ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE LA SITUACIÓN ACTUAL DE LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DE ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A. RESPECTO AL ESTÁNDAR ITIL V3, CON UNA PROPUESTA DE SOLUCIÓN ESPECÍFICA AL EVENTO MÁS CRÍTICO

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRONICA Y REDES DE INFORMACIÓN

GABRIEL ROBERTO LOPEZ FONSECA
gabriel.lopez@epn.edu.ec

DIRECTOR: Ing. Rodrigo Chancusig
rodrigch@panchonet.net

Quito, julio 2010

DECLARACION

Yo Gabriel Roberto López Fonseca, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Gabriel Roberto López Fonseca

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Gabriel Roberto López Fonseca, bajo mi supervisión.

Ing. Rodrigo Chancusig
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios por darme salud y fortaleza para realizar el presente proyecto de titulación, a pesar de los obstáculos que se hallaron en el camino. Así como a mis padres, quienes siempre me brindaron su apoyo para educarme y formarme como ser humano, gracias a mi hermanita Estefy y a mi tía Pao por su ayuda singular.

Una mención especial a la empresa Alianza CIA. de Seguros y Reaseguros S.A. por abrirme sus puertas y confiar en el éxito del presente trabajo de investigación. A los ejecutivos Marcelo Galeano, Elizabeth Vallejo, Ramiro Pérez; empleados de Alianza y puntos de venta SOAT a nivel nacional, por su colaboración durante el levantamiento de información de la compañía. A los miembros del Departamento de Sistemas, Pablo Herrera (Gerente), Juan Carlos Guamba, Patricio León y Juan Carlos Cevallos, por su apoyo, disponibilidad y apertura durante la elaboración de cada uno de los capítulos del presente estudio.

A mi director de Tesis Ing. Rodrigo Chancusig por su interés en dirigir este proyecto y su ayuda para culminar el mismo.

A la Escuela Politécnica Nacional representada por sus autoridades, profesores, personal administrativo y compañeros por su aporte durante todos estos años de estudio para mi madurez como profesional.

DEDICATORIA

A mis padres Gabriel, Elizabeth

y a mi hermanita Estefy

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación se ha estructurado en 6 capítulos.

En el primer capítulo se detalla el marco teórico del estándar ITIL V3, su estructura y aspectos básicos acerca de: Estructura, Estrategia de Servicio, Diseño de Servicio, Transición de Servicio, Operación de Servicio y Mejoramiento de Servicio. A continuación se presentan los procesos de ITIL a ser avaluados en la empresa a realizar el estudio.

En el segundo capítulo, se da una descripción sobre: la reseña histórica, misión, visión, sucursales, líneas de producción e infraestructura de la red de Alianza CIA de Seguros. A continuación se detallan el método y los indicadores a ser evaluados para gestión de: Nivel de Servicio, Continuidad de Servicio, Cambios, Configuraciones, Incidentes y Problemas, para ejecutivos, gerente de sistemas, empleados del Departamento de Sistemas, usuarios comunes y puntos de venta SOAT. Como parte final de este capítulo se presenta el método utilizado para realizar la evaluación de riesgos.

En el tercer capítulo se presentan los resultados de las encuestas aplicadas a los grupos que intervienen en la investigación, donde se detallan los estados de los indicadores, gráfico de cumplimiento y recomendaciones para los indicadores de grado de confianza críticos. A continuación se muestran los resultados del análisis de riesgos.

En el cuarto capítulo se desarrolla una solución de gestión para el evento más crítico. Donde se puntualizan los antecedentes y el desarrollo de la solución.

En el quinto capítulo se muestra el análisis de costos de la solución de gestión al evento más crítico. Aquí se detallan tres propuestas: una utilizando sólo personal interno de la empresa, otra con la participación de un técnico temporal y finalmente la tercera con personal interno asesorado por un consultor.

En el sexto y último capítulo están las conclusiones y recomendaciones que se han generado luego de la realización del proyecto.

PRESENTACIÓN

La tecnología en la época actual es una herramienta vital para las operaciones diarias de una empresa, ayudando que las tareas se ejecuten rápida, correcta y eficientemente, bajo una administración establecida en un estándar que garantice la calidad del servicio.

ITIL (Information Technology Infrastructure Library) V3, es un estándar para la administración de la infraestructura tecnológica, que propone guías de buenas prácticas de gestión para los procesos más comunes dentro del departamento de Tecnología. Esta es la herramienta adecuada para: de forma comparativa obtener el estado actual de gestión de la organización, y medir con sus respectivos indicadores los riesgos a los que la empresa se expone al no manejar sus procesos de acuerdo a las recomendaciones de un estándar de administración tecnológica como ITIL.

Para el mejoramiento continuo es indispensable monitorear el estado actual de la empresa, aquí se pueden observar los puntos críticos que son visibles gracias a un análisis de riesgos, estas actividades previas ayudan a estructurar un modelo de recomendaciones para la administración de la Infraestructura Tecnológica.

Al manejar un modelo definido de gestión la empresa logrará evaluar y optimizar los procesos actuales para que las actividades de dicha organización se apoyen en la tecnología y se desarrollen con normalidad. De esta manera la tecnología no será un obstáculo a los objetivos de la empresa por el contrario un facilitador al éxito de los servicios que ofrece, que se ajuste a las necesidades específicas de la organización.

En el presente proyecto de titulación se evalúa a Alianza CIA de Seguros y Reaseguros S.A. en los procesos de Gestión ITIL: Nivel de Servicio, Continuidad de Servicio, Cambios, Configuraciones, Incidentes y Problemas, los mismos que fueron elegidos entre el Departamento de Sistemas de la empresa y el autor.

El plan de gestión bajo las recomendaciones de ITIL para el proceso reconocido como crítico, ayuda a reducir el riesgo detectado con el fin de evitar que exista corte para los servicios vitales de la compañía.

CAPÍTULO I: MARCO TEÓRICO. ESTÁNDAR ITIL V3, ESTRUCTURA Y ASPECTOS BÁSICOS

1.1 INTRODUCCIÓN [1]

En la actualidad la información que maneja una empresa es la fuente vital de sus actividades. Su almacenamiento, análisis, producción y distribución dentro de la organización es la medida de calidad de los servicios de Tecnologías de Información [TI] que se proveen a la organización. La Administración de la empresa debe comprender que los servicios de tecnología son cruciales para el correcto funcionamiento del negocio, de ahí que es importante realizar inversiones adecuadas en los servicios críticos como en los sistemas que los apoyan. A pesar de la importancia que tiene la gestión de tecnología, muchas de las empresas no toman con seriedad su planificación. El éxito está en que los servicios que esta provee se acoplen directamente con las necesidades de la empresa y la apoyen en sus procesos diarios. Como resultado, las TI facilitarán la operación del negocio en lugar de entorpecerlo.

En caso de administración incorrecta de la tecnología se tiene riesgo de:

Incremento de costos y horas improductivas
Incumplimiento de los objetivos del negocio.

El estándar ITIL (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de Información, es una guía de gobernanza de TI que consta de varios libros o dominios, que proponen buenas prácticas para cumplir con una adecuada gestión de las tecnologías de la empresa.

[1] Basado en *An Introductory Overview of ITIL V3*.

1.2 NOCIONES DE ITIL[2]

ITIL fue publicado entre 1989 y 1995, por la Oficina de publicaciones del Gobierno Británico motivado por la Agencia Central de Comunicaciones y Telecomunicaciones.

En primera instancia su uso fue principalmente para el Reino Unido y los países bajos. La segunda versión fue publicada como un conjunto de libros entre el 2000 y 2004. Tanto la versión uno como la dos toman en cuenta la entrega y soporte de los servicios.

En el año 2007 ITIL V2 fue sustituida por una mejorada y consolidada tercera versión, la misma que consiste en 5 libros que cubren el ciclo de vida completo del servicio.
A continuación se presenta un mapa con la evolución de ITIL:

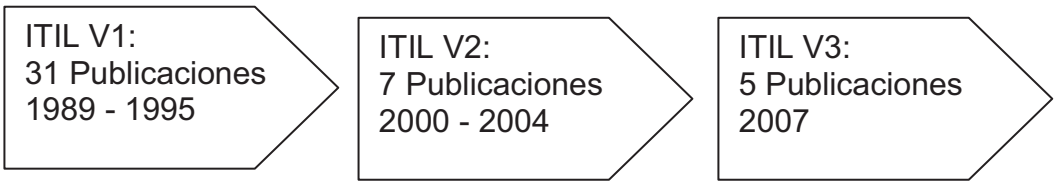

Figura 1-1: Evolución de ITIL

Los cinco libros de ITIL V3 cubren cada etapa del ciclo de vida del servicio (Figura 1-2). Así:

- Desde la definición inicial y análisis de los requerimientos del negocio en Estrategia del Servicio (Service Strategy) y Diseño del Servicio (Service Design).
- Migración en el ambiente real con Transición del Servicio (Service Transition).
- Hasta operación y mejoramiento en tiempo real con Operación de Servicio (Service Operation) y Mejora Continua de Servicio (Continual Service Improvement).

[2] Basado en *An Introductory Overview of ITIL V3, What is ITIL.*

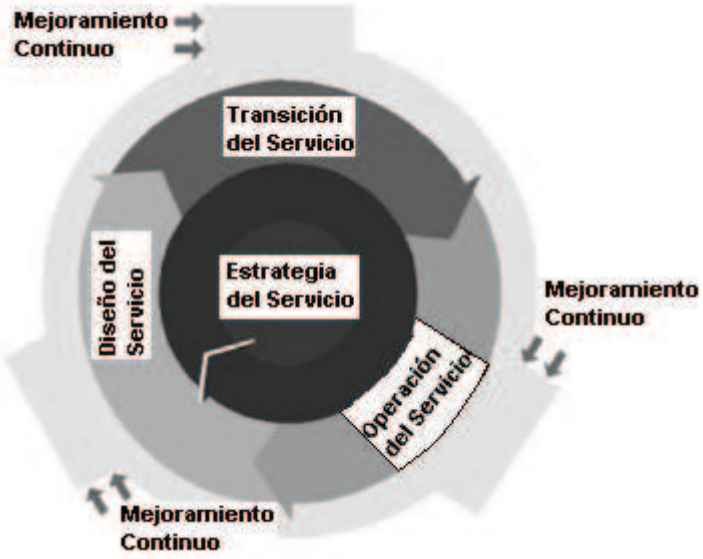

Figura 1-2: Core de ITIL[3]

ITIL es una infraestructura pública que describe las mejores prácticas de administración de servicios de TI, su estructura se enfoca en el monitoreo y mejoramiento continuo de los servicios de tecnología suministrados a la empresa.

El mejoramiento continuo ha sido la clave del éxito para que las organizaciones a lo largo del mundo realicen procesos y técnicas exitosas. Algunos de los beneficios encontrados son los siguientes:

- Incremento de la satisfacción de los usuarios y clientes respecto a los servicios de TI recibidos.
- Mejoramiento en la disponibilidad del servicio, dando como resultado el incremento de ganancias.
- Reducción de costos dado por la optimización en tiempo y recursos de trabajo.
- Reducción en tiempo de operación habitual.
- Mejora en el proceso de toma de decisiones y reduce riesgos.

Las guías de ITIL se pueden adaptar para el uso en diferentes clases de negocios y organizaciones estratégicas. La flexibilidad de la infraestructura permite que el Núcleo pueda ser implementado en una variedad de ambientes. La portabilidad

[3] Obtenido de ITIL versión 3.0, *Service Strategy,Introduction,ITIL and good practice in service management*

incrementa la validez de las guías a lo largo del tiempo, así como de sus opciones para funcionar en diferentes organizaciones.

1.2.1 ESTRUCTURA DE ITIL[4]

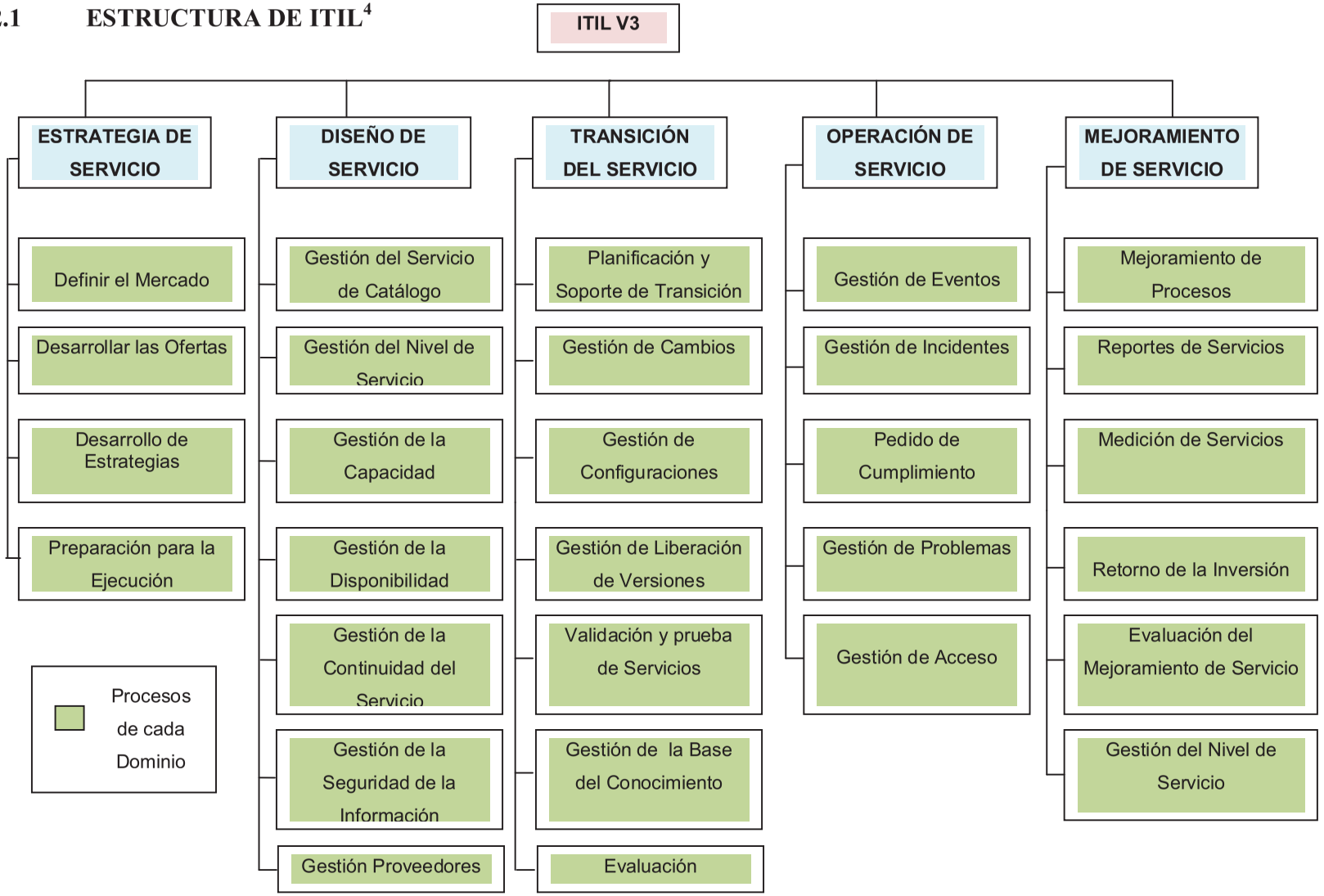

Figura 1-3: Estructura de ITIL

[4] Se basa en los cinco libros de ITIL V3, ver Anexo 1-1.

1.2.2 ESTRATEGIA DE SERVICIO [5]

El dominio Estrategia de Servicio (SS) provee una guía de cómo diseñar, desarrollar e implementar la gestión de un servicio. La estrategia que recomienda ITIL para desarrollar las guías, políticas y procesos se debe basar en el ciclo de vida de un proceso o core de ITIL, de ahí que la estrategia de servicio se basa en el contexto de Diseño de Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio.

La Estrategia de Servicio orienta a dar una guía global de cómo presentar los servicios en el mercado interno (la empresa) y externo (clientes), desarrollando el catálogo y el portafolio de servicios. Además se analizan los riesgos estratégicos a los que se enfrenta la organización.

Las empresas usan estas guías para fijar objetivos y expectativas de desempeño frente al nivel de servicio brindado a los clientes para identificar, seleccionar y priorizar oportunidades. La Estrategia de Servicio se asegura que la empresa está en la posición de manejar el costo y los riesgos que implica su portafolio de servicios, tomando en cuenta el rendimiento óptimo del servicio y no solo el correcto funcionamiento. Las decisiones realizadas al respecto de la Estrategia de Servicio poseen una influencia importante sobre las consecuencias positivas y negativas de la empresa.

Entre sus procesos se encuentran:

- Definir el Mercado: se refiere a servicios, estudio del cliente, y búsqueda de oportunidades.
- Desarrollo de Ofertas: detalla el lugar de mercado (conjunto de buenos resultados que pueden ser facilitados por un servicio), la orientación de la definición de los

[5] *Basado en ITIL versión 3.0, Service Strategy, Introduction,Service Strategy.*

servicios en base a los requerimientos de los usuarios y el portafolio y catálogo de servicios.

- Estrategias de activos: gestión de los recursos para dar un buen servicio a los usuarios.
- Preparación para la Ejecución: implica la formulación de estrategias para proveer un servicio.

1.2.3 DISEÑO DE SERVICIO [6]

El volumen de Diseño de Servicio provee guías para el diseño y el desarrollo de servicios, así como procesos para la gestión de servicios. Además detalla métodos y principios de diseño para convertir objetivos estratégicos en portafolio de servicios. El Diseño de Servicio no se limita a la creación de nuevos servicios, aquí se incluyen las mejoras y cambios necesarios para incrementar o mantener el nivel de servicio a los clientes durante el ciclo de vida de los servicios.

1.2.3.1 Gestión del Servicio de Catálogo[7]

Su propósito es proveer una única fuente de información consistente de todos los servicios acordados formalmente, y asegurar que sea de fácil acceso para el personal autorizado.

1.2.3.2 Gestión de Nivel de Servicio[8]

Realiza las negociaciones, los acuerdos y la documentación formal que reflejen el nivel de servicio que cumplan con los objetivos del negocio, a partir de esta referencia se debe realizar el monitoreo y la generación de reportes del nivel de servicio suministrado en contraste con el nivel de servicio acordado.

---

[6] *Basado en ITIL versión 3.0, Service Design, Introduction,Service Design*
[7] *Basado en ITIL versión 3.0, Service Design,Service Design Processes, Service Catalogue Management*
[8] *Basado en ITIL versión 3.0, Service Design,Service Design Processes, Service Level Management*

1.2.3.3 Gestión de la Capacidad[9]

Es un proceso que se extiende a través del ciclo de vida del servicio. Un factor clave en la Gestión de la Capacidad es que esté previsto en el Diseño de Servicios, aquí se proveen las predicciones y los indicadores de capacidad actual necesarios para alinear la capacidad con la demanda.

El objetivo de la Gestión de la Capacidad, es asegurar que el costo que implica sostener una capacidad para un servicio específico sea justificado, además en todas las áreas la capacidad debe estar en relación con sus necesidades actuales y proyecciones futuras.

1.2.3.4 Gestión de la Disponibilidad[10]

El objetivo del proceso de la Gestión de la Disponibilidad es asegurar que el nivel de servicio con respecto a la disponibilidad sea entregado de acuerdo a las necesidades del negocio, tomando en cuenta el costo frente al beneficio.

1.2.3.5 Gestión de la Continuidad del Servicio[11]

Son todas las actividades que involucran el mantener operativos los servicios de TI en la empresa. Para esto se trabaja en cada etapa del ciclo de vida de los servicios con planes de recuperación que deben estar alineados con el Plan de Continuidad de la Empresa, que a su vez se basa en las prioridades del negocio.

---

[9] *Basado en ITIL versión 3.0, Service Design, Service Design Processes, Capacity Management*
[10] *Basado en ITIL versión 3.0, Service Design, Service Design Processes, Availability Management*
[11] *Basado en ITIL versión 3.0, Service Design, Service Design Processes, IT Service Continuity Management*

1.2.3.6 Gestión de Seguridad de la Información[12]

El objetivo es alinear la seguridad informática con la del negocio y verificar que sea manejada efectivamente con referencia a todos los servicios y actividades que se desarrollen en la empresa.

1.2.3.7 Gestión de Proveedores[13]

Gestiona a los proveedores con los respectivos servicios que ofrecen, así se intenta dar transparencia y calidad a las TI.

1.2.4 TRANSICIÓN DEL SERVICIO[14]

Provee guías para el desarrollo y mejoramiento de las capacidades para la transición de servicios nuevos y modificados a la operatividad. En este volumen se muestra como los requerimientos de Estrategia de Servicio codificados en Diseño de Servicio son correctamente implementadas en la Operación de Servicio, mientras se controlan los riesgos de falla. Además provee buenas prácticas en el manejo de la complejidad relacionado con el cambio en servicios, previniendo consecuencias no deseables y permitiendo la innovación.

1.2.4.1 Planificación y Soporte de Transición[15]

Permite dar habilidad a la empresa para mejorar el manejo de grandes cantidades de cambios en servicios de TI. Además da guías para alinear los planes de transición con las necesidades de los usuarios.

---

[12] *Basado en ITIL versión 3.0, Service Design, Service Design Processes, Information Security Management*
[13] *Basado en ITIL versión 3.0, Service Design, Service Design Processes, Supplier Management*
[14] *Basado en ITIL versión 3.0, Service Transition, Introduction,Service Transition*
[15] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes, Transition Planning and Support*

1.2.4.2 Gestión de Cambios[16]

Los cambios se realizan de varias formas:

- Proactiva: Cuando se busca beneficios para el negocio como reducción de costos o mejoramiento de los servicios.
- Reactiva: Significa resolver errores y adaptarse al cambio de las circunstancias.

Los cambios deberían estar dirigidos a:

- Reducir la exposición a riesgos, limitar sólo al nivel que la empresa lo pueda sostener.
- Minimizar la severidad de cualquier impacto y falla.
- Ser exitoso en el primer intento.

Esta orientación ayuda a dar un beneficio directo a la parte operativa del negocio al planificar los beneficios y remover los riesgos con un ahorro de tiempo y dinero.

1.2.4.3 Gestión de Configuraciones[17]

Da soporte al negocio mediante la emisión de información actualizada y correcta sobre toda la infraestructura tecnológica de la empresa.

1.2.4.4 Gestión de Liberación de Versiones[18]

Tiene como objetivo establecer de forma efectiva el uso de servicios nuevos o que han sufrido algún cambio. Aquí se cubre toda la implementación, desde el diseño de la liberación hasta su inicio en producción.

---

[16] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes,Change Management*
[17] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes,Service Asset and Configuration Management*
[18] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes,Service Release Management*

1.2.4.5 Validación y prueba de Servicios[19]

Mediante la evaluación de los servicios se asegura que estos tengan la calidad que fue prevista durante el diseño y que cumplan con el propósito inicial.

1.2.4.6 Gestión de la Base del Conocimiento[20]

Su objetivo es asegurar que la información apropiada sea entregada al responsable en el lugar y hora correctos, para la toma de decisiones acertadas.

1.2.4.7 Evaluación[21]

Proceso genérico que considera si el rendimiento de algo ha sido aceptable.

1.2.5 OPERACIÓN DE SERVICIO[22]

Este volumen presenta buenas prácticas para la Gestión de Operación de Servicios. Las guías pretenden dar efectividad y eficiencia en el suministro y soporte de servicios, tomando en cuenta las necesidades de los clientes.
Esta guía muestra cómo mantener la estabilidad en la operación de servicios, a pesar de que existan cambios en diseño y niveles de servicio. Aquí las organizaciones tienen acceso a: guías con procesos detallados, métodos y herramientas para el uso en las perspectivas de control reactiva y proactiva.
A directores y operadores se les proporciona el conocimiento que les permita tomar mejores decisiones en áreas como la disponibilidad de servicios, control de la demanda, optimización de la capacidad de utilización, planeación de operaciones y resolución de problemas.

---

[19] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes, Service Validation and Testing*
[20] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes, Knowledge Management*
[21] *Basado en ITIL versión 3.0, Service Transition, Service Transition Processes, Evaluation*
[22] *Basado en ITIL versión 3.0, Service Operation, Introduction, Service Operation*

1.2.5.1 Gestión de Eventos[23]

Un evento es definido como cualquier suceso detectable que tiene algún tipo de relación con la infraestructura de TI, o que pueda causar un efecto negativo sobre los servicios de tecnología. Los eventos son típicamente creados por: servicio, equipo o herramienta de monitoreo.
Esta gestión provee mecanismos para detección temprana de incidentes.

1.2.5.2 Gestión de Incidentes[24]

En ITIL el incidente se define como:
Una interrupción no planificada o la reducción en la calidad de un servicio de TI. La falla de un ítem de configuración que no ha afectado un servicio todavía es también un incidente.
La gestión de Incidentes es el proceso en donde se tratan todos los incidentes de la organización, aquí se incluyen fallas, preguntas o consultas reportadas por los usuarios, usualmente vía llamadas telefónicas al soporte de escritorio o detectadas automáticamente por herramientas de monitoreo de eventos.

1.2.5.3 Pedido de Cumplimiento[25]

Se encarga de negociar los pedidos de servicio de los usuarios. En este proceso se incluye:
Brindar una vía para que los usuarios pidan servicios estándar, con un proceso definido de aprobación.
Dar información a los usuarios sobre niveles de servicio, información general.
Asistir a quejas y comentarios.

---

[23] *Basado en ITIL versión 3.0, Service Operation, Service Processes, Event Management*
[24] *Basado en ITIL versión 3.0, Service Operation, Service Processes, Incident Management*
[25] *Basado en ITIL versión 3.0, Service Operation, Service Processes, Request Fulfilment*

1.2.5.4 Gestión de Problemas[26]

ITIL define un problema como la causa de uno o más incidentes.

1.2.5.5 Gestión de Acceso[27]

Dar permisos de autorización a los usuarios para que puedan usar un servicio específico, de la misma forma se previene el acceso de personal no autorizado.

1.2.6 MEJORAMIENTO DE SERVICIO[28]

Su principal objetivo es realizar los cambios necesarios para que los servicios de TI se mantengan de acuerdo a los cambios del negocio, con esto se identificarán e implementarán mejoras que intervienen en todo el ciclo de vida: Estrategia de Servicio, Diseño de Servicio, Transición del Servicio y Operación del Servicio. El mejoramiento continuo busca todos los caminos para mejorar la efectividad, eficiencia, así como optimización de costos de los procesos.

1.2.6.1 Mejoramiento de Procesos[29]

Consta de 7 pasos entre los cuales se encuentran: definir qué debería y puede ser medido, levantar, procesar y analizar la información necesaria, presentar resultados e implementar acciones correctivas.

---

[26] *Basado en ITIL versión 3.0, Service Operation, Service Processes, Problem Management*
[27] *Basado en ITIL versión 3.0, Service Operation, Service Processes, Access Management*
[28] *Basado en ITIL versión 3.0, Service Improvement, Introduction*
[29] *Basado en ITIL versión 3.0, Service Improvement, Continual Service Improvement processes, 7-step Improvement Process.*

1.2.6.2 Reporte de Servicios

Detalla la elaboración de reportes tomando en cuenta: el propósito, a quien está dirigido y el uso que se le va a dar.

1.2.6.3 Medición de Servicios

Indica las técnicas necesarias para valorar la calidad de servicio que recibe el usuario final.

1.2.6.4 Retorno de la inversión

Muestra los aspectos que se debe tomar en cuenta para realizar un análisis correcto del beneficio obtenido respecto a una inversión.

1.2.6.5 Evaluación del Mejoramiento de Servicio

Describe las preguntas claves que deben ser realizadas para ayudar a la empresa a decidir si las iniciativas de mejoramiento aportan positivamente o no.

1.2.6.6 Gestión del Nivel de Servicio

Proporciona lecciones básicas sobre cómo gestionar la calidad del servicio.

1.3 JUSTIFICACIÓN DE PROCESOS A SER EVALUADOS EN ALIANZA CIA DE SEGUROS

1.3.1 ESTRATEGIA DE SERVICIO

1.3.1.1 Definir el Mercado

Este proceso no ha sido tomado en cuenta para la evaluación por ser actividades que son desarrolladas por el departamento de Mercadeo.

1.3.1.2 Desarrollo de Ofertas

La orientación de la definición de los servicios o el lugar de mercado se lo abarca en el estudio del proceso Gestión de Nivel de Servicio, el mismo que analiza los requerimientos de los usuarios, por esta razón el Desarrollo de Ofertas no ha sido considerado dentro de los procesos de evaluación.

1.3.1.3 Estrategias de activos

El uso de los recursos para dar un buen servicio se cubre en el proceso Gestión de Nivel de Servicio, el mismo que sugiere que en base a las necesidades de los usuarios varíe la asignación de recursos para que las labores que se apoyan en la tecnología se desarrollen con normalidad. Por tal motivo el proceso Estrategias de activos no ha sido considerado dentro de los procesos de evaluación.

1.3.1.4 Preparación para la Ejecución

Este proceso desarrolla el arte de proveer un servicio logrando la satisfacción de los usuarios, concepto que es parte de lo analizado en la Gestión de Nivel de Servicio,

por esto la Preparación para la Ejecución es un proceso que no ha sido considerado para la evaluación.

1.3.2 DISEÑO DE SERVICIO

1.3.2.1 Gestión del Servicio de Catálogo

La descripción de la necesidad de un catálogo de servicios, se la realiza en el proceso Gestión de Nivel de Servicio, por este motivo no es necesario analizarlo como un proceso individual.

1.3.2.2 Gestión de Nivel de Servicio

Este proceso ha sido elegido para evaluar la satisfacción del cliente relacionada directamente con el nivel de calidad que tienen los servicios recibidos. El éxito de la operación del negocio depende del correcto funcionamiento de las herramientas tecnológicas que utilizan los usuarios de la empresa. Además este proceso abarca a su vez a los procesos: Validación y prueba de Servicios.

1.3.2.3 Gestión de la Capacidad

Este proceso no ha sido elegido como parte del grupo a evaluar por ser íntimamente relacionado con la Gestión de Nivel de Servicio, ya que este orienta la capacidad que se debe diseñar para cada servicio, según los niveles de necesidad que presenten los usuarios de la empresa.

1.3.2.4 Gestión de la Disponibilidad

El proceso de Gestión de la Disponibilidad se lo abarca de forma conjunta con los procesos de Gestión de Nivel y Continuidad de Servicio, por esto no ha sido tomado en cuenta como uno de los elegidos para ser evaluados. El Nivel de Servicio indica

cuál será la disponibilidad necesaria para cada servicio y la Continuidad de Servicio ayudará a cumplir con la disponibilidad establecida para cada uno.

1.3.2.5 Gestión de Continuidad de Servicio

Este proceso ha sido elegido para la evaluación de la compañía, dado que sus actividades tienen como objetivo mantener los servicios de la empresa operando ininterrumpidamente. Además abarca los procesos de Gestión de la Disponibilidad, Gestión de Proveedores.

1.3.2.6 Gestión de Seguridad de la Información

Si bien el proceso de Seguridad es de vital importancia para una empresa este no ha sido elegido porque Alianza ya cuenta con un estudio referente a este tema, además la gerencia de sistemas presenta mayor interés en el estudio que se relaciona con la continuidad de sus servicios.

1.3.2.7 Gestión de Proveedores

Al manejar Alianza solamente dos proveedores de servicios externos, uno para comunicaciones y otro para el servicio de antivirus, la gerencia de sistemas no estima necesario realizar un estudio individual de este proceso, a pesar de esto en el Nivel de Servicio se evalúa la calidad que los proveedores externos están cumpliendo así como su nivel de respuesta ante problemas con el proceso Continuidad de Servicio.

1.3.3 TRANSICIÓN DEL SERVICIO

1.3.3.1 Planificación y Soporte de Transición

No ha sido tomado en cuenta como proceso para la evaluación de la empresa, porque este tema es tratado con mayor orientación a las necesidades de Alianza en el proceso Gestión de Cambios.

1.3.3.2 Gestión de Cambios

La Gestión de Cambios ha sido elegido como proceso de evaluación porque la empresa está interesada en revisar cómo se realizan las actividades de transición para sus servicios, además este proceso abarca a Planificación y Soporte de Transición, Gestión de Liberación de Versiones.

1.3.3.3 Gestión de Configuraciones

Este proceso ha sido elegido ya que va de la mano con la Gestión de Cambios. Este proceso se encarga de administrar todas las configuraciones con su respectivo historial, que ha futuro contribuirán para resolver fallas de diferentes servicios. La empresa está interesada en la evaluación de este punto porque reconoce que existen deficiencias en el manejo de esta información.

1.3.3.4 Gestión de Liberación de Versiones

La liberación de Versiones es un subconjunto de lo que abarca la Gestión de Cambios, por esta razón no fue elegido como un proceso para estudio individual.

1.3.3.5 Validación y Prueba de Servicios

La prueba de Servicio al tratar de verificar la calidad de un servicio dado, se encuentra con actividades similares a las realizadas por la Gestión de Nivel de Servicio, tomando en cuenta que este último posee mayor generalidad, la Validación y Prueba de Servicios no ha sido tomado en cuenta para la evaluación de la gestión de tecnología en Alianza.

1.3.3.6 Gestión de la Base del Conocimiento

A pesar de no ser uno de los procesos seleccionados para la evaluación de Alianza, este es implícitamente utilizado en las tareas de Gestión de Cambios y Configuraciones, por esto no es necesario su estudio de manera individual.

1.3.3.7 Evaluación

Detalla el proceso genérico de evaluación, el mismo que se aplica de forma particular para cada proceso seleccionado para evaluar la gestión tecnológica de Alianza.

1.3.4 OPERACIÓN DE SERVICIO

1.3.4.1 Gestión de Eventos

Este proceso toma en cuenta todos los eventos que tengan una relación con la infraestructura de las TI, la gerencia de sistemas no considera necesario evaluar la Gestión de Eventos a detalle, puesto que se prefiere analizar el comportamiento de los eventos cuando ya se convierten en incidentes y el poder de reacción del Departamento de Sistemas (DDS) ante ellos.

1.3.4.2 Gestión de Incidentes

La Gestión de Incidentes ha sido tomada en cuenta por ser el inicio de un posible inconveniente para las TI de la empresa, además la correcta administración de los incidentes de tecnología, para los usuarios es la buena imagen del DDS. La solución rápida y óptima de los incidentes apoyarán a un mejor desenvolvimiento de los usuarios en su trabajo, que como consecuencia provocará un mejor desempeño del negocio en conjunto.

1.3.4.3 Pedido de Cumplimiento

El Pedido de Cumplimiento se lo toma en consideración como tareas que involucran al proceso de Gestión de Nivel de Servicio, aquí se incluye la evaluación con respecto a: la vía y el proceso para hacer la petición de un servicio, dar información general sobre los servicios y asistir comentarios. Poe esta razón este proceso no es estudiado de forma individual.

1.3.4.4 Gestión de Problemas

La Gestión de Problemas ha sido elegida porque la gestión de Incidentes se relaciona directamente con este proceso. La causa de los incidentes son los problemas, mientras mejor trato se le den a los problemas mediante investigación y laboratorio de evaluación se resolverán de mejor manera los incidentes, a tal punto que se identifique los posibles problemas antes de convertirse en incidentes para los usuarios.

1.3.4.5 Gestión de Acceso

Este proceso se abarca con la Gestión de Nivel de Servicio para el aspecto de autorización de los usuarios según su perfil o necesidad, así como la prevención de personal no autorizado.

1.3.5 MEJORAMIENTO DE SERVICIO

1.3.5.1 Mejoramiento de Procesos

Este proceso ha sido tomado en cuenta como guía para la realización de la presente investigación, ya que se usaron los siete pasos propuestos como su estructura. No se aplica su evaluación individual porque la utilidad del proceso está es ser usado como base para el mejoramiento a su vez de otros procesos.

1.3.5.2 Reporte de Servicios

No se lo toma en cuenta para evaluarlo de forma individual, pero sus actividades son utilizadas como guías para la realización de reportes en Gestión de: Nivel de Servicio, Cambios, Configuraciones, Incidentes y Problemas.

1.3.5.3 Medición de Servicios

Las guías de este proceso se las abarca con mayor profundidad en la Gestión de Nivel de Servicio, puesto que valora la calidad de servicio que recibe el usuario final, ya sea este interno o externo. Por esta razón no ha sido tomado en cuenta para su estudio individual.

1.3.5.4 Retorno de la inversión

Este proceso no ha sido tomado en cuenta de forma individual porque sus actividades son implícitamente utilizadas para Gestión de: Nivel de Servicio, Continuidad de Servicio, Cambios, Configuraciones, Incidentes y Problemas. Siempre se realiza un análisis de costo - beneficio antes de cada implementación.

1.3.5.5 Evaluación del Mejoramiento de Servicio

Las actividades de este proceso se las toma en cuenta en la Gestión de: Nivel de Servicio, Continuidad de Servicio, Cambios, Configuraciones, Incidentes y Problemas. Por esta razón no se la tomó en cuenta para su estudio individual.

1.3.5.6 Gestión del Nivel de Servicio

Este proceso es tomado en cuenta pero como parte del dominio Diseño de Servicio, ya que en el dominio Mejoramiento de Servicio, sólo se proponen lecciones básicas sobre cómo gestionar la calidad del servicio.

A continuación se presenta una tabla resumen de cada uno de los 6 procesos elegidos para la evaluación de la Gestión de la empresa según ITIL.

Gestión de Nivel de Servicio			
Objetivos	**Obligaciones**	**Actividades**	**Reportes**
• Definir, documentar, acordar, monitorear, medir, reportar y revisar el nivel de servicio de las TI suministradas. • Proveer y mejorar las relaciones y comunicación entre el negocio y los clientes. • Asegurar que los indicadores sean específicos y medibles para todos los servicios de TI. • Incrementar la satisfacción de los clientes mediante la calidad del servicio suministrado. • Asegurar que las TI y los clientes tengan una clara y no ambigua expectativa del nivel de servicio.	• Asegura que los niveles de calidad de los servicios de TI acordados se cumplan.	• Negociar los acuerdos de Servicio. • Monitorear y medir el desempeño de los servicios. • Revisar y mejorar la satisfacción del cliente. • Producir reportes acerca de los servicios. • Producir un Plan de Mejoramiento Global • Desarrollar y documentar las relaciones que existen entre la empresa y clientes. • Desarrollar procedimientos para ingresar y solucionar todas las posibles quejas. • Mantener la documentación del manejo de Nivel de Servicio, disponible y actualizada.	• Calidad de los Servicios Operacionales. • Catálogo de Servicios. • Nivel de Satisfacción de los usuarios.

Tabla 1-1: Resumen de Gestión de Nivel de Servicio

Gestión de la Continuidad del Servicio

Objetivo

- Disponer de un conjunto de Planes de Continuidad de Servicios de TI, y de recuperación.
- Mantener los Planes de Continuidad de acuerdo a la realidad del negocio.
- Prevenir posibles amenazas que provoquen la paralización del negocio.
- Mantener capacitado al personal en contra de catástrofes.
- Asegurar mecanismos efectivos de continuidad.
- Evaluar los cambios sobre los Planes de Continuidad.
- Realizar mediciones proactivas que mejoren disponibilidad de Servicios.
- Negociar con proveedores su rápida respuesta frente a desastres.

Obligaciones

- Maneja los riesgos del negocio que han sido identificados en el Plan de Continuidad, y asegura que las medidas de recuperación para los servicios de TI estén alineadas con las necesidades, riesgos e impactos sobre el negocio.

Actividades

- Iniciación:
  - Establecer Políticas.
  - Asignar recursos.
- Requerimientos y Estrategia:
  - Evaluación de Riesgos.
  - Análisis de Impacto en el negocio.
  - Discutir opciones de recuperación.
- Implementación:
  - Redactar Planes de Continuidad
  - Evaluar Planes.
- Operación:
  - Enlazar con Gestión de Cambios para actualizar Planes.
  - Capacitar al Dto. de TI.
  - Mejorar Continuamente.
- Invocación de Planes de Continuidad.

Reportes

- Última versión del Análisis de Impacto del Negocio.
- Riesgos registrados.
- La última versión de los Planes de Continuidad del Negocio.
- Detalles de pruebas realizadas y planificadas.
- Contenidos de todos los planes Continuidad.
- Detalles de todos los recursos que ayudan a implementar los Planes de Continuidad.
- Detalles de todos los procesos de recuperación para sistemas y dispositivos de TI.

Tabla 1-2: Resumen de Gestión de Nivel de Servicio

Gestión de Cambios

Objetivos	Obligaciones	Actividades	Reportes
• Usar procedimientos estandarizados para realizar cambios. • Relacionarse con el Sistema de Manejo de Configuración. • Reducir riesgos.	• Responder a pedidos de cambios del negocio. • Implementar cambios que cumplan con el nivel de servicio acordado. • Contribuir a una gobernanza formal. • Monitorear los cambios a lo largo del ciclo de vida de los servicios. • Estimar calidad, tiempo y costo de un cambio. • Evaluar los riesgos asociados con la transición de un servicio. • Reducir el tiempo de restauración del servicio. • Favorecer al mejorameinto continuo.	• Crear y registrar el pedido de cambio. • Revisar la petición de cambio. • Evaluar el cambio. • Autorizar el cambio. • Coordinar la implementación de cambios. • Revisar y cerrar cambios	• Pedidos de Cambio rechazados y aprobados. • Planificación de Cambios. • Cambios realizados sin autorización.

Tabla 1-3: Resumen de Gestión de Cambios

Gestión de Configuraciones			
Objetivos	**Obligaciones**	**Actividades**	**Reportes**
• Gestionar de forma ordenada la configuración de equipos de TI. • Dar soporte a las necesidades del negocio y clientes. • Proveer con información de configuración acertada. • Reducir el número de configuraciones erróneas. • Optimizar los recursos que usan los servicios y las configuraciones de TI.	• Mejorar el pronóstico y la planificación de cambios. • Organizar e implementar los cambios con éxito. • Resolución de incidentes y problemas de acuerdo a los niveles de servicio establecidos. • Controla los servicios del negocio. • Ayuda a identificar el costo de un servicio.	• Manejo y Planificación de Configuraciones. • Identificación de la Configuración • Control de Configuración. • Asignación de estado a los ítems de configuración • Generación de reportes. • Verificación y auditoría.	• Detalles para soporte en la toma de decisiones. • Historia y progreso que han tenido las configuraciones de cada ítem.

Tabla 1-4: Resumen de Gestión de Configuraciones

Gestión de Incidentes

Objetivo	Obligaciones	Actividades	Reportes
• Restaurar la normal operación de los servicios lo más rápido posible. • Minimizar el impacto negativo de Incidentes sobre las operaciones del negocio. • Asegurar niveles de calidad y disponibilidad de servicios según los acuerdos internos de la empresa.	• Disminuir el tiempo que el negocio no pueda operar. • Dar la habilidad para alinear las actividades de tecnología con las prioridades del negocio. • Identificar potenciales mejoras a los servicios. • Determinar servicios adicionales o entrenamiento requerido en la empresa.	• Identificación de Incidentes. • Registro de Incidentes. • Categorización de Incidentes. • Dar prioridad a los Incidentes. • Diagnóstico Inicial. • Escalamiento de Incidentes • Investigación y Diagnóstico • Resolución y Recuperación. • Cierre de Incidente.	• Registros anteriores de Incidentes. • Acciones tomadas para resolución de Incidentes. • Acciones de diagnóstico implementadas para resolver un incidente. A futuro estos reportes ayudarán a resolver con mayor agilidad inicidentes similares.

Tabla 1-5: Resumen de Gestión de Incidentes

Gestión de Problemas

Objetivo	Obligaciones	Actividades	Reportes
• Administrar todos los problemas que han ocurrido en la organización, así como su ciclo de vida. • Prevenir que ocurran problemas que a su vez generan incidentes, que pueden hacerse recurrentes. • Causar el menor impacto para la organización frente a incidentes que no pueden ser evitados.	• Promover la disponibilidad de los servicios de TI. • Incrementar la productividad del negocio y del personal del departamento técnico. • Reducir costos en procedimientos que no funcionan. • Reducir incidencia de sucesos ya superados.	• Detección del Problema. • Ingreso del Problema • Categorización del Problema. • Priorización del Problema. • Diagnóstico e Investigación del Problema. • Soluciones Provisionales. • Creación de un Registro de Error Conocido. • Resolución del Problema. • Cierre del Problema. • Revisión de Problemas Importantes.	• Detalles de todos los elementos de la infraestructura de TI, así como de las relaciones entre ellos. • Conocimiento adquirido anteriormente acerca de incidentes y problemas, sobre cómo han sido superados para diagnosticar y resolverlos de forma rápida.

Tabla 1-6: Resumen de Gestión de Problemas

CAPÍTULO II: ANÁLISIS DE LA GESTIÓN ACTUAL DE IT DE ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A. CON REFERENCIA A ITIL V3

2.1 ALIANZA COMPAÑÍA DE SEGUROS[30]

A continuación se presenta información general de la compañía objeto de esta investigación.

2.1.1 RESEÑA HISTÓRICA

Alianza Compañía de Seguros y Reaseguros SA., inició sus operaciones en 1982, con su oficina Matriz ubicada en la ciudad de Quito y dos sucursales en las ciudades de Guayaquil y Cuenca. Posteriormente incursionó en el puerto de Manta, en donde funciona la sucursal desde 1990. La compañía desde el inicio de sus operaciones, opera en el ramo de seguros generales.

Los socios fundadores de la compañía fueron los señores Alvaro Ramón Florez Menéndez (+) y Carlos Romero Romero (+) de nacionalidad española, con amplia experiencia en el área de seguros.

La experiencia alcanzada por la compañía, durante estos años de servicio, la solvencia técnica, el respaldo de Reaseguradores locales e internacionales, la solidez financiera, el posicionamiento en el mercado en Seguros Generales y el servicio post venta, permiten que se posicione en el mercado como una empresa de primer nivel dentro del negocio de los seguros del país.

[30]Información facilitada por la Ejecutiva de Cuenta Ing. Paola Pérez

2.1.2 MISIÓN

"Ser una empresa que contribuye al desarrollo socioeconómico del país, brindando protección, seguridad y cobertura al patrimonio de nuestros asegurados, ante la posibilidad de que ocurran eventos inesperados. Prestando Servicios de Excelencia que garanticen la satisfacción del cliente y nos permita obtener resultados que sean en beneficio de nuestros colaboradores, buscando siempre maximizar el valor patrimonial".

2.1.3 VISIÓN

"Liderar el mercado de seguros ecuatoriano, alcanzando la excelencia en los servicios que préstamos a nuestros clientes, en el ámbito de Seguros Generales, que nos permita ser una empresa aseguradora reconocida en el mercado por su cultura organizacional".

2.1.4 SUCURSALES

- Quito.
- Cuenca.
- Guayaquil.
- Manta.
- Santo Domingo.
- Machala.
- Milagro.

