flujo sugerido por las buenas prácticas de ITIL.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

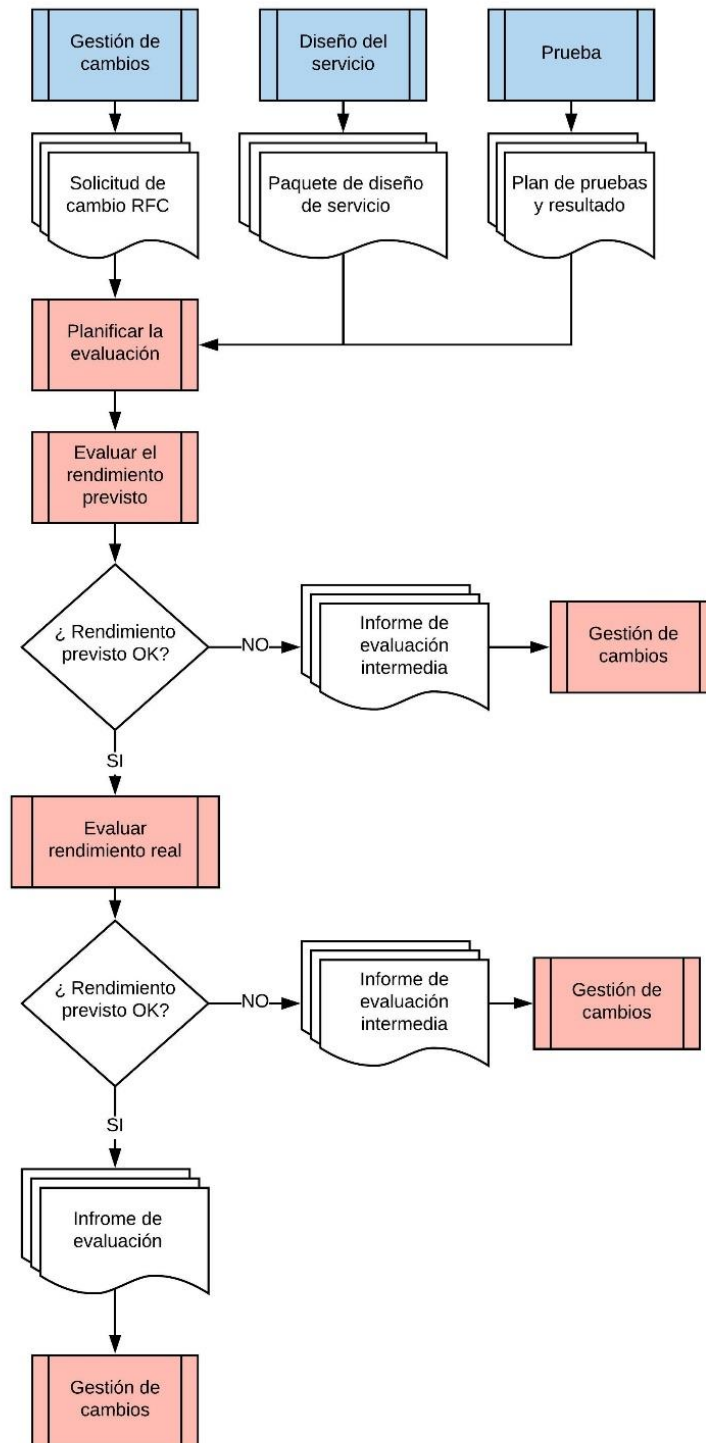
Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 37

Figura 11. Proceso para la evaluación de un cambio [5] [2]



	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 38

3.8 Gestión del conocimiento:

Este proceso va de la mano con la gestión de la seguridad de la información: Confidencialidad, integridad, disponibilidad, uso legítimo y confiabilidad para el apoyo de los diversos procesos en la toma de decisiones. Se debe contar con la adecuada documentación sobre los estándares, políticas, documentación de errores, entre otros. La estrategia para la gestión del conocimiento va orientada a la publicación y divulgación de la información mediante capacitaciones, boletines, avisos, aulas virtuales en la plataforma de la empresa garantizando el acceso únicamente a personal de la empresa, esto incluye áreas y unidades.

Para lo anterior, es necesario a partir de los formatos de documentación especificados crear en la página web apartados dedicados a cada tipo de documento de tal forma se tenga conciencia de la arquitectura de la información almacenada y publicada por orden cronológico de última actualización.

3.8.1 Sistema de gestión del conocimiento del servicio (SKMS):

Se debe contar con una plataforma (*"Plataforma robusta"*) que supla los requerimientos del SKMS y en donde confluyan herramientas, bases de datos, herramientas previamente creadas orientadas al servicio, repositorios y documentación que posibiliten la gestión del conocimiento, de la información (servicios y experiencia u conocimientos del personal vinculado) y de los datos en general (proveedores, Stakeholders, entre otros).

3.8.2 Biblioteca definitiva de medios (DML):

Se debe contar con una plataforma en la cual se almacenan las versiones definitivas y autorizadas de los diferentes elementos de configuración de cada servicio teniendo como base el formato de productos en explotación y proyectos, y las bases de datos previamente diseñadas con el fin de llevar el registro y la trazabilidad de los mismos. La plataforma adicionalmente debe relacionar los servicios con su correspondiente documentación y finalmente contar con un apartado dedicado al inventario de software.

Figura 12. Estructura DML [2]





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 39

4. OPERACIÓN DEL SERVICIO [8]

Se establecen las siguientes políticas con el objetivo de que se lleve a cabo una adecuada coordinación y la ejecución de las actividades y procesos para la prestación de los servicios a los usuarios y clientes finales, junto con la gestión de la infraestructura necesaria para la prestación y el soporte de cada uno de los servicios. Adicionalmente, se especifica que los roles que se mencionan a continuación siguiendo las buenas prácticas de ITIL se incluyen en el organigrama estructural del área de desarrollo siendo asignados a unidades específicas.

Roles:

- Equipo de incidentes: equipo a cargo de la solución de incidentes, se encuentra bajo la unidad de gestión de incidentes y problemas en el área de monitoreo y control de riesgos.
- Gestor de acceso: se encarga de conceder acceso a usuarios para que usen el servicio y del manejo de las políticas de seguridad establecidas, se encuentra bajo la unidad de monitoreo en el área de monitoreo y control de riesgos.
- Gestor de instalaciones de T.I: gestiona el entorno físico donde está la infraestructura de T.I, se encuentra bajo la unidad de infraestructura de T.I en el área de infraestructura de telecomunicaciones.
- Gestor de operaciones de T.I: Se encarga de que las actividades operativas se ejecuten de forma puntual y confiable, se encuentra bajo la unidad de monitoreo en el área de monitoreo y control de riesgos.
- Gestor de problemas: Encargado de gestionar el ciclo de vida de los problemas de la mano con la prevención de incidentes y la minimización de impacto, se encuentra bajo la unidad de gestión de incidentes y problemas en el área de monitoreo y control de riesgos.
- Gestor de cumplimiento de solicitud de servicio: se encargan de la realización de ciertos tipos de solicitudes del servicio, se encuentra en la unidad de diseño del área de desarrollo y nuevas tecnologías.
- Operador T.I: Es el encargado de preparar copias de seguridad, tareas programadas entre otras relacionadas, se encuentra bajo la unidad de copias de seguridad del área de monitoreo y control de riesgos.
- Soporte de primera línea: Registra y clasifica incidentes reportados, se encarga de ultimar esfuerzos en mantener la continuidad del servicio de no lograrlo, transfiere el incidente a soporte de segunda línea. Se encuentra bajo la unidad de soporte en el área de monitoreo y control de riegos.
- Soporte de segunda línea: Se encarga de incidentes que no pudieron ser resueltos en la primera línea de soporte, de igual forma se encuentra en la unidad de soporte.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

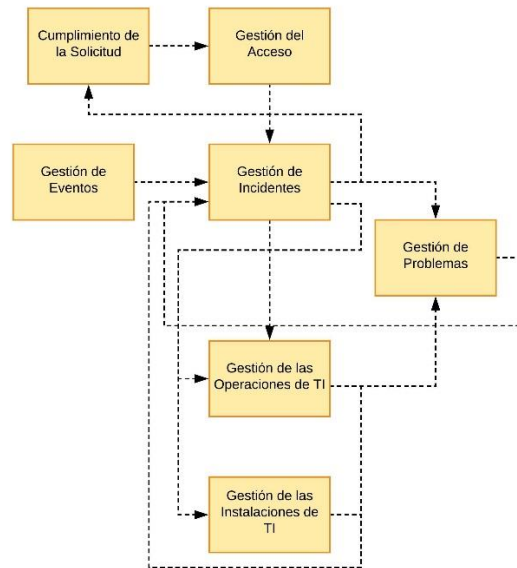
Versión: 1.0.0

Fecha: 14-10-2019

Página: 40

Teniendo como base las buenas prácticas de ITIL, se procede a orientar los procesos de la operación del servicio bajo el siguiente diagrama, cumpliendo los requerimientos de los usuarios, resolver fallos en el servicio, entre otros:

Figura 13. Procesos operación del servicio [2].



4.1 Gestión de eventos:

Se establece el proceso a seguir con el objetivo de notificar, detectar, registrar, categorizar, correlacionar, actuar y cerrar cada uno de los eventos que se lleguen a presentar durante la prestación del servicio bajo su monitorización. Por lo anterior se toma como referencia el siguiente diagrama de flujo (*Ver imagen 11*) en donde:

- El proceso inicia cuando ocurre un evento.
- Se registra el evento y se correlaciona en primer o segundo nivel.
- Se categoriza según su nivel de importancia (los de tipo informativo se cierran al no tener impacto en la continuidad del servicio).
- Detectar si produce incidentes, problemas o cambios.
- Plantear una solución efectiva.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

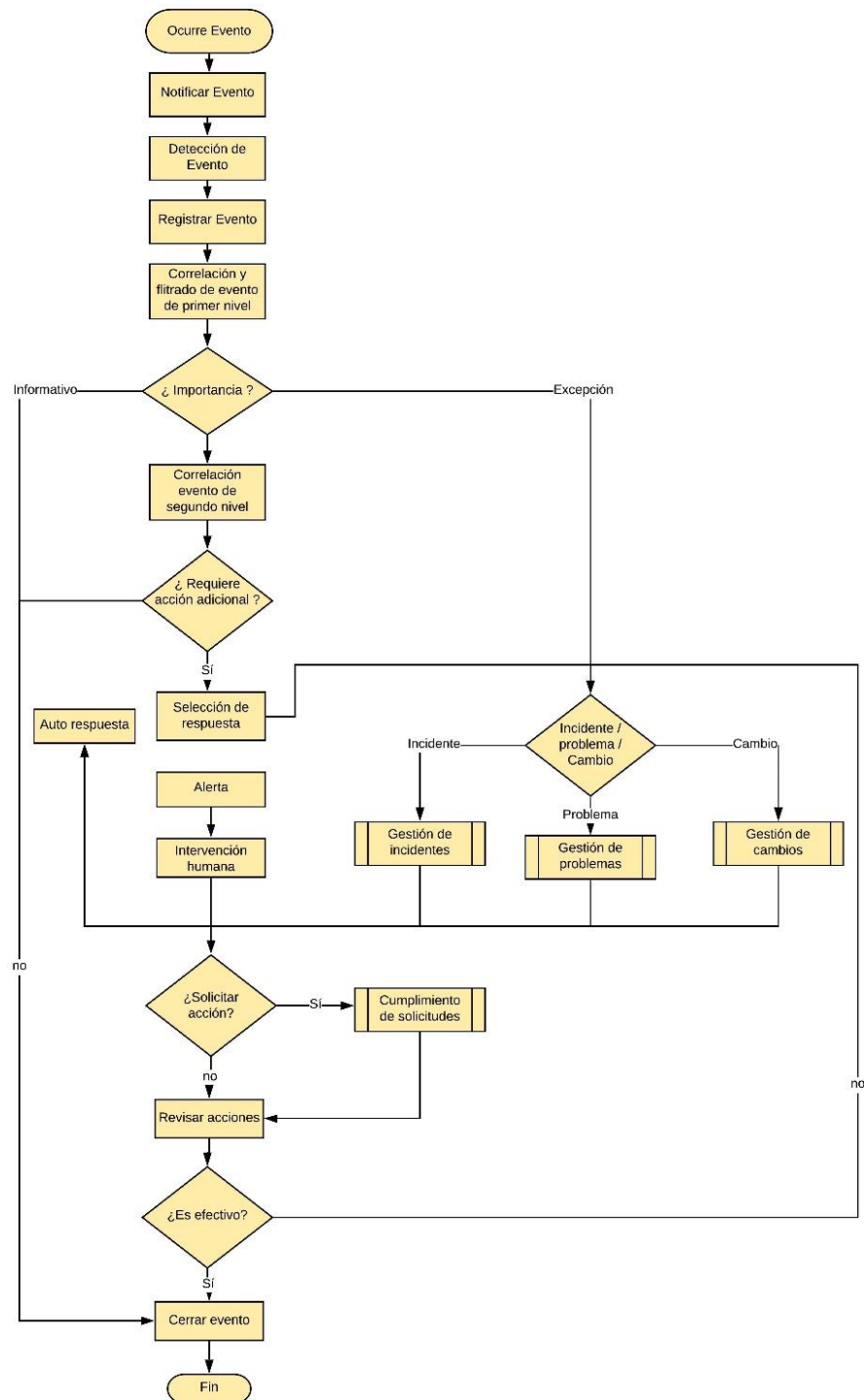
Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 41