2.1.5 LÍNEAS DE PRODUCCIÓN

- Incendio.
- Transporte.
- Casco marítimo.
- Fidelidad pública y privada.
- Vehículos.

- Accidentes personales.
- Robo y/o asalto.
- Casco aéreo.
- Cumplimiento de contrato.
- Seriedad de oferta.
- Buen uso de anticipo.
- Garantías aduaneras.
- Responsabilidad civil.
- Rotura de maquinaria.
- Equipo y maquinaria de contratistas.
- Todo riesgo para contratistas.
- Montaje de maquinaria.
- Equipo electrónico.
- Multiriesgo.
- SOAT.

2.2 INFRAESTRUCTURA DE LA RED DE ALIANZA COMPAÑÍA DE SEGUROS[31]

2.2.1 DIAGRAMA GENERAL DE CONECTIVIDAD ENTRE SUCURSALES

La estructura de red de Alianza CIA. de Seguros y Reaseguros S.A., tiene una topología tipo estrella, donde el nodo central es la sucursal de Quito.
El proveedor de los enlaces dedicados entre Quito y las sucursales es MEGADATOS.

A continuación se presenta el diagrama general de la red:

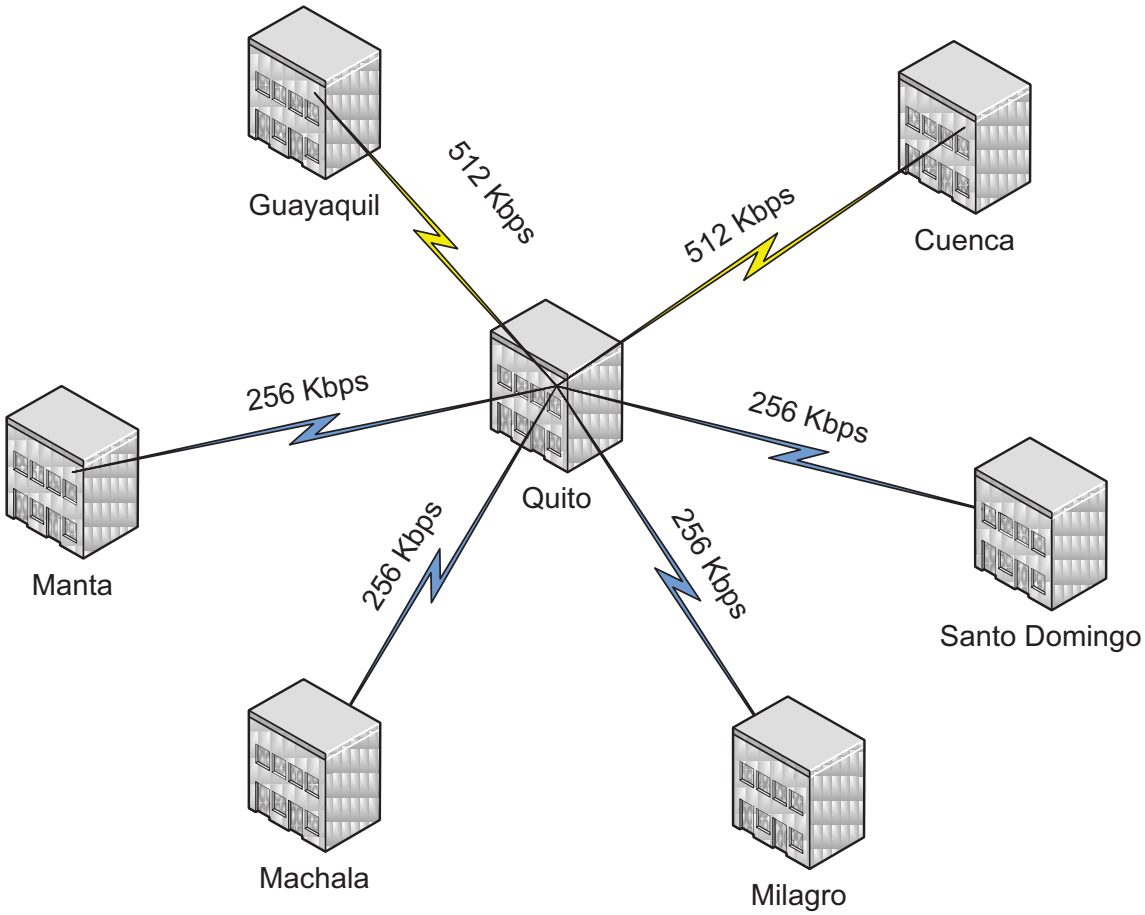

Figura 2-1: Diagrama General de la red de Alianza CIA de Seguros y Reaseguros S.A.

[31] Información facilitada por el Operario del Departamento de Sistemas Ing. Patricio León.

2.2.2 SUCURSAL QUITO

Oficina principal ubicada en Av. 12 de Octubre N 24-359 y Baquerizo Moreno, teléfono PBX 256-6143

2.2.2.1 Diagrama de Red

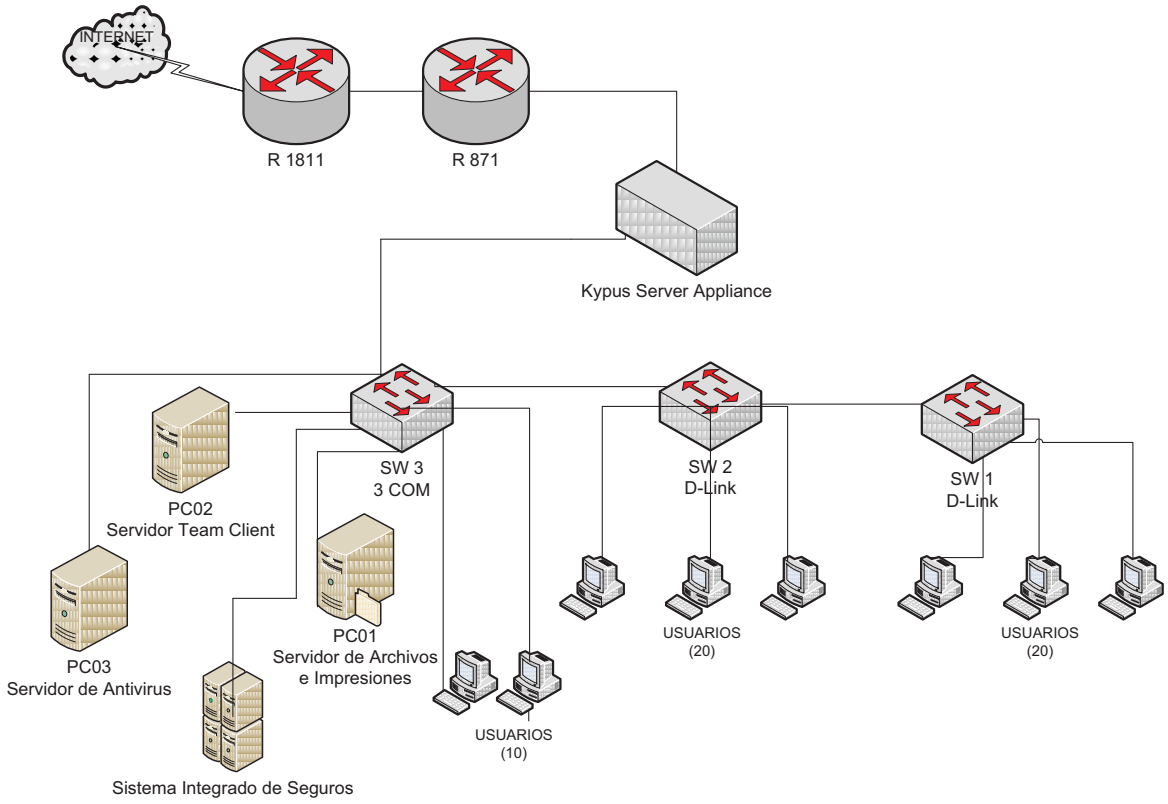

Figura 2-2: Diagrama de Red Sucursal Quito

2.2.2.2 Servidores

En esta ciudad se concentran todos los servicios de tecnología, a continuación se presentan las características de cada uno de ellos:

Servidores en computadores no dedicados:

ID	SERVICIOS	MARCA	TIPO	RAM	DISCO	PROCESADOR
PC01	Transferencia de archivos Impresiones Active Directory	COMPAQ	ML 370	512 MB	40 GB	2.8 GHz
PC02	THIN CLIENT	-	CLON	2 GB	320 GB	Core2Quad 2.4 GHz
PC03	Antivirus – Mcafee	-	CLON	4 GB	500 GB	Core2Quad 2.4 GHz

Tabla 2-1: Detalle de Servidores de Sucursal Quito en equipos no dedicados

Servidores en Equipos Dedicados:

ID	SERVICIOS	MARCA	TIPO	RAM	DISCO	PROCESADOR
Kypus	Firewall Correo Electrónico Filtro de Contenido FTP DHCP	Kypus	Server Appliance	2 GB	160 GB	P4 3.6 Ghz
AS400	Sistema Integrado de Seguros	IBM	9406-520	2 GB	140 GB	2400CPW

Tabla 2-2: Detalle de Servidores de Sucursal Quito en equipos dedicados

2.2.2.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	D-Link	DES-1024R	24
SW2	D-Link	DES-1024R	24
SW3	3COM	4200	26

Tabla 2-3: Detalle de Switches de Sucursal Quito

Router:

ID	MARCA	SERIE	PUERTOS LAN
R871	CISCO	871	4
R1811	CISCO	1811	8

Tabla 2-4: Detalle de Routers de Sucursal Quito

2.2.3 SUCURSAL GUAYAQUIL

Oficina ubicada en Av. 9 de Octubre y G. Córdova Edificio San Francisco 300 piso 11 Oficina 1, teléfono PBX 256-4555.

2.2.3.1 Diagrama de Red

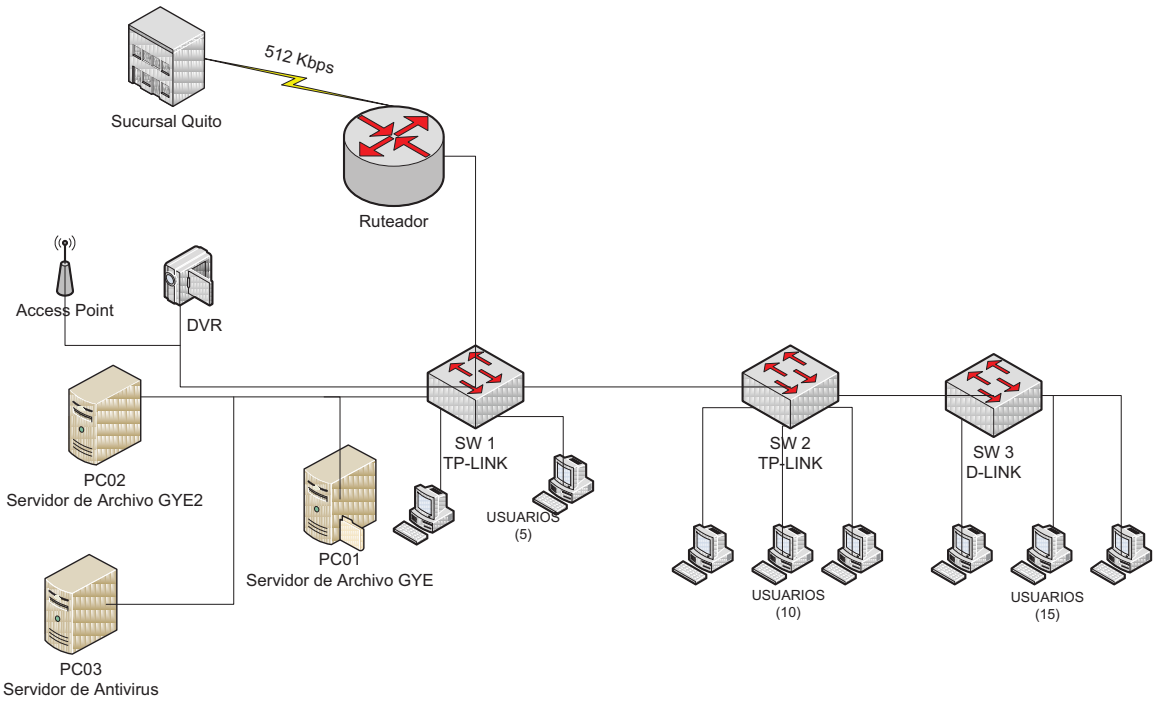

Figura 2-3: Diagrama de Red Sucursal Guayaquil

2.2.3.2 Servidores

A continuación se presentan las características de cada uno de los servidores locales:

Servidores en computadores no dedicados:

ID	SERVICIOS	MARCA	TIPO	RAM	DISCO	PROCESADOR
PC01	Transferencia de archivos	COMPAQ	DESKPRO	192 MB	40 GB	P III 1 GHz
PC02	Transferencia de archivos	-	CLON	2 GB	320 GB	Dual Core 2.2 GHz
PC03	Antivirus – Mcafee	-	CLON	2 GB	320 GB	Dual Core 2.2 GHz

Tabla 2-5: Detalle de Servidores de Sucursal Guayaquil en equipos no dedicados

Servidores en Equipos Dedicados:

ID	SERVICIOS	MARCA	TIPO	RAM	DISCO	SENSORES
DVR	Grabador de Vídeo digital	ROXSAT	4CH .H264	1 GB	500 GB	4 Entradas y 1 salida

Tabla 2-6: Detalle de Servidores de Sucursal Guayaquil en equipos dedicados

2.2.3.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	TP-Link	TL-SG1024	24
SW2	TP-Link	TL-SG1024	24
SW3	D-Link	DES-1024R+	24

Tabla 2-7: Detalle de Switches de Sucursal Guayaquil

Access Point:

ID	MARCA	TIPO	PROTOCOLOS
WIRELESS	D-Link	AIR PLUS X TREME G	802.11 b/g

Tabla 2-8: Detalle de AP de Sucursal Guayaquil

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	871	4

Tabla 2-9: Detalle de Router de Sucursal Guayaquil

2.2.4 SUCURSAL CUENCA

Oficina ubicada en Capulíes 186 y Cañaro, teléfono 282-3972.

2.2.4.1 Diagrama de Red

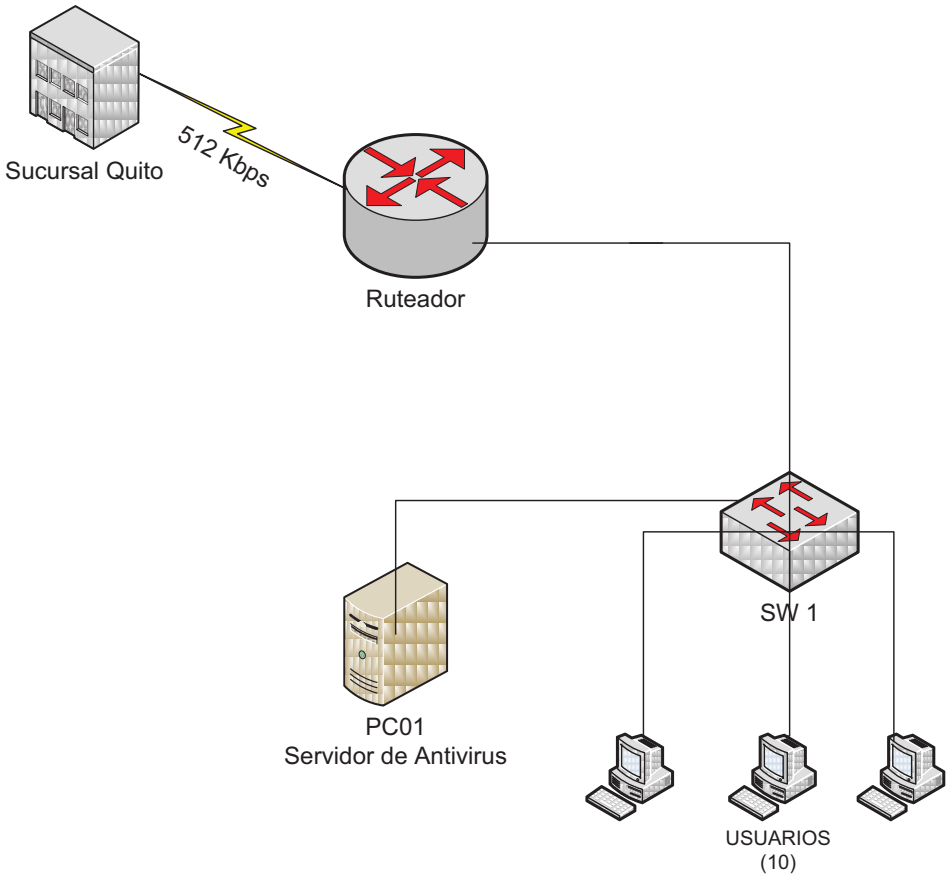

Figura 2-4: Diagrama de Red Sucursal Cuenca

2.2.4.2 Servidores

A continuación se presentan las características de cada uno de los servidores locales:

Servidores en computadores no dedicados:

ID	SERVICIOS	MARCA	TIPO	RAM	DISCO	PROCESADOR
PC01	Antivirus – Mcafee	-	CLON	2 GB	320 GB	Dual Core 2.2 GHz

Tabla 2-10: Detalle de Servidores de Sucursal Cuenca en equipos no dedicados

2.2.4.3 Equipos de Conectividad

Switch:

ID	MARCA	TIPO	PUERTOS
SW1	TP-Link	TL-SG1024	24

Tabla 2-11: Detalle de Switches de Sucursal Cuenca

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	871	4

Tabla 2-12: Detalle de Router de Sucursal Cuenca

2.2.5 SUCURSAL MANTA

Oficina ubicada en Barrio Umiña, Av. Flavio Reyes Calle 26, Edificio Aries planta baja, teléfono 262-2870.

2.2.5.1 Diagrama de Red

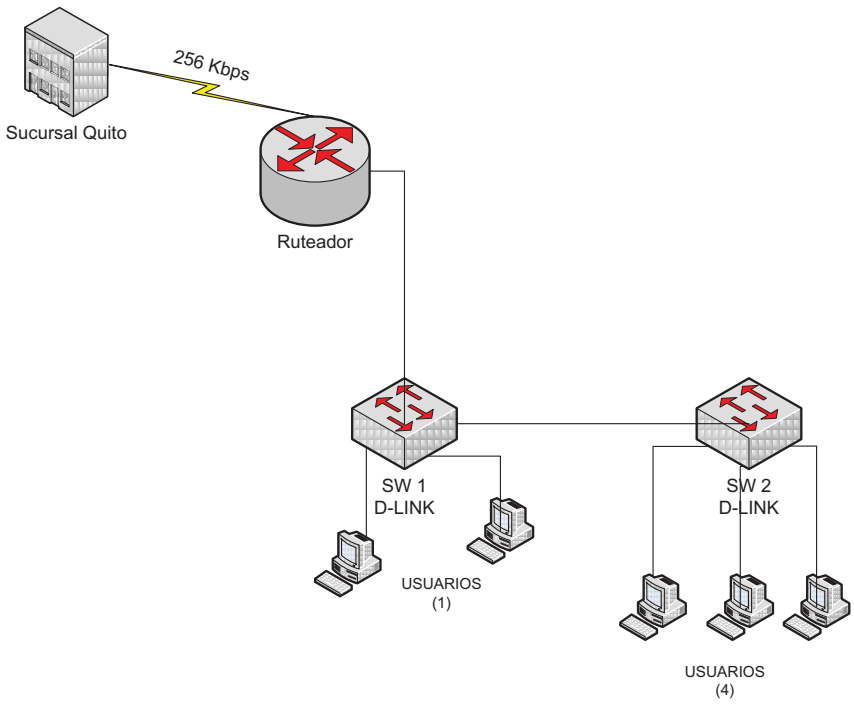

Figura 2-5: Diagrama de Red Sucursal Manta

2.2.5.2 Servidores

La sucursal de Manta no posee servidores locales. Los usuarios actualizan su antivirus enlazándose con el servidor de repositorios de Guayaquil.

2.2.5.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	D-Link	DES-1008D	8
SW2	D-Link	DES-1024R+	24

Tabla 2-13: Detalle de Switches de Sucursal Manta

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	1601R	1

Tabla 2-14: Detalle de Router de Sucursal Manta

2.2.6 SUCURSAL SANTO DOMINGO

2.2.6.1 Diagrama de Red

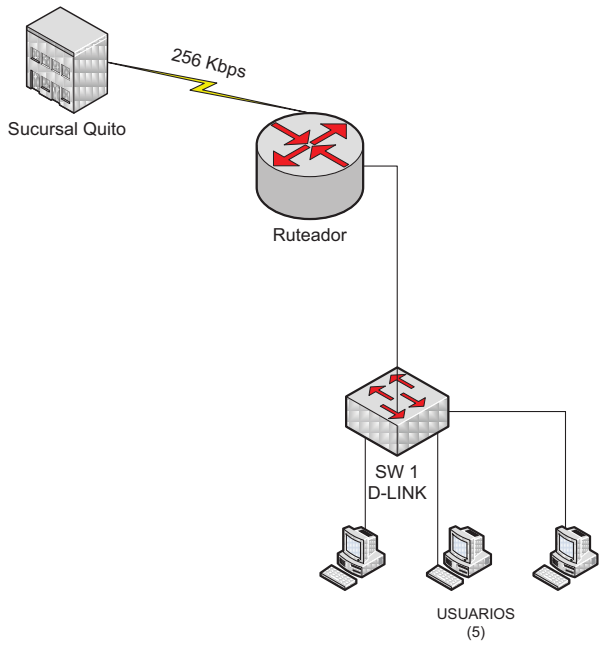

Figura 2-6: Diagrama de Red Sucursal Santo Domingo

2.2.6.2 Servidores

La sucursal de Santo Domingo no posee servidores locales. Los usuarios actualizan su antivirus enlazándose con el servidor de repositorios de Quito.

2.2.6.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	D-Link	DES-1008D	8

Tabla 2-15: Detalle de Switches de Santo Domingo

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	1601R	1

Tabla 2-16: Detalle de Router de Santo Domingo

2.2.7 SUCURSAL MACHALA

2.2.7.1 Diagrama de Red

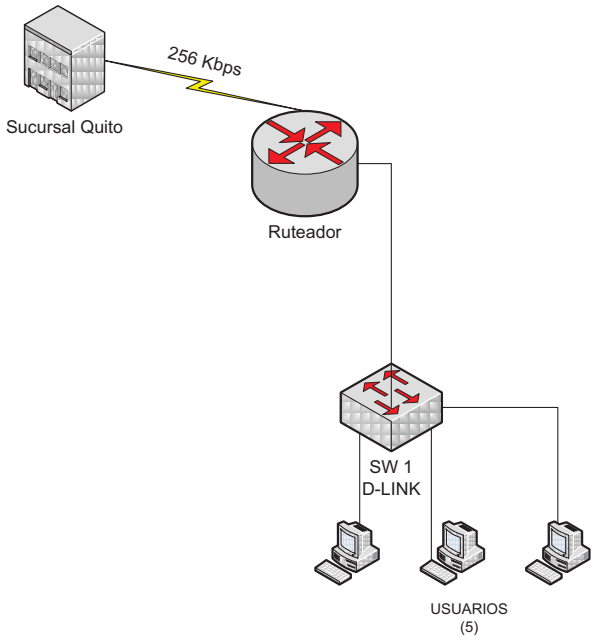

Figura 2-7: Diagrama de Red Sucursal Machala

2.2.7.2 Servidores

La sucursal de Machala no posee servidores locales. Los usuarios actualizan su antivirus enlazándose con el servidor de repositorios de Guayaquil.

2.2.7.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	D-Link	DES-1008D	8

Tabla 2-17: Detalle de Switches de Machala

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	871	4

Tabla 2-18: Detalle de Switches de Machala

2.2.8 SUCURSAL MILAGRO

2.2.8.1 Diagrama de Red

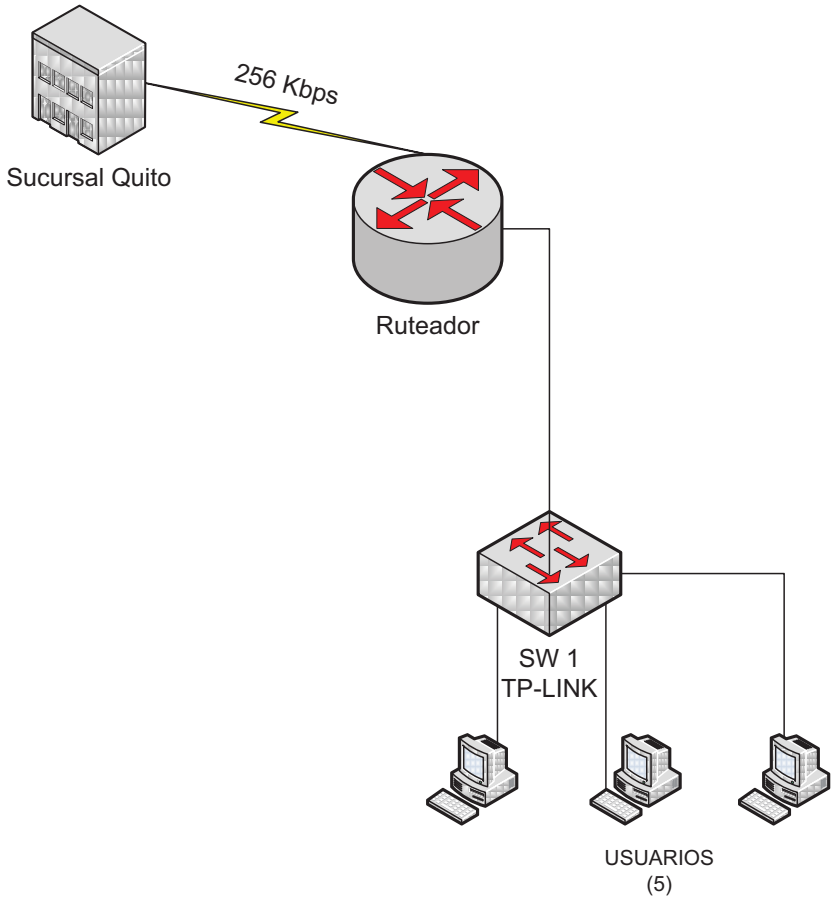

Figura 2-8: Diagrama de Red Sucursal Milagro

2.2.8.2 Servidores

La sucursal de Milagro no posee servidores locales. Los usuarios actualizan su antivirus enlazándose con el servidor de repositorios de Guayaquil.

2.2.8.3 Equipos de Conectividad

Switches:

ID	MARCA	TIPO	PUERTOS
SW1	TP-Link	TL-SG1024	24

Tabla 2-19: Detalle de Switches de Machala

Router:

ID	MARCA	SERIE	PUERTOS LAN
ROUTER	CISCO	1601R	1

Tabla 2-20: Detalle de Router de Machala

2.3 RECOPILACIÓN DE INFORMACIÓN DE LOS PROCESOS DE GESTIÓN DE TI

El levantamiento de información se basa en encuestas realizadas al personal de la compañía. Los entrevistados han sido clasificados en los siguientes grupos:

Ejecutivos (3): Las encuestas al personal Ejecutivo de la empresa se las realizó personalmente de parte del autor, ver anexo 2-1.
Gerente de Sistemas: La entrevista se la realizó en una reunión directamente con el Ing. Pablo Herrera, ver anexo 2-2.
Empleados del DDS: Los dos operadores de Quito y el de Guayaquil, enviaron la respuesta a la encuesta vía correo electrónico. Previo a este punto se realizó una introducción de ITIL para el personal operativo del área de Sistemas, ver anexo 2-3.
Usuarios Comunes: Los usuarios internos de la empresa, fueron evaluados utilizando la creación de un aula virtual llamada ITIL V3, en el portal "Futuro Virtual Educativo"[32], ver anexo 2-4.
Puntos de Venta SOAT a Nivel Nacional: Los Puntos de Venta fueron entrevistados vía telefónica, directamente por el autor, ver anexo 2-5.

Para cada grupo existen encuestas determinadas que se adaptan a sus roles y actividades específicas.

Las encuestas pueden ser de dos tipos:

[32] El enlace para la encuesta es: http://www.ecuadorfuturo.com/educativo/course/category.php?id=10, seleccionar ITIL V3.

Con preguntas de respuesta cerrada, valoradas según las buenas prácticas de ITIL V3.
Con preguntas de respuesta abierta para evaluar las métricas que sugieren las buenas prácticas de ITIL V3.

Todos los grupos de usuarios poseen los dos tipos de encuestas, con la excepción de los usuarios comunes y puntos de venta SOAT que sólo tienen preguntas con respuesta cerrada.

2.3.1 INDICADORES A SER EVALUADOS PARA EJECUTIVOS

2.3.1.1 Gestión de Nivel del Servicio

Descripción

Los indicadores elegidos en la sección de “Respuesta Cerrada”, tienen como objetivo encontrar qué nivel de conocimiento tienen los ejecutivos respecto a los servicios que reciben de parte del DDS, su satisfacción en calidad y su predisposición de apoyo para la mejora de los servicios de tecnología.
Las métricas se encargan de obtener un detalle de los servicios con sus respectivas calidades, esto ayuda a observar para cuáles servicios existe satisfacción y para cuáles no.

Respuesta Cerrada

Conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.
Entrega de documentación formal que informe los servicios que provee el DDS.
Calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.
Grado de apoyo a proyectos que mejoren el nivel de servicio que provee el DDS.

Métricas

Cumplimiento de la calidad de Servicios requerida.

Servicio 1 (Calidad).

Servicio 2 (Calidad).

Servicio N (Calidad).

2.3.1.2 Gestión de Continuidad del Servicio

Descripción

El indicador de “Respuesta Cerrada”, busca confirmar el apoyo que estarían dispuestos a dar los ejecutivos para la realización de planes de contingencia, que aseguren alta disponibilidad para los servicios que se apoyan en la tecnología.

En las “Métricas” se busca conocer las emergencias que han afectado al grupo de Ejecutivos así como tiempo de duración y nivel de preparación frente a las mismas. Adicionalmente se consulta a este grupo, sobre los cortes del servicio más importante de la empresa, en este caso el Sistema de Seguros, con este dato se conocerá la disponibilidad actual aparente del servicio.

Respuesta Cerrada

Nivel de apoyo para el desarrollo de planes de contingencia que aseguren la continuidad del servicio en épocas de emergencia.

Métricas

Nivel de preparación frente a emergencias sufridas.

Emergencia 1 (Nivel de preparación).

Emergencia 2 (Nivel de preparación).

Emergencia N (Nivel de preparación).

Tiempo que han afectado emergencias pasadas el normal desempeño del trabajo.

Emergencia 1 (Tiempo).

Emergencia 2 (Tiempo).

Emergencia N (Tiempo).

Disponibilidad del Sistema de Seguros.

2.3.1.3 Gestión de Cambios

Descripción

Los indicadores de “Respuesta Cerrada” para Gestión de Cambios, buscan conocer como se manejan los cambios desde el punto de vista de los Ejecutivos de la empresa, usando las siguientes premisas. En primer lugar se consulta si por los menos las peticiones de cambios son receptadas por un DDS, el mismo que cuando planifique la realización de un cambio debe informar a sus usuarios sobre esta transición, para que su trabajo no se vea afectado. Adicionalmente la realización de un cambio según ITIL debe tener el objetivo de realizar innovación y mejoramiento, de ahí que se consulta a los ejecutivos la percepción de mejora o por el contrario de enmendación de errores cuando de implementar cambios se refiere. Luego para conocer la satisfacción de los Ejecutivos que se da de forma general, se pregunta el Nivel de satisfacción de los cambios realizados por el DDS, a pesar de esto ITIL sugiere registrar una calificación formal de la calidad del servicio recibido, por esto se añade un indicador que consulta si existe un método de calificación para marcar la satisfacción de los ejecutivos. Finalmente dentro de “Respuesta Cerrada”, se consulta si los ejecutivos han recibido reportes de parte del DDS con respecto al éxito dentro de un periodo específico, esto porque ITIL sugiere que se generen informes para evaluar la calidad de los servicios prestados, durante un período dado.

Para las métricas se tomaron en cuenta los indicadores que pueden ser medidos de los utilizados en “Respuesta Cerrada”. De ahí se obtuvo al porcentaje de cambios que fueron solicitados por los ejecutivos frente a los que realmente fueron atendidos, así como los cambios que no fueron debidamente notificados y provocaron que se afecte el trabajo normal de los usuarios.

Respuesta Cerrada

Recepción de cambios de software o hardware de parte del DDS.

Notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.

Frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.

Frecuencia de cambios realizados por el DDS que tengan como objetivo correcciones.

Nivel de satisfacción de los cambios realizados por el DDS.

Método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.

Indicadores que muestren el éxito en la implementación de cambios de parte del DDS a lo largo del 2009.

Métricas

Cambios implementados vs solicitados.

Número de cambios que afectaron el desenvolvimiento normal del trabajo.

2.3.1.4 Gestión de Configuraciones[33]

Descripción

Dado que la Gestión de Configuraciones es un proceso que mayormente posee actividades realizadas netamente por el DDS, sólo existen dos indicadores en "Respuesta Cerrada" y ninguno para "Métricas". A pesar de esto, se considera necesario conocer si se percibe la realización de configuraciones de forma metódica y ordenada, así como el nivel de apoyo para automatizar procesos de configuración. Estos indicadores sólo se aplican a la Ejecutiva Elizabeth Vallejo, debido a que el DDS se reporta directamente a la dependencia que dirige esta ejecutiva.

Respuesta Cerrada

Realización de configuraciones por el DDS de forma metódica y ordenada.

Apoyo en proyectos que tengan como objetivo la automatización de configuración de equipos.

[33] La Gestión de Configuraciones sólo se aplica a la Gerente de Administración Financiera, Elizabeth Vallejo

2.3.1.5 Gestión de Incidentes

Descripción

Los indicadores de “Respuesta Cerrada”, para el grupo de Ejecutivos tienen como objetivo verificar el apoyo de este grupo daría para el desarrollo de la Gestión de Incidentes. Luego se evalúa el método con el que el DDS atiende a los incidentes que son generados por los ejecutivos, es decir el método de gestión de su incidente.

La prevención de un incidente debe ser la primera opción para que este no suceda y afecte a los usuarios, de ahí que ITIL sugiere dar recomendaciones a los usuarios para que de alguna manera prevengan las amenazas informáticas. Por esto se sugieren como indicadores a “Notificación de posibles amenazas tecnológicas” y “Capacitación a los usuarios de parte del DDS”.

Para este grupo además se busca conocer si con frecuencia los incidentes de tecnología los afectan o si se repiten con frecuencia incidentes específicos. Esto ayuda a identificar si el grupo es afectado en consideración por incidentes tecnológicos.

Los incidentes en ocasiones se generan por carencia de recursos tecnológicos, por esto se añadió un indicador que busca conocer de forma general la satisfacción de la tecnología frente a las necesidades de los usuarios.

El DDS para explotar el potencial de la tecnología que maneja y prevenir amenazas emergentes, debe estar en continua actualización. Por esto existe un indicador que mide la percepción de la evolución de la tecnología en la empresa.

El usuario muchas veces al recibir un mal servicio ya sea con tiempos de solución altos o falta de apertura para recibir sugerencias, tiende a tratar de resolverlo él mismo con un procedimiento intuitivo que puede llevar a que el incidente se agrave. Por esto se tienen a los indicadores “apertura del DDS para recibir sugerencias” y a “Satisfacción del usuario frente al tiempo de solución de incidentes”.

Finalmente como según ITIL todo servicio debe ser calificado formalmente, se coloca al indicador “Método de calificación del servicio recibido de parte del DDS”.

Los indicadores para “Métricas”, tratan de medir u obtener con mayor detalle información acerca de los indicadores de “Respuesta Cerrada”. Por esto se coloca

a “Tiempo promedio de solución de incidentes”, para conocer en concreto tiempos de solución según este grupo. De la misma manera a “Incidentes Frecuentes”, para los cuales en conjunto con la gerencia de sistemas, se tomó en cuenta varios incidentes tipo para conocer la frecuencia en que sucede cada uno. Finalmente como conclusión se inserta al indicador “Calificación general para el DDS respecto a resolución de incidentes”, para conocer el nivel de satisfacción del grupo a pesar de alguna falencia percibida.

Respuesta Cerrada

Grado de apoyo a proyectos que mejoren el servicio prestado por las tecnologías de Información.
Método de Gestión de su incidente.
Notificación de posibles amenazas tecnológicas.
Frecuencia de incidentes que afectan el normal desempeño de su trabajo.
Satisfacción de los recursos tecnológicos asignados.
Percepción de la evolución de la tecnología en la empresa.
Apertura del DDS para recibir sugerencias.
Capacitación a los usuarios de parte del DDS.
Satisfacción del usuario frente al tiempo de solución de incidentes.
Frecuencia de incidentes específicos.
Método de calificación del servicio recibido de parte del DDS.

Métricas

Tiempo promedio de solución de incidentes.
Incidentes frecuentes.
Calificación general para el DDS respecto a resolución de incidentes.

2.3.1.6 Gestión de Problemas

Descripción

Los indicadores para Gestión de Problemas sólo son del tipo “Respuesta Cerrada”. A continuación se describe a cada uno de ellos.

Con el fin de comprobar si existe diferencia de prioridades entre resolución de incidentes y problemas, se inserta el indicador “Urgencia para restablecer sus actividades laborales inmediatamente”, esta representa que los incidentes sean resueltos antes de los problemas.

Debido a que los problemas requieren un estudio profundo para su resolución, por ser causantes de los incidentes, se estima necesario contar con personal dedicado para realizar este análisis, de ahí que es importante evaluar al segundo indicador.

Finalmente el tercer indicador, ayuda a evaluar si los incidentes que se han realizado han sido relacionados con un problema específico, ya que si es así el momento en que se repite el incidente se corta de raíz el problema que antes ya debía ser identificado. Si sucede lo contrario denota que no existe un estudio profundo de los problemas ocurridos.

Respuesta Cerrada

Urgencia para restablecer sus actividades laborales inmediatamente.

Apoyo a desarrollar un equipo especialista para resolver problemas de TI.

Rapidez en resolución de incidentes que ya han sucedido anteriormente.

2.3.2 INDICADORES A SER EVALUADOS PARA GERENTE DE SISTEMAS

2.3.2.1 Gestión del Nivel de Servicio

Descripción

El indicador “Monitoreo del Servicio de Internet recibido”, es útil para constatar que se cumpla el acuerdo firmado de calidad entre Alianza y la empresa proveedora de Internet. Por otro lado el monitoreo de Internet suministrado, permite controlar la calidad que se les otorga a los usuarios de este servicio. Como parte de la gestión de calidad es importante tomarlo en cuenta. Como respaldo al monitoreo se encuentran los indicadores de: “Historial del servicio de Internet” e “Historial de la calidad de los servicios suministrados”.

Dado que el Sistema de Seguros se encuentra en Quito y las sucursales se conectan a él de forma distribuida por los enlaces WAN dedicados, se estima

necesario incluir al indicador “Monitoreo de enlaces WAN”, para control de la calidad de enlace.

Una forma de fijar un nivel de calidad que se obliga a cumplir al proveedor de servicios es mediante un contrato, para evaluar este tema se insertó el indicador “Contratos formales de nivel de servicio”. Así mismo para generar dichos contratos en primer lugar se procede con lo que evalúa el indicador “Identificación de necesidades para implementar un servicio”, con las necesidades identificadas se procede con la especificación de los niveles de calidad, lo cual es referente al indicador “Especificación del nivel de servicio para los usuarios de la red corporativa”. Con la intervención de los indicadores nombrados se logra evaluar la generación de calidad para los servicios de Alianza.

Con el objetivo de conocer si el nivel de calidad ha sido satisfactorio o no, tanto de servicios recibidos como los que suministra Alianza, se toma en cuenta al ítem “Indicadores para identificar desempeño de proveedores de tecnología”, con el afán de tener argumentos que sugieran si se realiza la renovación del contrato con dichos proveedores o no y al ítem “Indicadores de satisfacción de usuarios internos” para según esta información mejorar o mantener el nivel de los servicios que suministra a la empresa el DDS.

Cuando un servicio falla el usuario de este debe tener a su disposición una vía de comunicación confiable con su proveedor, para que se recupere el servicio a su nivel de calidad normal, lo más rápido posible. Para evaluar este tópico se insertan los indicadores: “Efectividad de vía de comunicación con proveedores externos” y “Efectividad de vía de comunicación entre los usuarios y el DDS”.

Finalmente el indicador “Mejoramiento de servicios basados en monitoreo”, valora cómo evoluciona la calidad de los servicios frente al continuo cambio de las necesidades de los usuarios.

Las “Métricas” toman en cuenta a los indicadores de “Respuesta Cerrada” que pueden ser medidos, de ahí se toma en cuenta a: Servicios que son monitoreados su calidad con reportes históricos, los servicios que han cumplido con el nivel de calidad especificado ya sean internos o de proveedores externos, servicios con calidad formal definida, servicios que cuentan con niveles de satisfacción identificados y frecuencia en que se revisan los niveles de calidad. Además para “Métricas” se tomaron en cuenta indicadores que dan información útil con

parámetros. Dentro de este tipo se encuentra: “Disponibilidad de los servicios que provee el DDS”, para conocer cómo se mantiene actualmente el horario de atención para cada servicio. Y el indicador “Características de encargado de Nivel de Servicio”, debido a que ITIL recomienda un perfil de una persona experta en tecnología y con inteligencia emocional para poder negociar con los usuarios y proveedores un nivel de calidad adecuado.

Respuesta Cerrada

Monitoreo del Servicio de Internet recibido.
Monitoreo del Servicio de Internet suministrado.
Monitoreo de enlaces WAN.
Historial del servicio de Internet.
Historial de la calidad de los servicios suministrados.
Contratos formales de nivel de servicio.
Especificación del nivel de servicio para los usuarios de la red corporativa.
Identificación de necesidades para implementar un servicio.
Indicadores para identificar desempeño de proveedores de tecnología.
Indicadores de satisfacción de usuarios internos.
Efectividad de vía de comunicación con proveedores externos.
Efectividad de vía de comunicación entre los usuarios y el DDS.
Mejoramiento de servicios basados en monitoreo.

Métricas

Disponibilidad de los servicios que provee el DDS.
Monitoreo de Nivel de Calidad de Servicios y Reportes Históricos.
- Servicio 1.
- Servicio 2.
- Servicio N.

Cumplimiento de calidad de Servicios en un periodo específico.
- Servicio 1.
- Servicio 2.
- Servicio N.

Control de Calidad de proveedores externos y Reportes Históricos.

Servicio 1.

Servicio 2.

Servicio N.

Características de encargado de Nivel de Servicio.

Definición formal del nivel de calidad de Servicios.

Servicio 1.

Servicio 2.

Servicio N.

Satisfacción de los usuarios por servicio.

Servicio 1.

Servicio 2.

Servicio N.

Frecuencia de revisión de niveles de servicio internos y externos actuales.

2.3.2.2 Gestión de Continuidad de Servicio

Descripción

Como único indicador de “Respuesta Cerrada”, “Conocimiento del DDS sobre los planes de emergencia existentes”, evalúa si el Gerente de Sistemas ha desarrollado planes contra emergencias y además si ha trasmitido el conocimiento de estos a los miembros del DDS.

A continuación para las métricas se tiene:

“Implementación de planes de contingencia ante emergencias”, este indicador busca conocer para qué servicios existen planes ante emergencias, de esta forma se generarán planes para los servicios principales que no los posean. De la misma manera se aplica para el indicador “Equipos o Sistemas que poseen un plan en caso de falla”.

“Lineamiento formal para recuperación al estado anterior de servicios”, en este ítem se evalúa lo ordenado que son los procesos para recuperar servicios, de esta premisa depende el éxito de la recuperación de un servicio.

“Planes de emergencia evaluados antes de ser puestos en marcha”, los planes generados deben siempre tener una etapa de evaluación, antes de ser utilizados

en los servicios en producción, con esto se evitan sucesos inesperados que provoquen fallas peores a las ya presentadas.

“Frecuencia de revisión de los Planes de Emergencia ya desarrollados”, es importante tomar en cuenta este parámetro porque a pesar de que un plan ya ha sido evaluado y aprobado para su implementación, este se debe ajustar a las variaciones que sufre la empresa a lo largo del tiempo, no puede quedarse estática.

“Entrenamiento del DDS para utilizar correctamente los Planes de Emergencia”, este indicador es útil para denotar la responsabilidad del Gerente de Sistemas en la planificación de la capacitación a los a los miembros del DDS, para que los planes de emergencia se desarrollen de forma adecuada.

“Análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización”, al realizar un análisis de amenazas y vulnerabilidades se pueden conocer debilidades que pueden causar cortes de servicio, y tomar acciones correctivas para disminuir el riesgo. Por lo expuesto este indicador es necesario para el Gerente de Sistemas.

“Catástrofes enfrentadas con su tiempo de resolución”, es necesario tomar en cuenta este ítem, para medir el nivel de respuesta ante emergencias desde la perspectiva del Gerente de Sistemas. Así se conocerán las emergencias para las cuales se encuentra el DDS menos preparado.

“Eficiencia de planes de Emergencia utilizados en catástrofes reales”, con el fin de encontrar posibles correctivos que se puede dar a los planes de emergencia ya desarrollados, se evalúa la eficiencia presentada cuando los planes ya han sido utilizados en crisis reales.

Respuesta Cerrada

Conocimiento del DDS sobre los planes de emergencia existentes.

Métricas

Implementación de planes de contingencia ante emergencias.

Servicio 1.

Servicio 2.

Servicio N.

Equipos o Sistemas que poseen un plan en caso de falla.

Equipo o Sistema 1.

Equipo o Sistema 2.

Equipo o Sistema N.

Lineamiento formal para recuperación al estado anterior de servicios.

Servicio 1.

Servicio 2.

Servicio N.

Planes de emergencia evaluados antes de ser puestos en marcha.

Plan 1.

Plan 2.

Plan N.

Frecuencia de revisión de los Planes de Emergencia ya desarrollados.

Plan 1.

Plan 2.

Plan N.

Entrenamiento del DDS para utilizar correctamente los Planes de Emergencia.

Plan 1.

Plan 2.

Plan N.

Análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización.

Servicio 1.

Servicio 2.

Servicio N.

Catástrofes enfrentadas con su tiempo de resolución.

Catástrofe 1.

Catástrofe 2.

Catástrofe N.

Eficiencia de planes de Emergencia utilizados en catástrofes reales.

Plan 1.

Plan 2.

Plan N.

2.3.2.3 Gestión de Cambios

Descripción

Para “Uso de cambios recientes para solucionar incidentes”, “Reconocimiento de incidentes que podrían ser producidos por un cambio”, “Coordinación de cambios con los departamentos afectados” y “Difusión de la planificación de un cambio” los cambios deben ser relacionados con los posibles incidentes que pueden causar, para durante su implementación, tomar las acciones de prevención necesarias. Para el indicador “Análisis de riegos de un cambio propuesto”, la idea es similar ya que un riesgo puede implicar que se generen varios incidentes. Además la identificación del riesgo determina adicionalmente si la implementación de un cambio es factible o no.