Figura 14. Proceso gestión de eventos (Sugerido por: [8])



	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 42

Nota: Según ITIL se define como evento a un suceso que afecta de forma directa la infraestructura de T.I o la prestación de un servicio T.I.

4.2 Gestión de incidentes:

Se establece una gestión de incidentes durante todo el ciclo de vida del servicio siguiendo el siguiente modelo:

- a. Identificación
 - b. Registro
 - c. Categorización
 - d. Priorización
 - e. Diagnóstico inicial
 - f. Escalado
 - g. Investigación y veredicto de diagnostico
 - h. Resolución y restauración.
 - i. Monitoreo y cierre.
- Responsabilidades: el modelo debe ser aplicado y es responsabilidad del equipo de incidentes que como se definió en los roles, es el equipo a cargo de la solución de incidentes y se encuentra bajo la unidad de incidentes y planes de contingencia en el área de monitoreo y control de riesgos. Dicho equipo debe llevar el control sistemático de tiempo utilizado hasta llegar al monitoreo y cierre del incidente, y finalmente la recuperación del servicio interrumpido.

En adición a lo anterior ITIL proporciona el siguiente diagrama de flujo (ver figura) para el manejo de incidentes, diagrama que tiene diferentes entradas que deben ser proporcionadas por el cliente según sea su incidente, estas deben ser constantemente monitoreadas.

El registro de incidentes debe ser orientado por la guía de documentación y tal como se establece, debe contar con fecha y hora; así mismo se debe diligenciar el correspondiente formato con el objetivo de conocer la trazabilidad del incidente y su estado actual hasta su cierre, en el registro debe quedar asignado su nivel de impacto y el nivel de urgencia que requiere. Una vez se cierre el incidente se debe al igual que su proceso de solución, documentar.

Nota: Se define incidente como todo evento que interrumpa o pueda llegar a interrumpir la prestación de un servicio T.I



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

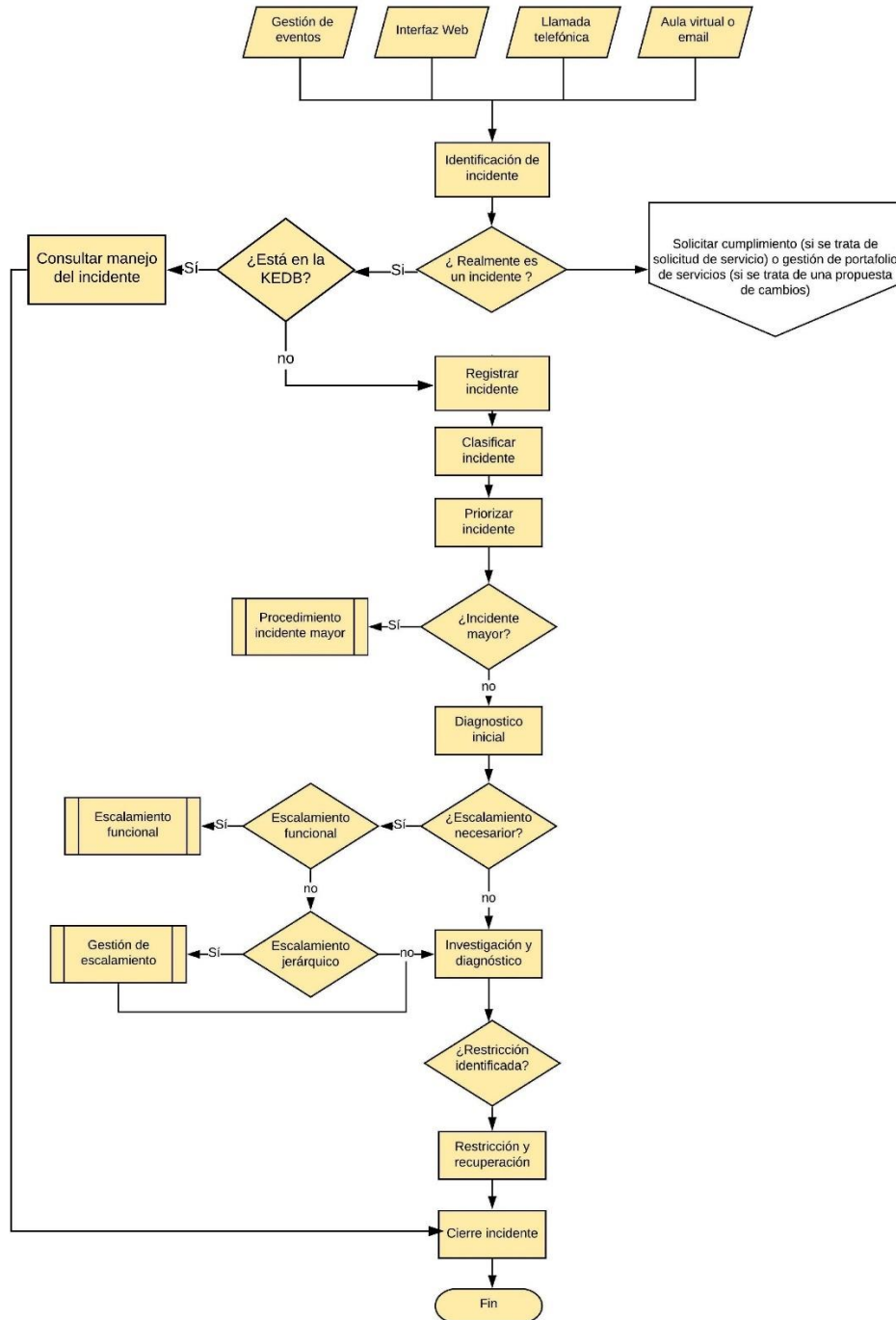
Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 43

Figura 15. Proceso de gestión de incidentes (modificado [8])





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 44

4.3 Cumplimiento de solicitudes:

Se establece el área de atención al cliente y sus correspondientes unidades como canal para que los usuarios soliciten y reciban los servicios estándar, adicionalmente se debe poner a disposición de los clientes un medio de comunicación online en el cual puedan también realizar la solicitud. En este contexto se establece el siguiente proceso (presencial, online – Página web, online – email o por teléfono) para el debido tratamiento de las peticiones de servicio realizadas por el cliente:

- a. Recibir la solicitud: cabe resaltar que al recibir la solicitud se debe revisar si debe ser tratada como solicitud, como cambio o como incidente. De ser solicitud se continua continúa con el presente proceso.
- b. Registrar y validar la solicitud
- c. Clasificar solicitud
- d. Priorizar solicitud
- e. Autorizar solicitud (la solicitud puede ser devuelta en este paso, se debe informar al quien la realizó y los motivos de devolución)
- f. Revisar solicitud: se escala al personal especializado que pueda atender la solicitud.
- g. Ejecutar modelos de solicitud (modelos que den respuesta a la solicitud establecidos en las unidades a las que sean remitidas).
- h. Cerrar solicitud (se evalúa el proceso).



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

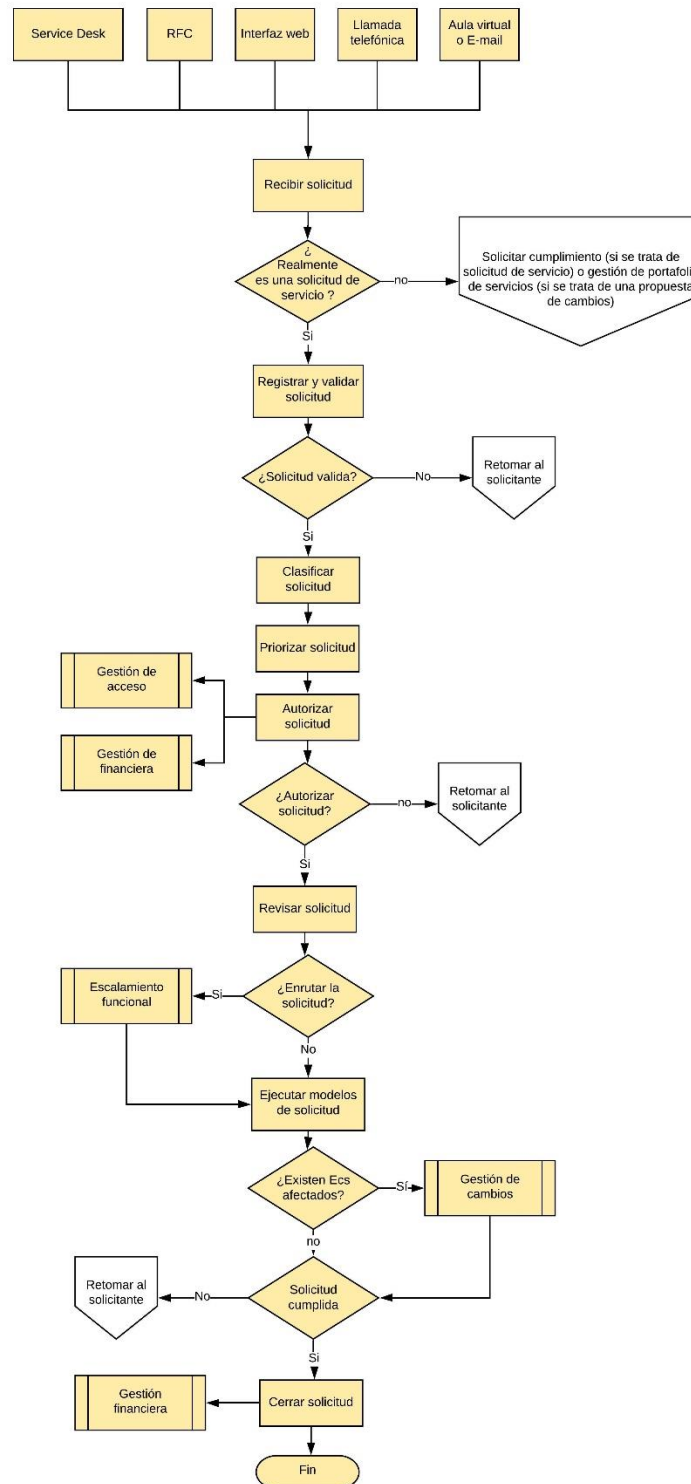
Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 45

Figura 16. Proceso para el cumplimiento de solicitudes (modificado [8]).





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 46

4.4 Gestión de problemas:

Se establece el proceso a seguir para el manejo de problemas (identificación. Investigación, documentación, análisis y eliminación del problema) y la documentación de los mismos con el objetivo de minimizar el impacto y prevenir futuras incidencias (se debe conformar la biblioteca de errores conocidos para diagnósticos rápidos):

- a. Detección del problema.
 - b. Registro del problema.
 - c. Clasificación del problema.
 - d. Investigar y diagnosticar el problema.
 - e. Encontrar solución temporal.
 - f. Registrar en biblioteca de errores conocidos.
 - g. Resolver problema.
 - h. Cerrar problema.
 - i. Documentación completa del proceso.
- Responsabilidades: el modelo debe ser aplicado y es responsabilidad del gestor de problemas, encargado de gestionar el ciclo de vida de los problemas de la mano con la prevención de incidentes y la minimización de impacto, se encuentra bajo la unidad de planes de contingencia en el área de monitoreo y control de riesgos. Adicionalmente debe planear y gestionar el soporte para los procesos y herramientas de la gestión de problemas.
 - Los problemas en gran medida pueden ser reportados por los clientes, es por ello que al igual que los incidentes se debe disponer a través del área de atención al cliente y sus unidades (presencial, online – Página web, online – email o por teléfono).
 - Una vez se llegue a la resolución del problema se debe proceder a realizar las correspondientes RFC necesarias para que sean intervenidas por el equipo de gestión de cambios, finalmente se cierra el problema y se completa la documentación del proyecto.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