Se toma en cuenta a “Cambios impulsados por realizar innovación y mejoramiento” y “Cambios impulsados por realizar modificaciones o correcciones”, debido a que se quiere evaluar, en qué nivel según la Gerencia de Sistemas, los cambios son orientados para mejorar, en lugar de que su impulso sea para realizar correcciones, lo que según ITIL es considerado como negativo.

La realización de un cambio implica la posible intervención de varias configuraciones, de ahí que Gestión de Cambios y Configuraciones deben estar ligadas una a la otra, por esto se toma en cuenta al indicador “Independencia entre cambios y configuraciones”.

Para el apoyo en la aprobación de un cambio se debe identificar claramente sus aspectos positivos, de ahí que se usa el indicador “Definición clara de las ventajas de realizar un cambio en su petición”. Además este ítem se apoya en los indicadores “Filtro de condiciones antes de la aprobación de un cambio” y “Certeza de la razón para realizar el cambio”.

El “Registro de todos los cambios realizados sobre un dispositivo específico”, evalúa la forma de mantener actualizado el estado de cada equipo de la empresa. A este a su vez lo apoya con la misma idea el indicador “Registro de cada detalle durante el ciclo de vida del cambio”. Para que este registro sea ordenado ITIL sugiere generar un sistema para colocar esta información, de ahí la existencia del indicador “Registro de cambios en el sistema de manejo de configuraciones”.

Cuando existen cambios comunes que la empresa requiere, se debe generar un proceso establecido para disminuir los tiempos de implementación de un cambio. Esto lo evalúa el indicador “Elaboración de procesos modelos para afrontar cambios que se repiten o son comunes para la organización”.

Para que un cambio no se desarrolle con normalidad y por completo en su implementación es necesario contar con el material necesario, por esto se evalúa al indicador “Identificación de recursos necesarios antes de la realización de un cambio”. Caso contrario existieran retrasos innecesarios. De la misma manera se necesita el apoyo financiero para la adquisición de recursos, esta planificación se evalúa con el indicador “Realización de un análisis financiero durante la planeación de un cambio”.

Para que los procesos que se utilizaron para la implementación de un cambio sean aceptados para su futura implementación, se debe evaluar el resultado que provocaron luego de su finalización. De ahí el uso del indicador “Evaluación de procesos de cambio luego de su implementación”.

En ocasiones cuando ya se vuelve común el pedido e implementación de un cambio, este es preferible que sea considerado como una solicitud de servicio. En esto se apoya el indicador “Registro de cambios estándar como pedidos de cambio”.

En toda implementación ITIL sugiere que exista un responsable que se haga cargo del éxito del proyecto, para que coordine las actividades necesarias. El indicador que toma en cuenta este punto es “Registro del responsable de la petición de cambio”.

Los pedidos de cambio no deben ser negados de forma absoluta, por esto ITIL sugiere que exista una segunda revisión, representada por el indicador: “Recalificación de pedido de cambios en caso de ser negados en primera instancia”.

Durante la implementación de un cambio específico, se deben hacer pruebas de funcionamiento. Esto se evalúa con el indicador “Realización de pruebas piloto antes de la implementación de un cambio”.

ITIL sugiere que una vez finalizada una implementación, esta debe ser evaluada con los objetivos que se propusieron en su diseño y planificación, por esto se toma en cuenta al indicador “Comprobación de cumplimiento de objetivos al

finalizar la implementación de un cambio". De la mano con este va el indicador que mide la satisfacción de los usuarios, "Comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio". Otros indicadores que ayudan a evaluar la post-implementación son: "Comprobación de cumplimiento de costos al finalizar la implementación de un cambio", "Cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio" y "Documentación del proceso de evaluación post implementación de cambios".

ITL se basa en el mejoramiento continuo, por esto es necesario tomar las malas experiencias para corregirlas y no cometer los mismos errores en el futuro, de esta idea se inserta el siguiente indicador, "Registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio".

Según la teoría de Gestión de Cambios de ITIL V3, el administrador de cambios debe estar en contacto directo con la Gestión de Problemas, ya que para resolver problemas en muchos casos se necesitarán realizar cambios. Por otro lado el administrador de cambios en lo posible no debe estar relacionado con la gestión de incidentes ya que estos se preocupan de restituir el servicio afectado con procesos estándar. Para evaluar estas dos premisas se colocaron los indicadores: "Participación del administrador de problemas en la administración de cambios" y "Participación del administrador de incidentes en la administración de cambios".

Al final se encuentra el indicador "Método para registro de cambios", el cual implica varias guías ITIL para registro de cambios, con esta información se conocerán las guías que se toman en cuenta actualmente.

En la sección de "Métricas", primero se obtiene una referencia con el indicador "Número de cambios solicitados al DDS en un periodo específico", con este luego se procede a realizar comparaciones mediante los indicadores: "Número de cambios solicitados que han sido registrados automáticamente en un periodo específico", "Número de cambios planeados que se han realizado en la organización durante un periodo específico", "Número de cambios realizados con carácter de emergencia durante un periodo específico" y "Número de cambios que no han tenido éxito en un periodo específico", las mismas que son comparativas sugeridas por ITIL.

Como ítem final en “Métricas”, se siguiere a “Servicios que han tenido mejora gracias a cambios en la organización”, lo cual busca saber si los servicios con mejoras por cambios han sido identificados. Esto implica que los cambios se realizan pensando en una mejora específica.

Respuesta Cerrada

Uso de cambios recientes para solucionar incidentes.

Análisis de riegos de un cambio propuesto.

Reconocimiento de incidentes que podrían ser producidos por un cambio.

Cambios impulsados por realizar innovación y mejoramiento.

Cambios impulsados por realizar modificaciones o correcciones.

Independencia entre cambios y configuraciones.

Definición clara de las ventajas de realizar un cambio en su petición.

Coordinación de cambios con los departamentos afectados.

Difusión de la planificación de un cambio.

Registro de todos los cambios realizados sobre un dispositivo específico.

Elaboración de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.

Registro de cada detalle durante el ciclo de vida del cambio.

Registro de cambios en el sistema de manejo de configuraciones.

Filtro de condiciones antes de la aprobación de un cambio.

Identificación de recursos necesarios antes de la realización de un cambio.

Evaluación de procesos de cambio luego de su implementación

Registro de cambios estándar como pedidos de cambio.

Registro del responsable de la petición de cambio.

Certeza de la razón para realizar el cambio.

Recalificación de pedido de cambios en caso de ser negados en primera instancia.

Realización de un análisis financiero durante la planeación de un cambio.

Realización de pruebas piloto antes de la implementación de un cambio.

Comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.

Comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.
Registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.
Comprobación de cumplimiento de costos al finalizar la implementación de un cambio.
Cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.
Documentación del proceso de evaluación post implementación de cambios.
Participación del administrador de problemas en la administración de cambios.
Participación del administrador de incidentes en la administración de cambios.
Método para registro de cambios.

Métricas

Número de cambios solicitados al DDS en un periodo específico
Número de cambios solicitados que han sido registrados automáticamente en un periodo específico
Número de cambios planeados que se han realizado en la organización durante un periodo específico.
Número de cambios realizados con carácter de emergencia durante un periodo específico.
Número de cambios que no han tenido éxito en un periodo específico.
Servicios que han tenido mejora gracias a cambios en la organización.

2.3.2.4 Gestión de Configuraciones

Descripción

Para indicadores de “Respuesta Cerrada” se tiene:
“Existencia de bitácora actualizada con la información de la infraestructura de comunicaciones de la organización”, evalúa que exista una bitácora actualizada, la misma que contribuye a que las configuraciones se basen en información verídica, y se realicen correctamente. De aquí se desprenden los indicadores: “Constancia que el encargado del manejo de configuraciones se asegura que han

sido apropiadamente registrados los cambios", "Existencia de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía", "Documentación de cada equipo configurable con sus características propias", "Acceso a todo el ciclo de vida de configuraciones de un equipo específico", "Registro de cada equipo configurable con su estado actual", "Registro de la versión de cada ítem configurable".

Los planes o procesos establecidos deben estar en un sitio accesible para los posibles participantes, caso contrario no se podrán aplicar las directivas diseñadas. Esto se valora en el indicador "Disponibilidad de los procesos para recuperación de desastres de cada equipo configurable".

En algunas ocasiones configuraciones de equipos mal realizadas, pueden llegar a suspender el servicio al que dar soporte. Por esto es recomendable identificar a los equipos configurables críticos, como lo menciona el indicador "Consideración del nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable".

ITIL sugiere que cada configuración sea registrada con ciertos parámetros definidos, por esto se diseñó el indicador "Método de registro de Configuraciones".

El indicador "Registro de cada equipo configurable con atributos que lo relacionen con manejo de cambios, problemas e incidentes", es importante relacionarlo con cambios porque así se conocerán las configuraciones estándar para los diferentes tipos de cambios. Se relaciona con problemas e incidentes para tomar en cuenta cuáles de estos pueden ocurrir al momento de realizar alguna configuración específica.

El área de desarrollo de software debe tomar en cuenta los datos técnicos de la infraestructura de tecnología, con el fin de acoplar el software a la tecnología de la empresa, es decir que sea compatible. El indicador correspondiente es: "Toma en cuenta el desarrollo de software de la organización los datos del manejo de configuraciones".

Se inserta el indicador, "Relación del manejo de configuraciones con el manejo de cambios", dado que un cambio puede involucrar varias configuraciones estándar.

Para realizar una verificación el estado de una configuración luego de su implementación se diseñaron los siguientes ítems: "Documentación de los detalles de verificación al cierre de una configuración", "Registro de responsable de cada

configuración” y “Control del correcto funcionamiento al finalizar la configuración de un ítem”.

Como apoyo para que se realice de forma correcta una configuración se usan los siguientes indicadores antes de la implementación: “Planificar previamente a la implementación de una configuración”, “Evaluación de cada configuración antes de su registro” y “Identificación concreta de ítems configurables para cada configuración registrada”.

Con respecto a las “Métricas”, para obtener un valor de referencia se usa el indicador “Número de configuraciones solicitadas al DDS en un periodo específico”, luego para obtener la estadística de tipos de eventos referentes a configuraciones se diseñaron los indicadores: “Número de configuraciones realizadas que fueron solicitadas al DDS durante un periodo específico”, “Número de configuraciones que no han tenido éxito en un periodo específico”, “Número de configuraciones sin autorización realizadas que fueron solicitadas al DDS durante un periodo específico”, “Número de configuraciones realizadas con carácter de emergencia durante un periodo específico” y “Número de servicios han tenido mejora gracias a configuraciones en la organización durante un periodo específico”.

Respuesta Cerrada

Existencia de bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.

Constancia que el encargado del manejo de configuraciones se asegura que han sido apropiadamente registrados los cambios.

Existencia de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.

Documentación de cada equipo configurable con sus características propias.

Disponibilidad de los procesos para recuperación de desastres de cada equipo configurable.

Consideración del nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable.

Acceso a todo el ciclo de vida de configuraciones de un equipo específico.

Método de registro de Configuraciones.

Registro de cada equipo configurable con su estado actual.
Registro de cada equipo configurable con atributos que lo relacionen con manejo de cambios, problemas e incidentes.
Toma en cuenta el desarrollo de software de la organización los datos del manejo de configuraciones.
Relación del manejo de configuraciones con el manejo de cambios.
Documentación de los detalles de verificación al cierre de una configuración.
Registro de responsable de cada configuración.
Planificar previamente a la implementación de una configuración.
Control del correcto funcionamiento al finalizar la configuración de un ítem.
Evaluación de cada configuración antes de su registro.
Identificación concreta de ítems configurables para cada configuración registrada.
Registro de la versión de cada ítem configurable.

Métricas

Número de configuraciones solicitadas al DDS en un periodo específico.
Número de configuraciones realizadas que fueron solicitadas al DDS durante un periodo específico.
Número de configuraciones que no han tenido éxito en un periodo específico.

- Falla 1.
- Falla 2.
- Falla N.

Número de configuraciones sin autorización realizadas que fueron solicitadas al DDS durante un periodo específico.
Número de configuraciones realizadas con carácter de emergencia durante un periodo específico.
Número de servicios han tenido mejora gracias a configuraciones en la organización durante un periodo específico.

- Servicio 1.
- Servicio 2.
- Servicio N.

2.3.2.5 Gestión de Incidentes

Descripción:

Para “Respuesta Cerrada”, se tiene en primer lugar a “Existencia de personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos”, el cual es necesario evaluar cuando se dan este tipo de eventos, ya que si no existen técnicos los incidentes se quedarán sin ser atendidos.

ITIL recomienda que debe existir una escala definida para solucionar un incidente, es decir primero lo intenta solucionar un técnico de soporte, si este no lo puede arreglar va el técnico con más experiencia en el área, a continuación podría ser el Gerente de Sistemas y finalmente el proveedor o técnico especialista, por esto se inserta a “Utilización de un escalamiento de solución para resolver incidentes de usuario”. Además se debe mantener el usuario informado sobre el progreso de la solución, esto se siguiere en: “Informe al usuario sobre el escalamiento de su incidente” y “Informado al usuario sobre el cierre del incidente”.

Como información gerencial que permite tomar decisiones para mejorar la Gestión de Incidentes, se inserta a: “Conocimiento de estado actual de incidentes abiertos”, “Conocimiento del número de incidentes que se encuentran abiertos”, “Conocimiento de quién es el responsable de la solución de un incidente abierto”, “Conocimiento de los usuarios que mantienen incidentes sin resolver”, “Conocimiento de tiempo de respuesta y solución para un incidente específico”, “Acceso a la bitácora de cambios que se relacionan con un incidente específico”, “Conocimiento con exactitud del tiempo que tomó la resolución de un incidente específico” , “Identificación de los incidentes críticos para la empresa”, “Registro del técnico que recibe cada incidente que ha sido abierto” y “Hora crítica del día en la cual ocurren la mayoría de incidentes”.

Cuando se da un incidente sobre un usuario, se debe restituir el servicio que fue afectado lo más pronto posible, para una vez superada esta etapa se puede dar paso a la verificación de la causa, esto es evaluado en el indicador: “Soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó“.

ITIL recomienda que se clasifiquen a los incidentes por la solución tipo que necesitan, para reducir tiempos de solución. Por esto se evalúan a los

indicadores: “Agrupación de incidentes por solución tipo” y “Resolución de incidentes tomando en cuenta el banco de soluciones”.

Al cierre de un incidente el personal de soporte de escritorio debe documentar los detalles de incidentes, esto se valora en el indicador “Poseer un servicio de soporte de escritorio que se encargue de los detalles del cierre de incidentes”. Entre estos detalles se encuentra lo sugerido por los indicadores: “Registro de los niveles de satisfacción del usuario luego del cierre de un incidente”, “Conocimiento con exactitud del tiempo que tomó la resolución de un incidente específico” y “Registro de técnico que cierra el incidente”.

Para que los usuarios realicen ordenadamente y registrando su solicitud de servicio ITIL sugiere evaluar el indicador: “Poseer un lineamiento formal en la empresa, para que los usuarios realicen un pedido de servicio”. Este a su vez debe seguir un lineamiento de registro con parámetros definidos, este se evalúa en el indicador “Método para registro de incidentes”.

Cuando existe un incidente crítico, ITIL sugiere que sea tratado de forma individual y establecida, para prevenir daños mayores, de ahí sobresale el siguiente ítem: “Poseer un proceso propio de manejo para cada incidente crítico”.

En “Métricas”, se dan indicadores para obtener mayor detalle de estadísticas de indicadores como: “Tiempo de solución promedio de un incidente”, “Frecuencia de incidentes comunes”, “Número de incidentes registrados a diario”, “Número de incidentes atendidos en un periodo específico”, “Identificación de incidentes frecuentes para la organización”, “Porcentaje de incidentes que se han resuelto en el tiempo esperado durante un periodo específico”, “Número de incidentes que han sido reabiertos del total de ocurridos en un periodo específico” y “Número de incidentes que han sido resueltos sin la necesidad de una visita, del total de ocurridos en un periodo específico”. Luego estos indicadores serán analizados en comparación a parámetros definidos en el análisis.

Adicionalmente para evaluar posibles falencias en la actualización de software y hardware que podrían estar produciendo incidentes, se insertan a los indicadores: “Frecuencia de actualizaciones de software a los usuarios” y “Frecuencia de actualizaciones de hardware a los usuarios”.

Respuesta Cerrada

Existencia de personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos.

Utilización de un escalamiento de solución para resolver incidentes de usuario.

Conocimiento de estado actual de incidentes abiertos.

Conocimiento del número de incidentes que se encuentran abiertos.

Conocimiento de quién es el responsable de la solución de un incidente abierto.

Conocimiento de los usuarios que mantienen incidentes sin resolver.

Conocimiento de tiempo de respuesta y solución para un incidente específico.

Acceso a la bitácora de cambios que se relacionan con un incidente específico.

Soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.

Informe al usuario sobre el escalamiento de su incidente.

Informado al usuario sobre el cierre del incidente.

Agrupación de incidentes por solución tipo.

Resolución de incidentes tomando en cuenta el banco de soluciones.

Poseer un servicio de soporte de escritorio que se encargue de los detalles del cierre de incidentes.

Registro de los niveles de satisfacción del usuario luego del cierre de un incidente.

Conocimiento con exactitud del tiempo que tomó la resolución de un incidente específico.

Registro de técnico que cierra el incidente.

Poseer un lineamiento formal en la empresa, para que los usuarios realicen un pedido de servicio.

Identificación de los incidentes críticos para la empresa.

Poseer un proceso propio de manejo para cada incidente crítico.

Registro del técnico que recibe cada incidente que ha sido abierto.

Método para registro de incidentes.

Métricas

Tiempo de solución promedio de un incidente.

Frecuencia de incidentes comunes.

Programas de ofimática.

Falla física de su PC.

Virus.

Internet.

Sistema de la empresa.

Frecuencia de actualizaciones de software a los usuarios.

Frecuencia de actualizaciones de hardware a los usuarios.

Número de incidentes registrados a diario.

Número de incidentes atendidos en un periodo específico.

Identificación de incidentes frecuentes para la organización.

Incidente 1.

Incidente 2.

Incidente N.

Porcentaje de incidentes que se han resuelto en el tiempo esperado durante un periodo específico.

Número de incidentes que han sido reabiertos del total de ocurridos en un periodo específico.

Número de incidentes que han sido resueltos sin la necesidad de una visita, del total de ocurridos en un periodo específico.

Hora crítica del día en la cual ocurren la mayoría de incidentes.

2.3.2.6 Gestión de Problemas

Descripción

ITIL hace una clara diferenciación entre problemas e incidentes, por esto se evalúa para el Gerente de sistemas el indicador ”Diferenciación entre problemas e incidentes”. La diferencia también abarca la prioridad de solución entre problemas e incidentes, por esto se inserta el indicador “Orden de resolución de problemas e incidentes en su organización”.

Dado que problemas generan incidentes, ITIL recomienda que se tome en cuenta la información de gestión de problemas para ayudar a la resolución de incidentes, esto se denota en el indicador “Uso de la administración de problemas para la resolución de incidentes”.

Los problemas al ser los posibles causantes de la pérdida de servicio, deben ayudar con información para mejorar la Continuidad de Servicio, el indicador referente a este tema es “Apoyo del manejo de problemas a la continuidad del servicio”.

La Gestión de Problemas implican la realización de análisis y reuniones de grupos de trabajo para dar solución a problemas o de forma proactiva identificar vulnerabilidades. A esto hace referencia el indicador “Existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades”.

La identificación proactiva de problemas se la puede hacer con el apoyo de un correcto monitoreo, donde la base es la fecha y hora, por esto se inserta el indicador “Sincronización de la infraestructura de comunicaciones de la compañía directamente con un servidor NTP”. Esto va de la mano con el servidor de LOGS el cual registra los mensajes de los sistemas, a su vez este se relaciona con el indicador “Existencia de una base histórica de eventos TI que genera información automáticamente”.

Para la resolución de problemas ITIL recomienda que se utilice un procedimiento definido, con los pasos a seguir y los datos necesarios. De esta manera se interpreta al indicador “Identificación concreta de las entradas para el proceso de resolución de problemas”.

La conclusión de la solución de problemas también debe poseer un proceso definido que se valora con el indicador “Registro de las salidas del proceso de resolución de problemas”.

La Gestión de Problemas debe apoyarse a sí misma retroalimentándose según las experiencias obtenidas para mejorar la resolución de problemas similares futuros. El indicador correspondiente a este tema es “Apoyo de la resolución de problemas en la base de datos de administración de problemas”.

Como información gerencial para toma de decisiones se valoran a los indicadores “Posibilidad de verificar los problemas cerrados en un periodo de tiempo específico”, “Conocimiento concreto del estado de un problema”.

La Gestión de Problemas debe apoyarse en el Gestión de cambios para dar solución a problemas, esto se valora en el indicador “Administración compartida entre gestión de problemas y cambios”.

Por la diferencia de concepto en prioridad de resolución de Problemas e Incidentes, deben tener administraciones separadas. El indicador correspondiente a este tema es “Administración compartida entre gestión de problemas e incidentes”.

Según la gravedad de los problemas se va requerir personal dedicado a estudiarlos para resolverlos y en lo posible tomar las necesarias para que no se vuelvan a repetir, el indicador referente a esto es “Existencia de personal designado para investigación especializada de problemas”.

Para el análisis posterior de las causas verdaderas y lo que en realidad solucionó un problema es necesario guardar acciones que ayudaron a mitigar un problema a pesar de que hayan sido de prueba, por esto se incluye el indicador “Registro de la o las acciones intuitivas que han mitigado un problema”.

Un problema no debe ser cerrado a pesar de haber sido mitigado parcialmente, por eso es importante evaluar el indicador “Cierre del problema cuando ejecuta una acción intuitiva que lo atenúa”.

ITIL sugiere la creación de una base de datos de errores conocidos, los cuales se derivan de los problemas, por esto luego de ser identificado un problema tipo este se lo registrará en esta base. El indicador referente es el siguiente “Registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema”. Además el objetivo de identificar los errores conocidos es ayudar en la solución de problemas futuros, por esto se inserta a “Solución de problemas con apoyo en la base de datos de errores conocidos”.

Luego de un suceso de error crítico, ITIL recomienda realizar varias actividades que se identifican en los siguientes indicadores: “Revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico”, “Revisión de los procedimientos erróneos, luego del suceso de un error crítico”, “Revisión de que se puede mejorar en el futuro, luego del suceso de un error crítico”, “Revisión de qué se puede hacer para que no suceda otra vez un error crítico, luego del suceso”, “Análisis si la responsabilidad del error crítico era de una empresa proveedora de servicios, luego del suceso”, “Buscar las acciones necesarias inmediatamente, en caso de que un problema crítico sea responsabilidad de una empresa proveedora” y Registro de datos de retroalimentación respecto a problemas críticos”.

Como lo dice el estándar para todos los procesos, se debe manejar un método de registro específico, por esto se inserta el indicador de evaluación “Método para registro de problemas”.

En la sección de “Métricas”, se busca conocer estadísticas referentes a los indicadores: “Número de problemas que han sido resueltos frente a los registrados en un período específico”, “Número de problemas que no han sido resueltos en el tiempo esperado durante un periodo específico”, y “Tendencia de problemas críticos a incrementarse”.

Finalmente como ítem informativo se coloca a “Problemas críticos a los que se ha enfrentado la empresa”, para conocer desde el punto de vista de los Operadores del DDS, cuáles fueron considerados como problemas críticos.

Respuesta Cerrada

Diferenciación entre problemas e incidentes.

Uso de la administración de problemas para la resolución de incidentes.

Orden de resolución de problemas e incidentes en su organización.

Apoyo del manejo de problemas a la continuidad del servicio.

Existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.

Sincronización de la infraestructura de comunicaciones de la compañía directamente con un servidor NTP (servidor que provee la fecha y hora a sus clientes a través de la red usando el protocolo “Network Time Protocol”).

Identificación concreta de las entradas para el proceso de resolución de problemas.

Existencia de una base histórica de eventos TI que genera información automáticamente.

Registro de las salidas del proceso de resolución de problemas.

Apoyo de la resolución de problemas en la base de datos de administración de problemas.

Posibilidad de verificar los problemas cerrados en un periodo de tiempo específico.

Conocimiento concreto del estado de un problema.

Administración compartida entre gestión de problemas y cambios.

Administración compartida entre gestión de problemas e incidentes.
Existencia de personal designado para investigación especializada de problemas.
Registro de la o las acciones intuitivas que han mitigado un problema.
Cierre del problema cuando ejecuta una acción intuitiva que lo atenúa.
Registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.
Solución de problemas con apoyo en la base de datos de errores conocidos.
Revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.
Revisión de los procedimientos erróneos, luego del suceso de un error crítico.
Revisión de que se puede mejorar en el futuro, luego del suceso de un error crítico.
Revisión de qué se puede hacer para que no suceda otra vez un error crítico, luego del suceso.
Análisis si la responsabilidad del error crítico era de una empresa proveedora de servicios, luego del suceso.
Buscar las acciones necesarias inmediatamente, en caso de que un problema crítico sea responsabilidad de una empresa proveedora.
Registro de datos de retroalimentación respecto a problemas críticos.
Método para registro de problemas.

Métricas

Número de problemas que han sido resueltos en un periodo específico frente a los registrados.
Número de problemas que no han sido resueltos en el tiempo esperado durante un periodo específico.
Tendencia de problemas críticos a incrementarse.
Tiempo de solución promedio de un problema.
Problemas críticos a los que se ha enfrentado la empresa.

- Servicio 1.
- Servicio 2.
- Servicio N.

2.3.3 INDICADORES A SER EVALUADOS PARA OPERADORES DEL DEPARTAMENTO DE SISTEMAS

2.3.3.1 Gestión del Nivel de Servicio

Descripción

Con respecto a “Respuesta Cerrada” Los Operadores de Sistemas deben tener acceso al “Historial del servicio de Internet” (indicador), con el fin de mantener monitoreada la calidad de este servicio.

Los Operadores de Sistemas con el fin de mantener la calidad que se acordó con los proveedores de servicios, se inserta el indicador “Conocimiento del Nivel de Servicio que están obligados a cumplir los proveedores”, así conocerán cuándo el servicio cae sobre niveles no aceptables.

Como para los servicios externos, los Operadores de Sistemas deben conocer la calidad que los usuarios de la red interna deben recibir, así podrán hacer los correctivos necesarios cuando detecten una caída de calidad, el indicador referente es “Especificación del nivel de servicio para los usuarios de la red corporativa”. Esto va de la mano con el indicador “Conocimiento de qué servicios ofrece el DDS a la organización”.

Cuando un servicio falla el usuario de este debe tener a su disposición una vía de comunicación confiable con su proveedor, para que se recupere el servicio a su nivel de calidad normal, lo más rápido posible. Para evaluar este tópico se insertan los indicadores: “Efectividad de vía de comunicación con proveedores externos” y “Efectividad de vía de comunicación entre los usuarios y el DDS”.

En “Métricas” se busca mayor detalle, para indicadores de “Respuesta Cerrada”, así se tienen a los siguientes: “Conocimiento de los servicios que provee el DDS”, “Control de Calidad de proveedores externos y Reportes Históricos”, “Monitoreo de Nivel de Calidad de Servicios Internos y Reportes Históricos”, “Definición formal del nivel de calidad de Servicios Internos” y “Satisfacción de los usuarios por servicio”.

Respuesta Cerrada

Historial del servicio de Internet.

Conocimiento del Nivel de Servicio que están obligados a cumplir los proveedores.

Especificación del nivel de servicio para los usuarios de la red corporativa.

Efectividad de vía de comunicación con proveedores externos.

Efectividad de vía de comunicación entre los usuarios y el DDS.

Conocimiento de qué servicios ofrece el DDS a la organización.

Métricas

Conocimiento de los servicios que provee el DDS.

Control de Calidad de proveedores externos y Reportes Históricos.

- Servicio 1.
- Servicio 2.
- Servicio N.

Monitoreo de Nivel de Calidad de Servicios Internos y Reportes Históricos.

- Servicio 1.
- Servicio 2.
- Servicio N.

Definición formal del nivel de calidad de Servicios Internos.

- Servicio 1.
- Servicio 2.
- Servicio N.

Satisfacción de los usuarios por servicio.

- Servicio 1.
- Servicio 2.
- Servicio N.

2.3.3.2 Gestión de Continuidad del Servicio

Descripción

Para la Continuidad de Servicio, sólo se han considerado “Métricas”, con el fin de conocer a más detalle los parámetros de este tema. Primero se evalúa cuáles son los planes de emergencia que conoce como Operador de Sistemas, el indicador

es “Planes de emergencia presentados al DDS”. Así se conocerá para qué servicios el DDS conoce planes de emergencia.

Luego una vez conocidos los planes de emergencia, los Operadores de Sistemas deben recibir una capacitación para implementar el plan adecuadamente, el indicador que hace referencia a este tema es “Entrenamiento para proceder correctamente con los planes de emergencia”.

Así como para los servicios es necesario conocer para qué equipos existe un plan de contingencia, ya que dentro del pan de un servicio se puede abarcar varios planes de equipos individuales. El indicador de referencia es “Equipos con plan de contingencia en caso de falla”. De igual forma en este caso es necesario de parte de los Operadores de Sistemas conocer el procedimiento a seguir para cumplir con el plan correctamente, esto se relaciona con el indicador “Conocimiento del lineamiento para proceder a la recuperación del estado anterior de equipos”.

“Tiempo necesario para resolución de catástrofes”, este indicador sirve para medir el nivel de respuesta ante emergencias desde la perspectiva de los Operadores de Sistemas. Así se conocerán las emergencias para las cuales se encuentra el DDS menos preparado.

“Eficiencia de planes utilizados en catástrofes reales”, con el fin de encontrar posibles correctivos que se puede dar a los planes de emergencia ya desarrollados, se evalúa la eficiencia presentada cuando los planes ya han sido utilizados en crisis reales. Este ítem ayuda a resaltar cuáles con los planes para los que mejor se ha encontrado preparado el DDS.

Métricas

Planes de emergencia presentados al DDS.

- Plan 1.
- Plan 2.
- Plan N.

Entrenamiento para proceder correctamente con los planes de emergencia.

- Plan 1.
- Plan 2.
- Plan N.

Equipos con plan de contingencia en caso de falla.

Equipo 1.

Equipo 2.

Equipo N.

Conocimiento del lineamiento para proceder a la recuperación del estado anterior de equipos.

Equipo 1.

Equipo 2.

Equipo N.

Tiempo necesario para resolución de catástrofes.

Catástrofe 1 (Tiempo).

Catástrofe 2 (Tiempo).

Catástrofe N (Tiempo).

Eficiencia de planes utilizados en catástrofes reales.

Plan 1 (Eficiencia).

Plan 2 (Eficiencia).

Plan N (Eficiencia).

2.3.3.3 Gestión de Cambios

Descripción

Para los indicadores “Uso de cambios recientes para solucionar incidentes” y “Reconocimiento de incidentes que podrían ser producidos por un cambio”, son importantes porque los cambios deben ser relacionados con los posibles incidentes que pueden causar, para durante su implementación, tomar las acciones de prevención necesarias.

El Operador de Sistemas debe registrar los cambios que ha realizado sobre los equipos, para mantener actualizado su estado. Esto es evaluado en el indicador “Registro de cambios sobre dispositivos específicos“.

Se toma en cuenta a “Cambios impulsados por realizar innovación y mejoramiento” y “Cambios impulsados por realizar modificaciones o correcciones”, debido a que se quiere evaluar, en qué nivel según los Operadores de Sistemas,

los cambios son orientados para mejorar, en lugar de que su impulso sea para realizar correcciones, lo que según ITIL es considerado como negativo.

Cuando existen cambios comunes que la empresa requiere, se debe generar un proceso establecido para disminuir los tiempos de implementación de un cambio. Esto lo evalúa el indicador “Elaboración de procesos modelos para afrontar cambios que se repiten o son comunes para la organización”.

Para que un cambio no se desarrolle con normalidad y por completo en su implementación es necesario contar con el material necesario, por esto se evalúa al indicador “Identificación de recursos necesarios antes de la realización de un cambio”. Caso contrario existieran retrasos innecesarios.

Para que los procesos, que se utilizaron para la implementación de un cambio sean aceptados para su futura implementación, se debe evaluar el resultado que provocaron luego de su finalización. De ahí el uso del indicador “Evaluación de procesos de cambio luego de su implementación”.

Para el apoyo en la aprobación de un cambio se debe identificar claramente sus aspectos positivos, de ahí que se usa el indicador “Certeza de la razón para realizar el cambio”.

Durante la implementación de un cambio específico, se deben hacer pruebas de funcionamiento. Esto se evalúa con el indicador “Realización de pruebas piloto antes de la implementación de un cambio”.

ITIL sugiere que una vez finalizada una implementación, esta debe ser evaluada con los objetivos que se propusieron en su diseño y planificación, por esto se toma en cuenta al indicador “Comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio”. De la mano con este va el indicador que mide la satisfacción de los usuarios, “Comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio”. Otro indicador que ayuda a evaluar la post-implementación es “Cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio”.

ITL se basa en el mejoramiento continuo, por esto es necesario tomar las malas experiencias para corregirlas y no cometer los mismos errores en el futuro, de esta idea se inserta el siguiente indicador, “Registro de los eventos no planificados

que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio".

Al final se encuentra el indicador "Método para registro de cambios", el cual implica varias guías ITIL para registro de cambios, los Operadores de Sistemas deberían utilizar esta forma de registro.

En la sección de "Métricas", se busca conocer estadísticas según los Operadores de Sistemas acerca de cambios, los indicadores utilizados son los siguientes: "Número de cambios realizados frente a los solicitados, en un periodo específico", "Número de cambios realizados en un periodo específico, que no han sido registrados", "Número de cambios que no han tenido éxito en un periodo específico", "Número de cambios realizados con carácter de emergencia durante un periodo específico".

Como ítem final en "Métricas", se siguiere a "Servicios que han tenido mejora gracias a cambios en la organización", lo cual busca saber si los servicios con mejoras por cambios han sido identificados. Esto implica que los cambios se realizan pensando en una mejora específica.

Respuesta Cerrada

Uso de cambios recientes para solucionar incidentes.

Registro de cambios sobre dispositivos específicos.

Reconocimiento de incidentes que podrían ser producidos por un cambio.

Cambios impulsados por realizar innovación y mejoramiento.

Cambios impulsados por realizar correcciones.

Elaboración de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.

Identificación de recursos necesarios antes de la realización de un cambio.

Evaluación de procesos de cambio luego de su implementación

Certeza de la razón para realizar el cambio.

Realización de pruebas piloto antes de la implementación de un cambio.

Comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.

Comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.

Registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.
Cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.
Método para registro de Cambios.

Métricas

Número de cambios realizados frente a los solicitados, en un periodo específico.
Número de cambios realizados en un periodo específico, que no han sido registrados.
Número de cambios que no han tenido éxito en un periodo específico.
Número de cambios realizados con carácter de emergencia durante un periodo específico.
Servicios que han tenido mejora gracias a cambios en la organización.

- Servicio 1.
- Servicio 2.
- Servicio N.

2.3.3.4 Gestión de Configuraciones

Descripción

Para indicadores de “Respuesta Cerrada” se tiene:
“Existencia de bitácora actualizada con la información de la infraestructura de comunicaciones de la organización”, evalúa que exista una bitácora actualizada, la misma que contribuye a que las configuraciones se basen en información verídica, y se realicen correctamente. De aquí se desprenden los indicadores: “Existencia de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía”, “Documentación de cada equipo configurable con sus características propias”, “Acceso a todo el ciclo de vida de configuraciones de un equipo específico”, “Registro de los cambios en una configuración”.
El área de desarrollo de software debe tomar en cuenta los datos técnicos de la infraestructura de tecnología, con el fin de acoplar el software a la tecnología de la

empresa, es decir que sea compatible. El indicador correspondiente es: “Desarrollo de software de la organización tomando en cuenta los datos del manejo de configuraciones”.

Para realizar una verificación el estado de una configuración luego de su implementación se diseñaron los siguientes ítems: “Documentación de los detalles de verificación al cierre de una configuración”, “Registro de responsable de cada configuración” y “Control del correcto funcionamiento al finalizar la configuración de un ítem”.

Como apoyo para que se realice de forma correcta una configuración se usan los siguientes indicadores antes de la implementación: “Planificar previamente a la implementación de una configuración”, “Evaluación de cada configuración antes de su registro” y “Identificación concreta de ítems configurables para cada configuración registrada”.

Cada equipo configurable debe tener un proceso para recuperarse de un desastre, estos deben ser conocidos por los Operadores del DDS para que puedan ser ejecutados. Esto se valúa con el indicador “Conocimiento de que procesos se deben llevar a cabo para realizar la recuperación de desastres de cada equipo configurable”.

Con respecto a las “Métricas”, para obtener un valor de referencia se usa el indicador “Número de configuraciones solicitadas al DDS en un periodo específico”, luego para obtener la estadística de tipos de eventos referentes a configuraciones se diseñaron los indicadores: “Número de Configuraciones realizadas sin éxito frente al total de realizadas, durante un periodo específico”, “Número de configuraciones sin autorización realizadas que fueron solicitadas al DDS durante un periodo específico”, “Número de configuraciones realizadas con carácter de emergencia durante un periodo específico” y “Número de servicios han tenido mejora gracias a configuraciones en la organización durante un periodo específico”.

Respuesta Cerrada

Existencia de bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.

Registro de los cambios en una configuración.

Existencia de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.
Conocimiento de que procesos se deben llevar a cabo para realizar la recuperación de desastres de cada equipo configurable.
Acceso a todo el ciclo de vida de configuraciones de un equipo específico.
Documentación de cada equipo configurable con sus características propias.
Desarrollo de software de la organización tomando en cuenta los datos del manejo de configuraciones.
Documentación de los detalles de verificación, al cierre de una configuración.
Registro de responsable de cada configuración.
Planificar previamente a la implementación de una configuración.
Control del correcto funcionamiento al finalizar la configuración de un ítem.
Identificación concreta de ítems configurables para cada configuración registrada.

Métricas

Número de Configuraciones realizadas sin éxito frente al total de realizadas, durante un periodo específico.
Número de configuraciones sin autorización realizadas que fueron solicitadas al DDS durante un periodo específico.
Número de configuraciones realizadas con carácter de emergencia durante un periodo específico.
Número de servicios han tenido mejora gracias a configuraciones en la organización durante un periodo específico.

Servicio 1.
Servicio 2.
Servicio N.

2.3.3.5 Gestión de Incidentes

Descripción:

Para “Respuesta Cerrada”, se tiene que ITIL recomienda que debe existir una escala definida para solucionar un incidente, es decir primero lo intenta solucionar

un técnico de soporte, si este no lo puede arreglar va el técnico con más experiencia en el área, a continuación podría ser el Gerente de Sistemas y finalmente el proveedor o técnico especialista, por esto se inserta a “Utilización de un escalamiento de solución para resolver incidentes de usuario”. Además se debe mantener el usuario informado sobre el progreso de la solución, esto se siguiere en: “Informe al usuario sobre el escalamiento de su incidente” y “Informado al usuario sobre el cierre del incidente”.

Como información gerencial que permite tomar decisiones para mejorar la Gestión de Incidentes, se inserta a: “Conocimiento de quién es el responsable de la solución de un incidente abierto”, “Conocimiento de los usuarios que mantienen incidentes sin resolver”, “Conocimiento de tiempo de respuesta y solución para un incidente específico”, “Acceso a la bitácora de cambios que se relacionan con un incidente específico”, y “Hora crítica del día en la cual ocurren la mayoría de incidentes”.

Cuando se da un incidente sobre un usuario, se debe restituir el servicio que fue afectado lo más pronto posible, para una vez superada esta etapa se puede dar paso a la verificación de la causa, esto es evaluado en el indicador: “Soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó“.

ITIL recomienda que se clasifiquen a los incidentes por la solución tipo que necesitan, para reducir tiempos de solución. Por esto se evalúan a los indicadores: “Agrupación de incidentes por solución tipo” y “Resolución de incidentes tomando en cuenta el banco de soluciones”.

Al cierre de un incidente el personal de soporte de escritorio debe documentar los detalles de incidentes, como “Registro de los niveles de satisfacción del usuario luego del cierre de un incidente”, y “Registro de técnico que cierra el incidente”.

Para comprobar que los Operadores del DDS siguen un lineamiento de registro con parámetros definidos, se evalúa el indicador “Método para registro de incidentes”.

En “Métricas”, se dan indicadores para obtener mayor detalle de estadísticas de indicadores como: “Tiempo de solución promedio de un incidente”, “Frecuencia de incidentes comunes”, “Número de incidentes registrados a diario”, “Identificación

de incidentes frecuentes para la organización". Luego estos indicadores serán analizados en comparación a parámetros definidos en el análisis.

Adicionalmente para evaluar posibles falencias en la actualización de software y hardware que podrían estar produciendo incidentes, se insertan a los indicadores: "Frecuencia de actualizaciones de software a los usuarios" y "Frecuencia de actualizaciones de hardware a los usuarios".

Respuesta Cerrada

Utilización de un escalamiento de solución para resolver incidentes de usuario.

Conocimiento de quién es el responsable de la solución de un incidente abierto.

Conocimiento de los usuarios que mantienen incidentes sin resolver.

Conocimiento de tiempo de respuesta y solución para un incidente específico.

Acceso a la bitácora de cambios que se relacionan con un incidente específico.

Soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.

Informe al usuario sobre el escalamiento de su incidente.

Informado al usuario sobre el cierre del incidente.

Agrupación de incidentes por solución tipo.

Resolución de incidentes tomando en cuenta el banco de soluciones.

Registro de los niveles de satisfacción del usuario luego del cierre de un incidente.

Registro de técnico que cierra el incidente.

Método para registro de Incidentes.

Métricas

Tiempo de solución promedio de un incidente.

Frecuencia de incidentes comunes.

- Programas de ofimática.
- Falla física de su PC.
- Virus.
- Internet.
- Sistema de la empresa.

Frecuencia de actualizaciones de software a los usuarios.

Frecuencia de actualizaciones de hardware a los usuarios.

Número de incidentes registrados a diario.

Identificación de incidentes frecuentes para la organización.

Incidente 1.

Incidente 2.

Incidente N.

Hora crítica del día en la cual ocurren la mayoría de incidentes.

2.3.3.6 Gestión de Problemas

Descripción:

ITIL hace una clara diferenciación entre problemas e incidentes, por esto se evalúa para los Operadores del DDS la prioridad de solución entre problemas e incidentes, por esto se inserta el indicador “Orden de resolución de problemas e incidentes”, así como el entendimiento de su diferenciación con el indicador “Orden de ocurrencia de problemas e incidentes”.

La Gestión de Problemas implican la realización de análisis y reuniones de grupos de trabajo para dar solución a problemas o de forma proactiva identificar vulnerabilidades. A esto hace referencia el indicador “Existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades”.

La identificación proactiva de problemas se la puede hacer con el apoyo de un correcto monitoreo, por ejemplo con un servidor de LOGS el cual registra los mensajes de los sistemas, a su vez este se relaciona con el indicador “Existencia de una base histórica de eventos TI que genera información automáticamente”.

La Gestión de Problemas debe apoyarse a sí misma retroalimentándose según las experiencias obtenidas para mejorar la resolución de problemas similares futuros. El indicador correspondiente a este tema es “Apoyo de la resolución de problemas en la base de datos de administración de problemas”.

Según la gravedad de los problemas se va requerir personal dedicado a estudiarlos para resolverlos y en lo posible tomar las necesarias para que no se vuelvan a repetir, el indicador referente a esto es “Existencia de personal designado para investigación especializada de problemas”.

Para el análisis posterior de las causas verdaderas y lo que en realidad solucionó un problema es necesario guardar acciones que ayudaron a mitigar un problema a pesar de que hayan sido de prueba, por esto se incluye el indicador “Registro de la o las acciones intuitivas que han mitigado un problema”.

Un problema no debe ser cerrado a pesar de haber sido mitigado parcialmente, por eso es importante evaluar el indicador “Cierre del problema cuando ejecuta una acción intuitiva que lo atenúa”.

ITIL sugiere la creación de una base de datos de errores conocidos, los cuales se derivan de los problemas, por esto luego de ser identificado un problema tipo este se lo registrará en esta base. El indicador referente es el siguiente “Registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema”. Además el objetivo de identificar los errores conocidos es ayudar en la solución de problemas futuros, por esto se inserta a “Solución de problemas con apoyo en la base de datos de errores conocidos”.

Luego de un suceso de error crítico, ITIL recomienda realizar varias actividades que se identifican en los siguientes indicadores: “Revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico”, “Revisión de los procedimientos erróneos, luego del suceso de un error crítico”, “Revisión de qué se puede hacer para que no suceda otra vez un error crítico, luego del suceso”.

Como lo dice el estándar para todos los procesos, se debe manejar un método de registro específico, por esto se inserta el indicador de evaluación “Registro adecuado de problemas”.

En la sección de “Métricas”, se busca conocer estadísticas referentes a los indicadores: “Número de problemas que han sido resueltos frente a los registrados en un período específico”, “Número de problemas que no han sido resueltos en el tiempo esperado durante un periodo específico”, y “Tendencia de problemas críticos a incrementarse”.

Finalmente como ítem informativo se coloca a “Problemas críticos a los que se ha enfrentado la empresa”, para conocer desde el punto de vista de los Operadores del DDS, cuáles fueron considerados como problemas críticos.

Respuesta Cerrada

Orden de ocurrencia de problemas e incidentes.

Orden de resolución de problemas e incidentes.

Existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.

Existencia de una base histórica de eventos IT que genera información automáticamente.

Apoyo de la resolución de problemas en la base de datos de administración de problemas.

Existencia de personal designado para investigación especializada de problemas.

Registro de la o las acciones intuitivas que han mitigado un problema.

Cierre del problema cuando ejecuta una acción intuitiva que lo atenúa.

Registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.

Solución de problemas con apoyo en la base de datos de errores conocidos.

Revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.

Revisión de los procedimientos erróneos, luego del suceso de un error crítico.

Revisión de qué se puede hacer para que no suceda otra vez un error crítico, luego del suceso.

Registro adecuado de problemas.

Métricas

Número de problemas que han sido resueltos frente a los registrados en un período específico.

Número de problemas que no han sido resueltos en el tiempo esperado durante un periodo específico.

Tendencia de problemas críticos a incrementarse.

Problemas críticos a los que se ha enfrentado la empresa.

- Servicio 1.
- Servicio 2.
- Servicio N.