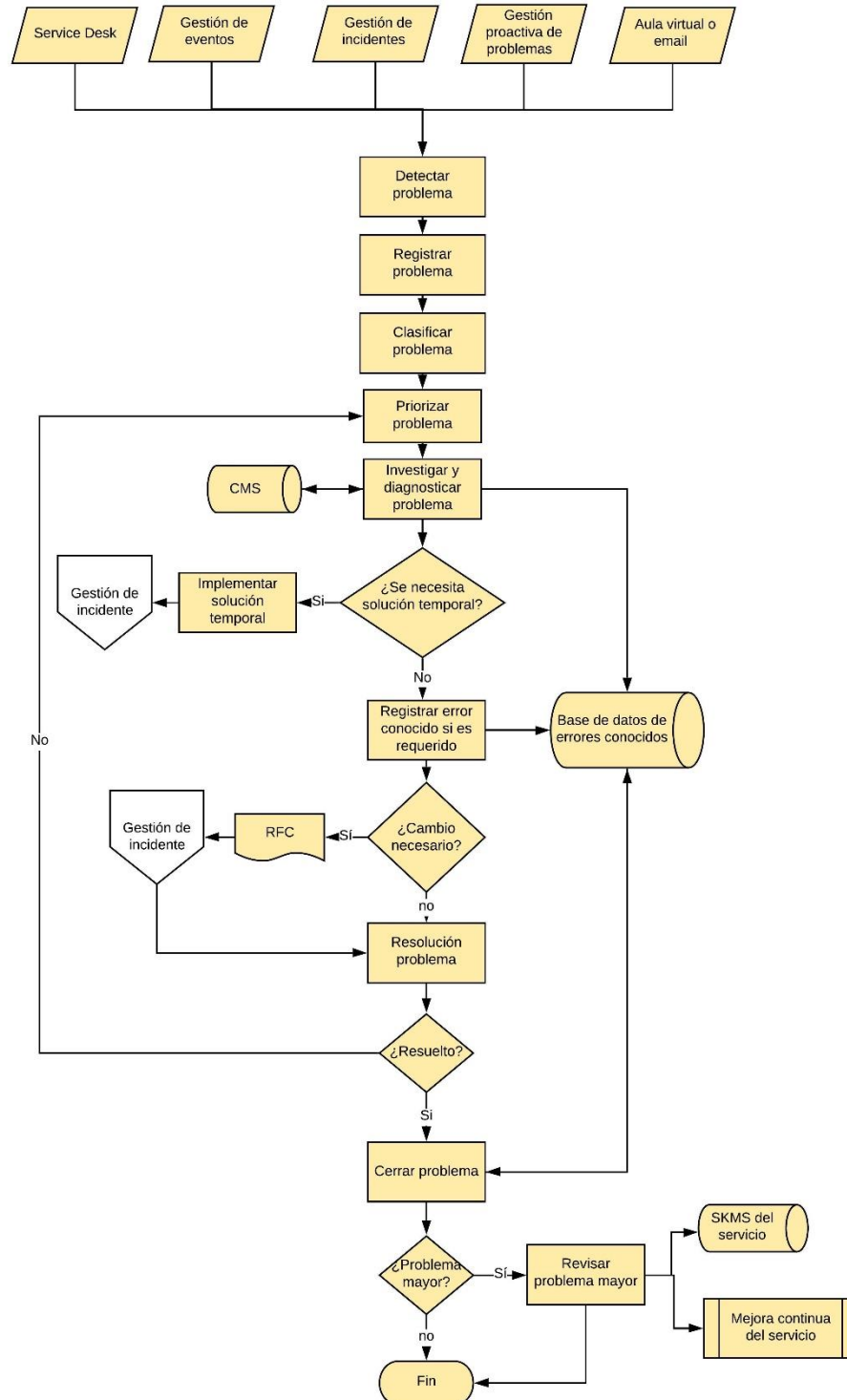
Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 47

Figura 17. Proceso para la gestión de problemas (modificado [8]).





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 48

4.4.1 Base de datos de errores conocidos (KEDB):

Formato que alimente la base de datos previamente diseñada (KEDB) con la siguiente información: Id de falla, nombre corto de la falla, descripción exacta del problema, diagnostico, causas, síntomas y solución detallada. La información insertada en la base de datos mediante el formato y la plataforma asignada, debe contar con las correspondientes relaciones hacia los apartados de incidentes y problemas anteriormente tratados. El responsable de la creación de la presente base de datos es el gestor de problemas designado, base de datos que en este contexto debe ser utilizada por el equipo de gestión de incidentes y de problemas

Nota: Según las buenas prácticas de ITIL, la base de datos debe contener información crucial para el diagnóstico y resolución de incidentes en corto tiempo contribuyendo a la mejora en la calidad del servicio prestado.

4.5 Gestión de acceso:

Se establecen las directrices que debe seguir el gestor de acceso para la concesión de acceso a usuarios para que hagan uso de los servicios, datos u otros activos bajo el manejo de las políticas de seguridad establecidas garantizando la confidencialidad, disponibilidad e integridad de los activos.

Mediante el sistema de gestión se deben proporcionar privilegios a los diferentes tipos de usuarios teniendo como base específicamente las políticas de acceso lógico descritas anteriormente. Adicionalmente y para mayor claridad se pone a disposición del gestor de acceso el siguiente proceso para el tratamiento de accesos [4]:

- a. Solicitar el acceso.
- b. Verificar.
- c. Proporcionar privilegios: Se debe limitar controlar la asignación y uso de privilegios como se establece en las políticas con el fin de evitar fallas en los sistemas, se resaltan los siguientes ítems:
 - Identificación de privilegios asociados a cada servicio o producto del sistema.
 - Tener el debido proceso para la asignación y verificación de privilegios.
- d. Verificar y monitorear el estado de identidad.
- e. Registrar y dar seguimiento de acceso: el registro de accesos debe comprender el registro de usuarios (personal y externos) con el fin de otorgar y revocar el acceso a sistemas, bases de datos y servicios bajo las siguientes pautas:
 - Uso de identificadores únicos.
 - Verificación de autorización de usuario.
 - Verificación de nivel de acceso.
 - Informar a los usuarios sobre sus derechos y deberes de acceso debidamente diligenciado (firmado), aceptando términos y condiciones.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

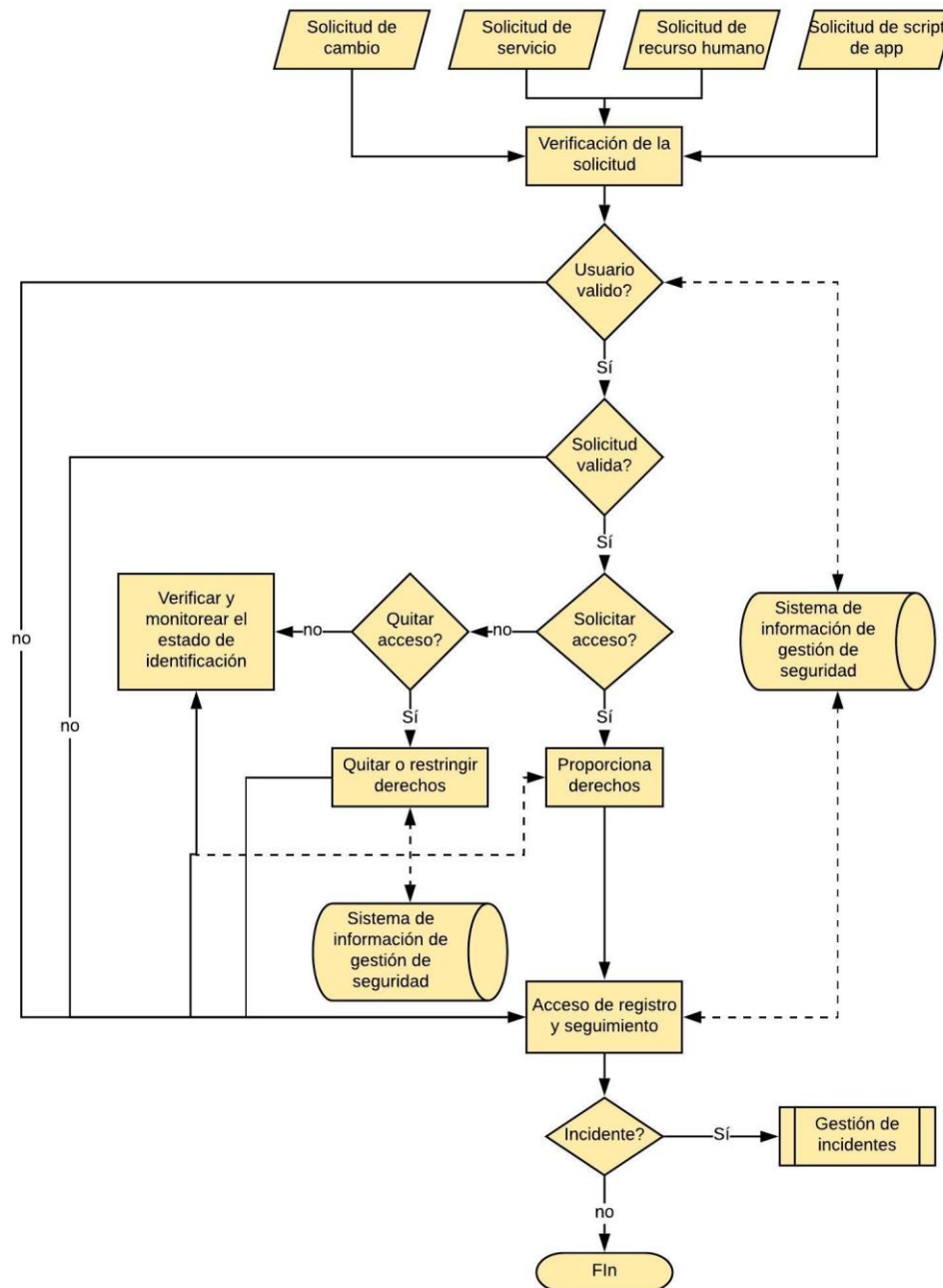
Versión: 1.0.0

Fecha: 14-10-2019

Página: 49

- Las excepciones deben ser debidamente justificadas y aprobadas.
 - Seguimiento según lo establezcan las políticas de seguridad de la información previamente establecidas.
- f. Eliminar o restringir privilegios.

Figura 18. Proceso para la gestión de acceso [8]





POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 50

4.6 Funciones:

Las funciones que establece ITIL en su fase de operación y que deben ser definidos en la estrategia del servicio son:

- a. **Service Desk:** En la división de desarrollo de la empresa el Service Desk se establece como una unidad perteneciente al área de atención al cliente y es el punto de contacto entre la empresa y los usuarios recibiendo incidentes, problemas y solicitudes de servicio (incluye solicitudes de cambio, de configuración y de infraestructura) mediante los medios de comunicación disponibles. Para mayor claridad se listan las tareas que según ITIL debe realizar el Service Desk:
 - Registrar, categorizar y priorizar las peticiones abiertas por los clientes.
 - Proporcionar una primera línea de soporte, realizando un primer diagnóstico y resolviendo peticiones.
 - Asignar las peticiones que no pueda resolver.
 - Monitorizar la resolución de las peticiones, escalando aquellas para las que exista riesgo de incumplir el acuerdo de nivel de servicio.
 - Mantener informados a los clientes del estado de sus peticiones.
 - Cerrar las peticiones resueltas, previa validación con los usuarios.
 - Medir el nivel de satisfacción de los usuarios.
- b. **Gestión Técnica:** Como su nombre lo indica hace referencia a las competencias técnicas para dar soporte a los servicios y a la infraestructura por medio de la definición de roles y grupos de soporte garantizando la calidad en la prestación de servicios. Por lo anterior y siguiendo las buenas prácticas de ITIL se establecen las siguientes actividades para cumplir con los requerimientos de la gestión técnica:
 - Identificar el conocimiento y conocimiento especializado requeridos para gestionar y operar la infraestructura de TI y para entregar los servicios.
 - Documentar las capacidades que existen en la organización, así como las habilidades que deben de ser desarrolladas.
 - Iniciar programas de capacitación para desarrollar y mejorar las capacidades en los recursos técnicos apropiados.
 - Diseñar y entregar capacitación.
 - Reclutar y contratar los recursos con las habilidades que no pueden ser desarrolladas internamente.
 - Procurar capacidades para actividades específicas en que las capacidades requeridas no estén disponibles internamente o en el mercado abierto, o donde sea más rentable para hacerlo.
- c. **Gestión de Aplicaciones:** El equipo de trabajo designado debe gestionar las diversas aplicaciones que soportan los procesos de la división de desarrollo y proyectos T.I mediante herramientas software, al igual que en la gestión técnica se debe