2.3.4 INDICADORES A SER EVALUADOS PARA USUARIOS COMUNES

2.3.4.1 Gestión de Nivel del Servicio

Descripción

Los indicadores elegidos, tienen como objetivo encontrar qué nivel de conocimiento tienen los usuarios comunes respecto a los servicios que reciben de parte del DDS, para mejorar el aprovechamiento que este grupo da a los servicios de TI. Además se evalúa la satisfacción en general de calidad en contraste con las necesidades laborales del grupo, esto para detectar demanda insatisfecha. Finalmente para detectar donde se encuentran los bajos niveles de calidad según este grupo, se utilizaron indicadores específicos de calidad para los servicios más comunes según el DDS.

Respuesta Cerrada

Conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.

Entrega de documentación formal que informe los servicios que provee el DDS.

Calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.

Calidad de Servicios específicos:

- Sistema de Seguros.
- Servicio de Internet.
- Correo Electrónico.
- Soporte Técnico.
- Capacitación Informática.
- Reportes de Sistema AS400.

2.3.4.2 Gestión de Continuidad del Servicio

Descripción

El primer indicador busca conocer de manera general si el grupo de usuarios comunes está informado sobre procedimientos que se deben seguir en caso de

una emergencia, esto ayuda a medir la preparación de este grupo para que el negocio siga funcionando a pesar de que se vivan momentos de crisis.
Los indicadores que se encuentran a continuación contribuyen para conocer en referencia al tiempo en estado de emergencia, cuáles son las incidencias para las cuales se necesita más preparación.

Respuesta Cerrada

Nivel de preparación frente a emergencias sufridas.
Tiempo que han afectado emergencias pasadas el normal desempeño del trabajo.

Virus.
Problema con el Sistema de Seguros.
Falla de Internet.
Falla de Correo Electrónico.
Corte de energía eléctrica.

2.3.4.3 Gestión de Cambios

Descripción

Los indicadores de “Respuesta Cerrada” para Gestión de Cambios, buscan conocer como se manejan los cambios desde el punto de vista de los usuarios comunes de la empresa, usando las siguientes premisas. En primer lugar se consulta si por los menos las peticiones de cambios son receptadas por un DDS, el mismo que cuando planifique la realización de un cambio debe informar a sus usuarios sobre esta transición, para que su trabajo no se vea afectado. Adicionalmente la realización de un cambio según ITIL debe tener el objetivo de realizar innovación y mejoramiento, de ahí que se consulta a los usuarios comunes la percepción de mejora o por el contrario de enmendación de errores cuando de implementar cambios se refiere. Luego para conocer la satisfacción de los usuarios comunes que se da de forma general, se pregunta el Nivel de satisfacción de los cambios realizados por el DDS, a pesar de esto ITIL sugiere registrar una calificación formal de la calidad del servicio recibido, por esto se añade un indicador que consulta si existe un método de calificación para marcar la satisfacción de los usuarios comunes. A continuación, se encuesta el porcentaje

de cambios que han satisfecho a los usuarios comunes frente a los que fueron solicitados, con este ítem se obtiene la efectividad que tiene el DDS en la realización de cambios, para el grupo de los usuarios comunes. Finalmente se toma en cuenta al número de cambios promedio semanal que no fueron debidamente notificados y provocaron que se afecte el trabajo normal de los usuarios, este indicador es importante porque permite conocer la frecuencia promedio en la que el DDS, no planifica de forma adecuada la realización de un cambio.

Respuesta Cerrada

Recepción de cambios de software o hardware de parte del DDS.

Notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.

Frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.

Frecuencia de cambios realizados por el DDS que tengan como objetivo correcciones.

Nivel de satisfacción de los cambios realizados por el DDS.

Método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.

Número de cambios solicitados e implementados correctamente en un periodo específico.

Número de cambios no notificados que han afectado el desenvolvimiento normal del trabajo.

2.3.4.4 Gestión de Configuraciones

Descripción

Dado que la Gestión de Configuraciones es un proceso que mayormente posee actividades realizadas netamente por el DDS, sólo se toma en cuenta un indicador para el grupo de usuarios comunes, el mismo que busca conocer si se percibe la realización de configuraciones de forma metódica y ordenada. Este ítem ayuda a conocer si los usuarios comunes tienen confianza en los procesos que realiza el DDS, en referencia a Gestión de Configuraciones.

Respuesta Cerrada

Configuraciones realizadas por el DDS de forma metódica y ordenada.

2.3.4.5 Gestión de Incidentes

Descripción

Para este grupo se busca conocer si con frecuencia los incidentes de tecnología los afectan o si se repiten con frecuencia incidentes específicos. Esto ayuda a identificar si el grupo es afectado en consideración por incidentes tecnológicos.

Los incidentes en ocasiones se generan por carencia de recursos tecnológicos, por esto se añadió un indicador que busca conocer de forma general la satisfacción de la tecnología frente a las necesidades de los usuarios.

El DDS para explotar el potencial de la tecnología que maneja y prevenir amenazas emergentes, debe estar en continua actualización. Por esto existe un indicador que mide la percepción de la evolución de la tecnología en la empresa.

El usuario muchas veces al recibir un mal servicio ya sea con tiempos de solución altos o falta de apertura para recibir sugerencias, tiende a tratar de resolverlo él mismo con un procedimiento intuitivo que puede llevar a que el incidente se agrave. Por esto se tienen a los indicadores “apertura del DDS para recibir sugerencias” y a “Satisfacción del usuario frente al tiempo de solución de incidentes”.

La prevención de un incidente debe ser la primera opción para que este no suceda y afecte a los usuarios, de ahí que ITIL sugiere dar recomendaciones a los usuarios para que de alguna manera prevengan las amenazas informáticas. Por esto se sugieren como indicador a “Capacitación a los usuarios de parte del DDS”.

Luego se evalúa el método con el que el DDS atiende a los incidentes que son generados por los ejecutivos, es decir el método de gestión de su incidente.

Como según ITIL todo servicio debe ser calificado formalmente, se coloca al indicador “Método de calificación del servicio recibido de parte del DDS”.

Si bien “Tiempo en general que le toma al DDS solucionar un incidente”, es un indicador de respuesta cerrada, se diseñaron opciones con intervalos de tiempo definidos con el objetivo de obtener con mayor detalle información acerca del tiempo promedio que le toma al DDS solucionar un incidente.

El indicador “Calificación general para el DDS respecto a resolución de incidentes”, es un complemento para que los usuarios comunes a pesar de las falencias que presente el DDS, coloque una calificación general del servicio de resolución de incidentes.

Finalmente en conjunto con la gerencia de sistemas de la empresa, se eligieron varios incidentes tipo para estudiar su frecuencia dentro del grupo de usuarios comunes, el resultado de este análisis permite conocer el incidente que genera mayores problemas a este grupo.

Respuesta Cerrada

Frecuencia de incidentes tecnológicos que afecten el normal desempeño del trabajo.

Satisfacción de los recursos tecnológicos asignados.

Percepción de la evolución de la tecnología en la empresa.

Apertura del DDS para recibir sugerencias.

Capacitación a los usuarios de parte del DDS.

Satisfacción respecto a tiempo de solución de incidentes.

Frecuencia de incidentes específicos.

Método de Gestión de su incidente.

Método de calificación del servicio recibido de parte del DDS.

Tiempo en general que le toma al DDS solucionar un incidente.

Calificación general para el DDS respecto a resolución de incidentes.

Frecuencia de incidentes como.

- Programas de Ofimática.
- Falla física del computador.
- Virus Informáticos.
- Problemas de Internet.
- Sistema de Seguros.
- Correo Electrónico.

2.3.4.6 Gestión de Problemas

Descripción

Con el fin de comprobar si existe diferencia de prioridades entre resolución de incidentes y problemas, se inserta el indicador "Urgencia para restablecer sus actividades laborales inmediatamente", esta representa que los incidentes sean resueltos antes de los problemas.

Finalmente el segundo indicador, ayuda a evaluar si los incidentes que han ocurrido han sido relacionados con un problema específico, ya que si es así el momento en que se repite el incidente se cortaría de raíz el problema, que antes ya debía ser identificado. Si sucede lo contrario denota que no existe un estudio profundo de los problemas ocurridos.

Respuesta Cerrada

Urgencia para restablecer sus actividades laborales inmediatamente.

Rapidez en resolución de incidentes que ya han sucedido anteriormente.

2.3.5 INDICADORES A SER EVALUADOS PARA PUNTOS DE VENTA SOAT A NIVEL NACIONAL

2.3.5.1 Gestión de Nivel del Servicio

Descripción

Dado que los puntos de venta SOAT usan solamente el servicio del Sistema para la venta de SOAT, la evaluación de la calidad de servicio se enfoca en el sistema de seguros y el soporte técnico que brinda el personal de Alianza. Con estos indicadores se podrá conocer la percepción que tienen los usuarios respecto al sistema y el soporte.

Respuesta Cerrada

Calidad de Servicios específicos.

- Sistema de Seguros.
- Soporte Técnico.

2.3.5.2 Gestión de Continuidad del Servicio

Descripción

Los indicadores diseñados para la Gestión de Continuidad de Servicio, se enfocan en el sistema SOAT. El primero tiene como objetivo conocer si existe algún tipo de capacitación hacia los usuarios en caso que se dé una emergencia, este indicador dice que tan preparado está el usuario para apoyar en la continuidad del servicio durante una crisis.

El segundo indicador busca conocer la percepción del usuario en referencia a la disponibilidad del sistema SOAT, con esto se podrá ubicar en qué sectores existe una posible falla de continuidad de servicio.

Respuesta Cerrada

Notificación de procedimientos a seguir en caso de emergencias, tales como el corte de suministro eléctrico.

Disponibilidad del Sistema de SOAT.

2.3.5.3 Gestión de Cambios

Descripción

El primer indicador es útil para conocer si Alianza cuenta con una vía de recepción de sugerencias de cambios, que puedan ser realizadas por los puntos de venta SOAT.

A continuación el segundo indicador representa qué tan bien planificado se encontraba un cambio, según los puntos de venta SOAT. Una calificación negativa de este ítem implica que cambios realizados por Alianza, provocaron un mal funcionamiento del sistema SOAT, que no estaba previsto.

Finalmente como una calificación general se coloca el indicador de “Satisfacción de cambios realizados por Alianza”, para conocer la calificación que le da este grupo, a pesar de las falencias del servicio de SOAT.

Respuesta Cerrada

Recepción de cambios de parte de Alianza, para emisión de SOAT.

Notificación de la realización de cambios que afecten a su entorno de trabajo con el SOAT.
Satisfacción de cambios realizados por Alianza.

2.3.5.4 Gestión de Configuraciones

Descripción

No existen indicadores para este grupo de usuarios, debido a que la Gestión de Configuraciones no puede ser percibida por los Puntos de Venta SOAT.

2.3.5.5 Gestión de Incidentes

Descripción

El usuario muchas veces al recibir un mal servicio ya sea con tiempos de solución altos o falta de apertura para recibir sugerencias, tiende a tratar de resolverlo él mismo con un procedimiento intuitivo que puede llevar a que el incidente se agrave. Por esto se tienen a los indicadores “Recepción de sugerencias hechas a Alianza para mejorar el servicio de SOAT” y a “Satisfacción respecto al tiempo de solución de incidentes”, este último está ligado con el indicador “Tiempo para dar solución a un incidente”.
La prevención de un incidente debe ser la primera opción para que este no suceda y afecte a los usuarios, de ahí que ITIL sugiere dar recomendaciones a los usuarios para que de alguna manera prevengan las amenazas informáticas. Por esto se sugieren como indicador a “Capacitación para el manejo del Sistema SOAT”.
Para este grupo, además se busca conocer si se repiten con frecuencia incidentes específicos, referentes al sistema SOAT. Esto ayuda a identificar si el grupo es afectado en consideración por incidentes que pueden ser solucionados por el equipo de soporte SOAT, de Alianza.
El indicador “Calificación general para Alianza respecto a resolución de incidentes”, es un complemento para que los Puntos de Venta SOAT a pesar de las falencias que presente la empresa, coloque una calificación general del servicio de resolución de incidentes.

Finalmente el indicador “Frecuencia en que el trabajo normal se ve afectado por problemas con el Sistema de SOAT”, permite conocer en el grado de alto, medio y bajo, que tan frecuente suceden problemas en general, para los Puntos de Venta SOAT.

Respuesta Cerrada

Recepción de sugerencias hechas a Alianza para mejorar el servicio de SOAT.
Capacitación para el manejo del Sistema SOAT.
Satisfacción respecto al tiempo de solución de incidentes.
Frecuencia de incidentes específicos.
Tiempo para dar solución a un incidente.
Calificación general para Alianza respecto a resolución de incidentes
Frecuencia en que el trabajo normal se ve afectado por problemas con el Sistema de SOAT.

2.3.5.6 Gestión de Problemas

Descripción

Con el fin de comprobar si existe diferencia de prioridades entre resolución de incidentes y problemas, se inserta el indicador “Urgencia para restablecer sus actividades laborales inmediatamente”, esta representa que los incidentes sean resueltos antes de los problemas.
Finalmente el segundo indicador, ayuda a evaluar si los incidentes que han ocurrido han sido relacionados con un problema específico, ya que si es así el momento en que se repite el incidente se cortaría de raíz el problema, que antes ya debía ser identificado. Si sucede lo contrario denota que no existe un estudio profundo de los problemas ocurridos.

Respuesta Cerrada

Urgencia para restablecer sus actividades laborales inmediatamente.
Rapidez en resolución de incidentes que ya han sucedido anteriormente.

2.4 MÉTODO DE EVALUACIÓN DE INDICADORES

2.4.1 NIVEL DE CUMPLIMIENTO DE LOS INDICADORES DE PREGUNTAS CERRADAS CON RESPECTO A ITIL

2.4.1.1 Porcentaje Total de Respuestas (#Total)

#Total = (# Resp. Correctas + # Resp. Incorrectas + # Resp. SR + #Resp. Parcial)*100

Donde:
 # Resp. Correctas: Número de Respuestas Correctas.
 # Resp. Incorrectas: Número de Respuestas Incorrectas.
 # Resp. SR: Número de Respuestas sin responder.
#Resp. Parcial: Número de Respuestas Correctas Parcialmente.

2.4.1.2 Porcentaje Ponderado de Respuestas (#Ponderado)

#**Ponderado** = (# Resp. Correctas * 100 + (# Resp. Incorrectas + # Resp. SR)* 0 + #Resp. Parcial * 50)

2.4.1.3 Porcentaje de Cumplimiento (#Cumplimiento)

$$\frac{\qquad\qquad\qquad\qquad}{}$$

Con esta ecuación se logra obtener el nivel de cumplimiento para cada indicador.

2.4.2 EVALUACIÓN DE MÉTRICAS (PREGUNTAS ABIERTAS)

El análisis de preguntas abiertas en general se hará en base a comparaciones entre las actividades totales y sus derivadas. Por ejemplo:

Si se evalúa la efectividad de realización de cambios se tienen tres parámetros: Tiempo “T”, Número de cambios solicitados en un tiempo “T”, Número de cambios sin éxito en un Tiempo “T”.

Para detalle de Tablas utilizadas en calificación de métricas, ver Anexo 2-6

2.4.3 CÁLCULO DE LA PROBABILIDAD DE AMENAZA DE CADA INDICADOR

2.4.3.1 Probabilidad de Ocurrencia (Prob. de Amenaza)

Esta ecuación da como resultado la probabilidad de amenaza. Cálculo que es necesario para realizar el Análisis de Riesgos. El resultado encontrado implica la probabilidad de que una amenaza se cumpla.

2.4.4 INTERPRETACIÓN DE CUMPLIMIENTO DE INDICADORES

Con el fin de determinar el estado de cada indicador de una manera objetiva, se usará la Tabla 2-21 sugerida por el Departamento de Auditoría Interna de la Escuela Politécnica Nacional, para identificar el grado de confianza del #Cumplimiento.

Se toman los lineamientos de una institución pública, debido a que poseen normas concretamente definidas para la realización de auditorías, las mismas que son dispuestas por la Contraloría General del Estado. Por otro lado las empresas de tipo privado se rigen bajo sus normas internas y no dependen de terceros, con el propósito de dar generalidad al método propuesto por el autor para evaluar la gestión de tecnologías de información, se eligieron las normas que gobiernan a las empresas del Estado.

#Cumplimiento [%]	GC
15 - 50	B
51 - 59	MB
60 - 66	MM
67 - 75	MA
76 - 95	A

Tabla 2-21a: Interpretación de Cumplimiento de Indicadores, usado en Auditoría Interna de la EPN

Donde:

GC: Grado de Confianza.

B: Bajo.

MB: Moderado Bajo.

MM: Moderado Moderado.

MA: Moderado Alto.

A: Alto.

De esta manera se puede observar en la Tabla 2-21, que de un cumplimiento de 15% hasta un 50%, se considera que el grado de confianza es bajo, siendo este el inferior de todos. Esto se da cuando por ejemplo una actividad se cumple sólo parcialmente o hasta la mitad en referencia al total.

Moderado Bajo, se lo cataloga como moderado por estar cercano al 50% de grado de confianza y bajo por ser el rango inferior de los dos moderados. MB implica que una actividad se la realiza por lo menos un poco más de la mitad, pero todavía no es satisfactoria.

Para el caso de Moderado Moderado, viene a ser cercano a la mitad y representa al rango intermedio de los moderados. Al ir su grado de confianza del 60% a 66% se dice que la actividad evaluada tiene un nivel de cumplimiento igual a este rango. Si bien no es un indicador satisfactorio, se le puede calificar como medianamente satisfactorio.

Un grado de confianza Moderado Alto, representa que las actividades evaluadas si bien están en un rango medio o moderado, son el rango más alto de estas, significando que el grado de confianza en este caso con el rango de 67% a 75% es satisfactorio.

El último rango de 76% a 95% correspondiente al grado de confianza Alto, representa la calificación más alta al momento de evaluar las actividades de tecnología. Al estar por encima del rango moderado y cerca del 100%, se la califica como muy satisfactoria a la actividad que se gane este grado de confianza.

En caso de existir, el #Cumplimiento de 0% a 14% tendrá un GC Bajo y de 96% a 100% será Alto, en la Tabla 2-21 no se los toma en cuenta porque son asumidos como ideales[34].
El rango inferior de 0% a 14% o ideal inferior se lo considera como ideal porque la Unidad de Auditoría Interna de la EPN, asume que al menos entre las dependencias involucradas se habrá enviado algún tipo de documento, es así que el cero absoluto no lo consideran existente.
Para la presente investigación en ciertas ocasiones se necesitan de estos rangos ideales. Ideal inferior en caso de que no se cumpla una actividad específica en absoluto, por ejemplo si el DDS, no coloca un identificador único a cada incidente. El rango ideal superior se lo usará si por el contrario la actividad específica se cumple, como por ejemplo si se registra el técnico que cierra un incidente, si lo hace obtendrá un 100%.
Con el fin de mantener el estándar dado por la Contraloría General del Estado, al rango ideal inferior se lo unió al GC Bajo y al ideal superior se lo integró con el GC Alto.

2.5 EVALUACIÓN DE RIESGOS

2.5.1 DEFINICIONES GENERALES

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
Análisis de Riesgos: Es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

[34] Referencia de la entrevista con Patricia Pérez, Auditor Interno 2 de la EPN, 10 años de experiencia.

Método para Evaluación de Riesgos: El método base a ser usado es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), ver Anexo 2-7.

El método MAGERIT es un libro, que tiene por objetivo describir las técnicas utilizadas en los proyectos de análisis y gestión de riesgos, fue desarrollado por el Ministerio de Administraciones Públicas de España. Propone tres tipos de técnicas específicas:

1. Uso de tablas para la obtención sencilla de resultados.
2. Técnicas algorítmicas para la obtención de resultados elaborados.
3. Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información.

De las tres técnicas propuestas, se eligió al análisis mediante tablas, porque se adapta mejor al sistema de indicadores que se manejan en la presente investigación, ya que mediante un cruce de tablas entre impactos y probabilidad de amenaza, se puede obtener un riesgo totalmente tabulado de acuerdo a las amenazas encontradas. En parte es usado el análisis algorítmico enfocándose en el modelo cuantitativo porque en las tablas se colocan valores específicos para el cálculo del riesgo por indicador. Los árboles de ataque si bien son útiles para conocer el comportamiento que puede tener el atacante, para anticiparse a lo que pudiera ocurrir, no presenta el resultado de riesgos de forma tabular cuantitativamente como es necesario para la presente investigación.

Es así que esta metodología sugiere como base la realización de:

Matriz de Impacto: Está compuesta por los diferentes tipos de impactos que pueden recibir las amenazas. Los impactos implican cuál sería el nivel de gravedad en caso de que ocurra una amenaza, esta puede variar según la naturaleza del impacto.

Para el caso de esta investigación, en consenso con la Gerencia de Sistemas se estimó que los impactos a ser tomados en cuenta son para: resultados, operaciones, aspecto regulatorio, reputación y aspecto económico.

Cabe aclarar que todos los impactos tienen un mismo peso al momento de calcular el impacto promedio, titulado como “Impacto” dentro de la matriz, esto debido a que todos los impactos son de igual importancia, a pesar de que uno tenga más impacto que otro dependiendo del indicador. Dar pesos diferentes entre impactos sería como restarle importancia a la ocurrencia de los que fueron calificados como importantes por la Gerencia de Sistemas de la empresa.
La escala que sugiere MAGERIT para calificar los impactos es de 5 escalones, es decir del 1 al 5, los mismos que se representan por un estado de riesgo como el siguiente:

Riesgo	Estado de Riesgo	Siglas
1	Muy Bajo	MB
2	Bajo	B
3	Medio	M
4	Alto	A
5	Muy Alto	MA

Tabla 2-21b: Interpretación del Estado de Riesgo, usado en el estándar MAGERIT.

Matriz de ocurrencia: Contiene la probabilidad de ocurrencia de los posibles hechos. En este caso este ítem se representa por la probabilidad de que ocurra cada amenaza. Las amenaza se relaciona con un indicador, mismo que proviene de una pregunta de las encuestas realizadas a cada grupo que forma parte de este estudio. Así para generar una amenaza lo que se hace es colocar en forma negativa un indicador, es decir transformar al indicador de tal manera que su ocurrencia de un resultado negativo en la empresa. Por ejemplo para el ítem 1 de la Tabla 2-22 dice “Falta de conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS”, fue transformado a negativo del indicador “Conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS” obtenido del numeral 2.3.1.1 correspondiente a Gestión de Nivel de Servicio para el grupo de Ejecutivos. La forma de calcular la probabilidad de amenaza se lo realiza en el numeral 2.4.3.

Matriz de riesgos: Está conformada por la matriz de ocurrencia y la matriz de impacto.

Estimación del Estado de Riesgo:

Riesgo = Impacto * Probabilidad de Ocurrencia

Al multiplicar estos dos valores se obtiene el riesgo para cada amenaza.

Donde:

Impacto: El promedio de los impactos identificados para una amenaza.

A continuación se presenta la Matriz de riesgos modelo para cada grupo de usuarios:

- Ejecutivos.
- Gerente de Sistemas.
- Operadores del DDS.
- Usuarios Comunes.
- Puntos de Venta SOAT.

2.5.3 MATRIZ DE RIESGOS: EJECUTIVOS

2.5.3.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.								
2	No entrega de documentación formal que informe los servicios que provee el DDS.								
3	Baja calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.								
4	Falta de apoyo a proyectos que mejoren el nivel de servicio que provee el DDS.								
5	Falta de cumplimiento de la calidad del Servicio de Sistema Empresarial								
6	Falta de cumplimiento de la calidad del Servicio de Internet								
7	Falta de cumplimiento de la calidad del Servicio de Correo								
8	Falta de cumplimiento de la calidad del Servicio de Videoconferencia								
9	Falta de cumplimiento de la calidad del Servicio de Soporte								
10	Falta de cumplimiento de la calidad del Servicio de Asesoría								
11	Falta de cumplimiento de la calidad del Servicio de Capacitación								
12	Falta de cumplimiento de la calidad del Servicio de Desarrollo								

13	Falta de cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros								

Tabla 2- 22: Modelo Matriz de Riesgos - Gestión de Nivel de Servicio para Ejecutivos

2.5.3.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apoyo para el desarrollo de planes de contingencia que aseguren la continuidad del servicio en épocas de emergencia.								
2	Falta de preparación frente a emergencias de corte de suministro eléctrico								
3	Falta de preparación frente a emergencias de corte de Internet								
4	Falta de preparación frente a emergencias de virus								
5	Tiempo extendido en estado de emergencia por corte de suministro eléctrico.								
6	Tiempo extendido en estado de emergencia por corte de Internet.								
7	Tiempo extendido en estado de emergencia por virus.								
8	Falta de disponibilidad del Sistema de Seguros.								

Tabla 2-23: Modelo Matriz de Riesgos - Gestión de Continuidad de Servicio para Ejecutivos

2.5.3.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios de software o hardware de parte del DDS.								
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.								
3	Baja frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.								
4	Alta frecuencia de cambios realizados por el DDS que tengan como objetivo modificaciones o correcciones.								
5	Bajo Nivel de satisfacción de los cambios realizados por el DDS.								
6	Falta de método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.								
7	Falta de indicadores que muestren el éxito en la implementación de cambios de parte del DDS a lo largo del 2009.								
8	Bajo porcentaje de cambios implementados frente a los solicitados								
9	Número elevado de cambios que no le han sido notificados y han afectado el desenvolvimiento normal de su trabajo								

Tabla 2-24: Modelo Matriz de Riesgos - Gestión de Cambios para Ejecutivos

2.5.3.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No realización de configuraciones de forma metódica y ordenadamente por el DDS.								
2	Falta de apoyo a proyectos que tengan como objetivo la automatización de configuración de equipos.								

Tabla 2-25: Modelo Matriz de Riesgos - Gestión de Configuraciones para Ejecutivos

2.5.3.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apoyo a proyectos que mejoren el servicio prestado por las tecnologías de Información.								
2	Falta de un método de Gestión de incidentes.								
3	Falta de notificación de posibles amenazas tecnológicas.								
4	Alta frecuencia de incidentes que afectan el normal desempeño de su trabajo.								
5	Falta de satisfacción de los recursos tecnológicos asignados.								
6	Falta de evolución de la tecnología en la empresa.								
7	Falta de apertura del DDS para recibir sugerencias.								
8	Falta de capacitación a los usuarios de parte del DDS.								
9	No satisfacción del usuario frente al tiempo de solución de incidentes.								
10	Alta frecuencia de incidentes específicos.								
11	Falta de método de calificación del servicio recibido de parte del DDS.								
12	Tiempo prolongado para dar solución a un incidente								
13	Baja calificación general para el DDS respecto a resolución de incidentes.								

Tabla 2-26: Modelo Matriz de Riesgos - Gestión de Incidentes para Ejecutivos

2.5.3.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.								
2	Falta de apoyo a desarrollar un equipo especialista para resolver problemas de TI.								
3	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.								

Tabla 2-27: Modelo Matriz de Riesgos - Gestión de Problemas para Ejecutivos

2.5.4 MATRIZ DE RIESGOS: GERENTE DE SISTEMAS

2.5.4.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de monitoreo del Servicio de Internet recibido								
2	Falta de monitoreo del Servicio de Internet suministrado								
3	Falta de monitoreo de enlaces WAN								
4	Falta de historial del servicio de Internet recibido.								
5	Falta de historial de la calidad de enlaces WAN.								
6	Falta de historial de la calidad de los servicios suministrados.								
7	Falta de Contratos formales de nivel de servicio.								
8	No especificación del nivel de servicio para los usuarios de la red corporativa.								
9	No Identificación de necesidades para implementar un servicio.								
10	Falta de Indicadores para identificar desempeño de proveedores de tecnología.								
11	Vía de comunicación con proveedores externos, no efectiva.								
12	Vía de comunicación entre los usuarios y el DDS, no efectiva.								
13	Falta de Mejoramiento de servicios basados en monitoreo.								
14	Baja disponibilidad de los servicios que provee el DDS.								
15	Falta de monitoreo de nivel de calidad de los servicios que provee el DDS.								
16	Bajo cumplimiento del Nivel de Servicio de servicios suministrados.								

17	Falta de monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.								
18	Falta de un encargado para manejar los niveles de servicio de la organización.								
19	No definición formal de la calidad de los servicios que provee el DDS.								
20	No conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.								
21	Falta de revisión de los niveles de servicio de lo suministrado y de proveedores externos.								

Tabla 2-28: Modelo Matriz de Riesgos - Gestión de Nivel de Servicio para Gerente de Sistemas

2.5.4.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.								
2	Falta de desarrollado formal de planes de respuesta ante una emergencia.								
3	Falta de desarrollado de un plan en caso de falla para equipos o sistemas.								
4	Falta de un lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.								
5	Falta de evaluación de planes de respuesta ante emergencias o recuperación antes de ser puestos en marcha.								
6	No revisión de los planes de emergencia ya desarrollados.								
7	Falta de entrenamiento del DDS para utilizar correctamente los planes de emergencia.								
8	Falta de análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización.								
9	Tiempo prolongado en solución de catátrofes.								

Tabla 2-29: Modelo Matriz de Riesgos - Gestión de Continuidad de Servicio para Gerente de Sistemas

2.5.4.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de revisión a los últimos cambios realizados para solucionar incidentes.								
2	Falta de análisis de riegos sobre las implicaciones que podría producir un cambio propuesto.								
3	No tomar en cuenta los posibles incidentes que producirá la ejecución del cambio.								
4	Baja frecuencia de cambios realizados que tengan como objetivo innovación y mejoramiento.								
5	Alta frecuencia de cambios realizados que tengan como objetivo modificaciones o correcciones.								
6	Independencia entre manejo de cambios y configuraciones.								
7	No definir las ventajas de realizar el cambio en cada petición.								
8	No coordinar cada cambio con los departamentos que serán afectados.								
9	La planificación de un cambio no es pública ni notificada al personal de la organización.								
10	No registro de todos los cambios realizados sobre un dispositivo específico.								
11	No existencia de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.								
12	No registro de cada detalle del ciclo de vida del cambio.								
13	No registro del manejo de cambios en el sistema de manejo de configuraciones.								
14	Falta de un filtro de condiciones predeterminadas antes de la aprobación de un cambio.								
15	No identificación de los recursos necesarios antes de la realización de un cambio.								

16	Falta de evaluación al finalizar el ciclo de un proceso de cambio.								
17	Registro como un pedido de cambio a los cambios estándar de rutina.								
18	No registro del responsable de la petición de cambio.								
19	No identificación de la razón para realizar el cambio.								
20	No existencia de recalificación de pedido de cambios en caso de ser negados en primera instancia.								
21	Falta de análisis financiero durante la planeación de un cambio.								
22	No realización de pruebas piloto antes de la implementación de un cambio.								
23	No comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.								
24	No comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.								
25	No registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.								
26	No comprobación de cumplimiento de costos al finalizar la implementación de un cambio.								
27	No comprobación del cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.								
28	Falta de documentación del proceso de evaluación post implementación de cambios.								
29	El encargado de la administración de problemas no participa en la administración de cambios.								
30	El encargado de la administración de incidentes participa en la administración de cambios.								

31	Bajo número de cambios solicitados registrados automáticamente.								
32	Bajo número de cambios realizados frente a los solicitados.								
33	Alto número de cambios realizados con carácter de emergencia frente al total de realizados.								
34	Alto número de cambios realizados sin éxito frente al total de realizados.								
35	Falta de identificación de mejoras en servicios gracias a la realización de cambios.								
36	Falta de un método para registro de Cambios.								

Tabla 2-30: Modelo Matriz de Riesgos - Gestión de Cambios para Gerente de Sistemas

2.5.4.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.								
2	Registro no apropiado de los cambios en el manejo de configuraciones de parte del encargado.								
3	Falta de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.								
4	Falta de documentación de cada equipo configurable con sus características propias.								
5	Falta de levantamiento de procesos para recuperación de desastres de cada equipo configurable.								
6	Falta de cálculo del nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable.								
7	Falta de acceso a todo el ciclo de vida de configuraciones de un equipo específico.								
8	No registro de cada equipo configurable con su estado actual.								
9	Ninigún registro de cada equipo configurable posee atributos que lo relacionen con manejo de cambios, problemas e incidentes.								
10	No toma en cuenta los datos del manejo de configuraciones para el desarrollo de software de la organización.								
11	Falta de relación de manejo de configuraciones con el manejo de cambios.								
12	No documentación de los detalles de verificación al cierre de una configuración.								

13	Falta de un responsable o ejecutor para cada configuración registrada.								
14	No realización de una planificación previa a la implementación de una configuración.								
15	Falta de control del correcto funcionamiento al finalizar la configuración de un ítem.								
16	Falta de evaluación antes del registro de cada configuración.								
17	Falta de identificación concreta de los ítems configurables para cada configuración registrada.								
18	No registro de versión de cada ítem configurable.								
19	Bajo número de configuraciones realizadas frente a las solicitadas.								
20	Falta de un método de registro de Configuraciones.								
21	Alto número de configuraciones realizadas sin éxito frente al total de realizadas.								
22	Alto número de configuraciones realizadas sin autorización.								
23	Alto número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.								
24	No identificación de servicios que han tenido mejora gracias a configuraciones en la organización.								

Tabla 2-31: Modelo Matriz de Riesgos - Gestión de Configuraciones para Gerente de Sistemas

2.5.4.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No toma en cuenta personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos.								
2	No utiliza un escalamiento de solución para resolver incidentes de usuario.								
3	Falta de conocimiento del estado actual de incidentes abiertos.								
4	Falta de conocimiento del número de incidentes que se encuentran abiertos.								
5	Falta de conocimiento de quién es el responsable de la solución y cierre de un incidente abierto.[35]								
6	Falta de conocimiento de quienes son los usuarios que mantienen incidentes sin resolver.								
7	Falta de conocimiento de tiempo de respuesta y solución para un incidente específico.								
8	Falta de acceso a la bitácora de cambios que se relacionan con un incidente específico.								
9	No proveer un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.								
10	No informar al usuario sobre el escalamiento de su incidente.								
11	No informar al usuario sobre el cierre del incidente.								
12	No agrupación de incidentes por su naturaleza.								
13	No agrupación de incidentes por su solución tipo.								
14	No resolución de incidentes tomando en cuenta un banco de soluciones.								

[35] Representa a las preguntas 5 y 18 de la Tabla 3-21, porque implican un impacto y una amenaza similar.

15	Falta de respaldos de la configuración del sistema y equipos para realizar una restauración al estado anterior de los mismos.								
16	Falta de registro de los detalles del cierre de incidentes.								
17	No registro de los niveles de satisfacción del usuario luego del cierre de un incidente.								
18	Falta de un lineamiento específico para que los usuarios realicen un pedido de servicio.								
19	No identificación de los incidentes críticos para su empresa.								
20	No poseer procesos de manejo propios para cada incidente crítico.								
21	No registrar de cada incidente abierto el nombre del técnico que lo recibió.								
22	Tiempo prolongado en resolver incidentes.								
23	Baja frecuencia en la realización de actualizaciones de software.								
24	Baja frecuencia en la realización de actualizaciones de hardware.								
25	Bajo porcentaje de incidentes que se han resuelto en el tiempo esperado.								
26	Alto porcentaje de incidentes que han sido reabiertos del total en un periodo específico.								
27	Bajo porcentaje de incidentes resueltos sin la necesidad de una visita.								
28	Falta de Método para registro de Incidentes.								

Tabla 2-32: Modelo Matriz de Riesgos - Gestión de Incidentes para Gerente de Sistemas

2.5.4.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No diferenciación entre problemas e incidentes.								
2	No tomar en cuenta como base para la resolución de incidentes, la administración de problemas.								
3	Resolución de problemas antes de los incidentes en su organización.								
4	No usar como apoyo a la continuidad del servicio el manejo de problemas.								
5	No existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.								
6	No poseer un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT.								
7	No mantener la infraestructura de comunicaciones sincronizada en tiempo con un reloj interno directamente del servidor NTP de la compañía.								
8	No identificación concreta de las entradas para el proceso de resolución de problemas.								
9	No registro de las salidas del proceso de resolución de problemas.								
10	No apoyo de la resolución de problemas en la base de datos de administración de problemas.								
11	Falta de conocimiento de los problemas cerrados en un periodo de tiempo específico.								
12	Falta de conocimiento concreto del estado de un problema.								
13	Mala coordinación entre administración de problemas y la de cambios.								
14	Objetivos no diferenciados entre problemas e incidentes.								

15	Falta de personal designado para investigación especializada de problemas.								
16	No registro de la o las acciones intuitivas que han mitigado un problema.								
17	Cierre del problema cuando ejecuta una acción intuitiva que atenúa el problema.								
18	No registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.								
19	Soluciona problemas sin apoyo en la base de datos de errores conocidos.								
20	Falta de revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.								
21	Falta de revisión de los procedimientos erróneos, luego del suceso de un error crítico.								
22	Falta de revisión de que se puede mejorar en el futuro, luego del suceso de un error crítico.								
23	Falta de análisis de qué se puede hacer para que no suceda otra vez un suceso de un error crítico, luego de sucedido.								
24	Falta de análisis si la responsabilidad del hecho era de una empresa proveedora de servicios, luego del suceso de un error crítico.								
25	Falta de acciones inmediantas en caso de que un problema crítico sea responsabilidad de una empresa proveedora.								
26	Falta de registro de datos de retroalimentación respecto a problemas críticos.								
27	Falta de Método para registro de problemas.								
28	Bajo número de problemas resueltos frente a los registrados.								
29	Bajo porcentaje de problemas que se han resuelto en el tiempo esperado.								

30	Alta tendencia a que se incrementen los problemas críticos.								

Tabla 2-33: Modelo Matriz de Riesgos - Gestión de Problemas para Gerente de Sistemas

2.5.5 MATRIZ DE RIESGOS: OPERADORES DEL DDS

2.5.5.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de historial del servicio de Internet								
2	Falta de Indicadores para identificar desempeño de proveedores de tecnología.								
3	Falta de conocimiento del nivel de servicio que los usuarios de la organización deben recibir.								
4	Vía de comunicación con proveedores externos, no efectiva.								
5	Vía de comunicación entre los usuarios y el DDS, no efectiva.								
6	Falta de conocimiento de qué servicios ofrece el DDS a la organización								
7	Falta de monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.								
8	Falta de monitoreo de nivel de calidad de los servicios que provee el DDS.								
9	No definición formal de la calidad de los servicios que provee el DDS.								
10	No conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.								

Tabla 2-34: Modelo Matriz de Riesgos - Gestión de Nivel de Servicio para Operadores del DDS

2.5.5.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.								
2	Falta de entrenamiento del DDS para utilizar correctamente los planes de emergencia.								
3	Falta de desarrollado de un plan en caso de falla para equipos o sistemas.								
4	Falta de un lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.								
5	Tiempo prolongado en solución de catátrofes.								

Tabla 2-35: Modelo Matriz de Riesgos - Gestión de Continuidad de Servicio para Operadores del DDS

2.5.5.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de revisión a los últimos cambios realizados para solucionar incidentes.								
2	No registro de cambios que se realizaron sobre un dispositivo específico.								
3	No tomar en cuenta los posibles incidentes que producirá la ejecución del cambio.								
4	Baja frecuencia de cambios realizados que tengan como objetivo innovación y mejoramiento.								
5	Alta frecuencia de cambios realizados que tengan como objetivo modificaciones o correcciones.								
6	No existencia de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.								
7	No identificación de los recursos necesarios antes de la realización de un cambio.								
8	Falta de evaluación al finalizar el ciclo de un proceso de cambio.								
9	No identificación de la razón para realizar el cambio.								
10	No realización de pruebas piloto antes de la implementación de un cambio.								
11	No comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.								
12	No comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.								
13	No registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.								

14	No comprobación del cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.								
15	Falta de un método para registro de Cambios.								
16	Bajo número de cambios realizados frente a los solicitados.								
17	Bajo número de cambios solicitados registrados.								
18	Alto número de cambios realizados sin éxito frente al total de realizados.								
19	Alto número de cambios realizados con carácter de emergencia frente al total de realizados.								
20	Falta de identificación de mejoras en servicios gracias a la realización de cambios.								

Tabla 2-36: Modelo Matriz de Riesgos - Gestión de Cambios para Operadores del DDS

2.5.5.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.								
2	Registro no apropiado de los cambios en el manejo de configuraciones.								
3	Falta de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.								
4	Falta de levantamiento de procesos para recuperación de desastres de cada equipo configurable.								
5	Falta de acceso a todo el ciclo de vida de configuraciones de un equipo específico.								
6	No registro de cada equipo configurable con su estado actual.								
7	No toma en cuenta los datos del manejo de configuraciones para el desarrollo de software de la organización.								
8	No documentación de los detalles de verificación al cierre de una configuración.								
9	Falta de un un responsable o ejecutor para cada configuración registrada.								
10	No realización de una planificación previa a la implementación de una configuración.								
11	Falta de control del correcto funcionamiento al finalizar la configuración de un ítem.								
12	Falta de identificación concreta de los ítems configurables para cada configuración registrada.								
13	Alto número de configuraciones realizadas sin éxito frente al total de realizadas.								

14	Alto número de configuraciones realizadas sin autorización.								
15	Alto número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.								
16	No identificación de servicios que han tenido mejora gracias a configuraciones en la organización.								

Tabla 2-37: Modelo Matriz de Riesgos - Gestión de Configuraciones para Operadores del DDS

2.5.5.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No utiliza un escalamiento de solución para resolver incidentes de usuario.								
2	Falta de conocimiento de quién es el responsable de la solución y cierre de un incidente abierto.								
3	Falta de conocimiento de quienes son los usuarios que mantienen incidentes sin resolver.								
4	Falta de conocimiento de tiempo de respuesta y solución para un incidente específico.								
5	Falta de acceso a la bitácora de cambios que se relacionan con un incidente específico.								
6	No proveer un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.								
7	No informar al usuario sobre el escalamiento de su incidente.								
8	No informar al usuario sobre el cierre del incidente.								
9	No agrupación de incidentes por su naturaleza.								

10	No agrupación de incidentes por su solución tipo.								
11	No resolución de incidentes tomando en cuenta un banco de soluciones.								
12	No registro de los niveles de satisfacción del usuario luego del cierre de un incidente.								
13	No registro del técnico que cierra el incidente.								
14	Tiempo prolongado en resolver incidentes.								
15	Baja frecuencia en la realización de actualizaciones de software.								
16	Baja frecuencia en la realización de actualizaciones de hardware.								
17	Falta de Método para registro de Incidentes.								

Tabla 2-38: Modelo Matriz de Riesgos - Gestión de Incidentes para Operadores del DDS

2.5.5.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No diferenciación entre problemas e incidentes.								
2	Resolución de problemas antes de los incidentes en su organización.								
3	No existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.								
4	No poseer un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT.								
5	No apoyo de la resolución de problemas en la base de datos de administración de problemas.								
6	Falta de personal designado para investigación especializada de problemas.								
7	No registro de la o las acciones intuitivas que han mitigado un problema.								
8	Cierre del problema cuando ejecuta una acción intuitiva que atenúa el problema.								
9	No registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.								
10	Soluciona problemas sin apoyo en la base de datos de errores conocidos.								
11	Falta de revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.								
12	Falta de revisión de los procedimientos erróneos, luego del suceso de un error crítico.								
13	Falta de análisis de qué se puede hacer para que no suceda otra vez un suceso de un error crítico, luego de sucedido.								

14	No registro adecuado de problemas.								
15	Bajo número de problemas resueltos frente a los registrados.								
16	Bajo porcentaje de problemas que se han resuelto en el tiempo esperado.								
17	Alta tendencia a que se incrementen los problemas críticos.								

Tabla 2-39: Modelo Matriz de Riesgos - Gestión de Problemas para Operadores del DDS

2.5.6 MATRIZ DE RIESGOS: USUARIOS COMUNES

2.5.6.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.								
2	No entrega de documentación formal que informe los servicios que provee el DDS.								
3	Baja calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.								
4	Falta de cumplimiento de la calidad del Servicio de Sistema Empresarial.								
5	Falta de cumplimiento de la calidad del Servicio de Internet.								
6	Falta de cumplimiento de la calidad del Servicio de Correo.								
7	Falta de cumplimiento de la calidad del Servicio de Soporte.								
8	Falta de cumplimiento de la calidad del Servicio de Capacitación.								
9	Falta de cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros.								

Tabla 2-40: Modelo Matriz de Riesgos - Gestión de Nivel de Servicio para Usuarios Comunes

2.5.6.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de preparación frente la emergencias como corte de suministro eléctrico.								
2	Tiempo extendido en estado de emergencia por virus.								
3	Falta de disponibilidad del Sistema de Seguros.								
4	Tiempo extendido en estado de emergencia por corte de Internet.								
5	Tiempo extendido en estado de emergencia por corte de Correo Electrónico.								
6	Falta de preparación frente la emergencias de corte de suministro eléctrico.								
7	Tiempo extendido en estado de emergencia por corte de suministro eléctrico.								

Tabla 2-41: Modelo Matriz de Riesgos - Gestión de Continuidad de Servicio para Usuarios Comunes

2.5.6.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios de software o hardware de parte del DDS.								
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.								
3	Baja frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.								
4	Alta frecuencia de cambios realizados por el DDS que tengan como objetivo modificaciones o correcciones.								
5	Bajo Nivel de satisfacción de los cambios realizados por el DDS.								
6	Falta de método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.								
7	Bajo porcentaje de cambios que han sido satisfechos frente a los solicitados.								
8	Número elevado de cambios que no le han sido notificados y han afectado el desenvolvimiento normal de su trabajo.								

Tabla 2-42: Modelo Matriz de Riesgos - Gestión de Cambios para Usuarios Comunes

2.5.6.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No realización de configuraciones de forma metódica y ordenadamente por el DDS.								

Tabla 2-43: Modelo Matriz de Riesgos - Gestión de Configuraciones para Usuarios Comunes

2.5.6.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Alta frecuencia de incidentes que afectan el normal desempeño de su trabajo.								
2	Falta de satisfacción de los recursos tecnológicos asignados.								
3	Falta de evolución de la tecnología en la empresa.								
4	Falta de apertura del DDS para recibir sugerencias.								
5	Falta de capacitación a los usuarios de parte del DDS.								
6	No satisfacción del usuario frente al tiempo de solución de incidentes.								
7	Alta frecuencia de incidentes específicos.								
8	Falta de un método de Gestión de incidentes.								
9	Falta de método de calificación del servicio recibido de parte del DDS.								
10	Tiempo prolongado para dar solución a un incidente.								
11	Baja calificación general para el DDS respecto a resolución de incidentes.								
12	Alta frecuencia de incidentes con Programas de Ofimática.								
13	Alta frecuencia de incidentes de Falla Física de su computador.								
14	Alta frecuencia de incidentes de virus.								
15	Alta frecuencia de incidentes de Internet.								

16	Alta frecuencia de incidentes con Sistema de la empresa.								
17	Alta frecuencia de incidentes con el Correo Electrónico Corporativo.								