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 51

implementar las actividades mencionadas para dar cumplimiento a los requisitos de la gestión. Adicionalmente se debe designar a esta gestión, personal con las habilidades adecuadas para el mantenimiento de aplicaciones operacionales, el manejo de fallas, entre otras.

- d. Gestión de operaciones de T.I: la presente gestión abarca las unidades del área de infraestructura de telecomunicaciones en el diagrama estructural y se establecen los siguientes roles que deben ser previamente asignados:

- Control de operaciones de TI: Se debe designar el personal necesario para el monitoreo y control de los servicios e infraestructura T.I (centro de redes de operación).
- Gestión de instalaciones: Personal que se encarga de la gestión del ambiente físico donde se encuentra la infraestructura T.I siguiendo estrictamente las políticas de seguridad del entorno físico.
- Rol dual de gestión de operaciones de T.I: Se deben ejecutar actividades y estándares de desempeño definidos con anterioridad en las políticas.

5. MEJORA CONTINUA DEL SERVICIO [9]

Se establecen políticas para la identificación e implementación de mejoras en los procesos y actividades del servicio con el objetivo de garantizar la calidad, eficiencia y efectividad de los mismos.

5.1 Planificar, Hacer, Verificar y Actuar (PDCA):

Estrategia de mejora continua, propuesta por ITIL y por otros marcos de trabajo para la mejora de la calidad de los servicios y para la identificación de nuevas oportunidades de mejora del servicio. Las cuatro etapas descritas a continuación se deben aplicar de forma sistemática y reevaluadas periódicamente en reuniones específicas del equipo de trabajo.

- a. Planificar: Definir qué quiere, qué necesita y que se va a hacer a modo de propuesta en la división del área de desarrollo, establecer pre requisitos, objetivos, actividades necesarias, asignación de roles y responsabilidades con su correspondiente documentación de dichos procesos.
- b. Hacer: evaluación y verificación de actividades establecidas, se debe determinar los planes y procedimientos a seguir, documentarlos, asignarlos, divulgarlos y ejecutarlos (ITIL recomendando el uso de pruebas piloto).
- c. Verificar: Monitoreo del comportamiento de las mejoras propuestas en los ambientes controlados (pruebas piloto) mediante la recopilación, medición,



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 52

validación y evaluación de datos obtenidos con el fin de determinar si se alcanzaron satisfactoriamente los objetivos propuestos.

- d. Actual: Reuniones necesarias para la retroalimentación de los resultados obtenidos con el fin de mejorar, ajustar o corregir las actividades que no cumplieron con sus objetivos (se toman decisiones al respecto).

5.2 Proceso de mejora:

Se establece el siguiente proceso propuesto por ITIL para una realización correcta y exitosa de la implementación de mejoras en la empresa y propiamente en la división de desarrollo y proyectos T.I con el objetivo de identificar mejores oportunidades para mejora de servicios, procesos y herramientas, reducir los costos de prestar el servicio, garantizando la calidad del servicio, identificar los procesos o actividades que necesiten ser medidos y analizados en busca de mejoras, y conocer en detalle las variables a medir para definir resultados.

- a. Definir lo que hay que medir: Mediante la definición de la división de desarrollo y proyectos T.I, identificar el comportamiento actual de la misma y establecer los servicios que se deben medir para vislumbrar cuales son los que no están cumpliendo los objetivos.
- b. Definir lo que se puede medir: Encontrar los parámetros que se puedan medir y que pueden contribuir al desarrollo del servicio.
- c. Recolectar datos: Monitoreo constante para la obtención de información que permita identificar acciones o tendencias que contribuyan a adecuar la mejora.
- d. Procesar los datos: Transformación de la información a formatos adecuados para que puedan ser analizados.
- e. Analizar los datos: Análisis de datos que permitan tomar decisiones enfocadas al cumplimiento de los objetivos.
- f. Presentación y uso de la información: presentación de la información de forma comprensible para la posterior toma de decisiones e implementación de mejoras.
- g. Implementación de acciones correctivas: Implementación de acciones que contribuyan a la mejora operacional y restructuración del servicio.

5.3 Medición del servicio:

Se establecen las directrices para la medición de los servicios ofertados en el portafolio, las tres medidas básicas para lograr el propósito de la presente gestión son:

- a. Disponibilidad del servicio.
- b. Confiabilidad del servicio.
- c. Desempeño del servicio.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 53

Aplicando las buenas prácticas de ITIL se establece que el servicio se debe dividir, medir e informar en componentes, sistemas y aplicaciones de forma individual y posteriormente de forma colectiva, esto con el objetivo de abordar el servicio de extremo a extremo de tal forma se logre una medición más clara.

5.3.1 Retorno de la inversión:

El retorno sobre la inversión (ROI) se define como una razón financiera que compara el beneficio o la utilidad obtenida en relación a la inversión realizada. Es por ello que se establece de la mano de ITIL que para la realización del análisis del retorno de la inversión se deben contemplar costos no solo de inversión sino también costos internos, costos de recursos, costos de herramienta, de consultoría y demás. Dicho análisis debe definir o cuantificar el retorno que va a tener Interlink S.A a partir de los mencionados costos adicionando o contemplando los siguientes factores:

- a. Costos del tiempo de inactividad: tiempo y cantidad de productividad perdida por inactividades y pérdidas de ingresos del cliente al no poder operar.
- b. Costo de retrabajo: actividades que han fallado y decidir si se retiran del portafolio o se reestructuran contemplando el tiempo y costo del retrabajo.
- c. Costo por redundancia: Costos debido a actividades, procesos o métodos que se realizan de forma redundante.
- d. Costo de proyectos que no generan valor: evaluar proyectos que no agregan valor a la empresa y tomar decisiones sobre estos.
- e. Costo por la entrega de servicio, aplicación o solicitud con tiempo de retraso: impacto que tiene en la empresa la entrega tardía.
- f. Costo de escalar incidentes y no lograr resolverlos.

5.4 Preguntas de negocio:

ITIL propone una serie de preguntas a base de orientación para que desde la división de desarrollo y proyectos T.I se analicen y sean respondidas a la hora de realizar cambios y mejoras a futuro con el objetivo de buscar nuevas oportunidades para la mejora de servicios ofertados y de la división de desarrollo y proyectos T.I.

- a. ¿Qué es lo que se quiere?: se sugiere analizar desde la misión, visión, objetivos y metas de la empresa y de la división y determinar si están acordes a lo que se está realizando de lo contrario se debe redefinir.
- b. ¿Dónde estamos ahora?: Se debe analizar el portafolio de productos y servicios que se están ofreciendo al cliente.
- c. ¿Qué es lo que necesitamos?: con el análisis anterior se determina si los servicios están acordes a la misión y están cumpliendo con los objetivos.



POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA

Código: PEPPM-P01

Versión: 1.0.0

Fecha: 14-10-2019

Página: 54

- d. ¿Cuánto podemos afrontar?: Determinar la capacidad que tienen los servicios ofertados para afrontar la situación actual y futuras de la mano con lo definido en la fase de estrategia del servicio.
- e. ¿Qué conseguiremos?: se deben determinar los resultados esperados con la implementación de una mejora continua.
- f. ¿Qué hemos conseguido?: Teniendo como base la operación del servicio se debe determinar en detalle lo que se ha logrado hasta el momento.
- g. ¿Se satisfacen con ellos nuestras necesidades?: Se debe determinar si se han logrado satisfacer las necesidades o si se lograron los resultados esperados.

5.5 Requerimientos de nivel de servicio (SLR):

Se definen especificaciones mediante los siguientes formatos para el uso y el entendimiento de los SLR que, a nivel de concepto, estos requerimientos describen las expectativas que tiene un cliente hacia un proveedor en este caso Interlink acerca de los servicios que oferta.

Tabla 4. Requisitos de nivel de servicio (sugerido por: [2])

Identificador	Nombre del servicio	Descripción	Cliente
Identificador	# interrupciones permitidas	Umbrales de disponibilidad	Cliente

5.5.1 Plan de mejora del servicio:

Se establece un plan de formal para la implementación de los servicios de T.I, de tal forma que se pueda gestionar y documentar de forma ágil cada iniciativa de mejora continua y todo su proceso de implementación. Se plantean dos tipos de mejora:

- a. Internas: nacen desde la empresa y específicamente de la división de desarrollos y proyectos T.I.

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 55

- b. Externas: La empresa consulta con los clientes sobre los productos y servicios si los acuerdos a nivel de servicios SLA son los adecuados, de lo contrario se deben realizar mejoras.

Para lo anterior se debe hacer uso de los siguientes formatos en concordancia con el plan de mejora que se propone:

- Identificación de servicio o proceso que requiere mejora o que a pesar de su óptimo funcionamiento se puede mejorar con el fin de aumentar la satisfacción del cliente u optimizar procesos.
- Documentar (teniendo como guía el formato de documentación) la propuesta o iniciativa de mejora junto con sus correspondientes soportes que den validez y soporte a la propuesta.
- Presentar el documento anterior ante la unidad correspondiente (personal de la empresa) o ante las diversas unidades del área de atención al cliente (externos).
- La propuesta de mejora se debe aprobar o denegar en un máximo de 15 días, en este proceso se debe realizar un estudio en cuento a estimación de costos.
- Si se aprueba la propuesta, se asigna la persona o el personal encargado de ejecutar la propuesta.
- Si se deniega se debe dar resolución a la persona o personas que hayan presentado la propuesta con su correspondiente justificación (pueden presentar mejoras de la propuesta y volver a presentarla).
- Al asignar la propuesta a un equipo de trabajo, este deberá entregar el estudio correspondiente junto con el formato de iniciativa de mejora 2.
- Una vez se ejecute la propuesta se hace el balance de la mejora.
- Se documenta el proceso de mejora realizado, se archiva y se cierra el proceso.

Tabla 5. Formato 1 para iniciativas de mejora (Sugerido por: [2])

Identificador	Nombre del servicio o proceso	Persona a cargo	Propietario de la iniciativa	Descripción de iniciativa	Origen de la iniciativa

	POLÍTICAS PARA ENTREGABLES, PRUEBAS Y PUESTA EN MARCHA	Código: PEPPM-P01
		Versión: 1.0.0
		Fecha: 14-10-2019
		Página: 56

Tabla 6. Formato 2 para iniciativas de mejora (Sugerido por: [2])

Identificador	Resultado esperado de la iniciativa	Estimación de costo	Resultado obtenido	Fecha inicio	Fecha de terminación

6. Referencias

- [1] D. Cannon, ITIL® Service Strategy, Londres: Crown, 2011.
- [2] J. C. Gutiérrez Cantor, B. N. Guzmán Prieto y D. S. Chisco Quintero, «Respositorio: Esciala de Ingeniería Julio Garavito,» 2018. [En línea]. Available: <https://repositorio.escuelaing.edu.co/bitstream/001/703/1/Chisco%20Quintero%20David%20Santiago%20-%202017.pdf>.
- [3] L. Hunnebeck, ITIL® Service Design, Londres: Crown, 2011.
- [4] UVI, «Universitaria Virtual Internacional,» 2013. [En línea]. Available: <https://www.uvirtual.edu.co/Documents/Documentos-Institucionales/POLITICA-SEGURIDAD.pdf>. [Último acceso: 28 Octubre 2019].
- [5] AXELOS, ITIL® Service Transition, United Kingdom: The Stationery Office, 2011.
- [6] S. Rance, ITIL® Service Transition, Londres: Crown, 2011.
- [7] Publishing, Van Haren, Transición del servicio basada en ITIL V3, Amersfoort: Van Haren Publishing, 2008.
- [8] R. Steinberg, ITIL® Service Operation, Londres: Crown, 2011.
- [9] V. Lloyd, ITIL® Continual Service Improvement, Londres: Crown, 2011.