Tabla 2-44: Modelo Matriz de Riesgos - Gestión de Incidentes para Usuarios Comunes

2.5.6.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.								
2	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.								

Tabla 2-45: Modelo Matriz de Riesgos - Gestión de Problemas para Usuarios Comunes

2.5.7 MATRIZ DE RIESGOS: PUNTOS DE VENTA SOAT

2.5.7.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de cumplimiento de la calidad del Servicio del Sistema de SOAT.								
2	Falta de cumplimiento de la calidad del Servicio de Soporte Técnico.								

Tabla 2-46: Modelo Matriz de Riesgos en Gestión de Nivel de Servicio para Puntos de Venta SOAT

2.5.7.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de preparación frente la emergencias como corte de suministro eléctrico.								
2	Baja disponibilidad del Sistema de SOAT.								

Tabla 2-47: Modelo Matriz de Riesgos para Gestión de Continuidad de Servicio en Puntos de Venta SOAT

2.5.7.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios para emisión de SOAT de parte de Alianza.								
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo con el SOAT.								
3	Bajo Nivel de satisfacción de los cambios realizados por Alianza.								

Tabla 2-48: Modelo Matriz de Riesgos para Gestión de Continuidad de Servicio en Puntos de Venta SOAT

2.5.7.4 Gestión de Configuraciones

No existen indicadores para este grupo de usuarios.

2.5.7.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apertura de Alianza para recibir sugerencias.								
2	Falta de capacitación a los usuarios de parte de Alianza.								
3	No satisfacción del usuario frente al tiempo de solución de incidentes.								
4	Alta frecuencia de incidentes específicos.								
5	Tiempo prolongado para dar solución a un incidente.								
6	Baja calificación general para Alianza respecto a resolución de incidentes.								
7	Alta frecuencia de incidentes con el Sistema SOAT.								

Tabla 2-49: Modelo Matriz de Riesgos para Gestión de Continuidad de Servicio en Puntos de Venta SOAT

2.5.7.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.								
2	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.								

Tabla 2-50: Modelo Matriz de Riesgos para Gestión de Continuidad de Servicio en Puntos de Venta SOAT

CAPÍTULO III: FORMULACIÓN DE RESULTADOS DE LA GESTIÓN DE IT PARA ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.

En el presente capítulo se detallarán los porcentajes de cumplimiento de indicadores para cada dominio ITIL, de los cinco grupos involucrados, con los Grados de Confianza correspondientes y recomendaciones para GC Bajos. Más adelante se mostrará el resultado del análisis de riesgos.

3.1 EJECUTIVOS

El grupo de Ejecutivos presenta los siguientes resultados, con respecto al Porcentaje de Cumplimiento[36].

3.1.1 GESTIÓN DE NIVEL DE SERVICIO

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	#Cumplimiento	Prob. de Amenaza
1	¿Conoce el nivel de calidad de los servicios que debe recibir de parte del DDS?	0	0	0	**0,00**	**1,00**
2	¿Ha recibido un documento formal informando los servicios que provee el DDS?	0	0	0	**0,00**	**1,00**
3	¿La calidad de servicio que recibe del DDS se ajusta a sus necesidades laborales?	100	100	100	**100,00**	**0,00**
4	¿Apoyaría proyectos que mejoren el nivel de servicio que provee el DDS?	100	100	100	**100,00**	**0,00**
5	Cumplimiento de la calidad del Servicio de Sistema Empresarial	100	100	100	**100,00**	**0,00**
6	Cumplimiento de la calidad del Servicio de Internet	50	100	100	**83,33**	**0,17**
7	Cumplimiento de la calidad del Servicio de Correo	50	100	100	**83,33**	**0,17**
8	Cumplimiento de la calidad del Servicio de Videoconferencia	50	x[37]	x	**50,00**	**0,50**

[36] El detalle de las encuestas aplicadas a Ejecutivos, con sus respectivos totales para cada pregunta de respuesta cerrada o de métricas, puede ser encontrado en el Anexo 2-1, del capítulo 2.

[37] El símbolo 'x' significa que la pregunta no aplica al encuestado.

9	Cumplimiento de la calidad del Servicio de Soporte	100	100	100	**100,00**	**0,00**
10	Cumplimiento de la calidad del Servicio de Asesoría	100	x	x	**100,00**	**0,00**
11	Cumplimiento de la calidad del Servicio de Capacitación	x	100	50	**75,00**	**0,25**
12	Cumplimiento de la calidad del Servicio de Desarrollo	x	100	x	**100,00**	**0,00**
13	Cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros	x	x	50	**50,00**	**0,50**
				#Cumpl. Promedio	**72,436**	

Tabla 3-1: Porcentaje de Cumplimiento - Gestión de Nivel de Servicio para Ejecutivos

3.1.1.1 Estados de Indicadores de Nivel de Servicio

Como se estableció en la Tabla 2-21 del Capítulo 2, con respecto al grado de confianza de cada indicador, se determina que en la Tabla 3-1: el 30,77% tiene un GC Bajo, es decir que los servicios que provee el DDS y su calidad en general no son conocidos por los ejecutivos. El 7,69% es Moderado Alto, es decir que el servicio de capacitación según los ejecutivos es satisfactorio. Finalmente el 61,54% es Alto, lo que significa que los ejecutivos se sienten satisfechos con el servicio de Internet, correo electrónico, sistema empresarial, soporte, asesoría y desarrollo. Además hay la predisposición de los ejecutivos para dar apoyo a programas de mejoramiento de nivel de servicio.

En promedio los indicadores de Nivel de Servicio para el grupo de Ejecutivos tienen una calificación de Moderado Alto, es decir en general la gestión de calidad de las tecnologías es satisfactoria, para el grupo de ejecutivos.

N.	#Cumplimiento	GC
1	0,00	B
2	0,00	B
8	50,00	B
13	50,00	B
11	75,00	MA
6	83,33	A
7	83,33	A
3	100,00	A
4	100,00	A
5	100,00	A
9	100,00	A
10	100,00	A
12	100,00	A

Tabla 3-1: Grado de Confianza - Gestión de Nivel de Servicio para Ejecutivos

3.1.1.2 Gráfico de Cumplimiento de Nivel de Servicio

En la Figura 3-1, se muestra que los indicadores referentes a: falta de conocimiento del nivel de calidad de servicio que debe ser recibido, tienen una calificación de 0, en contraste con: calidad de servicio general dada por el DDS, apoyo a proyectos de mejora, calidad de servicios como Sistema Empresarial, soporte, asesoría, y desarrollo que tienen un cumplimiento de 100.

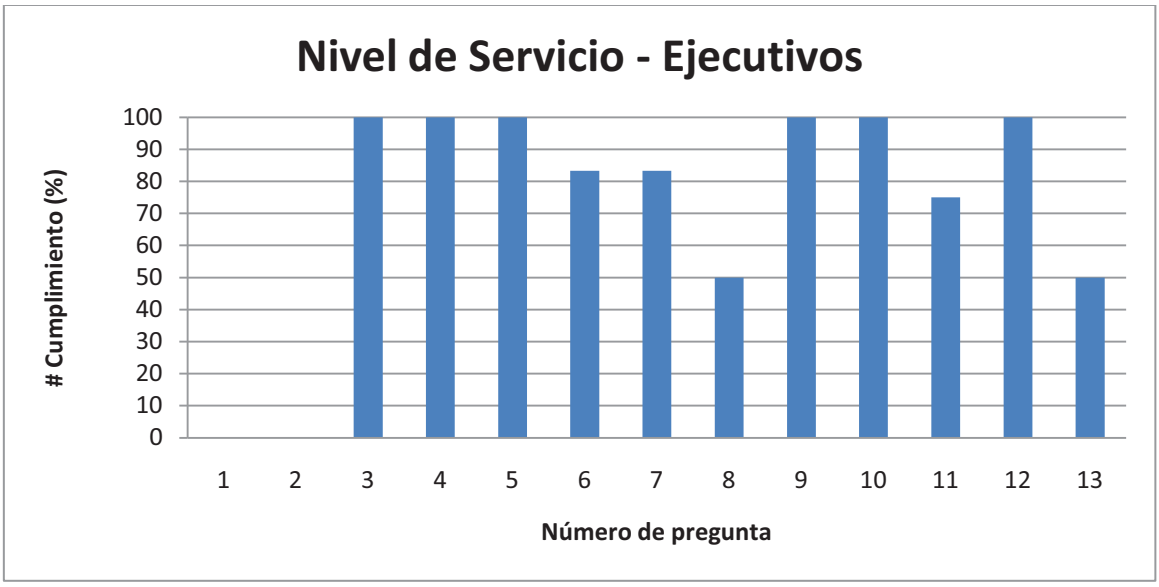

Figura 3-1: Gráfico de Cumplimiento - Gestión de Nivel de Servicio para Ejecutivos

3.1.1.3 Recomendaciones

El primer indicador, donde se consulta "¿Conoce el nivel de calidad de los servicios que debe recibir de parte del DDS?" tiene una calificación de cero absoluto, es decir ningún ejecutivo conoce cuál es el nivel de servicio que debe recibir de parte del DDS. Al no estar familiarizado con la calidad que el ejecutivo debe recibir, se puede dar que reciba más o menos nivel de servicio del requerido. En los dos casos es un inconveniente para la empresa. Si recibe más de lo necesario la empresa está desperdiciando recursos, por el contrario si la calidad es baja el trabajo de los ejecutivos tendrá resultados deficientes.
Todos los ejecutivos encuestados no conocen formalmente los servicios que presta el DDS, según lo consultado en el ítem 2 "¿Ha recibido un documento formal informando los servicios que provee el DDS?" esto provoca que los ejecutivos no exploten completamente el potencial del equipo de tecnología para apoyarlos en su trabajo, o por otro lado puede causar que por falta de conocimiento los operarios del DDS realicen tareas que no les atribuyen.
Por esto se deben establecer los servicios que ofrece el DDS con los respectivos niveles de calidad que requieran los ejecutivos.

El servicio de Video Conferencia sólo fue mencionado por Marcelo Galeano (Subgerente General), y lo catalogó como medianamente eficiente, según lo encuestado en el ítem 8 "Cumplimiento de la calidad del Servicio de Videoconferencia". Este servicio debe ser promocionado a los posibles usuarios de la compañía, consultando sus necesidades y expectativas del servicio, con esta información se podrá diseñar el servicio de acuerdo a las necesidades de la empresa. Con esto más usuarios lo empezarán a utilizar y se sentirán satisfechos con el nivel de calidad recibido.

El servicio de Reportes del Sistema de Seguros, evaluado en el ítem 13 de la encuesta "Cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros" es muy importante para obtener datos comparativos que ayudan a la toma de decisiones. Para un ejecutivo esto es de vital importancia, pero en la organización no está definido ni promocionado. De los ejecutivos encuestados sólo lo nombró Ramiro Pérez (Gerente de Riesgos), quién lo califica con un 50%

de eficacia. Si bien el servicio existe se lo debe definir formalmente y plantear cursos de capacitación según los requerimientos de los usuarios.

3.1.2 GESTIÓN DE CONTINUIDAD DE SERVICIO

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	#Cumplimiento	Prob. de Amenaza
1	¿Apoyaría planes de contingencia que aseguren la continuidad del servicio en época de emergencia?	100	100	100	**100,000**	**0,00**
2	Preparación frente a emergencias de corte de suministro eléctrico	100	100	50	**83,333**	**0,17**
3	Preparación frente a emergencias de corte de Internet	0	x	x	**0,000**	**1,00**
4	Preparación frente a emergencias de virus	x	50	x	**50,000**	**0,50**
5	Tiempo en estado de emergencia por corte de suministro eléctrico.	6,25	6,25	6,25	**6,250**	**0,94**
6	Tiempo en estado de emergencia por corte de Internet.	6,25	x	x	**6,250**	**0,94**
7	Tiempo en estado de emergencia por virus.	x	6,25	x	**6,250**	**0,94**
8	Disponibilidad del Sistema de Seguros.	100	100	100	**100,000**	**0,00**
				#Cumpl. Promedio	**44,010**	

Tabla 3-3: Porcentaje de Cumplimiento - Gestión de Continuidad de Servicio para Ejecutivos

3.1.2.1 Estados de Indicadores de Continuidad de Servicio

La Tabla 3-4 indica que el 62,5 % tiene un cumplimiento Bajo, es decir los ejecutivos no están preparados para emergencias de corte de Internet, virus y reconocen altos tiempos de respuesta ante emergencias de suministro eléctrico, Internet y virus.

Sólo el 37,5 % es Alto, es decir existe la predisposición de los ejecutivos para dar apoyo en mejorar la continuidad de los servicios de TI, además califican como satisfactoria la preparación a cortes de energía y la disponibilidad del sistema de seguros.

En promedio los indicadores de Gestión de Continuidad de Servicio para los ejecutivos tienen un cumplimiento bajo, es decir la Gestión de Continuidad de los servicios de TI desde el punto de vista de los ejecutivos no es satisfactoria.

N.	#Cumplimiento	GC
3	0,000	B
4	50,000	B
5	6,250	B
6	6,250	B
7	6,250	B
1	100,000	A
2	83,333	A
8	100,000	A

Tabla 3-4: Grado de Confianza – Gestión de Continuidad de Servicio para Ejecutivos

3.1.2.2 Gráfico de Cumplimiento de Continuidad de Servicio

La figura 3-2, indica que no existe una preparación ante emergencias tecnológicas de parte de los ejecutivos, pero existe la predisposición para dar apoyo a planes que reduzcan esta debilidad.

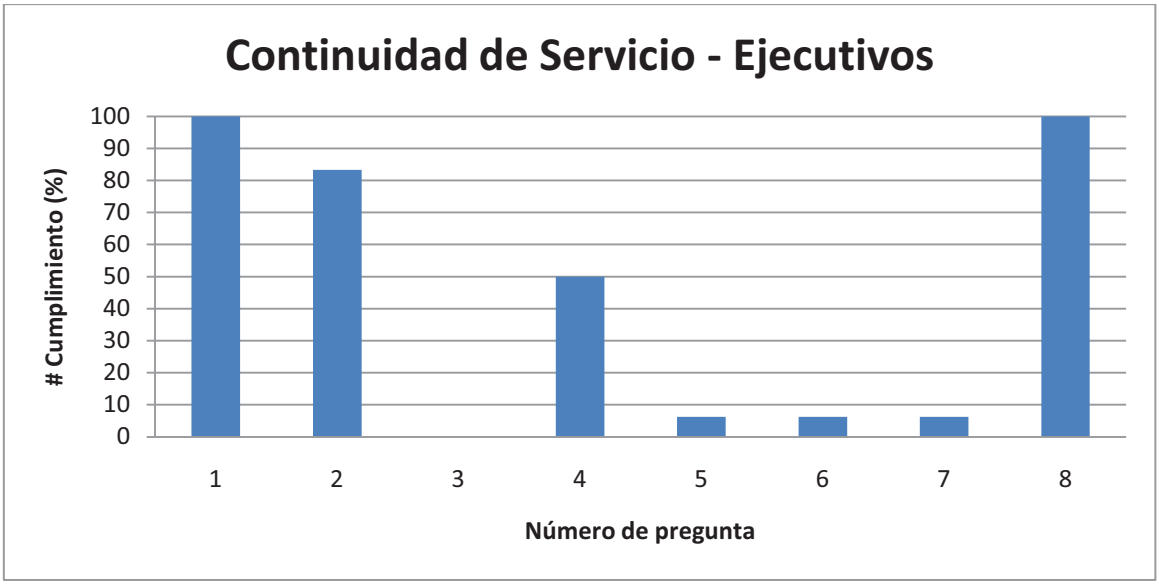

Figura 3- 2: Gráfico de Cumplimiento - Gestión de Continuidad de Servicio para Ejecutivos

3.1.2.3 Recomendaciones

El Internet para los ejecutivos es una herramienta primaria para realizar sus actividades diarias. La falta de preparación ante una falla de este, provocaría que ciertas labores de ejecutivos se paralicen. Por esto se debe tener un plan de contingencia que asegure la continuidad del servicio en caso de que el daño persista por un tiempo extendido. Por ejemplo para los ítems 3 “Preparación frente a emergencias de corte de Internet” y 6 “Tiempo en estado de emergencia por corte de Internet” Marcelo Galeano comentó en la entrevista que en una ocasión el servicio se vió paralizado por alrededor de 8 horas, por una falla del proveedor.

Los problemas de virus en los computadores de una empresa es tema de todos los días. El nivel de daño depende de la precaución de los usuarios ante estas amenazas, Elizabeth Vallejo (Gerente Financiera) mencionó respecto los ítems 4 “Preparación frente a emergencias de virus” y 7 “Tiempo en estado de emergencia por virus” que en una ocasión se vio afectada 24 horas por un virus, durante este periodo se privó del uso de la información que alojaba su ordenador. Para evitar esta interrupción del uso de información, se debe educar al usuario para que respalde información vital para su trabajo así como de las precauciones básicas de seguridad ante ataques informáticos. De esta forma el usuario tomando en

cuenta estas indicaciones las hará hábitos para minimizar al máximo la interrupción de sus labores por motivo de este problema.

Todos los equipos computacionales necesitan de energía eléctrica para su funcionamiento, de ahí que en caso de cortes de energía se debe tener prevista una fuente de energía alterna. En Alianza CIA de Seguros S.A., Quito se contaba con una planta de energía para estos contratiempos, pero cuando tenía que empezar a funcionar por falta de energía, esta no operó por su falta de mantenimiento, dato obtenido del ítem 5 de la encuesta “Tiempo en estado de emergencia por corte de suministro eléctrico” Esto implicó que la empresa no opere sus equipos por alrededor de 24 horas, a esto se suma que todas las sucursales del país estaban vetadas del uso del Sistema Central de Seguros debido a que en Quito se concentran todos los servidores de la empresa. En este caso los ejecutivos deben apoyar y comprobar que se realice el mantenimiento de la planta de energía y probar su funcionamiento a pesar de que no existan cortes de energía eléctrica.

3.1.3 GESTIÓN DE CAMBIOS

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	#Cumplimiento	Prob. de Amenaza
1	¿En caso de la necesidad de un cambio de software o hardware su solicitud es receptada por el DDS?	100	100	100	**100**	**0**
2	¿Es notificado cuándo se realizará un cambio que afecte a su entorno de trabajo?	100	100	100	**100**	**0**
3	¿En general los cambios realizados por el DDS tienen como objetivo innovación y mejoramiento?	100	100	100	**100**	**0**
4	¿En general los cambios realizados por el DDS tienen como objetivo correcciones?	100	100	100	**100**	**0**
5	¿Habitualmente los cambios realizados por el DDS lo han satisfecho?	100	100	100	**100**	**0**
6	¿Tiene la oportunidad de calificar su nivel de satisfacción respecto a un cambio realizado por el DDS?	0	0	0	**0**	**1**
7	¿Posee indicadores que muestren el éxito en la implementación de cambios de parte del DDS a lo largo del 2009?	0	0	0	**0**	**1**
8	Cambios implementados vs solicitados	x	100	x	**100**	**0**
9	Notificación de Cambios	100	100	100	**100**	**0**
				#Cumpl. Promedio	**77,778**	

Tabla 3-5: Porcentaje de Cumplimiento - Gestión de Cambios para Ejecutivos

3.1.3.1 Estados de Indicadores de Gestión de Cambios

En la Tabla 3-6, se puede apreciar que el 22,2 % tiene un cumplimiento Bajo, es decir no tienen los ejecutivos una vía para comunicar su satisfacción respecto a un cambio y no se generan informes para los ejecutivos que detallen el éxito de implementación a lo largo de un periodo.

El 77,8 % posee un nivel Alto, esto implica que: las solicitudes de cambio de parte de los ejecutivos son receptadas por el DDS, cuando hay un cambio los ejecutivos son notificados para que no se afecte su trabajo, los ejecutivos resaltan que los cambios son orientados a mejorar y no a corregir, los cambios generalmente satisfacen a los ejecutivos y los cambios solicitados por ellos son implementados en su totalidad por el DDS.

A pesar de los niveles bajos encontrados, la Gestión de Cambios en promedio tiene un cumplimiento Alto o muy satisfactorio.

N.	#Cumplimiento	GC
6	0	B
7	0	B
1	100	A
2	100	A
3	100	A
4	100	A
5	100	A
8	100	A
9	100	A

Tabla 3-6: Grado de Confianza - Gestión de Cambios para Ejecutivos

3.1.3.2 Gráfico de Cumplimiento de Gestión de Cambios

La Figura 3-3, indica que en el Manejo de Cambios la evaluación es buena a excepción de los indicadores que tienen que ver con el método de evaluar el desempeño en la implementación de Cambios.

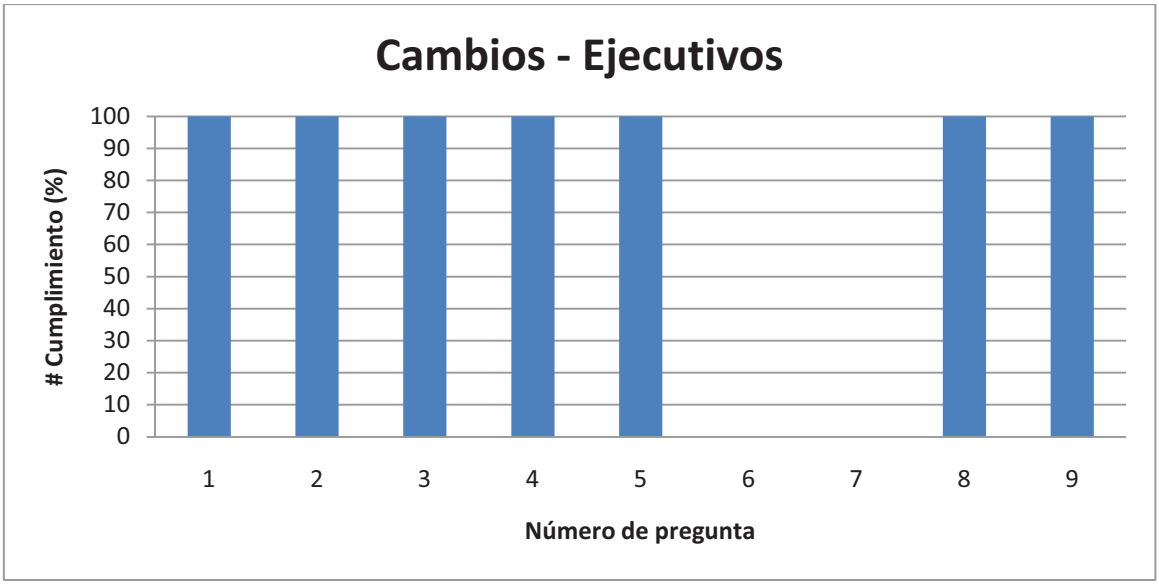

Figura 3-3: Gráfico de Cumplimiento - Gestión de Cambios para Ejecutivos

3.1.3.3 Recomendaciones

Todos los ejecutivos entrevistados según el ítem 6 “Tiene la oportunidad de calificar su nivel de satisfacción respecto a un cambio realizado por el DDS” confirman que no se registra su nivel de satisfacción respecto a los cambios realizados por el DDS. Al no registrar la calificación de ejecutivos, existe la incertidumbre si el trabajo realizado se ha hecho correctamente o no. La evaluación de una actividad ayuda a identificar las falencias que pueden ser mejoradas. Se debe implementar un método de evaluación con respecto a los cambios que afecten a los ejecutivos de la empresa, realizados por el DDS.

La Falta de evaluación provoca que no existan indicadores que determinen el éxito de la implementación de cambios en un cierto período de tiempo, esto lo confirma el ítem 7 de la encuesta “Posee indicadores que muestren el éxito en la implementación de cambios de parte del DDS a lo largo del 2009”. Se deben definir indicadores de cumplimiento acertado para los cambios realizados por el DDS, así se identificaran falencias en proceso de realización de cambios.

3.1.4 GESTIÓN DE CONFIGURACIONES

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	Total Parcial	Prob de Ocurrencia
1	¿En general las configuraciones realizadas por el DDS se realizan de forma metódica y ordenadamente?	x	0	x	0	1
2	¿Apoyaría proyectos que tengan como objetivo la automatización de configuración de equipos?	x	100	x	100	0
				#Cumpl. Promedio	50	

Tabla 3-7: Porcentaje de Cumplimiento - Gestión de Configuraciones para Ejecutivos

3.1.4.1 Estados de Indicadores de Gestión de Configuraciones

Respecto a Manejo de Configuraciones la Tabla 3-8, dice que de los dos indicadores el 50 % es Bajo, lo que implica que los ejecutivos representados por Elizabeth Vallejo no perciben que las configuraciones se realizan de forma metódica y ordenada. El resto es Alto, es decir que los ejecutivos de igual forma representados por Elizabeth Vallejo apoyan proyectos que tengan como objetivo el mejoramiento de procesos de configuraciones.

Como promedio se obtiene un cumplimiento bajo de 50%, es decir la Gestión de Configuraciones según el grupo de ejecutivos es no es satisfactoria.

N.	#Cumplimiento	GC
1	0	B
2	100	A

Tabla 3-8: Grado de Confianza - Gestión de Configuraciones para Ejecutivos

3.1.4.2 Gráfico de Cumplimiento de Gestión de Configuraciones

La figura 3-4, indica que de parte del grupo de Ejecutivos[38] existe la percepción de que no se llevan métodos formales para realizar configuraciones de tecnología, pero existe el apoyo del 100 % para automatizar este proceso.

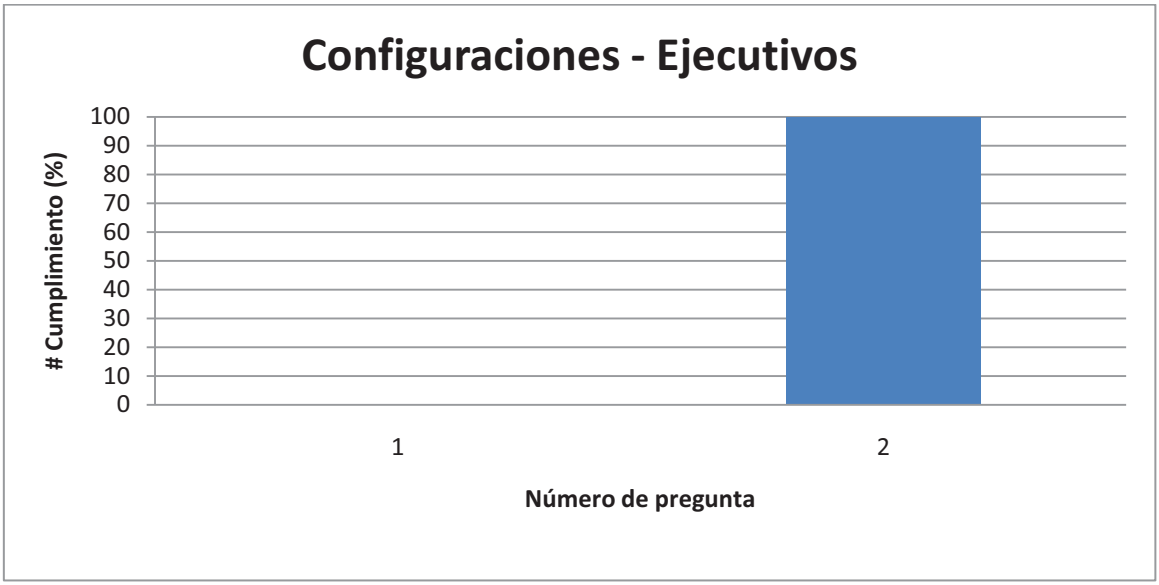

Figura 3-4: Gráfico de Cumplimiento - Gestión de Configuraciones para Ejecutivos

3.1.4.3 Recomendaciones

Elizabeth Vallejo es el ejecutivo encargado de coordinar la gerencia del DDS, por esto ha sido elegida para evaluar los indicadores de la Gestión de Configuraciones. El punto crítico en este proceso es que no se percibe que las configuraciones se realizan de forma metódica y ordenadamente, cómo se lo obtuvo del ítem 1 de la encuesta “En general las configuraciones realizadas por el DDS se realizan de forma metódica y ordenadamente”. El ejecutivo encargado de evaluar las actividades del DDS debe apoyar el uso de procesos formales y metódicos para las configuraciones de los equipos computacionales de Alianza CIA de Seguros S.A. De esta forma las configuraciones se realizarán más eficientemente dando como resultado la mejora del apoyo tecnológico a las operaciones de la empresa.

[38] La encuesta de Manejo de Configuraciones sólo se aplica a la Ejecutiva Elizabeth Vallejo.

3.1.5 GESTIÓN DE INCIDENTES

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	#Cumplimiento	Prob. de Amenaza
1	¿Daría su apoyo a proyectos que mejoren el servicio prestado por las tecnologías de Información?	100	100	100	**100,00**	**0.000**
2	Método de Gestión de incidentes.	20	100	20	**46,67**	**0.533**
3	¿Ha sido informado de los incidentes tecnológicos críticos para su empresa?	100	100	0	**66,67**	**0.333**
4	¿Los incidentes de tecnología no afectan con frecuencia el normal desempeño de su trabajo?	100	100	0	**66,67**	**0.333**
5	¿Cree que los recursos tecnológicos han sido asignados de acuerdo a las necesidades actuales del negocio?	100	50	0	**50,00**	**0.500**
6	¿Cree que la tecnología usada en la empresa ha evolucionado de forma continua para mejorar el servicio ofrecido?	100	100	100	**100,00**	**0.000**
7	¿Son atendidas las sugerencias hechas al DDS para mejorar el servicio de la tecnología?	100	100	100	**100,00**	**0.000**
8	¿Recibe cursos o entrenamientos cuando existe la necesidad de manejar nuevos programas informáticos?	100	50	100	**83,33**	**0.167**
9	¿En general el tiempo de solución a los incidentes de parte del DDS ha sido satisfactorio?	100	100	100	**100,00**	**0.000**
10	¿Se repiten con frecuencia incidentes específicos?	50	100	100	**83,33**	**0.167**
11	¿Tiene la oportunidad de calificar el servicio recibido de parte del DDS?	0	0	0	**0,00**	**1.000**
12	Tiempo para dar solución a un incidente.	100	100	100	**100,00**	**0.000**
13	Calificación general para el DDS respecto a resolución de incidentes.	100	100	100	**100,00**	**0.000**
				#Cumpl. Promedio	**76,667**	

Tabla 3-9: Porcentaje de Cumplimiento - Gestión de Incidentes para Ejecutivos

3.1.5.1 Estados de Indicadores de Gestión de Incidentes

La Tabla 3-10, muestra que el 23,1 % de indicadores para Gestión de Incidentes tiene un GC Bajo, es decir los ejecutivos no tienen una vía para calificar el servicio de atención de incidentes, el trato que se le da a los incidentes no es satisfactorio, así como la asignación adecuada de los recursos de tecnología según los ejecutivos no es satisfactoria.

El 15,4 % Moderado Moderado implica que es medianamente satisfactorio: la notificación de posibles incidentes críticos para la empresa y la frecuencia de que los incidentes afecten el trabajo normal de los ejecutivos.

Finalmente el 61,5 % tiene un nivel Alto, lo cual significa que es muy satisfactorio según los ejecutivos: el entrenamiento para manejar nuevos programas informáticos, no se repiten incidentes similares frecuentemente, la predisposición para dar apoyo a programas de mejoramiento a la atención de incidentes, la evolución de la tecnología para mejorar el servicio recibido, apertura del DDS para recibir sugerencias, el tiempo corto en que el DDS generalmente resuelve incidentes, buena calificación general para el DDS respecto a resolución de incidentes.

En promedio el cumplimiento que tiene la Gestión de Incidentes desde el punto de vista de los ejecutivos, es muy satisfactorio.

N.	#Cumplimiento	GC
11	0,000	B
2	46,667	B
5	50,000	B
3	66,667	MM
4	66,667	MM
8	83,333	A
10	83,333	A
1	100,000	A
6	100,000	A
7	100,000	A
9	100,000	A
12	100,000	A
13	100,000	A

Tabla 3-10: Grado de Confianza - Gestión de Incidentes para Ejecutivos

3.1.5.2 Gráfico de Cumplimiento de Gestión de Incidentes

La Figura 3-5, muestra que por alrededor del 50 y 60 de cumplimiento se encuentran los indicadores que tienen que ver con el Método de Gestionar Incidentes, además no existe una forma de calificar el servicio recibido de parte del DDS.

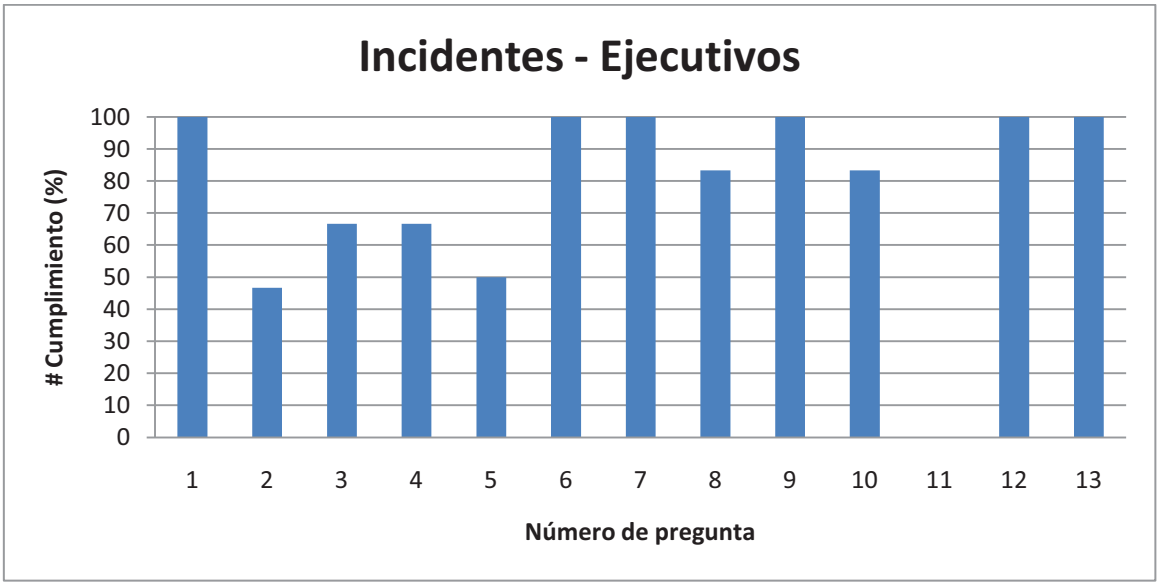

Figura 3-5: Gráfico de Cumplimiento - Gestión de Incidentes para Ejecutivos

3.1.5.3 Recomendaciones

Los 3 ejecutivos encuestados certifican, según lo encuestado en el ítem 11 "¿Tiene la oportunidad de calificar el servicio recibido de parte del DDS?" que no existe un método para calificar el servicio recibido con respecto a solución de incidentes. El ejecutivo por su importancia debe sugerir que se recepte su nivel de satisfacción, con esto se conocerá en que campos puede mejorar el DDS, así como que lo está realizando adecuadamente.

Los ejecutivos al momento de ser tomados en cuenta para calificar el servicio, percibirán que el equipo de Sistemas está buscando continuamente elevar su calidad de trabajo.

El método de gestión de Incidentes según lo encuestado en el ítem 2 "Método de Gestión de incidentes", tiene una calificación de 46,67 este ítem implica que: no se realiza una notificación cuando un incidente ha sido cerrado, no posee la empresa un lineamiento formal para realizar un pedido de servicio, existe falta de

conocimiento de quien es el técnico responsable de resolver el incidente y finalmente el no registro formal de inconvenientes.
Al momento de notificar el cierre de un incidente al ejecutivo, este confirmará que efectivamente el incidente ha sido solucionado, o también se puede dar el caso que al notificar el cierre resulte que la tarea no ha sido completada. Al no existir esta confirmación los incidentes pueden quedar sin resolución, o por el contrario es posible que se gasten recursos innecesarios al tratar de solucionar inconvenientes que ya estén corregidos. Por esto es necesario que los incidentes cerrados sean notificados al ejecutivo afectado.

Según el ítem 5 de la encuesta “¿Cree que los recursos tecnológicos han sido asignados de acuerdo a las necesidades actuales del negocio?”, existe una calificación parcial de 50 con respecto a la satisfacción de los recursos tecnológicos recibidos, se nota el malestar de los ejecutivos en el sentido que no se ha evaluado las necesidades para luego en base a estas asignar equipos o tecnología. Sólo Marcelo Galeano se encuentra de acuerdo con la asignación actual. En base a este indicador se debe realizar un reconocimiento de las necesidades entre los ejecutivos para evaluar cuáles podrían ser los equipos idóneos para su trabajo. Si persiste la inconformidad el trabajo de los ejecutivos se podría ver afectado.

3.1.6 GESTIÓN DE PROBLEMAS

N.	PREGUNTAS	Marcelo Galeano	Elizabeth Vallejo	Ramiro Pérez	#Cumplimiento	Prob. de Amenaza
1	¿Su incidente trata de ser generalmente resuelto inmediatamente para restablecer sus actividades laborales?	100	100	100	**100**	**0**
2	¿Apoyaría un equipo especialista en resolver problemas de TI?	100	100	100	**100**	**0**
3	¿Incidentes que ya han ocurrido antes son resueltos con mayor rapidez?	100	100	100	**100**	**0**
				#Cumpl. Promedio	**100**	

Tabla 3-11: Porcentaje de Cumplimiento - Gestión de Problemas para Ejecutivos

3.1.6.1 Estados de Indicadores de Gestión de Problemas

Según la Tabla 3-12, se indica que el 100 % los indicadores para Gestión de Problemas tienen un GC Alto, es decir es muy satisfactorio según los ejecutivos: la prioridad que se le da a resolver los incidentes inmediatamente, el apoyo a generar un equipo especialista para resolver problemas de TI, y la resolución en un tiempo más corto de incidentes que ya han ocurrido con anterioridad.

En promedio la Gestión de Problemas según los ejecutivos tiene un cumplimiento muy satisfactorio de 100%.

N.	#Cumplimiento	GC
1	100	A
2	100	A
3	100	A

Tabla 3-12: Grado de Confianza - Gestión de Problemas para Ejecutivos

3.1.6.2 Gráfico de Cumplimiento de Gestión de Problemas

La Figura 3-6, muestra que los 3 indicadores respecto a manejo de problemas tienen un cumplimiento de 100, entonces para el grupo de Ejecutivos esta gestión se está manejando de forma adecuada.

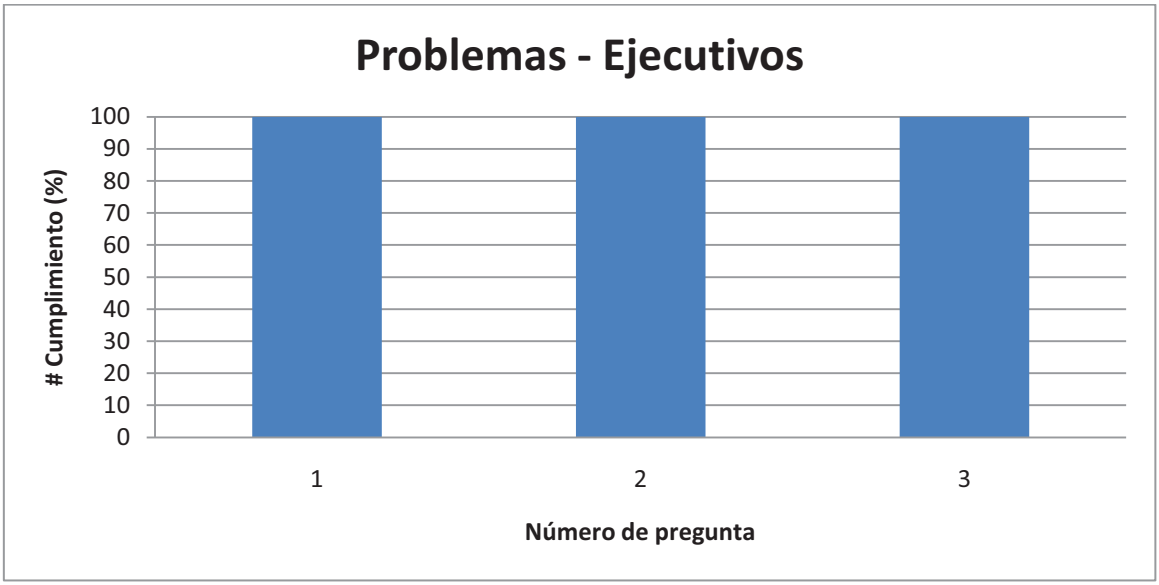

Figura 3-6: Gráfico de Cumplimiento - Gestión de Problemas para Ejecutivos

3.1.6.3 Recomendaciones

La Gestión de Problemas para Ejecutivos no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.2 GERENTE DE SISTEMAS

El grupo de Gerente de Sistemas presenta los siguientes resultados, con respecto al Porcentaje de Cumplimiento. El detalle de las encuestas aplicadas al Gerente de Sistemas, puede ser encontrado en el Anexo 2-2, del capítulo 2.

3.2.1 GESTIÓN DE NIVEL DE SERVICIO

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	¿Monitorea de forma automática la calidad del servicio de Internet recibido?	50	50	0,5
2	¿Monitorea de forma automática la calidad del servicio de Internet suministrado?	50	50	0,5
3	¿Monitorea el ancho de banda y el estatus de sus enlaces wan?	50	50	0,5
4	¿Existen reportes históricos del servicio de Internet?	0	0	1
5	¿Existen reportes históricos de la calidad de los enlaces wan?	0	0	1
6	¿Existen reportes históricos de la calidad de cada servicio que ofrece el DDS a los usuarios de la organización?	0	0	1,00
7	¿Mantiene contratos formales que especifican los niveles de servicio que prestan sus proveedores, en caso de no cuáles?	50	50	0,50
8	¿Tiene especificados los niveles de servicio para los usuarios de la red corporativa?	0	0	1
9	¿Identifica las necesidades de la empresa para la implementación de un servicio?	100	100	0
10	¿Posee indicadores para verificar el desempeño de sus proveedores de tecnología?	0	0	1
11	¿Existe una vía de comunicación rápida y confiable para contactarse con cada uno de los proveedores externos de tecnologías?	50	50	0,5
12	¿Los usuarios de la red tienen un medio para comunicarse rápidamente con el DDS?	50	50	0,5
13	¿Realiza planes para mejoramiento de los servicios basados en el monitoreo de la calidad actual de los mismos?	0	0	1
14	Disponibilidad de los servicios que provee el DDS.	100	100	0
15	Monitoreo de nivel de calidad de los servicios que provee el DDS.	0	0	1
16	Cumplimiento del Nivel de Servicio de lo suministrado.	0	0	1
17	Monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.	0	0	1
18	Encargado para manejar los niveles de servicio de la organización.	0	0	1
19	Definición formal de la calidad de los servicios que provee el DDS.	0	0	1
20	Conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.	0	0	1

21	Revisión de los niveles de servicio de lo suministrado y de proveedores externos.	0	0	**1**
		#Cumpl. Promedio	**23,81**	

Tabla 3-13: Porcentaje de Cumplimiento - Gestión de Nivel de Servicio para Gerente de Sistemas

El #Cumpl. Promedio 23.81 de la Tabla 3-13 significa que en promedio el GC para Gestión de Nivel de Servicio del Gerente de Sistemas es bajo.

3.2.1.1 Estados de Indicadores de Gestión de Nivel de Servicio

La Tabla 3-14, muestra que el 90,5 % de los indicadores de Nivel de Servicio tienen un GC Bajo, esto significa que: no existen reportes históricos sobre el servicio de Internet, la calidad de los enlaces wan, la calidad de los servicios suministrados en general, no se tienen especificados los niveles de servicio para los usuarios de la red corporativa, no posee indicadores para verificar el desempeño de los proveedores de tecnología, no se realiza mejoramiento de los servicios basados en un monitoreo, no se monitorean los niveles de calidad de los servicios que provee el DDS, no se conoce formalmente si los servicios suministrados tienen una calidad aceptable, no existe un monitoreo de los servicios que son recibidos de proveedores externos, no existe un perfil definido para el encargado de manejar los niveles de servicio de la organización, no hay una definición formal de la calidad de los servicios que provee el DDS, ni se conoce el nivel de satisfacción de los usuarios, no se realiza una revisión de los niveles de calidad de servicios internos y externos, no se monitorea de forma automática el servicio de Internet suministrado y recibido, no se monitorea el ancho de banda usado ni el estado de los enlaces wan, los contratos formales que especifican la calidad de los servicios de proveedores externos sólo se realizan de manera parcial así como la vía de comunicación confiable con dichos proveedores.

El 9,5% restante tiene un GC Alto, lo cual implica que la gerencia de sistemas de forma muy satisfactoria: se preocupa de identificar las necesidades de la empresa para realizar la implementación de un servicio, y así mismo ha generado el diseño de la disponibilidad de los servicios que provee el DDS.

N.	#Cumplimiento	GC
4	0	B
5	0	B
6	0	B
8	0	B
10	0	B
13	0	B
15	0	B
16	0	B
17	0	B
18	0	B
19	0	B
20	0	B
21	0	B
1	50	B
2	50	B
3	50	B
7	50	B
11	50	B
12	50	B
9	100	A
14	100	A

Tabla 3-14: Grado de Confianza - Gestión de Nivel de Servicio para Gerente de Sistemas

3.2.1.2 Gráfico de Cumplimiento de Gestión de Nivel de Servicio

La Figura 3-7, dice que la mayoría de indicadores de Nivel de Servicio se encuentran por debajo del 50 de cumplimiento, con la excepción de la disponibilidad de los servicios que tienen un nivel de 100, por ser diseñados de acuerdo a las necesidades de la empresa.

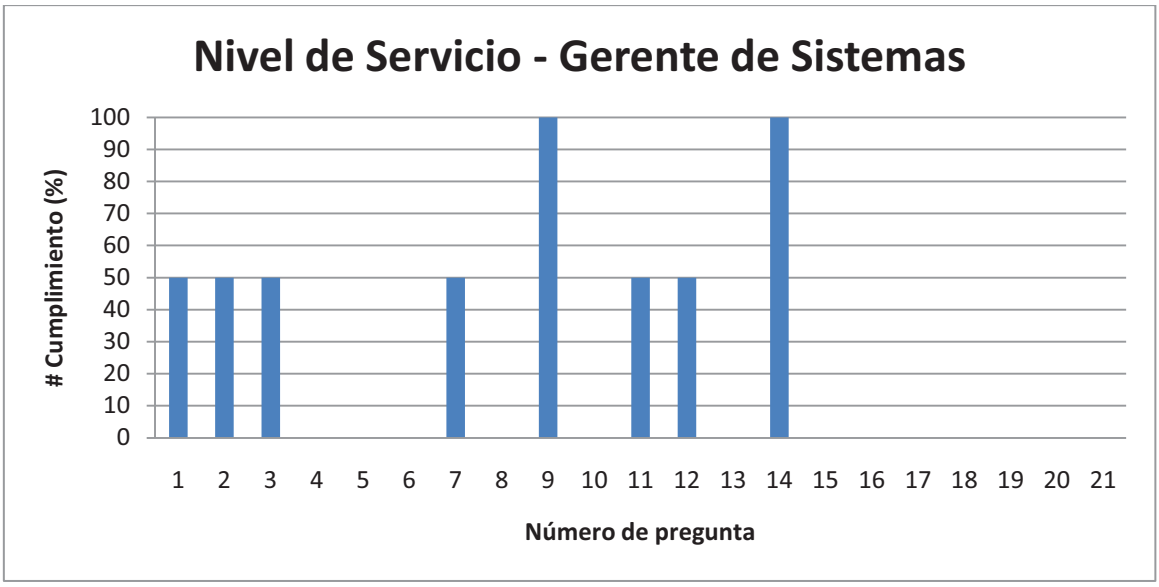

Figura 3-7: Gráfico de Cumplimiento - Gestión de Nivel de Servicio para Gerente de Sistemas

3.2.1.3 Recomendaciones

Según lo obtenido del ítem 4 de la encuesta "¿Existen reportes históricos del servicio de Internet?" La falta de existencia de reportes históricos del servicio de Internet recibido y suministrado a la compañía, dificulta la comprobación de la calidad que el proveedor está obligado a cumplir. Además sin el reporte de lo suministrado, no se puede constatar cuál ha sido la disponibilidad que ha tenido el servicio de Internet, y a su vez realizar comparaciones para determinar si los resultados se ajustan a las necesidades de la empresa. Por esto se deben utilizar las herramientas necesarias para generar los reportes históricos de Internet recibido y suministrado.

Así como para el servicio de Internet, el numeral 5 de la encuesta "¿Existen reportes históricos de la calidad de los enlaces wan?" los enlaces WAN con las sucursales deben ser monitoreados para verificar la calidad recibida. El origen de los problemas con las sucursales se debería apoyar directamente en el monitoreo de los enlaces WAN. En el historial se podrían revisar las horas de disponibilidad versus las horas de caída. Se debe disponer de utilitarios para monitoreo de enlaces WAN, con capacidad de almacenamiento. Esto se relaciona con el numeral 17 de la encuesta "Monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos", mismo que presenta un GC bajo.

El gerente de sistemas de la compañía afirma que para ningún servicio prestado, se tienen reportes de su calidad a lo largo del tiempo, esto según el numeral 6 de la encuesta "¿Existen reportes históricos de la calidad de cada servicio que ofrece el DDS a los usuarios de la organización?" y el numeral 15 "Monitoreo de nivel de calidad de los servicios que provee el DDS". Esto afecta para la determinación de la disponibilidad de los servicios. Se deben mantener bajo vigilancia todos los servicios sin excepción.

Debido a la negativa calificación del ítem 8 de la encuesta "¿Tiene especificados los niveles de servicio para los usuarios de la red corporativa?" y del numeral 19 "Definición formal de la calidad de los servicios que provee el DDS", la Gerencia de Sistemas debe definir los niveles de servicio formalmente para no errar en suministrar servicios de mala calidad, o malgastar recursos por no conocer las necesidades de los usuarios de la red. Con esto se puede auditar y verificar con elementos de juicio el cumplimiento de la responsabilidad del Departamento de Tecnología. Para esta definición se deben tener concretamente estipulados los servicios que provee el DDS a sus usuarios. Por esto el numeral 16 de la encuesta de ve afectado con un GC bajo "Cumplimiento del Nivel de Servicio de lo suministrado".

Debido al GC bajo del numeral 10 de la encuesta "¿Posee indicadores para verificar el desempeño de sus proveedores de tecnología?", se debe proponer indicadores para verificar el desempeño de los proveedores de tecnología, definido esto se pueden realizar análisis comparativos y calificar el desempeño que tienen estas entidades. Los servicios reconocidos como externos por el gerente de Sistemas son: Internet, comunicaciones, mantenimiento y soporte IBM.

Dado que el numeral 13 de la encuesta "¿Realiza planes para mejoramiento de los servicios basados en el monitoreo de la calidad actual de los mismos?", tiene un GC bajo, se recomienda considerar que el monitoreo es importante realizarlo porque ayuda a proceder con el mejoramiento continuo, una vez recopilados los reportes de los servicios se deben analizar las falencias y dar soluciones para que mejoren su eficiencia.

Dado en GC bajo del numeral 18 de la encuesta “Encargado para manejar los niveles de servicio de la organización”, es aconsejable seleccionar una persona encargada de gestionar el nivel de servicio en la organización, el perfil de este cargo es para alguien en primer lugar con altos conocimientos de tecnología además se debe complementar con una forma de ser comunicativa y sociable de tal manera que negocie sin problemas con usuarios internos y proveedores externos. El Gerente de Sistemas actualmente no tiene una persona encargada de lleno a este tema ni un perfil claro para la tarea.

El numeral 20 de la encuesta “Conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS” tiene un GC bajo, por esto se recomienda considerar que la opinión del usuario es importante, al pedirle que califique el servicio se pueden conocer sus sugerencias y expectativas. Se debe implementar un método para recibir la evaluación de los consumidores, actualmente no existe ninguna forma de saber el nivel de satisfacción interno.

El ítem 21 de la encuesta “Revisión de los niveles de servicio de lo suministrado y de proveedores externos” tiene un GC bajo por esto se recomienda que al definir el nivel de calidad para un grupo de servicios, se debe tomar en cuenta que estos no tienen una validez indefinida, por el contrario cumplen un ciclo de vida que debe ser revisado continuamente. La empresa no puede permanecer estática es cambiante porque el mercado así lo demanda, según los datos recogidos en la entrevista los niveles de servicio no se renuevan, por esto se sugiere que con el carácter de urgente se tome en cuenta la duración del ciclo de vida de las políticas de calidad para cada servicio.

Dado que el numeral 1 “¿Monitorea de forma automática la calidad del servicio de Internet recibido?” y el numeral 2 “¿Monitorea de forma automática la calidad del servicio de Internet suministrado?” tienen un GC bajo se recomienda que se utilicen herramientas de monitoreo automáticas como lo es CACTI de software libre o PRTG para Windows, esto a su vez ayudará a generar un historial del

servicio. La misma recomendación se aplica para el numeral 3 con GC bajo "¿Monitorea el ancho de banda y el estatus de sus enlaces wan?".

Con los proveedores de tecnología se deben mantener contratos formales de todos los servicios que ofrecen a la compañía, actualmente según el Gerente de Sistemas afirma que lo hacen parcialmente, se sugiere cambiar esta política para que el indicador suba al 100%, esta recomendación fue obtenida del numeral 7 de la encuesta "¿Mantiene contratos formales que especifican los niveles de servicio que prestan sus proveedores, en caso de no cuáles?".

Dada la necesidad de soporte en caso de falla, la empresa debe contar con un medio de comunicación rápido y efectivo con el proveedor de servicios. Este parámetro ayuda a minimizar el tiempo que se encuentre fuera de servicio la compañía, caso contrario se vuelve un problema adicional al ya existente. La misma recomendación se aplica para los usuarios internos con el DDS. Los dos casos actualmente tienen un #Cumplimiento de 50, según los numerales 11 "¿Existe una vía de comunicación rápida y confiable para contactarse con cada uno de los proveedores externos de tecnologías?" y 12 "¿Los usuarios de la red tienen un medio para comunicarse rápidamente con el DDS?" de la encuesta.

3.2.2 GESTIÓN DE CONTINUIDAD DE SERVICIO

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	¿Conoce el equipo del DDS la existencia de planes de emergencia?	50	50	0,5
2	Desarrollo formal de planes de respuesta ante una emergencia.	50	50	0,5
3	Desarrollo de un plan en caso de falla para equipos o sistemas.	50	50	0,5
4	Lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.	50	50	0,5
5	Evaluación de planes de respuesta ante emergencias o recuperación antes de ser puestos en marcha.	50	50	0,5
6	Revisión de los planes de emergencia ya desarrollados.	75	75	0,25
7	Entrenamiento del DDS para utilizar correctamente los planes de emergencia.	50	50	0,5
8	Análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización.	0	0	1
9	Tiempo en solución de catástrofes.	0	0	1
		#Cumpl. Promedio	41,67	

Tabla 3-15: Porcentaje de Cumplimiento - Gestión de Continuidad de Servicio para Gerente de Sistemas

3.2.2.1 Estados de Indicadores de Gestión de Continuidad de Servicio

La Tabla 3-16, muestra que el 88.9 % de indicadores para Gestión de Continuidad de Servicio tienen un GC Bajo, lo que implica que no se realiza un análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización, las catástrofes a pesar de existir no son reconocidas como tal, este es el caso de la crisis de energía eléctrica sufrida, los miembros del DDS sólo han sido informados parcialmente sobre los planes de emergencia existentes, de la misma manera planes para dar respuesta a una emergencia o para solucionar fallas de equipos han sido desarrollados parcialmente, los procesos para recuperar al estado anterior servicios sólo tiene un desarrollo parcial. Además la evaluación de planes para enfrentar emergencias sólo se la hace de forma parcial, así como el entrenamiento que debería recibir el DDS para que los aplique correctamente.

El 11.1 % restante es Moderado Alto, lo cual implica que es satisfactoria la revisión de los planes de emergencia ya desarrollados.

En promedio la Gestión de Nivel de Servicio es realizada de forma no satisfactoria por parte de la gerencia de Sistemas.

N.	#Cumplimiento	GC
8	0	B
9	0	B
1	50	B
2	50	B
3	50	B
4	50	B
5	50	B
7	50	B
6	75	MA

Tabla 3-16: Grado de Confianza - Gestión de Continuidad de Servicio para Gerente de Sistemas

3.2.2.2 Gráfico de Cumplimiento de Gestión de Continuidad de Servicio

En la Figura 3-8, se denota que las falencias más graves respecto a Continuidad de Servicio son la falta de un análisis de vulnerabilidades junto con la consecuencia que provoca el tiempo prolongado en solución de catástrofes.

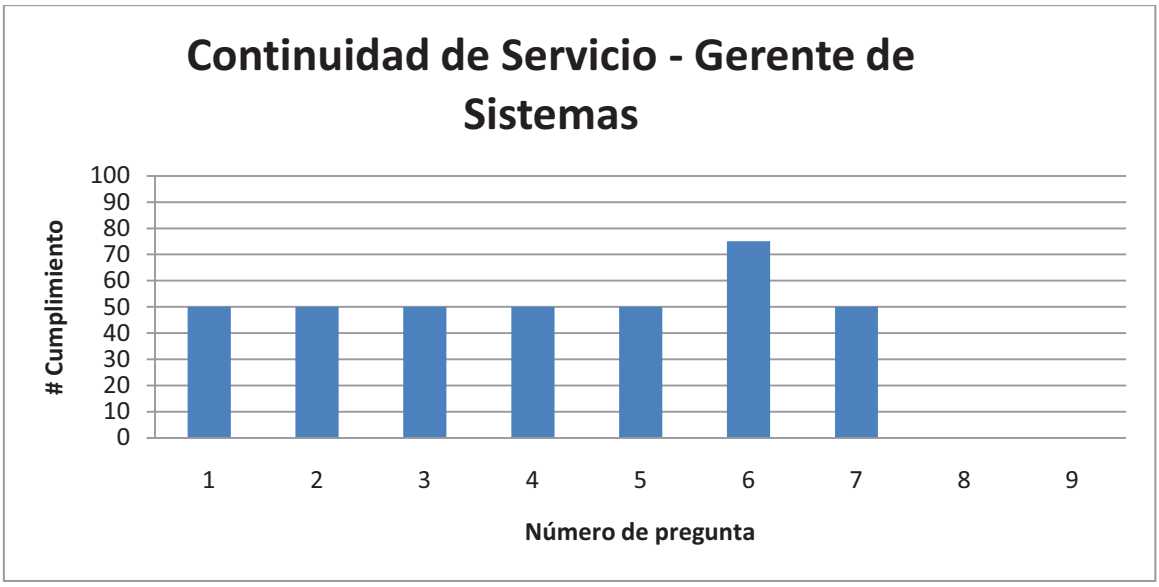

Figura 3-8: Gráfico de Cumplimiento - Gestión de Continuidad de Servicio para Gerente de Sistemas

3.2.2.3 Recomendaciones

La dirección de Sistemas debe preocuparse por realizar análisis de amenazas y vulnerabilidades para contrarrestar el posible impacto que pueden generar las amenazas en el aspecto tecnológico. El ítem 8 de la encuesta "Análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización" es de GC bajo, por esto se sugiere realizar un análisis de riesgos para identificar los puntos críticos en la empresa y a los que se les debe dar mayor atención. Actualmente no se está realizando ningún estudio de vulnerabilidades, con la excepción del presente Proyecto de Titulación.

Según a la pregunta 9 de la encuesta "Tiempo en solución de catástrofes", la empresa no está preparada para la solución de catástrofes de forma eficiente. Esto se corroboró en el inicio de los cortes de energía eléctrica, ya que debido a este inconveniente se perdió un día de trabajo. Las causas fueron que la planta eléctrica no estaba preparada para ponerse en funcionamiento ante una eventual emergencia, adicionalmente el UPS también tenía la vulnerabilidad que cuando se descarga completamente, al retorno de la energía este no se puede cargar y por ende no puede energizar a los equipos computacionales, a pesar de que ya retorne la energía. Estas debilidades se llegaron a conocer sólo cuando ocurrió el

problema. Durante la entrevista no se admitió haber pasado por este catástrofe, pero tiene que ser reconocido como un momento de emergencia que vivió la organización y como referente para tomar medidas de corrección que eviten pasar por eventos similares.

El ítem 1 de la encuesta “¿Conoce el equipo del DDS la existencia de planes de emergencia?” y el ítem 2 “Desarrollo formal de planes de respuesta ante una emergencia”, tienen un GC bajo, por esto se recomienda que los planes de emergencia deben ser desarrollados formalmente por la gerencia e indicados completamente a todo el equipo de Sistemas con su respectiva capacitación de puesta en marcha. Sólo así cumplirán el objetivo de dar continuidad a los servicios y no dificultar su levantamiento a la normalidad. Al presente su diseño formal y entrenamiento al DDS se lo ha hecho de forma parcial, los datos acerca de este último dato se lo obtuvo del ítem 7 de la encuesta “Entrenamiento del DDS para utilizar correctamente los planes de emergencia”.

Dado que en el numeral 3 “Desarrollo de un plan en caso de falla para equipos o sistemas” de la encuesta se reflejó un GC bajo, se recomienda que la gerencia deba incentivar el desarrollo de planes de contingencia para restablecer el funcionamiento de equipos y sistemas. Con esto el gerente y los operarios tendrán una idea clara de cómo proceder para cada equipo o sistema cuando este falle. Como complemento a este ítem se debe añadir el cómo proceder para regresar al estado anterior de funcionamiento para servicios, ya que durante la entrevista con la gerencia se afirma que sólo parcialmente se han desarrollado este tipo de planes, este tema se relaciona con el numeral 4 de la encuesta “Lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios”.

El numeral 5 “Evaluación de planes de respuesta ante emergencias o recuperación antes de ser puestos en marcha” de la encuesta, muestra que su GC es bajo, por esto se recomienda que los planes de emergencia deben ser siempre evaluados y simulados antes de ser puestos en marcha, el plan para el sistema de seguros ha sido evaluado parcialmente, esta política debe ser revisada

para que dicho plan sea revisado completamente antes de ser puesto en marcha. En este ítem es importante tomar en cuenta los procesos para el equipo Kypus y el servidor de antivirus Mcafee.

La falta de evaluación de estos procedimientos puede llevar a encontrarse con resultados no deseables que resulten en un tiempo extendido en que la compañía este fuera de servicio.

3.2.3 GESTIÓN DE CAMBIOS

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	¿Recurre a los últimos cambios realizados para solucionar incidentes?	50	**50**	**0,5**
2	¿Existe un análisis de riegos sobre las implicaciones que podrían producir un cambio propuesto?	0	**0**	**1**
3	¿Son tomados en cuenta los posibles incidentes que producirá la ejecución del cambio?	100	**100**	**0**
4	¿Generalmente los cambios son impulsados por realizar innovación y mejoramiento?	100	**100**	**0**
5	¿Generalmente los cambios son impulsados por realizar correcciones?	0	**0**	**1**
6	¿El manejo de cambios es independiente del manejo de configuraciones?	0	**0**	**1**
7	¿Para cada petición de cambio están claramente definidas las ventajas de realizar el cambio?	0	**0**	**1**
8	¿Cada cambio está coordinado con los departamentos que serán afectados?	100	**100**	**0**
9	¿La planificación de un cambio es pública y notificada al personal de la organización?	50	**50**	**0,5**
10	¿Existe un registro de todos los cambios realizados sobre un dispositivo específico?	0	**0**	**1**
11	¿Existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización?	0	**0**	**1**
12	¿Cada detalle del ciclo de vida del cambio es registrado?	0	**0**	**1**
13	¿Los registros del manejo de cambios son almacenados en el sistema de manejo de configuraciones?	0	**0**	**1**
14	¿Cada cambio pasa un filtro de condiciones predeterminadas antes de su aprobación?	50	**50**	**0,5**
15	¿Antes de la realización de un cambio se encuentran concretamente identificados los recursos necesarios?	50	**50**	**0,5**
16	¿Al finalizar el ciclo de un proceso de cambio realiza una evaluación del mismo?	50	**50**	**0,5**
17	¿Cambios estándar de rutina son registrados como un pedido de cambio?	50	**50**	**0,5**
18	¿Es registrado el responsable de la petición de cambio?	50	**50**	**0,5**
19	¿Se conoce con certeza la razón para realizar el cambio?	50	**50**	**0,5**
20	¿Existe recalificación de pedido de cambios en caso de ser negados en primera instancia?	0	**0**	**1**
21	¿Durante la planeación de un cambio se realiza un análisis financiero?	0	**0**	**1**
22	¿Realiza pruebas piloto antes de la implementación de un cambio?	50	**50**	**0,5**
23	¿Al finalizar la implementación de un cambio se comprueba cumplimiento de objetivos?	50	**50**	**0,5**

24	¿Al finalizar la implementación de un cambio se comprueba la satisfacción de los involucrados?	100	**100**	**0**
25	¿Al finalizar la implementación de un cambio se registran los eventos no planificados que tuvieron efectos negativos sobre la organización?	100	**100**	**0**
26	¿Al finalizar la implementación de un cambio se comprueba cumplimiento de costos?	0	**0**	**1**
27	¿Al finalizar la implementación de un cambio se comprueba cumplimiento de tiempos de ejecución?	50	**50**	**0,5**
28	¿El proceso de evaluación post implementación de cambios es documentado?	0	**0**	**1**
29	¿El encargado de la administración de problemas participa en la administración de cambios?	50	**50**	**0,5**
30	¿El encargado de la administración de incidentes participa en la administración de cambios?	50	**50**	**0,5**
31	Número de cambios solicitados registrados automáticamente.	0	**0**	**1**
32	Número de cambios realizados frente a los solicitados.	100	**100**	**0**
33	Número de cambios realizados con carácter de emergencia frente al total de realizados.	50	**50**	**0,5**
34	Número de cambios realizados sin éxito frente al total de realizados.	40	**40**	**0,6**
35	Identificación de mejoras en servicios gracias a la realización de cambios.	0	**0**	**1**
36	Método para registro de Cambios.	25	**25**	**0,75**
		#Cumpl. Promedio	**37,92**	

Tabla 3-17: Porcentaje de Cumplimiento - Gestión de Cambios para Gerente de Sistemas

3.2.3.1 Estados de Indicadores de Gestión de Cambios

La Tabla 3-18, indica que el 83,3 % de los indicadores para Gestión de Cambios tiene un GC Bajo, esto implica que: no existe un análisis de riegos sobre las implicaciones que podrían producir un cambio propuesto, los cambios son impulsados por realizar correcciones, el manejo de cambios es independiente del manejo de configuraciones, para cada petición de cambio no están claramente definidas las ventajas de realizar el cambio, no existe un registro de todos los cambios realizados sobre un dispositivo específico, no existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización, cada detalle del ciclo de vida del cambio no es registrado, Los registros del manejo de cambios no son almacenados en el sistema de manejo de configuraciones, no existe recalificación de pedido de cambios en caso de ser negados en primera instancia, durante la planeación de un cambio no se realiza un análisis financiero, al finalizar la implementación de un cambio no se comprueba cumplimiento de costos, el proceso de evaluación post implementación de cambios no es documentado, el número de cambios solicitados registrados automáticamente es bajo, no se identifica mejoras en servicios gracias a la realización de cambios, no se sigue un método para registro de Cambios, alto número de cambios realizados sin éxito frente al total de realizados, no recurre a los últimos cambios realizados para solucionar incidentes, la planificación de un cambio no es pública ni notificada al personal de la organización, cada cambio no pasa un filtro de condiciones predeterminadas antes de su aprobación, antes de la realización de un cambio se encuentran parcialmente identificados los recursos necesarios, al finalizar el ciclo de un proceso de cambio se realiza parcialmente una evaluación del mismo, los cambios estándar de rutina son parcialmente registrados como un pedido de cambio, es registrado el responsable de la petición de cambio parcialmente, se conoce parcialmente la razón para realizar cambios, se realiza parcialmente pruebas piloto antes de la implementación de un cambio, al finalizar la implementación de un cambio se comprueba parcialmente el cumplimiento de objetivos, al finalizar la implementación de un cambio se comprueba parcialmente el cumplimiento de tiempos de ejecución, el encargado de la administración de problemas tiende a no participar en la administración de cambios, el encargado de la administración de incidentes tiende a participar en la administración de

cambios, el número de cambios realizados con carácter de emergencia es alto frente al total de realizados.

El 16,7 restante tiene un GC Alto, es decir: son tomados en cuenta los posibles incidentes que producirá la ejecución de un cambio, generalmente los cambios son impulsados por realizar innovación y mejoramiento, cada cambio está coordinado con los departamentos que serán afectados, al finalizar la implementación de un cambio se comprueba la satisfacción de los involucrados, al finalizar la implementación de un cambio se registran los eventos no planificados que tuvieron efectos negativos sobre la organización, alto número de cambios realizados frente a los solicitados.

En promedio la Gestión de Cambios no es realizada de forma satisfactoria de parte de la gerencia de sistemas.

N.	#Cumplimiento	GC
2	0	B
5	0	B
6	0	B
7	0	B
10	0	B
11	0	B
12	0	B
13	0	B
20	0	B
21	0	B
26	0	B
28	0	B
31	0	B
35	0	B
36	25	B
34	40	B
1	50	B
9	50	B
14	50	B
15	50	B
16	50	B
17	50	B
18	50	B
19	50	B
22	50	B
23	50	B
27	50	B

29	50	B
30	50	B
33	50	B
3	100	A
4	100	A
8	100	A
24	100	A
25	100	A
32	100	A

Tabla 3-18: Grado de Confianza - Gestión de Cambios para Gerente de Sistemas

3.2.3.2 Gráfico de Cumplimiento de Gestión de Cambios

La Figura 3-9, dice que la mayoría de indicadores respecto a Gestión de Cambios, el Gerente de Sistemas tiene un cumplimento menor a 50. Pero con un manejo adecuado sobresale la correcta planificación, la búsqueda de mejorar, satisfacción de involucrados y respuesta a solicitudes de cambio.

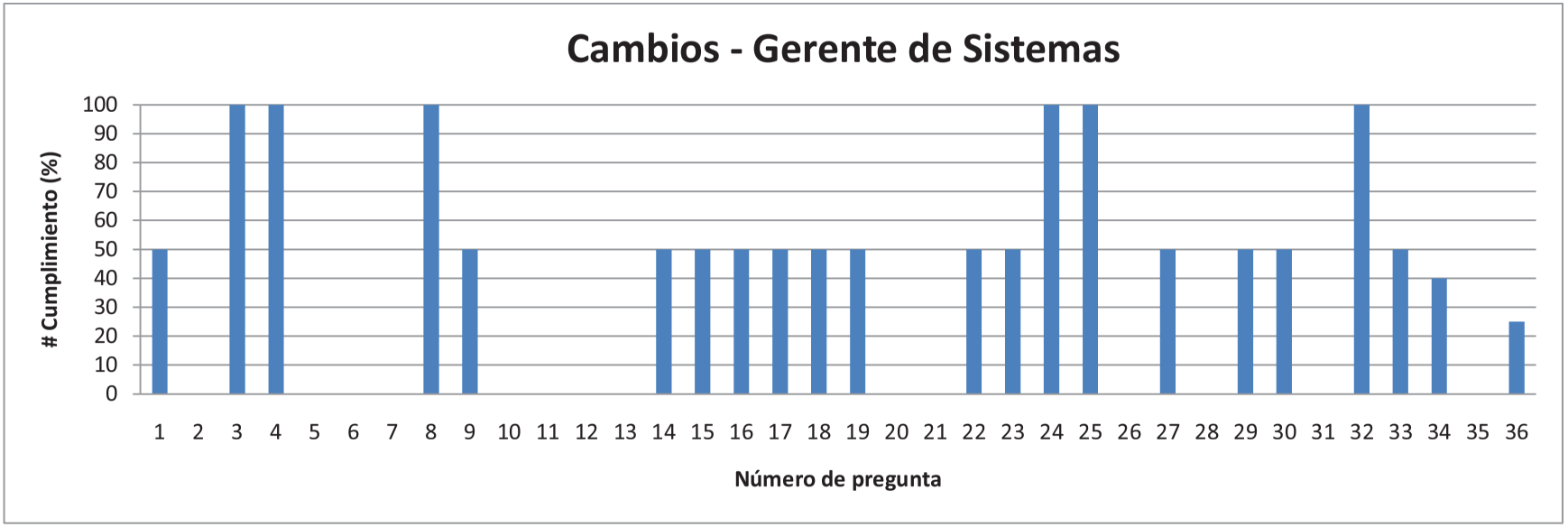

Figura 3-9: Gráfico de Cumplimiento - Gestión de Cambios para Gerente de Sistemas

3.2.3.3 Recomendaciones

Una buena práctica para solucionar incidentes es recurrir a los últimos cambios realizados. Pero según el ítem 1 de la encuesta "¿Recurre a los últimos cambios realizados para solucionar incidentes?", esta práctica se realiza en la empresa de forma parcial, principalmente porque según el numeral 10 de la encuesta "¿Existe un registro de todos los cambios realizados sobre un dispositivo específico?", no se registran los cambios realizados para un dispositivo o sistema específico, estos cambios se deben empezar a registrar en una base de datos, para mejorar el rendimiento de la resolución de incidentes. Si los cambios están claramente definidos, todo procedimiento sobre la tecnología de Alianza se ejecutará con mayor precisión.

Dado que el numeral 12 "¿Cada detalle del ciclo de vida del cambio es registrado?" de la encuesta tienen un GC bajo, se recomienda que la base de datos de cambios debe contener todo el ciclo de vida de un cambio.

Dado que el numeral 14 de la encuesta "¿Cada cambio pasa un filtro de condiciones predeterminadas antes de su aprobación?" tiene un GC bajo, se sugiere que cada cambio debe pasar por un filtro de condiciones antes de ser aprobado, este procedimiento se lo debe aplicar para todos sin excepción, no de forma parcial como se lo lleva actualmente. Dado que el ítem 7 de la encuesta "¿Para cada petición de cambio están claramente definidas las ventajas de realizar el cambio?" y el ítem 19 "¿Se conoce con certeza la razón para realizar el cambio?" tienen un GC bajo, se recomienda que dentro de su aprobación se debe tener claramente definido el objetivo que debe cumplir el cambio junto con las ventajas que se esperan. Actualmente según la Dirección de Sistemas en general, el objetivo se lo tiene parcialmente definido y las ventajas no se detallan.

Una vez aprobado, debido a que el ítem 2 "¿Existe un análisis de riegos sobre las implicaciones que podrían producir un cambio propuesto?" de la encuesta tuvo un GC bajo se recomienda analizar los riesgos que se pueden suscitar en caso de implementar un cambio. Con esto se podrá alertar y tomar las medidas necesarias con los departamentos y usuarios de la empresa que podrían ser afectados. En este proceso ayuda realizar simulaciones y pruebas piloto. Según el ítem 22 de la encuesta "¿Realiza pruebas piloto antes de la implementación de un cambio?" no

se realiza ningún análisis de riesgos para cambios pero las pruebas piloto se realizan al menos parcialmente.

Dado que el ítem 5 “¿Generalmente los cambios son impulsados por realizar correcciones?” de la encuesta presenta un GC bajo se recomienda que generalmente los cambios no se deben realizar impulsados por correcciones, por el contrario en deben ser para mejora de servicios. Si los cambios están sólo para solucionar fallas se debe realizar un estudio para disminuir al mínimo esta tendencia. El DDS tiene tendencia a realizar cambios por correcciones.

Dado que el ítem 6 de la encuesta “¿El manejo de cambios es independiente del manejo de configuraciones?” y el ítem 13 “¿Los registros del manejo de cambios son almacenados en el sistema de manejo de configuraciones?” tienen un GC bajo se recomienda que el manejo de cambios debe estar relacionado con el de configuraciones. La realización de un cambio implica tareas conocidas como configuraciones en el mundo de la tecnología. La Dirección de Sistemas las mantiene en una concepción diferente.
Dado que el numeral 11 “¿Existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización?” de la encuesta, tienen un GC bajo se recomienda que en base a la experiencia de la realización de cambios el DDS debe generar procesos modelos para afrontar cambios que se repiten o son comunes. Esta buena práctica ayuda a normalizar los procesos para que se realicen rápidamente y eficientemente. Actualmente no se tienen implementados procesos modelo para Gestión de Cambios en el Departamento de Tecnología de Alianza. Además estos modelos ayudarán a reducir el número de cambios fallidos, que se destacan en el numeral 34 de la encuesta “Número de cambios realizados sin éxito frente al total de realizados”.

Por lo que los numerales 21 de la encuesta “¿Durante la planeación de un cambio se realiza un análisis financiero?” y 15 “¿Antes de la realización de un cambio se encuentran concretamente identificados los recursos necesarios?” tienen un GC bajo, se recomienda que para la implementación de un cambio se deben identificar concretamente los recursos necesarios y su análisis financiero, esto

ayuda a que el proceso no se paralice por falta de materiales, personal o recurso financiero. Según la información obtenida del Gerente de Sistemas, el análisis financiero no se lo está realizando pero el de recursos se lo hace parcialmente.

La Dirección de Sistemas realiza parcialmente la evaluación de un cambio cuando este ha sido finalizado, dado que el ítem 16 "¿Al finalizar el ciclo de un proceso de cambio realiza una evaluación del mismo?" tiene un GC bajo, se sugiere que la revisión sea completa y se verifiquen el cumplimiento de objetivos (ítem 23 "¿Al finalizar la implementación de un cambio se comprueba cumplimiento de objetivos?"), costos (ítem 26 "¿Al finalizar la implementación de un cambio se comprueba cumplimiento de costos?") y tiempos de ejecución (ítem 27 "¿Al finalizar la implementación de un cambio se comprueba cumplimiento de objetivos?"), los mismos que no se están realizando correctamente al presente en el DDS. Es importante indicar que toda esta evaluación debe ser totalmente documentada, ya que actualmente según el ítem 28 "¿El proceso de evaluación post implementación de cambios es documentado?", no se lo realiza. Esto además ayudará a mejorar el indicador representado por la pregunta 35 de la encuesta "Identificación de mejoras en servicios gracias a la realización de cambios".

Dado que el ítem 17 de la encuesta "¿Cambios estándar de rutina son registrados como un pedido de cambio?" tiene un GC bajo, es aconsejable tomar en cuenta que los cambios estándar de rutina no se deben registrar como cambios propiamente dichos, estos se los debe catalogar como actividades dentro del manejo de incidentes. Actualmente este reconocimiento se lo está realizando de forma parcial.

Con el fin de automatizar los pedidos de cambio de los usuarios, se debe implementar un sistema que recoja estas demandas de forma automática, actualmente este servicio no se encuentra implementado, esta información es producto del numeral 31 "Número de cambios solicitados registrados automáticamente" de la encuesta.

Dado que el ítem 20 “¿Existe recalificación de pedido de cambios en caso de ser negados en primera instancia?” de la encuesta tiene un GC bajo, se recomienda que los cambios deben tener una segunda oportunidad de calificación en caso de ser negados en primera instancia. Con una reformulación puede ser que los cambios le sean útiles a la organización, actualmente se mantienen negadas cualquier tipo de recalificación.

Los resultados de la entrevista al Gerente de Sistemas indican que el personal que maneja problemas e incidentes también participa en el manejo de cambios, lo que implica una calificación del 50%, según el ítem 29 de la encuesta “¿El encargado de la administración de problemas participa en la administración de cambios?” y el ítem 30 “¿El encargado de la administración de incidentes participa en la administración de cambios?”. La guía ITIL, sugiere que el manejo de problemas y cambios si deberían estar relacionados pero el manejo de incidentes y cambios no lo deberían. Tomando en cuenta el personal de dos operarios en Quito, un operario en Guayaquil y un Gerente, para dar soporte a las 7 sucursales a nivel nacional es válida la compartición de responsabilidades, siempre y cuando se mantengan las diferencias entre las actividades de gestión de incidentes y problemas.

De los 10 cambios que se registraron en el mes (referencia de entrevista), el 50% se realizaron con carácter de emergencia, según el ítem 33 de la encuesta “Número de cambios realizados con carácter de emergencia frente al total de realizados.” Si bien es una respuesta parcial, esta debe reducirse, si los cambios urgentes persisten y tienden a crecer significa que se están cometiendo más errores que mejoras para la organización. Se debe tratar de reducir este indicador para que la tendencia de cambios realizados sea para generar adelantos en la organización.

El numeral 36 de la encuesta “Método para registro de Cambios” tiene un GC bajo, por esto se recomienda que el correcto registro de cambios comprenda: registrar cada petición de cambio con un identificador único, añadir fecha de proceso, colocar tipo de categoría y prioridad, además se debe señalar el responsable de la petición de cambio.

En la empresa el responsable de la petición es parcialmente conocido según el numeral 18 de la encuesta “¿Es registrado el responsable de la petición de cambio?”, los demás parámetros tienen un cumplimiento del 25%. Se debe mejorar este parámetro para que los futuros informes y análisis tengan elementos claros para su elaboración.

La planificación de un cambio es parcialmente divulgada a los involucrados, según la pregunta 9 de la encuesta “¿La planificación de un cambio es pública y notificada al personal de la organización?”, se debe procurar informar a todos los afectados para no generar molestias en su trabajo.

3.2.4 Gestión de Configuraciones

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	¿Posee una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización?	0	0	1
2	¿El encargado del manejo de configuraciones se asegura que han sido apropiadamente registrados los cambios?	100	100	0
3	¿Tiene un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía?	100	100	0
4	¿Tiene documentado cada equipo configurable con sus características propias?	0	0	1
5	¿Tiene levantado los procesos para recuperación de desastres de cada equipo configurable?	0	0	1
6	¿Se ha calculado el nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable?	0	0	1
7	¿Tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico?	0	0	1
8	¿Tiene a cada equipo configurable registrado con su estado actual?	0	0	1
9	¿El registro de cada equipo configurable posee atributos que lo relacionen con manejo de cambios, problemas e incidentes?	0	0	1
10	¿El desarrollo de software de la organización toma en cuenta los datos del manejo de configuraciones?	0	0	1
11	¿El manejo de configuraciones se encuentra relacionado con el manejo de cambios?	0	0	1
12	¿Al cierre de una configuración se documentan los detalles de verificación?	0	0	1
13	¿Cada configuración registrada posee un responsable o ejecutor?	0	0	1
14	¿Realiza una planificación previa a la implementación de una configuración?	0	0	1
15	¿Al finalizar la configuración de un ítem se controla su correcto funcionamiento?	0	0	1
16	¿Cada configuración está sujeta a una evaluación antes de su registro?	0	0	1
17	¿Cada configuración registrada posee concretamente identificado(s) su(s) ítem(s) configurable(s)?	0	0	1
18	¿Cada ítem configurable tiene registrada su versión?	0	0	1
19	Número de configuraciones realizadas frente a las solicitadas.	0	0	1
20	Método de registro de Configuraciones.	0	0	1
21	Número de configuraciones realizadas sin éxito frente al total de realizadas.	x	x	x
22	Número de configuraciones realizadas sin autorización.	x	x	x
23	Número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.	x	x	x

24	Identificación de servicios que han tenido mejora gracias a configuraciones en la organización.	x	x	x
		#Cumpl. Promedio	**10**	

Tabla 3-19: Porcentaje de Cumplimiento - Gestión de Configuraciones para Gerente de Sistemas

3.2.4.1 Estados de Indicadores de Gestión de Configuraciones

La Tabla 3-20, indica que la Gerencia de Sistemas respecto a Manejo de Configuraciones, tiene el 75 % de indicadores con GC Bajo, esto implica que: no posee la gerencia del DDS una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización, no se tiene documentado cada equipo configurable con sus características propias, no se tiene levantado los procesos para recuperación de desastres de cada equipo configurable, no se ha calculado el nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable, no se tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico, no se tiene a cada equipo configurable registrado con su estado actual, el registro de cada equipo configurable no posee atributos que lo relacionen con manejo de cambios, problemas e incidentes, el desarrollo de software de la organización no toma en cuenta los datos del manejo de configuraciones, el manejo de configuraciones no se encuentra relacionado con el manejo de cambios, al cierre de una configuración no se documentan los detalles de verificación, cada configuración registrada no posee un responsable o ejecutor, no se realiza una planificación previa a la implementación de una configuración, al finalizar la configuración de un ítem no se controla su correcto funcionamiento, cada configuración no está sujeta a una evaluación antes de su registro, cada configuración registrada no posee concretamente identificado(s) su(s) ítem(s) configurable(s), cada ítem configurable no tiene registrada su versión, bajo número de configuraciones realizadas frente a las solicitadas, no existe un método establecido de registro de Configuraciones.

El 8,3 % tiene un GC Alto, esto significa que: el encargado de registrar los cambios se preocupa por registrar si existe algún tipo de cambio y la empresa posee un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía. El 16,7 de las preguntas de la encuesta no pudieron ser evaluados, por no existir referencia.

En promedio la Gestión de Configuraciones es realizada de forma no satisfactoria según la encuesta a la gerencia de sistemas.

N.	#Cumplimiento	GC
1	0	B
4	0	B
5	0	B
6	0	B
7	0	B
8	0	B
9	0	B
10	0	B
11	0	B
12	0	B
13	0	B
14	0	B
15	0	B
16	0	B
17	0	B
18	0	B
19	0	B
20	0	B
2	100	A
3	100	A
21	X	N/A[39]
22	X	N/A
23	X	N/A
24	X	N/A

Tabla 3-20: Grado de Confianza - Gestión de Configuraciones para Gerente de Sistemas

3.2.4.2 Gráfico de Cumplimiento de Gestión de Configuraciones

La Figura 3-10, indica que respecto a Configuraciones tomando en cuenta a la Gerencia de Sistemas sólo sobresale como correcto el registro de Configuraciones de parte del encargado y el contar con un mapa que muestra los elementos de comunicaciones de la empresa, el resto tienen un cumplimento de cero absoluto.

[39] N/A indica que No Aplica ningún GC debido a que no existe número de cumplimiento.

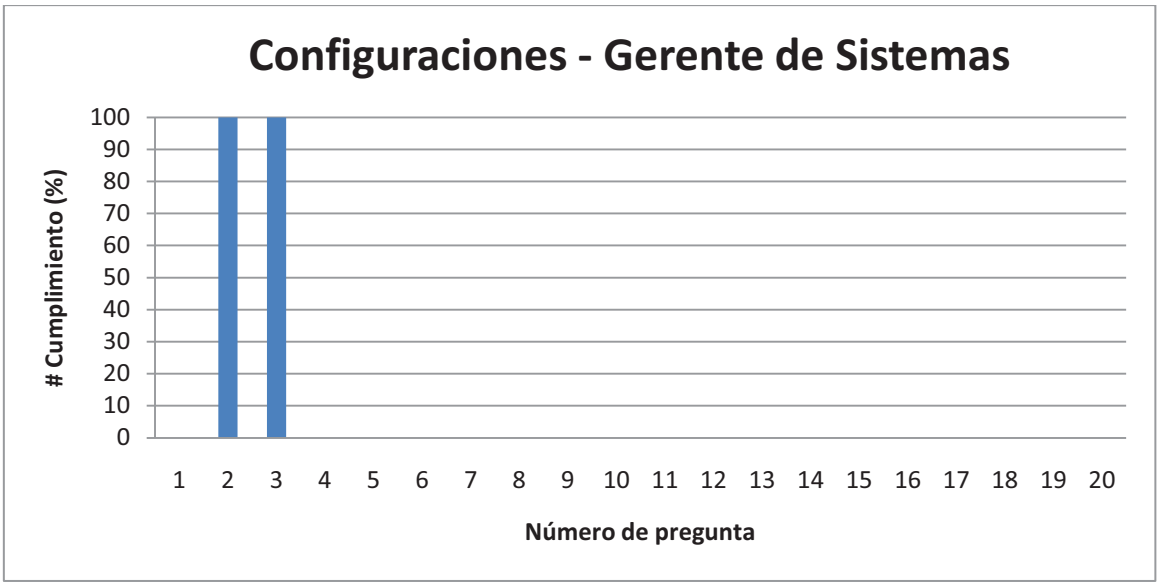

Figura 3-10: Gráfico de Cumplimiento - Gestión de Configuraciones para Gerente de Sistemas

3.2.4.3 Recomendaciones

Dado que los ítems 1 de la encuesta "¿Posee una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización?" y 4 "¿Tiene documentado cada equipo configurable con sus características propias?", tienen un GC bajo se debe contar con una bitácora actualizada de la información de infraestructura tecnológica de Alianza, donde para cada ítem se detallen sus características propias, como: estado actual (ítem 8 "¿Tiene a cada equipo configurable registrado con su estado actual?"), versión (ítem 18 "¿Cada ítem configurable tiene registrada su versión?"), código único. Esta información facilitará la administración y solución de problemas. Actualmente la Gerencia de Sistemas afirma que no poseen una bitácora con estas características.

Como el numeral 5 de la encuesta "¿Tiene levantado los procesos para recuperación de desastres de cada equipo configurable?" tiene un GC bajo se recomienda que para cada equipo configurable se debería poseer un documento formal del proceso a seguir en caso de falla, esto agilitaría la reparación de los mismos bajo un mismo estándar. Este documento en el DDS no existe.

Dado que el ítem 6 de la encuesta "¿Se ha calculado el nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable?", tiene un GC bajo,

se recomienda que cada equipo configurable tiene su función dentro del negocio de la empresa, en caso de falla el proceso que soporta quedará paralizado. Se debe calcular el nivel de perjuicio que puede causar la falta de un equipo, así se tomarán medidas de contingencia adecuadas para el tipo de vulnerabilidad que se presente. Este análisis no se encuentra desarrollado por el Departamento de Tecnología actualmente.

Debido a que el numeral 7 de la encuesta "¿Tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico?" tiene un GC bajo, se recomienda que las configuraciones durante todo el ciclo de vida de los equipos deben ser de total acceso para el personal técnico autorizado. La Gerencia de Sistemas afirma que no tiene acceso a este nivel de las configuraciones de los equipos, esto significa que el conocimiento no se ha sociabilizado completamente en el área y será un factor de desventaja al momento de solucionar problemas.

El ítem 9 de la encuesta "¿El registro de cada equipo configurable posee atributos que lo relacionen con manejo de cambios, problemas e incidentes?" tiene un GC bajo, por esto se recomienda que cuando se registra la configuración de un equipo este debe tener relación con el cambio que la generó, así como con los problemas e incidentes que pueden ser generados. El tener presente esta información ayuda a prevenir sucesos no deseables para la organización o tomar las medidas preventivas necesarias. Al presente la Dirección de Sistemas no conoce las relaciones que puede haber con cambios, problemas e incidentes. Estas recomendaciones además se aplican para el ítem de la encuesta "¿El manejo de configuraciones se encuentra relacionado con el manejo de cambios?".

El desarrollo de software es la principal actividad que realiza la Gerencia de Sistemas con la colaboración de dos miembros del departamento, lamentablemente no se toma en cuenta de forma detallada la configuración que tienen los equipos que van a utilizar los programas desarrollados, según el numeral 10 de la encuesta "¿El desarrollo de software de la organización toma en cuenta los datos del manejo de configuraciones?". La configuración actual de los equipos es crítica para la compatibilidad con los programas desarrollados, por

esto se sugiere que dichas características sean tomadas en cuenta de parte del personal de desarrollo.
La configuración de equipos de tecnología en ocasiones se realizada sin un orden establecido, cuando el personal se dice experto, la Dirección de Sistemas manifiesta que de esta manera se desarrolla esta actividad, según el ítem 14 de la encuesta "¿Realiza una planificación previa a la implementación de una configuración?", pero la recomendación dice lo contrario. Toda configuración debe ser planificada antes de ser implementada, de la misma forma se deben tener establecidos controles de correcto funcionamiento al finalizar la tarea.

Dado que el ítem 16 de la encuesta "¿Cada configuración está sujeta a una evaluación antes de su registro?" tiene un GC bajo, se recomienda que antes de ser una configuración aceptada para su implementación, debe pasar una evaluación de cumplimiento de objetivos, incluyendo la identificación concreta de los ítems configurables (ítem 17 "¿Cada configuración registrada posee concretamente identificado(s) su(s) ítem(s) configurable(s)?") que tendrán participación, este proceso no se realiza formalmente según la Gerencia de Sistemas, así mismo se debe seguir un método específico de registro de configuraciones (ítem 20 "Método de registro de Configuraciones").

Dado que el numeral 19 de la encuesta "Número de configuraciones realizadas frente a las solicitadas" tienen un GC bajo, se recomienda que las peticiones de configuración y las implementadas deben ser registradas para poder realizar su comparación, sin este dato no se tiene referencia para implementar correcciones o saber si el trabajo está bien realizado (ítem 15 "¿Al finalizar la configuración de un ítem se controla su correcto funcionamiento?"). Actualmente esta información no está disponible en el DDS.

Dado que el ítem 13 de la encuesta "¿Cada configuración registrada posee un responsable o ejecutor?" tiene un GC bajo, para el registro de configuraciones se sugiere al DDS que se registre al responsable o ejecutor de la configuración así como los detalles de verificación de funcionamiento luego de la implementación, que hasta el presente no se lo han estado realizando, según el ítem 12 de la

encuesta “¿Al cierre de una configuración se documentan los detalles de verificación?”. El responsable con sus detalles de verificación son importantes conocerlos para agilitar la solución en caso de falla.

3.2.5 GESTIÓN DE INCIDENTES

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	Toma en cuenta personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos?	50	**50**	**0,5**
2	¿Utiliza un escalamiento de solución para resolver incidentes de usuario?	50	**50**	**0,5**
3	¿Conoce el estado actual de incidentes abiertos?	50	**50**	**0,5**
4	¿Está informado del número de incidentes que se encuentran abiertos?	100	**100**	**0**
5	¿Conoce quién es el responsable de la solución de un incidente abierto?	100	**100**	**0**
6	¿Conoce quienes son los usuarios que mantienen incidentes sin resolver?	100	**100**	**0**
7	¿Conoce cuál es el tiempo de respuesta y solución para un incidente específico?	100	**100**	**0**
8	¿Puede acceder a la bitácora de cambios que se relacionan con un incidente específico?	0	**0**	**1**
9	¿Se provee un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó?	100	**100**	**0**
10	¿Es informado el usuario sobre el escalamiento de su incidente?	0	**0**	**1**
11	¿Es informado el usuario sobre el cierre del incidente?	50	**50**	**0,5**
12	¿Están los incidentes agrupados por su naturaleza?	0	**0**	**1**
13	¿Están los incidentes agrupados por su solución tipo?	0	**0**	**1**
14	¿Resuelve los incidentes tomando en cuenta el banco de soluciones?	50	**50**	**0,5**
15	¿Posee respaldos de la configuración del sistema y equipos para realizar una restauración al estado anterior de los mismos?	50	**50**	**0,5**
16	¿Posee un servicio de escritorio que se encargue de los detalles del cierre de incidentes?	50	**50**	**0,5**
17	¿Se registran los niveles de satisfacción del usuario luego del cierre de un incidente?	0	**0**	**1**
18	¿Es registrado el técnico que cierra el incidente?	0	**0**	**1**
19	¿Posee la empresa un lineamiento específico para que los usuarios realicen un pedido de servicio?	100	**100**	**0**
20	¿Tiene identificados los incidentes críticos para su empresa?	50	**50**	**0,5**
21	¿Cada incidente crítico posee su propio proceso de manejo?	50	**50**	**0,5**
22	¿Cada incidente abierto tiene registrado el nombre del técnico que lo recibió?	0	**0**	**1**
23	Tiempo en resolver incidentes.	100	**100**	**0**

24	Frecuencia en la realización de actualizaciones de software.	100	**100**	**0**
25	Frecuencia en la realización de actualizaciones de hardware.	100	**100**	**0**
26	Incidentes que se han resuelto en el tiempo esperado.	50	**50**	**0,5**
27	Porcentaje de incidentes que han sido reabiertos del total en un periodo específico.	95	**95**	**0,05**
28	Porcentaje de incidentes resueltos sin la necesidad de una visita.	90	**90**	**0,1**
29	Método para registro de Incidentes.	30	**30**	**0,7**
		%Cumpl Promedio	**55,69**	

Tabla 3-21: Porcentaje de Cumplimiento - Gestión de Incidentes para Gerente de Sistemas

3.2.5.1 Estados de Indicadores de Gestión de Incidentes

La Tabla 3-22, presenta que de los indicadores de Gestión de Incidentes según la Gerencia de Sistemas, el 62 % posee un GC Bajo, esto significa que: no se puede acceder a la bitácora de cambios que se relacionan con un incidente específico, no es informado el usuario sobre el escalamiento de su incidente, no están los incidentes agrupados por su naturaleza, no están los incidentes agrupados por su solución tipo, no se registran los niveles de satisfacción del usuario luego del cierre de un incidente, no es registrado el técnico que cierra el incidente, cada incidente abierto no tiene registrado el nombre del técnico que lo recibió, no se aplica un método para registro de Incidentes, no se toma en cuenta personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos, no utiliza un escalamiento de solución para resolver incidentes de usuario, no se conoce el estado actual de incidentes abiertos, el usuario no es informado sobre el cierre de su incidente, no se resuelven los incidentes tomando en cuenta el banco de soluciones, no poseen respaldos de la configuración del sistema y equipos para realizar una restauración al estado anterior de los mismos, no poseen un servicio de escritorio que se encargue de los detalles del cierre de incidentes, no se tienen identificados los incidentes críticos para su empresa, los incidentes críticos no poseen su propio proceso de manejo, los incidentes se han resuelto en el tiempo esperado de forma parcial.

El 38% tiene un GC Alto, esto implica que: bajo porcentaje de incidentes que han sido reabiertos del total en un periodo específico, alto porcentaje de incidentes resueltos sin la necesidad de una visita, la gerencia de sistemas está informada del número de incidentes que se encuentran abiertos, conocimiento de quién es el responsable de la solución de un incidente abierto, se conoce quienes son los usuarios que mantienen incidentes sin resolver, así como el tiempo de respuesta y solución para un incidente específico, se provee un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó, la empresa posee un lineamiento específico para que los usuarios realicen un pedido de servicio, el tiempo en resolver incidentes es menor a 30 minutos, la frecuencia en la realización de actualizaciones de software es menor a 1 año y la frecuencia en la realización de actualizaciones de hardware es menor a dos años.

N.	#Cumplimiento	GC
8	0	B
10	0	B
12	0	B
13	0	B
17	0	B
18	0	B
22	0	B
29	30	B
1	50	B
2	50	B
3	50	B
11	50	B
14	50	B
15	50	B
16	50	B
20	50	B
21	50	B
26	50	B
27	95	A
28	90	A
4	100	A
5	100	A
6	100	A
7	100	A
9	100	A

19	100	A
23	100	A
24	100	A
25	100	A

Tabla 3-22: Grado de Confianza - Gestión de Incidentes para Gerente de Sistemas

3.2.5.2 Gráfico de Cumplimiento de Gestión de Incidentes

La Figura 3-11, muestra que la Gerencia de Sistemas respecto a Gestión de Incidentes tiene falencias de: no existencia de una bitácora de cambios con relación a incidentes que producen y falta de registro de parámetros como escalamiento, origen, técnico responsable, satisfacción del usuario, etc. De los indicadores con alto cumplimiento resalta que la Gerencia trata de solucionar lo más rápido posible un incidente.

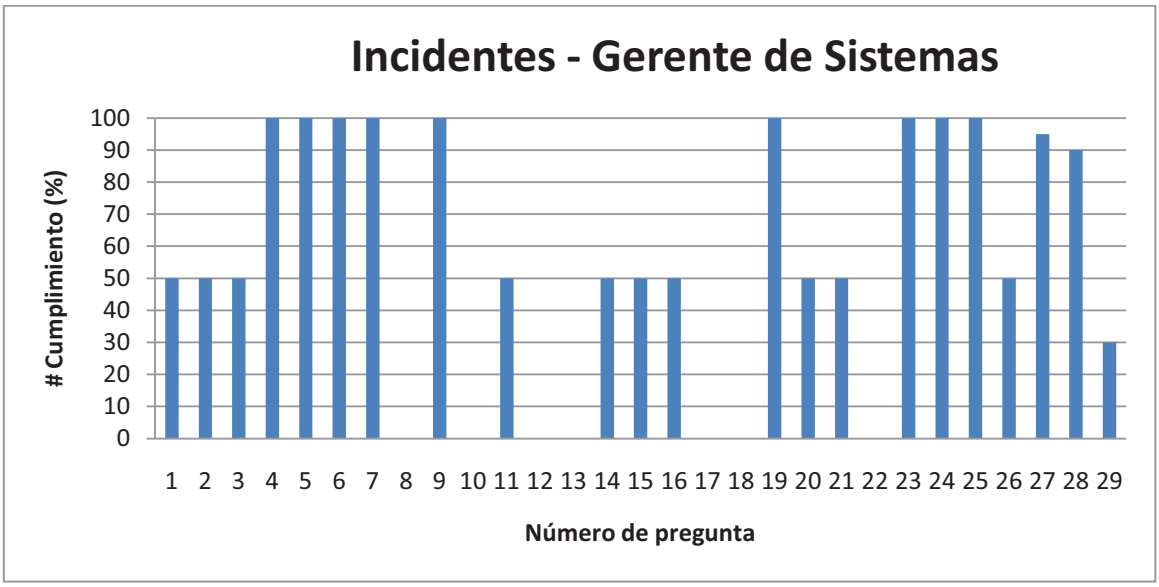

Figura 3-11: Gráfico de Cumplimiento - Gestión de Incidentes para Gerente de Sistemas

3.2.5.3 Recomendaciones

Cuando se implementan proyectos que no son cotidianos en la empresa, se debe tener en cuenta el personal técnico que de soporte a los usuarios. En Alianza se lo realiza parcialmente, según el ítem 1 de la encuesta “Toma en cuenta personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos?” pero se recomienda que exista una planificación completa para prevenir que los proyectos se retrasen por dar solución a problemas de los usuarios, o que estos paralicen su trabajo por incidentes con la tecnología que no pueden ser asumidos por no existir técnicos disponibles. Cuando la gerencia no piensa en este tipo de

inconveniente, los técnicos se encontrarán presionados por dos sectores, que ocasionarán que no se realicen bien ninguna de las dos actividades.

Los incidentes tienen varios niveles de complejidad, de acuerdo a esto se requieren técnicos de diferente experiencia para resolverlos, de ahí que si un incidente no puede ser resuelto en primera instancia este debe escalar hacia otra persona y así sucesivamente hasta por último si es requerido a los proveedores o fabricantes del producto. La Gerencia de Sistemas lo realiza al presente de forma parcial, según el numeral 2 de la encuesta "¿Utiliza un escalamiento de solución para resolver incidentes de usuario?". Además a medida que el incidente va escalando, esto debe ser informado al usuario. Al momento los usuarios no son informados de ninguna actividad de escalamiento de incidentes, como se lo obtuvo de la pregunta 10 de la encuesta "¿Es informado el usuario sobre el escalamiento de su incidente?".

La Dirección de Sistemas actualmente conoce sólo de forma parcial el estado actual de los incidentes que se encuentran abiertos o sin resolver, según el numeral 3 de la encuesta "¿Conoce el estado actual de incidentes abiertos?", debido a que ninguno se encuentra registrado. A nivel gerencial no se conoce su totalidad, ya que esto sólo lo conoce el técnico que los está atendiendo. Se sugiere que todo técnico registre los incidentes a su cargo, para que la gerencia tenga una visión global y reconozca falencias y fortalezas del actual manejo de incidentes.

La Gerencia de Sistemas debe tomar como política el informar a los usuarios cuando un incidente ha sido categorizado como cerrado. En Alianza se lo está realizando parcialmente, según el ítem 11 de la encuesta "¿Es informado el usuario sobre el cierre del incidente?", pero es necesario comprobar la completa conformidad del usuario con el estado de cerrado para su incidente.
Además al aceptar el usuario como cerrado a su incidente, debe registrar su nivel de satisfacción al respecto del servicio recibido. Al presente la Gerencia de Sistemas no ha establecido un método para recibir este grado de satisfacción,

esto se obtuvo del numeral 17 de la encuesta “¿Se registran los niveles de satisfacción del usuario luego del cierre de un incidente?”.
Todas estas actividades están dentro de los detalles de cierre que la política de servicio de escritorio debe establecer, la cual está sólo desarrollada parcialmente según el ítem 16 de la encuesta “¿Posee un servicio de escritorio que se encargue de los detalles del cierre de incidentes?”.

Dado que el numeral 12 de la encuesta “¿Están los incidentes agrupados por su naturaleza?” se recomienda que los incidentes deberían estar organizados por su naturaleza u origen de causa, esto ayuda a encontrar una solución tipo para eventos que se repitan en la organización (ítem 13 “¿Están los incidentes agrupados por su solución tipo?”), luego estas serán ingresadas a un banco de soluciones que permitirá reducir el tiempo necesario para dar solución a un incidente. La Gerencia de Sistemas no agrupa a los incidentes de esta manera pero usa un banco de soluciones parcialmente, según el numeral 14 de la encuesta “¿Resuelve los incidentes tomando en cuenta el banco de soluciones?”.

Se recomienda realizar un análisis de incidentes críticos para la empresa, esto ayuda a estar prevenido en caso de que ocurran eventos que puedan causar un gran daño a la organización al nivel de paralizar uno o varios servicios que se apoyen en la tecnología. Una vez identificados los incidentes críticos se deben establecer procesos propios para su correcto tratamiento.
La Dirección de Sistemas con respecto a la identificación y proceso de incidentes sólo lo ha realizado de forma parcial, según los numerales 20 de la encuesta “¿Tiene identificados los incidentes críticos para su empresa?”, y 21 “¿Cada incidente crítico posee su propio proceso de manejo?” respectivamente.

Según datos de la entrevista al Gerente de Sistemas, sólo el 50% de los incidentes resueltos se los ha cumplido en el tiempo esperado, el resto se han extendido y han provocado mayores inconvenientes, esto según el numeral 26 de la encuesta “Incidentes que se han resuelto en el tiempo esperado”. En gerencia se deben identificar los incidentes que se comportaron de esta manera y realizar los correctivos necesarios para disminuir el tiempo de solución.

Dado que el numeral 29 de la encuesta “Método para registro de Incidentes” tiene un GC bajo, se recomienda considerar que el éxito de la Gestión de Incidentes depende del correcto registro de sus características, de acuerdo a la entrevista a la Gerencia de Sistemas se identificaron falencias en los siguientes ítems: identificación única de cada incidente, fecha y hora de inicio de procesamiento, fecha y hora de cierre, identificación de servicio afectado, recalificación de categoría de incidente una vez que ha sido cerrado, estado actual de un incidente, técnico que abre (ítem 22 de la encuesta “¿Cada incidente abierto tiene registrado el nombre del técnico que lo recibió?”) y cierra un incidente (ítem 18 de la encuesta “¿Es registrado el técnico que cierra el incidente?”) y finalmente registro de detalles en general de un incidente. Estas características actualmente no se registran en lo absoluto según la Gerencia de Sistemas, por esto es recomendable que se empiecen a tomar en cuenta estos detalles en el registro de incidentes. Esta medida ayudará a mejorar el análisis de Gestión de Incidentes.

3.2.6 GESTIÓN DE PROBLEMAS

N.	PREGUNTAS	Pablo Herrera	#Cumplimiento	Prob. de Amenaza
1	Diferenciación de problemas e incidentes	50	**50**	**0,5**
2	¿Es tomada como base la administración de problemas para la resolución de incidentes?	0	**0**	**1**
3	Orden de resolución de problemas e incidentes en su organización.	0	**0**	**1**
4	¿Usa como apoyo a la continuidad del servicio el manejo de problemas?	100	**100**	**0**
5	¿Existen reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades?	0	**0**	**1**
6	¿Posee un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT?	0	**0**	**1**
7	¿La infraestructura de comunicaciones obtiene el tiempo de su reloj interno directamente de un servidor NTP de la compañía?	100	**100**	**0**
8	¿Tiene concretamente identificadas las entradas para el proceso de resolución de problemas?	0	**0**	**1**
9	¿Se registran las salidas del proceso de resolución de problemas?	0	**0**	**1**
10	¿Se apoya la resolución de problemas en la base de datos de administración de problemas?	0	**0**	**1**
11	¿Es posible verificar los problemas cerrados en un periodo de tiempo específico?	0	**0**	**1**
12	¿El estado de un problema es concretamente conocido?	100	**100**	**0**
13	¿El encargado de la administración de problemas es el mismo que de la de cambios?	100	**100**	**0**
14	¿El encargado de la administración de problemas es el mismo que de la de incidentes?	50	**50**	**0,5**
15	¿Existe personal designado para investigación especializada de problemas?	0	**0**	**1**
16	¿Es registrada la o las acciones intuitivas que han mitigado un problema?	0	**0**	**1**
17	Cuando ejecuta una acción intuitiva que atenúa el problema, ¿el registro del problema es cerrado?	50	**50**	**0,5**
18	Al finalizar el diagnóstico de un problema ¿es registrado en la base de datos de errores conocidos?	50	**50**	**0,5**
19	¿Soluciona problemas apoyándose en la base de datos de errores conocidos?	0	**0**	**1**
20	Luego del suceso de un error crítico, ¿son revisadas las tareas que se realizaron correctamente?	50	**50**	**0,5**
21	Luego del suceso de un error crítico, ¿son revisados los procedimientos erróneos?	50	**50**	**0,5**
22	Luego del suceso de un error crítico, ¿es revisado que se puede mejorar en el futuro?	50	**50**	**0,5**
23	Luego del suceso de un error crítico, ¿es examinado qué se puede hacer para que no suceda otra vez?	50	**50**	**0,5**

24	Luego del suceso de un error crítico, ¿se analiza si la responsabilidad del hecho era de una empresa proveedora de servicios?	50	**50**	**0,5**
25	En caso de que un problema crítico sea responsabilidad de una empresa proveedora, se buscan las acciones necesarias inmediatamente?	100	**100**	**0**
26	¿Registra datos de retroalimentación respecto a problemas críticos?	0	**0**	**1**
27	Método para registro de problemas.	25	**25**	**0,75**
28	Número de problemas resueltos frente a los registrados.	85	**85**	**0,15**
29	Porcentaje de problemas que se han resuelto en el tiempo esperado.	11,76	**11,76**	**0,88**
30	Tendencia a que se incrementen los problemas críticos.	100	**100**	**0**
		%Cumpl Promedio	**39,06**	

Tabla 3-23: Porcentaje de Cumplimiento - Gestión de Problemas para Gerente de Sistemas

3.2.6.1 Estados de Indicadores de Gestión de Problemas

La Tabla 3-24, muestra que el 73,3 % de los indicadores para Gestión de Problemas tienen un GC Bajo, lo que implica que: no es tomada como base la administración de problemas para la resolución de incidentes, no hay prioridad de resolución de problemas e incidentes en la empresa, no existen reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades, no posee un servidor de Logs centralizado para registro de la actividad de la infraestructura de TI, no tiene concretamente identificados los elementos necesarios para iniciar el proceso de resolución de problemas, no se registran las conclusiones del proceso de resolución de problemas, no se apoya la resolución de problemas en la base de datos de administración de problemas, no es posible verificar los problemas cerrados en un periodo de tiempo específico, no existe personal designado para investigación especializada de problemas, no es registrada la o las acciones intuitivas que han mitigado un problema, no soluciona problemas apoyándose en la base de datos de errores conocidos, no se registran los datos de retroalimentación respecto a problemas críticos, bajo porcentaje de problemas que se resuelven en el tiempo esperado, no se posee un método para registro de problemas, la diferenciación de problemas e incidentes se da parcialmente, parcialmente el encargado de la administración de problemas es el mismo que de la de incidentes, cuando se ejecuta una acción intuitiva que atenúa el problema en ciertas ocasiones se registra el problema como cerrado, al finalizar el diagnóstico de un problema sólo se registra parcialmente en la base de datos de errores conocidos, luego del suceso de un error crítico se revisan parcialmente las tareas que se realizaron correctamente, los procedimientos erróneos, lo que se puede mejorar en el futuro, las acciones que se pueden realizar para que no suceda otra vez y el análisis de si la responsabilidad del hecho era de una empresa proveedora de servicios.

El 26,7% tiene un GC Alto, es decir: hay un número muy satisfactorio de los problemas resueltos frente a los registrados, se usa como apoyo a la continuidad del servicio el manejo de problemas, la infraestructura de comunicaciones obtiene el tiempo de su reloj interno directamente de un servidor NTP de la compañía, el estado de un problema es concretamente conocido, el encargado de la administración de problemas es el mismo que de la de cambios, en caso de que

un problema crítico sea responsabilidad de una empresa proveedora, se buscan las acciones necesarias inmediatamente, existe una baja tendencia a que se incrementen los problemas críticos.

En promedio la Gestión de Problemas según lo evaluado a la gerencia de sistemas no es satisfactoria.

N.	#Cumplimiento	GC
2	0	B
3	0	B
5	0	B
6	0	B
8	0	B
9	0	B
10	0	B
11	0	B
15	0	B
16	0	B
19	0	B
26	0	B
29	11,765	B
27	25	B
1	50	B
14	50	B
17	50	B
18	50	B
20	50	B
21	50	B
22	50	B
23	50	B
24	50	B
28	85	A
4	100	A
7	100	A
12	100	A
13	100	A
25	100	A
30	100	A

Tabla 3-24: Grado de Confianza - Gestión de Problemas para Gerente de Sistemas

3.2.6.2 Gráfico de Cumplimiento de Gestión de Problemas

De la Figura 3-12, se puede resaltar que en referencia a la Gestión de Problemas la Gerencia de Sistemas falla en registro de eventos respecto a problemas, así como en la prioridad de resolución comparada con incidentes.

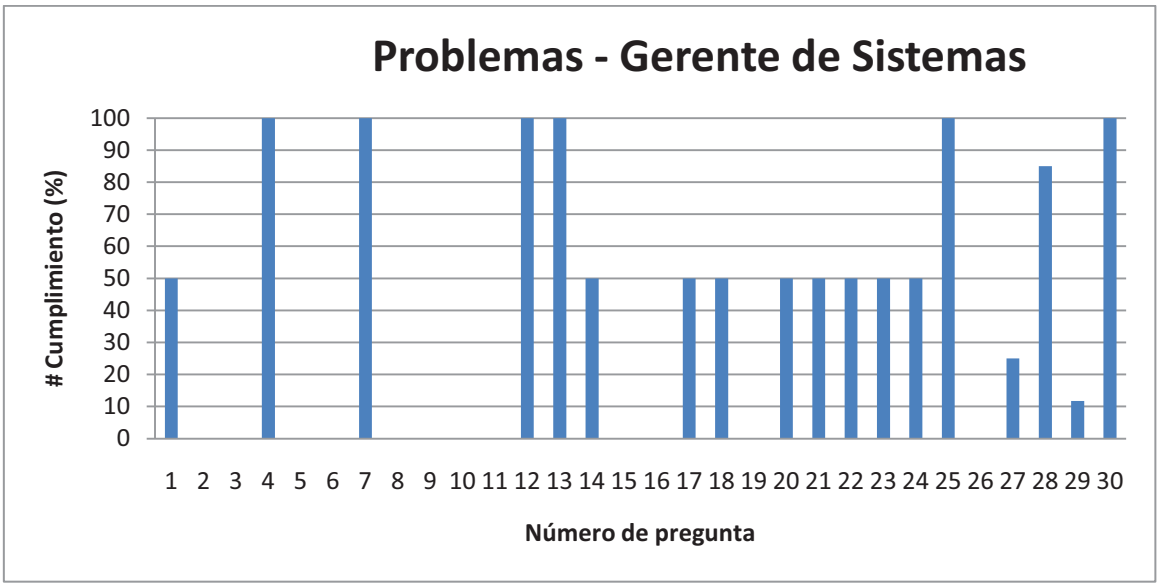

Figura 3-12: Gráfico de Cumplimiento - Gestión de Problemas para Gerente de Sistemas

3.2.6.3 Recomendaciones

Dado que el ítem 1 de la encuesta "Diferenciación de problemas e incidentes" tiene un GC bajo, se recomienda diferenciar los problemas de incidentes, porque cada uno tiene diferente prioridad y tiempo de resolución (ítem 3 de la encuesta "Orden de resolución de problemas e incidentes en su organización"). Cuando se trata de un incidente, se debe hacer todo lo posible para restituir el servicio enseguida, mientras que si se trata de un problema se debe investigar la causa y dar una solución completa a que no vuelva a ocurrir.

Según la Gerencia de Sistemas esto sólo se realiza parcialmente.

Por esta diferencia existente se sugiere que incluso el administrador de problemas sea una persona diferente a la que administra incidentes, en Alianza esto se cumple parcialmente lo cual es aceptable debido al reducido número de miembros del DDS, según el numeral 14 de la encuesta "¿El encargado de la administración de problemas es el mismo que de la de incidentes?".

El numeral 2 de la encuesta “¿Es tomada como base la administración de problemas para la resolución de incidentes?” tiene un GC bajo, por esto se recomienda que a pesar de que incidentes y problemas son diferentes, la gestión de problemas se debe tomar como base para resolver los incidentes, ya que estos son producidos por los problemas. Actualmente esta guía no es tomada en cuenta por la Dirección de Sistemas.

Como el ítem 5 de la encuesta “¿Existen reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades?” tiene un GC bajo se recomienda que la prevención de la ocurrencia de problemas se la debe realizar mediante reuniones para identificar vulnerabilidades y proponer actualizaciones. El hábito de realizar este tipo de actividades ayuda a disminuir problemas para la organización, ya que de esta manera se detectan antes de que puedan convertirse en incidentes. La Gerencia de Sistemas no realiza estas reuniones para el Departamento actualmente.

El numeral 6 de la encuesta “¿Posee un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT?”, posee un GC bajo por esto la gestión de problemas se debe apoyar en el monitoreo del funcionamiento de la infraestructura tecnológica, para esto se recomienda el uso de un servidor de Logs centralizado. Actualmente la compañía no cuenta con esta infraestructura.

Dado que el numeral 8 de la encuesta “¿Tiene concretamente identificadas las entradas para el proceso de resolución de problemas?” tiene un GC bajo, es necesario establecer siempre los elementos base para dar solución a los problemas, es decir por ejemplo: reconocer incidentes, servicios, equipos, etc. que se han producido a causa de este inconveniente. De la misma manera las salidas de la resolución de problemas (ítem 9 de la encuesta “¿Se registran las salidas del proceso de resolución de problemas?”) como los resultados obtenidos deben ser registradas, por ejemplo las acciones intuitivas que han mitigado un problema (ítem 16 de la encuesta “¿Es registrada la o las acciones intuitivas que han mitigado un problema?”). Es importante aclarar que por más que una de estas acciones intuitivas solucionen en parte el problema este no debe ser cerrado, con

respecto a esto la Gerencia de sistemas afirma esto sólo se cumple parcialmente, según el ítem 17 de la encuesta “Cuando ejecuta una acción intuitiva que atenúa el problema, ¿el registro del problema es cerrado?”.

Actualmente la Dirección de Sistemas no tiene un proceso formal para identificar las entradas de resolución de problemas, ni registro de resultados.
Sin estos registros no puede existir una base de datos sobre la gestión de problemas, la misma que apoyaría a la resolución de problemas. Por esto el numeral 10 de la encuesta “¿Se apoya la resolución de problemas en la base de datos de administración de problemas?” tiene un GC bajo, por lo que se recomienda la creación de esta base.

Dado que el ítem 15 de la encuesta “¿Existe personal designado para investigación especializada de problemas?” tiene un GC bajo, se debe tomar en cuenta que los problemas deben ser resueltos buscando su causa, se recomienda que el departamento cuente con un personal designado para investigación especializada de problemas. Al momento Alianza no cuenta con este personal.

Luego de un suceso de error crítico se debe aprender de las faltas cometidas, para esto se recomienda: revisadas las tareas que se realizaron correctamente (ítem 20 de la encuesta “Luego del suceso de un error crítico, ¿son revisadas las tareas que se realizaron correctamente?”), revisar los procedimientos erróneos (ítem 21 de la encuesta), analizar que se puede mejorar en el futuro (ítem 22 de la encuesta), examinar qué se puede hacer para que no vuelva a suceder (ítem 23 de la encuesta) y analizar si la responsabilidad del hecho era de una empresa proveedora de servicios (ítem 24 de la encuesta). Al momento estas guías se están cumpliendo parcialmente en Alianza. En adición todo lo realizado respecto al error crítico debe documentarse, al presente no se realiza ningún tipo de registro, según el ítem 26 de la encuesta “Luego del suceso de un error crítico, ¿son revisados los procedimientos erróneos?”.

Según el numeral 27 de la encuesta “Método para registro de problemas”, el registro de problemas tecnológicos en Alianza posee falencias en los siguientes

ítems: identificación única, fecha/hora de apertura y cierre (ítem 11 de la encuesta "¿Es posible verificar los problemas cerrados en un periodo de tiempo específico?"), prioridad y tipo. Al no tomarse en cuenta las características especificadas, no se cumple con un método adecuado para el registro de problemas, lo que provocaría en un futuro dificultades para el análisis y estudio de la Gestión de Problemas.

Además luego del diagnóstico de un problema se lo debe registrar en la base de errores conocidos, para que en caso de repetirse no se vuelvan a realizar algunas actividades de consulta o prueba, actualmente esto sólo se realiza parcialmente según el ítem 18 de la encuesta "Al finalizar el diagnóstico de un problema ¿es registrado en la base de datos de errores conocidos?", pero la gerencia de sistemas no se hace uso de esta base (ítem 19 de la encuesta "¿Soluciona problemas apoyándose en la base de datos de errores conocidos?").

El apoyo de la base de errores conocidos contribuirá a mejorar el ítem 29 de la encuesta "Porcentaje de problemas que se han resuelto en el tiempo esperado", mismo que tiene un nivel no satisfactorio.

3.3 OPERADORES DEL DEPARTAMENTO DE SISTEMAS

El grupo de Operadores del DDS presenta los siguientes resultados, con respecto al Porcentaje de Cumplimiento. El detalle de las encuestas aplicadas a los operadores del DDS, con sus respectivos totales para cada pregunta de respuesta cerrada o de métricas, puede ser encontrado en el Anexo 2-3, del capítulo 2.

3.3.1 GESTIÓN DE NIVEL DE SERVICIO

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	¿Existen reportes históricos del servicio de Internet?	100	0	0	**33,33**	**0,67**
2	¿Conoce los niveles de servicio que los proveedores están obligados a cumplir?	50	0	50	**33,33**	**0,67**
3	¿Conoce el nivel de servicio que los usuarios de la organización deben recibir?	100	0	0	**33,33**	**0,67**
4	¿Existe una vía de comunicación rápida y confiable para contactarse con cada uno de los proveedores externos de tecnologías?	0	0	0	**0,00**	**1,00**
5	¿Los usuarios de la red tienen un medio para comunicarse rápidamente con el DDS?	100	0	100	**66,67**	**0,33**
6	¿Conoce qué servicios ofrece el DDS a la organización?	100	50	50	**66,67**	**0,33**
7	Monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.	56.25	50	50	**52,08**	**0,48**
8	Monitoreo de nivel de calidad de los servicios que provee el DDS.	25	0	75	**33,33**	**0,67**
9	Definición formal de la calidad de los servicios que provee el DDS.	0	0	0	**0,00**	**1,00**
10	Conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.	50	0	0	**16,67**	**0,83**
				#Cumpl Promedio	**33,54**	

Tabla 3-25: Porcentaje de Cumplimiento - Gestión de Nivel de Servicio para Operadores del DDS

3.3.1.1 Estados de Indicadores de Gestión de Nivel de Servicio

La Tabla 3-26, respecto a GC muestra que el 70 % de los indicadores están en Bajo, esto implica que: no existe una vía de comunicación rápida y confiable para contactarse con cada uno de los proveedores externos de tecnologías, no existe una definición formal de la calidad de los servicios que provee el DDS, no se conoce el nivel de satisfacción del usuario respecto a los servicios que provee el DDS, no existen reportes históricos del servicio de Internet, no se conocen los niveles de servicio que los proveedores están obligados a cumplir, no se conoce el nivel de servicio que los usuarios de la organización deben recibir, no existe monitoreo del nivel de calidad de los servicios que provee el DDS.

El 10 % es Moderado Bajo lo que significa que, el monitoreo de la calidad de los servicios de proveedores externos en no satisfactoria.

El 20 % es Moderado Alto, lo que significa que: los usuarios de la red tienen un medio para comunicarse con el DDS satisfactorio según los operadores del DDS, la difusión de los servicios que ofrece el DDS a la organización es de igual forma satisfactoria.

N.	#Cumplimiento	GC
4	0,00	B
9	0,00	B
10	16,67	B
1	33,33	B
2	33,33	B
3	33,33	B
8	33,33	B
7	52,08	MB
5	66,67	MA
6	66,67	MA

Tabla 3-26: Grado de Confianza - Gestión de Nivel de Servicio para Operadores del DDS

3.3.1.2 Gráfico de Cumplimiento de Gestión de Nivel de Servicio

De la Figura 3-13, se determina que con cero absoluto se encuentran la comunicación confiable con proveedores y la falta de definición formal de los servicios que se proveen. Pero resaltan con un cumplimiento cerca de 70, la eficiencia que los usuarios tienen para comunicarse con el DDS y conocimientos de los servicios que prestan a la empresa.

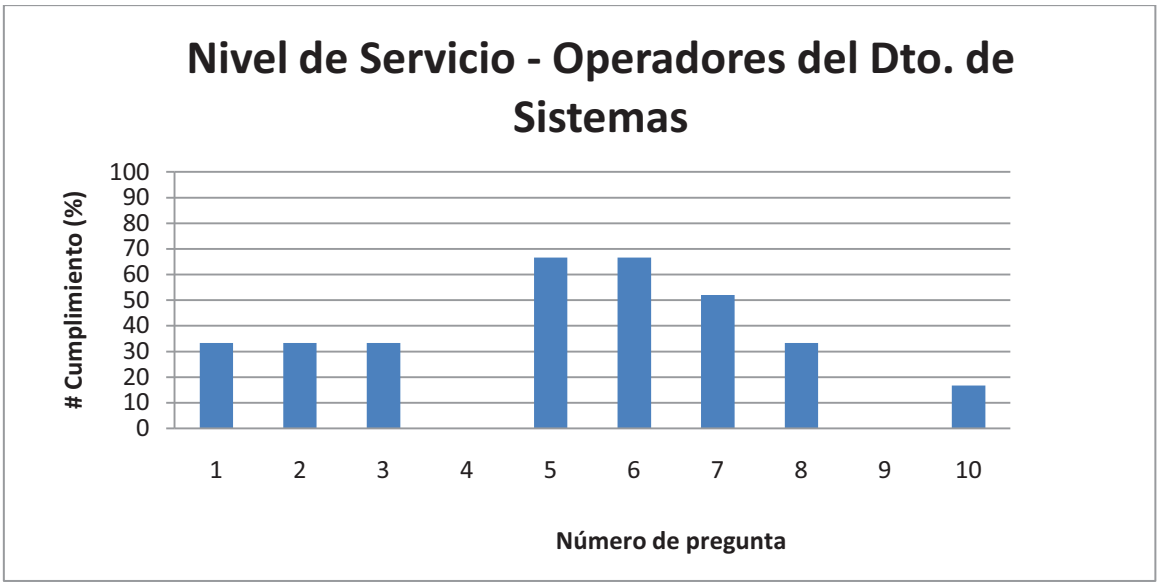

Figura 3-13: Gráfico de Cumplimiento - Gestión de Nivel de Servicio para Operadores del DDS

3.3.1.3 Recomendaciones:

Los empleados del DDS deberían proponer herramientas de monitoreo automático para el servicio de Internet recibido y suministrado. De los 3 técnicos sólo uno tiene conocimiento de la existencia de reportes históricos del servicio de Internet, esto según el ítem 1 de la encuesta "¿Existen reportes históricos del servicio de Internet?". La Gerencia de Sistemas debería verificar que todo el equipo de tecnología esté capacitado en iguales condiciones.

Dos de los tres técnicos conocen parcialmente los niveles de servicio que los proveedores están obligados a cumplir, y uno no los conoce en lo absoluto, esto según el numeral 2 de la encuesta "¿Conoce los niveles de servicio que los proveedores están obligados a cumplir?". Para que un técnico pueda alertar sobre el mal funcionamiento de un servicio interno o externo es primordial que conozca el nivel de calidad aceptable o acordado. Internamente el equipo de Sistemas debe definir formalmente la calidad de los servicios ofrecidos.

Con respecto a los servicios internos sólo un técnico está informado de la calidad que debe ser suministrada a los usuarios de Alianza, los demás no tienen ninguna referencia, este tema se relaciona con el ítem 3 de la encuesta "¿Conoce el nivel de servicio que los usuarios de la organización deben recibir?". Se deberían definir formalmente la calidad de los servicios para que los operadores los

provean de acuerdo a estos lineamientos, actualmente según este grupo ningún servicio ha sido definió formalmente, según el ítem 9 de la encuesta “Definición formal de la calidad de los servicios que provee el DDS”.

En caso de falla de un servicio a cargo de proveedores externos, el técnico debe tener una vía de comunicación rápida y confiable para contactarse con la empresa que sea requerida, el no conocimiento de números telefónicos, correos electrónicos y contactos alarga el tiempo de respuesta y solución. Al presente ninguno de los tres técnicos considera que se podría comunicar de una manera rápida y confiable con los proveedores de tecnología, esto según el ítem 4 de la encuesta “¿Existe una vía de comunicación rápida y confiable para contactarse con cada uno de los proveedores externos de tecnologías?”. La Gerencia de Sistemas debe proponer procedimientos base para contacto y capacitar al personal.

El monitoreo del nivel de calidad de los servicios que provee el DDS, se lo realiza de manera diferente para cada técnico. Esto se debería normalizar es decir, primero la Dirección debe asignar responsables de monitoreo y formalizar los procedimientos que deben seguir. Porque actualmente cada técnico procede según su criterio y otros simplemente no realizan ningún control de este tipo. Esta información según el numeral 8 de la encuesta “Monitoreo de nivel de calidad de los servicios que provee el DDS”.

Los técnicos deben ser incentivados y capacitados para que sigan procedimientos de mejoramiento continuo usando como referencia el nivel de satisfacción del usuario. Actualmente sólo un técnico lo realiza de forma parcial y los dos restantes no lo toman en cuenta, información obtenida del numeral 10 de la encuesta “Conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS”.

3.3.2 GESTIÓN DE CONTINUIDAD DE SERVICIO

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	Conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.	0	0	0	**0,00**	**1,00**
2	Entrenamiento del DDS para utilizar correctamente los planes de emergencia.	x	x	x	**x**	**x**
3	Desarrollado de un plan en caso de falla para equipos o sistemas.	16,67	0	50	**22,22**	**0,78**
4	Lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.	50	0	50	**33,33**	**0,67**
5	Tiempo en solución de catástrofes.	0	6,25	6,25	**4,17**	**0,96**
				#Cumpl Promedio	**26,56**	

Tabla 3-27: Porcentaje de Cumplimiento - Gestión de Continuidad de Servicio para Operadores del DDS

3.3.2.1 Estados de Indicadores de Continuidad de Servicio

Según se muestra en la Tabla 3-28, el 80 % de los indicadores presentan un GC Bajo, esto implica que: el equipo del DDS no conoce de la existencia de planes de emergencia, el tiempo de solución de catástrofes es mayor a 3 horas, no se ha desarrollado un plan en caso de falla para equipos o sistemas y no hay un lineamiento formal de cómo proceder para la recuperación al estado anterior de servicios.

El 20 % no pudieron ser evaluados, porque no hay referencia.

N.	#Cumplimiento	GC
1	0,00	B
5	4,17	B
3	22,22	B
4	33,33	B
2	x	N/A

Tabla 3-28: Grado de Confianza - Gestión de Continuidad de Servicio para Operadores del DDS

3.3.2.2 Gráfico de Cumplimiento de Gestión de Continuidad de Servicio

De la Figura 3-14, se observa que los Operadores del DDS tienen un cumplimiento de cero referente a conocimiento de planes de emergencia, y su más alto indicador pero con cumplimiento alrededor de 30 es el conocimiento de cómo proceder para la recuperación al estado anterior de servicios.

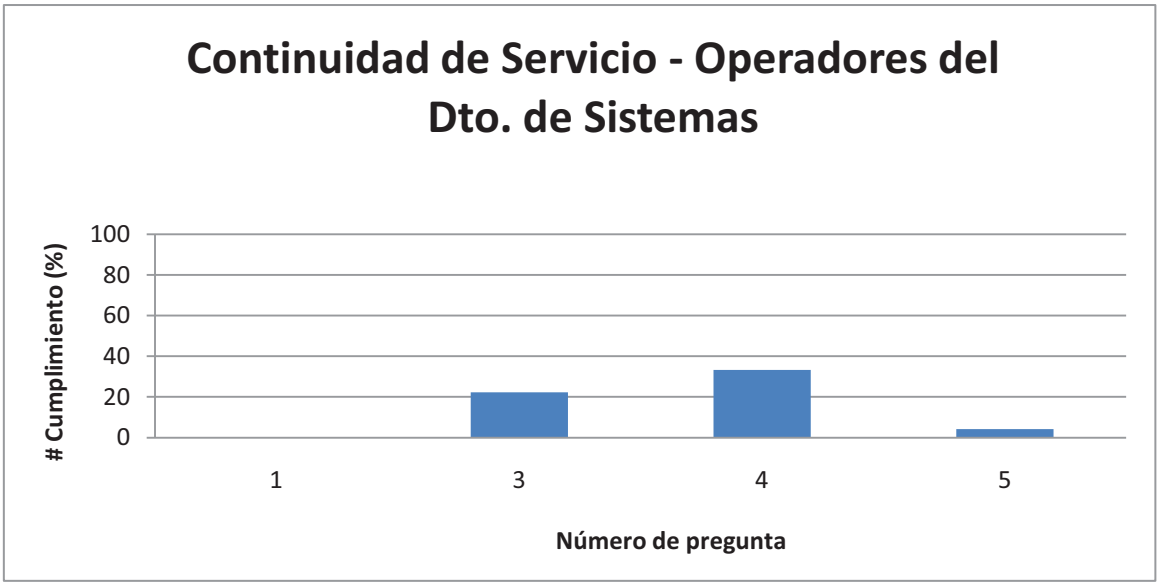

Figura 3-14: Gráfico de Cumplimiento - Gestión de Continuidad de Servicio para Operadores del DDS

3.3.2.3 Recomendaciones

El equipo de Sistemas al presente no conoce ningún plan de plan de respuesta ante una emergencia (ítem 1 de la encuesta “Conocimiento de la existencia de planes de emergencia de parte del equipo del DDS”), a pesar de que la gerencia afirma que existen parcialmente desarrollados planes para el Sistema de Seguros y el servicio de Internet, estos debían ser indicados a todos los técnicos, con su respectiva capacitación para que puedan ponerlos en práctica si la situación lo amerita. Los miembros del DDS deben dar ideas para la elaboración de estos planes de contingencia frente a situaciones críticas, donde en primer lugar se debería tratar los cortes de energía eléctrica, que causaron graves estragos para la compañía.

Un técnico conoce parcialmente el proceso que se debe realizar en caso de falla del Sistema de Seguros, otro frente a la necesidad se ha generado sus propios procedimientos para enfrentar emergencias con equipos de comunicaciones y

PCs de usuarios y el tercero no conoce ningún lineamiento. La gerencia en conjunto con los operadores del DDS, deben generar planes de acción en caso de falla de equipos y sistemas, información obtenida del ítem 3 de la encuesta “Desarrollado de un plan en caso de falla para equipos o sistemas”.

De manera similar al mantener procedimientos en caso de falla se deben establecer procesos para recuperar al estado anterior sistemas o equipos que prestan servicios. Dos de los técnicos conocen procesos de recuperación de forma parcial pero uno no lo conoce del todo (ítem 4 de la encuesta “Lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios”). Las guías de recuperación se las debe realizar en conjunto entre operarios y gerencia, de manera formal a que todos los empleados lo realicen siguiendo el mismo proceso.

Según la experiencia de dos técnicos la solución de catástrofes se la ha realizado en un tiempo mayor a tres horas. Un técnico no da referencia de ninguna emergencia a pesar de haber tenido cortes de suministro eléctrico anteriormente, esto según el numeral 5 de la encuesta “Tiempo en solución de catástrofes”. Se sugiere trabajar en planes de contingencia para reducir los tiempos en estado de emergencia.

3.3.3 GESTIÓN DE CAMBIOS

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	¿Recurre a los últimos cambios realizados para solucionar incidentes?	50	100	100	**83,33**	**0,17**
2	¿Tiene registrados los cambios que se realizaron sobre un dispositivo específico?	50	100	50	**66,67**	**0,33**
3	¿Son tomados en cuenta los posibles incidentes que producirá la ejecución del cambio?	50	100	50	**66,67**	**0,33**
4	¿Generalmente los cambios son impulsados por realizar innovación y mejoramiento?	50	100	100	**83,33**	**0,17**
5	¿Generalmente los cambios son impulsados por realizar correcciones?	50	100	0	**50,00**	**0,50**
6	¿Existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización?	50	0	50	**33,33**	**0,67**
7	¿Antes de la realización de un cambio se encuentran concretamente identificados los recursos necesarios?	50	0	100	**50,00**	**0,50**
8	¿Al finalizar el ciclo de un proceso de cambio realiza una evaluación del mismo?	50	50	100	**66,67**	**0,33**
9	¿Se conoce con certeza la razón para realizar el cambio?	50	100	50	**66,67**	**0,33**
10	¿Realiza pruebas piloto antes de la implementación de un cambio?	50	100	100	**83,33**	**0,17**
11	¿Al finalizar la implementación de un cambio se comprueba cumplimiento de objetivos?	50	100	100	**83,33**	**0,17**
12	¿Al finalizar la implementación de un cambio se comprueba la satisfacción de los involucrados?	100	100	100	**100,00**	**0,00**
13	¿Al finalizar la implementación de un cambio se registran los eventos no planificados que tuvieron efectos negativos sobre la organización?	50	0	0	**16,67**	**0,83**
14	¿Al finalizar la implementación de un cambio se comprueba cumplimiento de tiempos de ejecución?	50	0	0	**16,67**	**0,83**
15	Método para registro de Cambios.	25	12.5	25	**20,83**	**0,79**
16	Número de cambios realizados frente a los solicitados.	60	100	100	**86,67**	**0,13**
17	Número de cambios solicitados registrados.	40	100	100	**80,00**	**0,20**
18	Número de cambios realizados sin éxito frente al total de realizados.	100	100	100	**100,00**	**0,00**
19	Número de cambios realizados con carácter de emergencia frente al total de realizados.	50	100	100	**83,33**	**0,17**
20	Identificación de mejoras en servicios gracias a la realización de cambios.	50	0	100	**50,00**	**0,50**
					#Cumpl Promedio	**65,83**

Tabla 3-29: Porcentaje de Cumplimiento - Gestión de Cambios para Operadores del DDS

3.3.3.1 Estados de Indicadores de Gestión de Cambios

Según la Tabla 3-30, se determina que el 35 % de los indicadores poseen un GC Bajo, es decir: al finalizar la implementación de un cambio no se registran los eventos no planificados que tuvieron efectos negativos sobre la organización, al finalizar la implementación de un cambio no se comprueba el cumplimiento de tiempos de ejecución, no existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización, generalmente los cambios son impulsados por realizar correcciones parcialmente, antes de la realización de un cambio se encuentran parcialmente identificados los recursos necesarios, no hay un método definido para registro de Cambios, identificación parcial de mejoras en servicios gracias a la realización de cambios.

El 20 % es Moderado Moderado, lo que significa que de forma medianamente satisfactoria: se tiene registrados los cambios que se realizaron sobre un dispositivo específico, se toman en cuenta los posibles incidentes que producirá la ejecución de un cambio, se realiza una evaluación al finalizar el ciclo de un proceso de cambio, se conoce con certeza la razón para realizar el cambio.

Finalmente el 45 % tiene un GC Alto, lo cual implica que: existe un alto número de cambios solicitados registrados, recurre a los últimos cambios realizados para solucionar incidentes, generalmente los cambios son impulsados por realizar innovación y mejoramiento, se realizan pruebas piloto antes de la implementación de un cambio, al finalizar la implementación de un cambio se comprueba cumplimiento de objetivos, bajo número de cambios realizados con carácter de emergencia frente al total de realizados, alto número de cambios realizados frente a los solicitados, bajo número de cambios realizados sin éxito frente al total de realizados, al finalizar la implementación de un cambio se comprueba la satisfacción de los involucrados.

N.	#Cumplimiento	GC
13	16,67	B
14	16,67	B
6	33,33	B
5	50,00	B
7	50,00	B
15	20,83	B
20	50,00	B
2	66,67	MM

3	66,67	MM
8	66,67	MM
9	66,67	MM
17	80,00	A
1	83,33	A
4	83,33	A
10	83,33	A
11	83,33	A
19	83,33	A
16	86,67	A
18	100,00	A
12	100,00	A

Tabla 3-30: Grado de Confianza - Gestión de Cambios para Operadores del DDS

3.3.3.2 Gráfico de Cumplimiento de Gestión de Cambios

Respecto a la Figura 3-15, se observa que los indicadores más bajos se refieren a: documentación de efectos negativos que fueron causados por cambios, comprobación de tiempos de ejecución y métodos formales para registro de cambios. Pero resaltan con un cumplimiento de 100, la comprobación de satisfacción de involucrados y éxito en implementación de cambios.

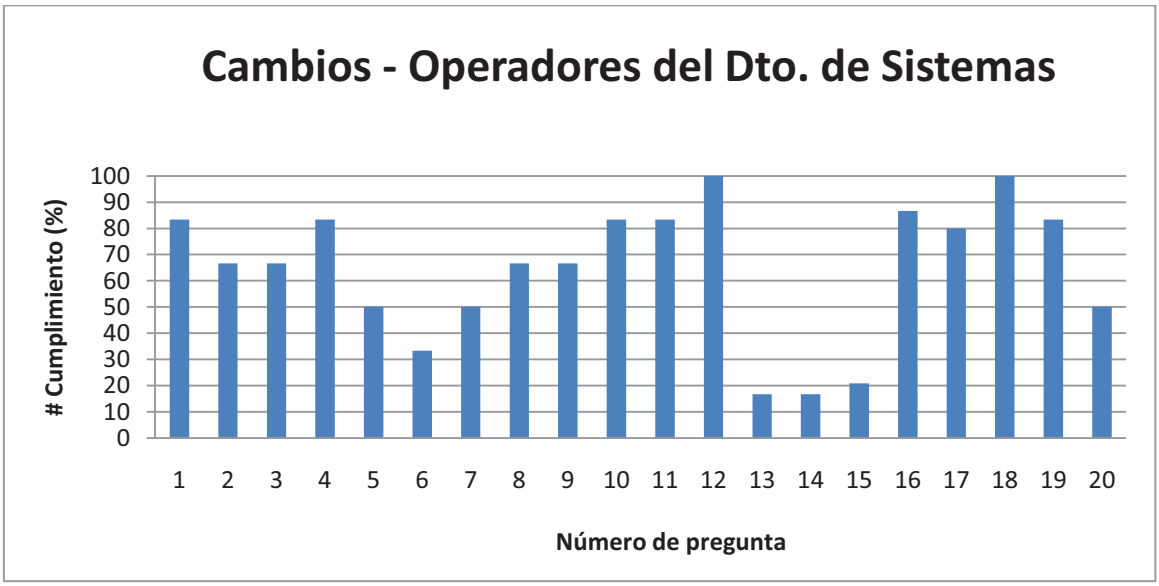

Figura 3-15: Gráfico de Cumplimiento - Gestión de Cambios para Operadores del DDS

3.3.3.3 Recomendaciones

El objetivo de la realización de cambios debe ser innovación y mejoramiento la tendencia no debe irse por realizar correcciones. Sólo un técnico lo administra con

la sugerencia mencionada, es decir del universo de cambios siempre la mayoría debe buscar una mejora, esto según ítem 5 de la encuesta “¿Generalmente los cambios son impulsados por realizar correcciones?”.

Para afrontar cambios comunes para la organización se deben formular procesos modelo con el fin de normalizar las acciones y realizarlas con mayor rapidez. Actualmente dos técnicos lo realizan parcialmente y uno no toma en cuenta la sugerencia, esta información se obtuvo del ítem 6 de la encuesta “¿Existen procesos modelos para afrontar cambios que se repiten o son comunes para la organización?”.

Los técnicos al realizar un cambio deben contar con los recursos necesarios, sin esto se aplazará el tiempo para completar la tarea o simplemente el cambio no tendrá éxito. Los técnicos deben identificar los recursos que necesiten y seguir todo el procedimiento necesario para contar con todos ellos a la hora de implementación. En Alianza un técnico lo realiza completamente otro parcialmente y el tercero no lo practica, esto del ítem 7 de la encuesta “¿Antes de la realización de un cambio se encuentran concretamente identificados los recursos necesarios?”.

En la implementación de un cambio existe la posibilidad de tener efectos negativos, estos deben ser documentados para tomarlos en cuenta en futuras implementaciones. El técnico de Guayaquil no lo toma en cuenta junto con otro de Quito. Sólo se lo realiza parcialmente por un técnico de Quito. Según el ítem 13 de la encuesta “¿Al finalizar la implementación de un cambio se registran los eventos no planificados que tuvieron efectos negativos sobre la organización?”

Los técnicos como ejecutores de los cambios, deben comprobar que los tiempos de implementación se den de a cuerdo a lo planificado. Al presente dos técnicos no realizan esta acción y uno los hace parcialmente, esto del ítem 14 de la encuesta “¿Al finalizar la implementación de un cambio se comprueba cumplimiento de tiempos de ejecución?”.

Los empleados del DDS, deben tomar en cuenta para el registro de cambios, dar un identificador único, registrar cada detalle del ciclo de vida del cambio, clasificar según el tipo o categoría y registrar el responsable de la petición de cambio. Estas

son falencias que se han encontrado para los operarios del DDS, ya que lo realizan parcialmente o no lo hacen, esto según el ítem 15 de la encuesta “Método para registro de Cambios”.

Los operarios del DDS deben estar en la capacidad de identificar las mejoras que producen los cambios, sólo así podrán verificar objetivos o sugerir mejoras a los procesos. Actualmente un técnico si lo identifica entre sus actividades, otro parcialmente y el tercero no lo realiza, información según ítem 20 de la encuesta “Identificación de mejoras en servicios gracias a la realización de cambios“.

3.3.4 GESTIÓN DE CONFIGURACIONES

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	¿Acostumbra llevar una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización?	100	50	50	**66,67**	**0,33**
2	¿Generalmente registra los cambios en una configuración?	100	100	100	**100,00**	**0,00**
3	¿Cuenta con un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía?	50	0	50	**33,33**	**0,67**
4	¿Conoce que procesos debe llevar a cabo para realizar recuperación de desastres de cada equipo configurable?	50	0	50	**33,33**	**0,67**
5	¿Tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico?	0	0	100	**33,33**	**0,67**
6	¿Puede conocer el estado actual de cada equipo configurable?	50	0	0	**16,67**	**0,83**
7	¿El desarrollo de software de la organización toma en cuenta los datos del manejo de configuraciones?	100	0	50	**50,00**	**0,50**
8	¿Al cierre de una configuración se documentan los detalles de verificación?	50	50	50	**50,00**	**0,50**
9	¿Registra su nombre como responsable o ejecutor cuando realiza una configuración?	0	50	0	**16,67**	**0,83**
10	¿Realiza una planificación previa a la implementación de una configuración?	50	100	100	**83,33**	**0,17**
11	¿Verifica el correcto funcionamiento luego de una configuración?	100	100	100	**100,00**	**0,00**
12	¿Cada configuración registrada posee concretamente identificado(s) su(s) ítem(s) configurable(s)?	50	50	50	**50,00**	**0,50**
13	Número de configuraciones realizadas sin éxito frente al total de realizadas.	x	100	100	**100,00**	**0,00**
14	Número de configuraciones realizadas sin autorización.	x	100	100	**100,00**	**0,00**
15	Número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.	x	90	80	**85,00**	**0,15**
16	Identificación de servicios que han tenido mejora gracias a configuraciones en la organización.	x	50	50	**50,00**	**0,50**
					#Cumpl Promedio	**60,52**

Tabla 3-31: Porcentaje de Cumplimiento - Gestión de Configuraciones para Operadores del DDS

3.3.4.1 Estados de Indicadores de Gestión de Configuraciones

La Tabla 3-32, indica que el 56,3 % de indicadores tiene un GC Bajo, esto implica que: no se puede conocer el estado actual de cada equipo configurable, no se registra el nombre del responsable o ejecutor cuando realiza una configuración, no se cuenta con un mapa completo con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía, no se conoce completamente que procesos debe llevar a cabo para realizar recuperación de desastres de cada equipo configurable, no se tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico, el desarrollo de software de la organización toma en cuenta parcialmente los datos del manejo de configuraciones, al cierre de una configuración se documentan parcialmente los detalles de verificación, cada configuración registrada posee parcialmente identificado(s) su(s) ítem(s) configurable(s), identificación parcial de servicios que han tenido mejora gracias a configuraciones en la organización.

El 6,3% es Modeado Moderado, significando que es medianamente satisfactorio el proceso de llevar una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.

Y el 37,4 % tiene un nivel Alto, implicando que: se realiza una planificación previa a la implementación de una configuración, existe bajo número de configuraciones realizadas con carácter de emergencia frente al total de realizadas, generalmente se registran las modificaciones en una configuración, se verifica el correcto funcionamiento luego de una configuración, bajo número de configuraciones realizadas sin éxito frente al total de realizadas, bajo número de configuraciones realizadas sin autorización.

N.	#Cumplimiento	GC
6	16,67	B
9	16,67	B
3	33,33	B
4	33,33	B
5	33,33	B
7	50,00	B
8	50,00	B
12	50,00	B
16	50,00	B
1	66,67	MM
10	83,33	A

15	85,00	A
2	100,00	A
11	100,00	A
13	100,00	A
14	100,00	A

Tabla 3-32: Grado de Confianza - Gestión de Configuraciones para Operadores del DDS

3.3.4.2 Gráfico de Cumplimiento de Gestión de Configuraciones

La Figura 3-16, muestra que los indicadores respecto a conocimiento del estado actual de equipos configurables y registro del ejecutor de una configuración se encuentran por debajo de 20 respecto a cumplimiento. Pero sobresalen con una calificación alta el registro de modificaciones en configuraciones, comprobación de buen funcionamiento, éxito en configuraciones y respeto a procesos de autorización.

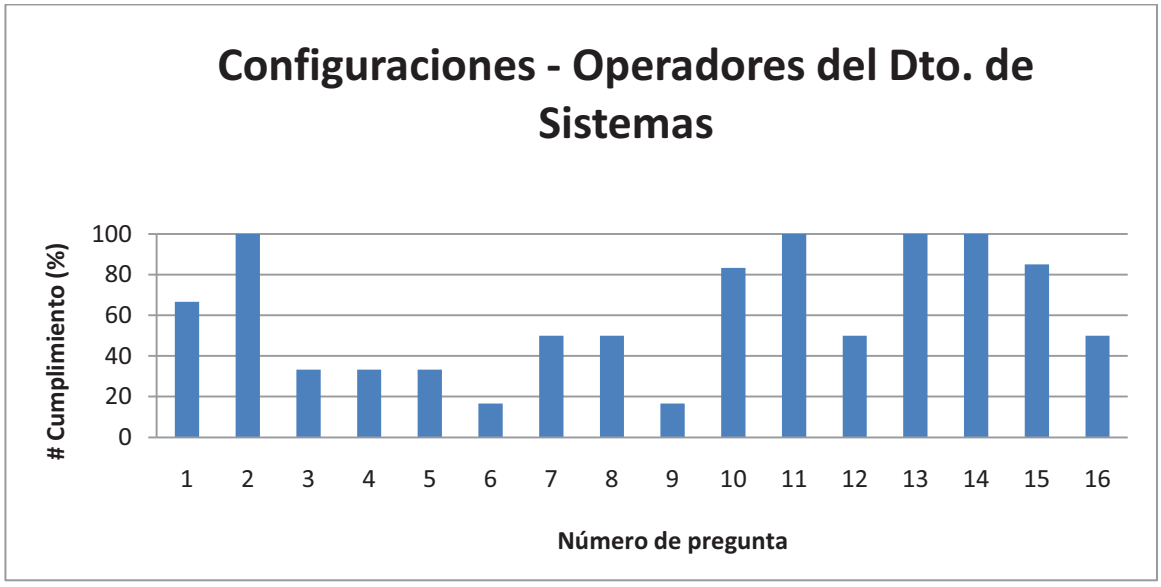

Figura 3-16: Gráfico de Cumplimiento - Gestión de Configuraciones para Operadores del DDS

3.3.4.3 Recomendaciones

A pesar de la existencia según la gerencia, de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía, un técnico no tiene conocimiento y dos afirman que lo conocen de forma parcial, esto según el numeral 3 de la encuesta "¿Cuenta con un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía?". Los técnicos deben sugerir que la información de la infraestructura

de tecnología se la debe difundir entre todos sus miembros, para con estas herramientas resolver de mejor manera inconvenientes de la empresa.

A pesar de la no existencia de procesos de recuperación de desastres, dos técnicos han desarrollado este tipo de procesos parcialmente y uno no tiene conocimiento, según el ítem 4 de la encuesta "¿Conoce que procesos debe llevar a cabo para realizar recuperación de desastres de cada equipo configurable?". Los operarios deben sugerir a la gerencia que se instauren procesos formales de recuperación para cada equipo configurable.

Los técnicos de Quito afirman que no tienen acceso al ciclo de vida de configuraciones de los equipos, mientras que el de Guayaquil si lo tiene, según la información obtenida del numeral 5 de la encuesta "¿Tiene acceso a todo el ciclo de vida de configuraciones de un equipo específico?". La gerencia debe facilitar el ingreso a esta información según las actividades de cada empleado.

El estado actual de un equipo dice si este trabaja de forma correcta o incorrecta, con esto se reconocen errores en la infraestructura y se resuelven incidentes rápidamente. Sólo un técnico conoce esta información de forma parcial, según el ítem 6 de la encuesta "¿Puede conocer el estado actual de cada equipo configurable?".

El personal técnico del DDS, debe tener presente que el desarrollo de software para su compatibilidad con los equipos tiene que tomar en cuenta sus características. Sólo un técnico toma en cuenta esta recomendación completamente, según el numeral 7 de la encuesta "¿El desarrollo de software de la organización toma en cuenta los datos del manejo de configuraciones?".

Todos los técnicos realizan de forma parcial el registro de los detalles de verificación al cierre de una configuración (ítem 8 de la encuesta "¿Al cierre de una configuración se documentan los detalles de verificación?"). Se debe incentivar que todos los detalles sean registrados, para definir responsabilidades en caso de falla.

Con el mismo propósito cada operario del DDS debe registrar su nombre en la configuración que haya realizado, actualmente sólo un técnico lo realiza de forma parcial, según la información del numeral 9 de la encuesta “¿Registra su nombre como responsable o ejecutor cuando realiza una configuración?”.

Una configuración en general puede abarcar a su vez configuraciones de varios equipos, o aplicaciones, para no fallar se deben tener concretamente identificados estos ítems. Actualmente todos los técnicos lo realizan de forma parcial, esto según el ítem 12 de la encuesta “¿Cada configuración registrada posee concretamente identificado(s) su(s) ítem(s) configurable(s)?”.

Todos los técnicos identifican de forma parcial las mejoras gracias a configuraciones en la organización (ítem 16 de la encuesta “Identificación de servicios que han tenido mejora gracias a configuraciones en la organización.”), deben pedir capacitación para conocer los avances que se esperan completamente. Así se incrementará el nivel de calidad de las configuraciones.

3.3.5 GESTIÓN DE INCIDENTES

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	¿Utiliza un escalamiento de solución para resolver incidentes de usuario?	100	50	0	**50,00**	**0,50**
2	¿Conoce quién es el responsable de la solución de un incidente abierto?	50	0	50	**33,33**	**0,67**
3	¿Conoce quienes son los usuarios que mantienen incidentes sin resolver?	50	0	100	**50,00**	**0,50**
4	¿Conoce cuál es el tiempo de respuesta y solución para un incidente específico?	50	0	50	**33,33**	**0,67**
5	¿Puede acceder a la bitácora de cambios que se relacionan con un incidente específico?	0	0	0	**0,00**	**1,00**
6	¿Se provee un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó?	0	0	50	**16,67**	**0,83**
7	¿Es informado el usuario sobre el escalamiento de su incidente?	0	100	100	**66,67**	**0,33**
8	¿Es informado el usuario sobre el cierre del incidente?	0	100	50	**50,00**	**0,50**
9	¿Están los incidentes agrupados por su naturaleza?	0	0	0	**0,00**	**1,00**
10	¿Están los incidentes agrupados por su solución tipo?	0	0	0	**0,00**	**1,00**
11	¿Resuelve los incidentes tomando en cuenta el banco de soluciones?	50	0	0	**16,67**	**0,83**
12	¿Se registran los niveles de satisfacción del usuario luego del cierre de un incidente?	0	0	50	**16,67**	**0,83**
13	¿Es registrado el técnico que cierra el incidente?	0	0	50	**16,67**	**0,83**
14	Tiempo en resolver incidentes.	100	100	100	**100,00**	**0,00**
15	Frecuencia en la realización de actualizaciones de software.	100	100	100	**100,00**	**0,00**
16	Frecuencia en la realización de actualizaciones de hardware.	100	70	50	**73,33**	**0,27**
17	Método para registro de Incidentes.	30	10	15	**18,33**	**0,82**
					#Cumpl Promedio	**37,75**

Tabla 3-33: Porcentaje de Cumplimiento - Gestión de Incidentes para Operadores del DDS

3.3.5.1 Estados de Indicadores de Gestión de Incidentes

Según la Tabla 3-34, el 76,5 % de indicadores tiene un GC Bajo, es decir: no se tiene acceso a la bitácora de cambios que se relacionan con un incidente específico, no se encuentran los incidentes agrupados por su naturaleza, los incidentes no están agrupados por su solución tipo, no se provee un soporte inicial rápido para solución del incidente por el contrario se identifica el problema que lo causó, no se resuelven los incidentes tomando en cuenta un banco de soluciones, no se registran los niveles de satisfacción del usuario luego del cierre de un incidente, no es registrado el técnico que cierra un incidente, no existe un método establecido para el registro de Incidentes, no se conoce quién es el responsable de la solución de un incidente abierto, no se conoce cuál es el tiempo de respuesta y solución para un incidente específico, se utiliza parcialmente un escalamiento de solución para resolver incidentes de usuario, se conoce parcialmente quienes son los usuarios que mantienen incidentes sin resolver, el usuario es informado parcialmente sobre el cierre de su incidente.

El 5,9% tiene un GC Moderado Moderado, es decir la notificación al usuario sobre el escalamiento de su incidente es medianamente satisfactoria.

De igual forma un 5,9% es Moderado Alto, lo que implica que la frecuencia en la realización de actualizaciones de hardware es satisfactoria porque tiende a darse cada 2 años.

Y con un nivel Alto el 11,7%, lo cual significa que: el tiempo en resolver incidentes es muy satisfactorio porque en promedio demora 30 minutos, de la misma manera muy satisfactoria la frecuencia en la realización de actualizaciones de software, porque tienden a realizarse cada año.

N.	#Cumplimiento	GC
5	0,00	B
9	0,00	B
10	0,00	B
6	16,67	B
11	16,67	B
12	16,67	B
13	16,67	B
17	18,33	B
2	33,33	B
4	33,33	B
1	50,00	B

3	50,00	B
8	50,00	B
7	66,67	MM
16	73,33	MA
14	100,00	A
15	100,00	A

Tabla 3-34: Grado de Confianza - Gestión de Incidentes para Operadores del DDS

3.3.5.2 Gráfico de Cumplimiento de Gestión de Incidentes

De la Figura 3-17 se concluye que en nivel cero se encuentran: existencia de bitácora de incidentes, y agrupación por origen y solución tipo. Con cumplimiento de 100 en contraste se muestra a: tiempo en resolución de incidentes y frecuencia en la realización de actualizaciones de software.

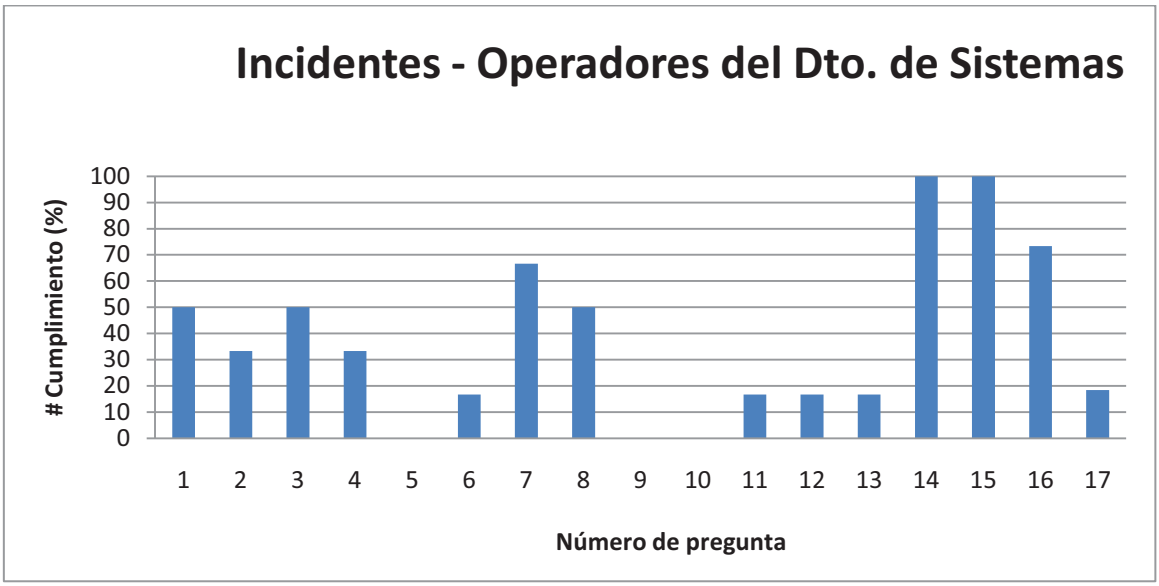

Figura 3-17: Gráfico de Cumplimiento - Gestión de Incidentes para Operadores del DDS

3.3.5.3 Recomendaciones

Dos técnicos no realizan completamente un escalamiento de solución para resolver incidentes de usuario, según el numeral 1 de la encuesta "¿Utiliza un escalamiento de solución para resolver incidentes de usuario?". Deben ser instruidos para escalar eventos que salgan de su alcance, además de los lineamientos de hasta dónde llega su responsabilidad. Esto ayuda a que la resolución de incidentes no se estanque.

Los operarios del DDS deben conocer quién es el responsable de incidentes abiertos y los usuarios afectados, de esta forma se incentivarán entre ellos para resolverlos con mayor rapidez o aportar con ideas para la resolución. Con respecto a responsable actualmente dos conocen esta información parcialmente y uno no tiene ninguna (ítem 2 “¿Conoce quién es el responsable de la solución de un incidente abierto?”), mientras que para afectados dos no cuentan con esta información de forma completa, esto según numeral 3 de la encuesta “¿Conoce quienes son los usuarios que mantienen incidentes sin resolver?”.

Los tiempos de respuesta y solución es necesario fijarlos como referencia para ciertos incidentes, esto ayuda a cumplir con un nivel de calidad de reacción establecida que el usuario considerará como satisfactorio. Actualmente dos técnicos conocen estos niveles de forma parcial y uno no lo conoce en lo absoluto, esto según el numeral 4 de la encuesta “¿Conoce cuál es el tiempo de respuesta y solución para un incidente específico?”.

Ningún técnico tiene acceso a la bitácora de cambios que se relacionen con un incidente específico, según el ítem 5 de la encuesta “¿Puede acceder a la bitácora de cambios que se relacionan con un incidente específico?”. Esto ocurre porque la gerencia no ha incentivado la generación de la relación entre cambios con incidentes que se producen. Esta información ayuda a los técnicos para que tomen las preventivas necesarias cuando implementan un cambio o solucionen incidentes con mayor eficiencia.

Un incidente siempre debe ser resuelto lo más rápido posible, y generalmente sin dar solución al problema que lo causó, en Alianza dos técnicos no usan esta recomendación y uno lo hace parcialmente, según el ítem 6 de la encuesta “¿Se provee un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó?”.

Sólo un técnico informa a los usuarios sobre el cierre de su incidente, otro lo hace parcialmente y el tercero no lo realiza, esto según el numeral 8 de la encuesta “¿Es informado el usuario sobre el cierre del incidente?”. Es importante que el

técnico informe al usuario para confirmar la solución y recibir comentarios o sugerencias.
Además en el cierre se debe registrar la satisfacción del usuario (ítem 12 de la encuesta "¿Se registran los niveles de satisfacción del usuario luego del cierre de un incidente?"), y el técnico que lo finaliza (ítem 13 de la encuesta "¿Es registrado el técnico que cierra el incidente?"), estos datos sólo son tomados por un técnico de forma parcial.

Los técnicos deben agrupar los incidentes por su naturaleza (ítem 9 de la encuesta "¿Están los incidentes agrupados por su naturaleza?"), para que se agrupen a su vez por una solución tipo (ítem 10 de la encuesta "¿Están los incidentes agrupados por su solución tipo?") y formar un banco de soluciones (ítem 11 de la encuesta "¿Resuelve los incidentes tomando en cuenta el banco de soluciones?"). Actualmente los técnicos del DDS no realizan este modelo de proceso, la gerencia debería diseñar el procedimiento y capacitar al personal.

Los técnicos tienen falencias en el registro de los siguientes ítems en incidentes: identificación única de cada incidente, fecha y hora de inicio de procesamiento, fecha y hora de cierre, identificación de servicio afectado, recalificación de categoría de incidente una vez que ha sido cerrado, técnico que abre y cierra un incidente, prioridad y finalmente registro de detalles en general de un incidente. Estos datos se obtuvieron del ítem 17 de la encuesta "Método para registro de Incidentes". La gerencia debería formalizar el proceso de registro tomando en cuenta estas debilidades.

3.3.6 GESTIÓN DE PROBLEMAS

N.	PREGUNTAS	Juan Guamba	Patricio León	Juan Cevallos	#Cumplimiento	Prob. de Amenaza
1	Diferenciación entre problemas e incidentes.	0,00	100,00	50	**50,00**	**0,50**
2	¿Busca resolver el problema raíz de los incidentes, antes del propio incidente?	0,00	0,00	0	**0,00**	**1,00**
3	¿Existen reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades?	100,00	0,00	100	**66,67**	**0,33**
4	¿Tiene una base histórica de eventos IT que genera información automáticamente?	50,00	0,00	0	**16,67**	**0,83**
5	¿Se apoya la resolución de problemas en la base de datos de administración de problemas?	100,00	0,00	50	**50,00**	**0,50**
6	¿Existe personal designado para investigación especializada de problemas?	50,00	0,00	50	**33,33**	**0,67**
7	¿Es registrada la o las acciones intuitivas que han mitigado un problema?	50,00	0,00	100	**50,00**	**0,50**
8	Cuándo ejecuta una acción intuitiva que atenúa el problema, ¿el registro del problema es cerrado?	100,00	100,00	0	**66,67**	**0,33**
9	Al finalizar el diagnóstico de un problema ¿es registrado en la base de datos de errores conocidos?	50,00	0,00	50	**33,33**	**0,67**
10	¿Soluciona problemas apoyándose en la base de datos de errores conocidos?	50,00	0,00	0	**16,67**	**0,83**
11	Luego del suceso de un error crítico, ¿son revisadas las tareas que se realizaron correctamente?	50,00	100,00	50	**66,67**	**0,33**
12	Luego del suceso de un error crítico, ¿son revisados los procedimientos erróneos?	50,00	100,00	50	**66,67**	**0,33**
13	Luego del suceso de un error crítico, ¿es examinado qué se puede hacer para que no suceda otra vez?	100,00	100,00	50	**83,33**	**0,17**
14	Registro adecuado de problemas.	0,00	0,00	0	**0,00**	**1,00**
15	Número de problemas resueltos frente a los registrados.	60,00	97,50	100	**85,83**	**0,14**
16	Porcentaje de problemas que se han resuelto en el tiempo esperado.	33,33	97,44	0	**43,59**	**0,56**
17	Tendencia a que se incrementen los problemas críticos.	100,00	100,00	100	**100,00**	**0,00**
					#Cumpl Promedio	**48,79**

Tabla 3-35: Porcentaje de Cumplimiento - Gestión de Problemas para Operadores del DDS

3.3.6.1 Estados de Indicadores de Gestión de Problemas

La Tabla 3-36, muestra que el 58,8 % de los ítems evaluados tienen un GC Bajo, es decir: se busca resolver el problema raíz de los incidentes, antes del propio incidente, no hay un registro adecuado de problemas, no se tiene una base de datos histórica de eventos de TI que genere información automáticamente, no se Solucionan problemas apoyándose en la base de datos de errores conocidos, no existe personal designado para investigación especializada de problemas, al finalizar el diagnóstico de un problema no se registra en la base de datos de errores conocidos, existe un bajo porcentaje de problemas que se han resuelto en el tiempo esperado, hay una diferenciación parcial entre problemas e incidentes, no se apoya la resolución de problemas en la base de datos de administración de problemas, se registran de forma parcial la o las acciones intuitivas que han mitigado un problema.

El 23,5 % es Moderado Moderado, lo que implica que de forma medianamente satisfactoria: se desarrollan reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades, el cierre de un problema a pesar de que sólo se ha llevado a cabo una acción intuitiva, la revisión de las tareas que se realizaron correctamente luego del suceso de un error crítico, se revisan los procedimientos erróneos luego del suceso de un error crítico.

Con un GC alto solamente el 17,7%, significando que: luego del suceso de un error crítico se está examinando que se puede hacer para que no suceda otra vez, alto número de problemas resueltos frente a los registrados, no existe tendencia a que se incrementen los problemas críticos.

N.	#Cumplimiento	GC
2	0,00	B
14	0,00	B
4	16,67	B
10	16,67	B
6	33,33	B
9	33,33	B
16	43,59	B
1	50,00	B
5	50,00	B
7	50,00	B
3	66,67	MM

8	66,67	MM
11	66,67	MM
12	66,67	MM
13	83,33	A
15	85,83	A
17	100,00	A

Tabla 3-36: Grado de Confianza - Gestión de Problemas para Operadores del DDS

3.3.6.2 Gráfico de Cumplimiento de Gestión de Problemas

La Figura 3-18 presenta niveles extremadamente bajos en prioridad entre problemas e incidentes y registro adecuado de problemas. En contraste con un cumplimiento mayor a 80 está el mejoramiento continuo, problemas resueltos frente a registrados y baja tendencia a que se incrementen problemas críticos.

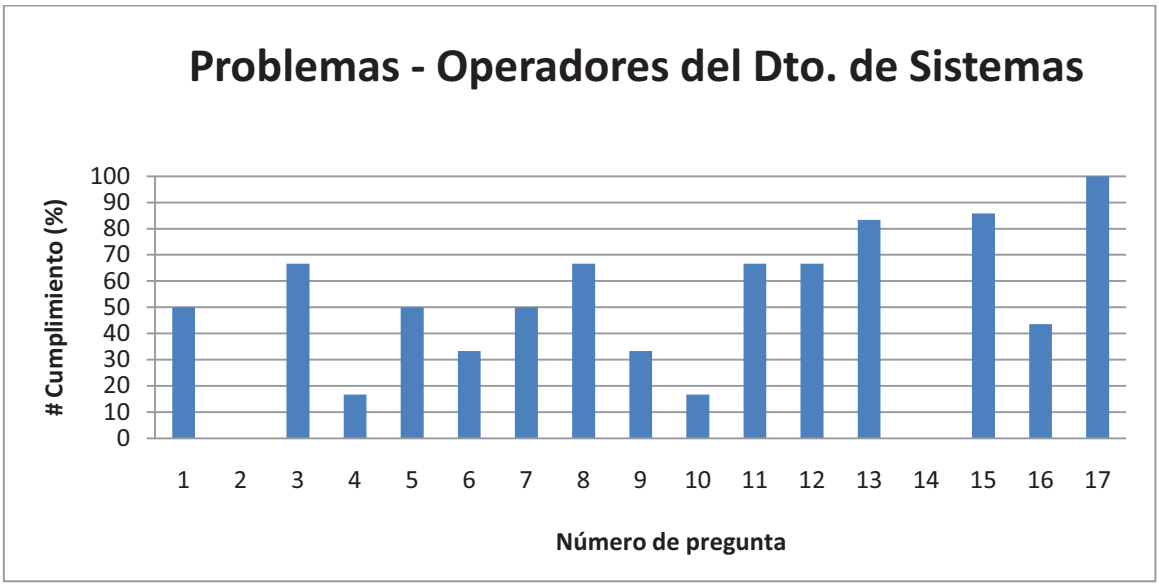

Figura 3-18: Gráfico de Cumplimiento - Gestión de Problemas para Operadores del DDS

3.3.6.3 Recomendaciones

La diferenciación entre problemas e incidentes es clave para dar prioridad de solución a los inconvenientes de la empresa, con este dato los técnicos conocerán de qué forma proceder para resolverlo. En Alianza ningún operario de Sistemas conoce cómo proceder ante dicha diferencia, según el ítem 1 de la encuesta "Diferenciación entre problemas e incidentes". La gerencia debe capacitar al personal en esta área para que el servicio no se quede paralizado más del necesario, por esto se debe dar la prioridad de solución al incidente para que el usuario no pare por un tiempo extendido sus actividades, luego de esto se

analizará al problema raíz. Actualmente ninguno de los Operadores del DDS tiene clara esta prioridad de resolución, según el ítem 2 de la encuesta "¿Busca resolver el problema raíz de los incidentes, antes del propio incidente?".

Es una buena práctica poseer una base histórica de eventos de tecnología con por ejemplo un servidor de Logs, al tener acceso a esta información los técnicos estarán en la capacidad de monitorear la infraestructura de tecnología, con el fin de detectar anomalías antes de que causen molestias. Al momento el DDS no cuenta con esta herramienta, según lo obtenido del ítem 4 de la encuesta "¿Tiene una base histórica de eventos IT que genera información automáticamente?".
Además los detalles de problemas deben ingresar a la base de datos de administración de problemas, para luego a su vez apoyar en la resolución de los mismos. Los técnicos deben ser capacitados para alimentar y realizar análisis de la base de datos. Actualmente Alianza no cuenta con esta base de datos, esto según el numeral 5 de la encuesta "¿Se apoya la resolución de problemas en la base de datos de administración de problemas?". Esta base de datos va de la mano con la base de errores conocidos, pero no se centra en registrar todos los incidentes, por el contrario sólo se ingresan los problemas que son frecuentes con la información que puede ser reutilizada cuando se suscite en el futuro otra vez uno de estos problemas. Actualmente sólo un técnico maneja parcialmente una base de errores conocidos y los otros dos no la manejan del todo, esto según el ítem 10 de la encuesta "¿Soluciona problemas apoyándose en la base de datos de errores conocidos?".
Para utilizar la información de la base de errores conocidos se debe en primera instancia educar a los Operadores del DDS, para que registren estos datos en dicha base. Actualmente dos técnicos lo realizan parcialmente y uno no lo realiza, esto según el numeral 9 de la encuesta "Al finalizar el diagnóstico de un problema ¿es registrado en la base de datos de errores conocidos?".

Los técnicos deben ser instruidos para que registren las acciones intuitivas que realizaron para atenuar un problema, con esto la persona que luego siga trabajando con el problema tendrá más elementos de juicio para tratarlo. El operario de Guayaquil afirma que si lo realiza, mientras que en Quito uno lo

realiza parcialmente y el otro no lo realiza del todo, estos datos se recopilaron del ítem 7 de la encuesta “¿Es registrada la o las acciones intuitivas que han mitigado un problema?”.

En el registro de problemas los técnicos deben colocar un identificador único para cada uno. Esto sirve para que sea de fácil acceso al momento de localizarlo.
En la actualidad esta práctica no se realiza por ningún técnico del equipo de Sistemas, según el ítem 14 de la encuesta “Registro adecuado de problemas”.

Según la entrevista realizada a los operarios del DDS, el porcentaje de los problemas resueltos en el tiempo esperado en promedio al mes es menor al 50%, según el ítem 16 de la encuesta “Porcentaje de problemas que se han resuelto en el tiempo esperado”. Para mejorar este indicador los técnicos y la gerencia deben trabajar en conjunto para buscar las mejoras necesarias para las falencias encontradas en general para la gestión de problemas.
Para mejorar la resolución de problemas se podría generar para ciertos casos un equipo dedicado a la investigación de un problema, actualmente dos técnicos conocen que de forma parcial se ha generado este tipo de grupo y un tercero que nunca lo ha conocido. Esta información se ha recopilado del ítem 6 de la encuesta “¿Existe personal designado para investigación especializada de problemas?”.

3.4 USUARIOS COMUNES

El grupo de Usuarios Comunes presenta los siguientes resultados, con respecto al Porcentaje de Cumplimiento. El detalle de las encuestas aplicadas a los usuarios comunes, con sus respectivos totales para cada pregunta, de respuesta cerrada o de métricas, puede ser encontrado en el Anexo 2-4, del capítulo 2.

3.4.1 GESTIÓN DE NIVEL DE SERVICIO

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿Conoce el nivel de calidad de los servicios que debe recibir de parte del DDS?	58,00	44,44	33,33	**45,26**	**0,55**
2	¿Ha recibido un documento formal informando los servicios que provee el DDS?	6,00	13,89	0,00	**6,63**	**0,93**
3	¿La calidad de servicio que recibe del DDS se ajusta a sus necesidades laborales?	70,00	44,44	66,67	**60,37**	**0,40**
4	¿Se siente satisfecho con la calidad del servicio del sistema AS400?	68,00	61,11	66,67	**65,26**	**0,35**
5	¿Se siente satisfecho con la calidad del servicio de Internet?	52,00	52,78	40,00	**48,26**	**0,52**
6	¿Se siente satisfecho con la calidad del servicio de Correo Electrónico?	90,00	69,44	60,00	**73,15**	**0,27**
7	¿Se siente satisfecho con la calidad del servicio de Soporte Técnico?	74,00	61,11	60,00	**65,04**	**0,35**
8	¿Se siente satisfecho con la calidad del servicio de Capacitación Informática?	36,00	30,56	20,00	**28,85**	**0,71**
9	¿Se siente satisfecho con la calidad del servicio de Reportes del Sistema AS400?	68,00	55,56	60,00	**61,19**	**0,39**
					#Cumpl Promedio	**50,44**

Tabla 3-37: Porcentaje de Cumplimiento - Gestión de Nivel de Servicio para Usuarios Comunes

3.4.1.1 Estados de Indicadores de Gestión de Nivel de Servicio

La Tabla 3-38, muestra que del número de indicadores totales el 44,4 % tiene un GC Bajo, esto implica que los usuarios comunes no han recibido un documento formal que informe de los servicios que provee el DDS ni de su calidad, no es satisfactoria la calidad de la capacitación informática ni la calidad del servicio de Internet.

De igual forma el 44,4% es Moderado Moderado, lo que significa que es medianamente satisfactoria la calidad de: servicio que provee el DDS según las necesidades de los usuarios, servicio del sistema de seguros y sus reportes, servicio de soporte técnico.

Finalmente como Moderado Alto se tiene solamente el 11,1%, es decir un indicador, el cual implica que los usuarios comunes califican como satisfactoria la calidad del servicio de correo electrónico.

En promedio la Gestión de Nivel de Servicio del punto de vista de los usuarios comunes es no satisfactoria.

N.	#Cumplimiento	GC
2	6,63	B
8	28,85	B
1	45,26	B
5	48,26	B
3	60,37	MM
9	61,19	MM
7	65,04	MM
4	65,26	MM
6	73,15	MA

Tabla 3-38: Grado de Confianza - Gestión de Nivel de Servicio para Usuarios Comunes

3.4.1.2 Gráfico de Cumplimiento de Gestión de Nivel de Servicio

La Figura 3-19, muestra que respecto al nivel de servicio para los usuarios de Alianza, con un cumplimiento menor a 10 se observa a la no definición formal de los servicios que provee el DDS pero con un nivel mayor a 50 se encuentra la satisfacción referente a servicios como el correo electrónico y el sistema de la empresa.

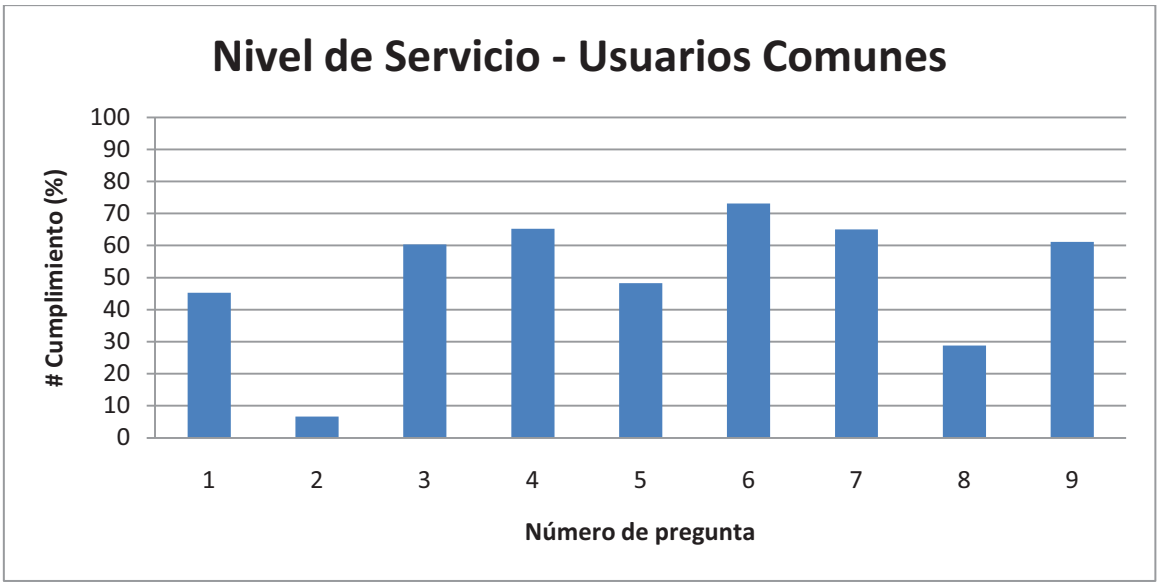

Figura 3-19: Gráfico de Cumplimiento - Gestión de Nivel de Servicio para Usuarios Comunes

3.4.1.3 Recomendaciones

Los usuarios de la red de Alianza Seguros, deben aprovechar al máximo las herramientas tecnológicas para realizar su trabajo rápida y correctamente. Actualmente según el ítem 2 de la encuesta "¿Ha recibido un documento formal informando los servicios que provee el DDS?" y el ítem 1 "¿Conoce el nivel de calidad de los servicios que debe recibir de parte del DDS?" menos del 50% de usuarios conocen cuales son los servicios que presta el DDS con sus respectivos niveles de calidad.

Según el ítem 5 "¿Se siente satisfecho con la calidad del servicio de Internet?" de la encuesta realizada a los usuarios solamente el 48% se siente satisfecho con el servicio de Internet, se debería consultar cómo se podría mejorarlo y darles un informativo de las ventajas y desventajas de llevar las políticas actuales.

Las herramientas informáticas en ciertos casos para ser explotadas al máximo requieren capacitación, según el ítem 8 "¿Se siente satisfecho con la calidad del servicio de Capacitación Informática?" al presente sólo el 28% de los usuarios se sienten satisfechos con este servicio. Para mejorar la productividad laboral se deben investigar cuáles son las necesidades de preparación y orientarlas a las tareas tipo de cada usuario.

3.4.2 GESTIÓN DE CONTINUIDAD DE SERVICIO

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿Ha sido notificado que procedimientos seguir en caso de emergencias, tales como el corte de energía eléctrica?	44	30,56	3,57	**26,04**	**0,74**
2	En promedio a la semana ¿Por cuánto tiempo afecta un problema de virus, el normal desempeño de su trabajo?	80	71,88	72,32	**74,73**	**0,25**
3	En promedio a la semana ¿Por cuánto tiempo afecta un problema de caída del Sistema AS400, el normal desempeño de su trabajo?	78	64,24	62,50	**68,25**	**0,32**
4	En promedio a la semana ¿Por cuánto tiempo afecta un problema de falla del Internet, el normal desempeño de su trabajo?	76	67,36	60,71	**68,03**	**0,32**
5	En promedio a la semana ¿Por cuánto tiempo afecta un problema de falla de Correo Electrónico, el normal desempeño de su trabajo?	71,75	71,53	72,32	**71,87**	**0,28**
6	Cuando empezaron los cortes de Energía Eléctrica ¿Por cuánto tiempo afectó dicha emergencia, el normal desempeño de su trabajo?	32	13,19	7,14	**17,45**	**0,83**
7	Durante la época de Cortes de Suministro Eléctrico. Diariamente ¿Por cuánto tiempo se vio afectado el normal desempeño de su trabajo?	38,75	13,54	8,93	**20,41**	**0,80**
					#Cumpl Promedio	**49,54**

Tabla 3-39: Porcentaje de Cumplimiento - Gestión de Continuidad de Servicio para Usuarios Comunes

3.4.2.1 Estados de Indicadores de Gestión de Continuidad de Servicio

La Tabla 3-40, indica que el 42,9% de los indicadores tienen un GC Bajo, es decir cuando empezaron los cortes de energía eléctrica y durante la época de esta emergencia éstos afectaron el normal desempeño de los usuarios por más de 3 horas a la semana.

El restante 57,1% es Moderado Alto, lo que implica que según los usuarios comunes las emergencias respecto a los servicio de Internet, sistema de seguros, correo electrónico y virus han sido manejadas de forma satisfactoria.

En promedio la Gestión de Continuidad de Servicio desde el punto de vista de los usuarios comunes no es satisfactoria.

N.	#Cumplimiento	GC
6	17,45	B
7	20,41	B
1	26,04	B
4	68,03	MA
3	68,25	MA
5	71,87	MA
2	74,73	MA

Tabla 3-40: Grado de Confianza - Gestión de Continuidad de Servicio para Usuarios Comunes

3.4.2.2 Gráfico de Cumplimiento de Gestión de Continuidad de Servicio

La Figura 3-20, muestra que con niveles bajos se distinguen a: preparación frente a emergencias, y el tiempo que crisis como la del estiaje afectaron el trabajo normal. A pesar de esto con un cumplimiento mayor a 60 se encuentran las pocas interrupciones que existen servicios como el correo electrónico, el Internet y el sistema de la empresa.

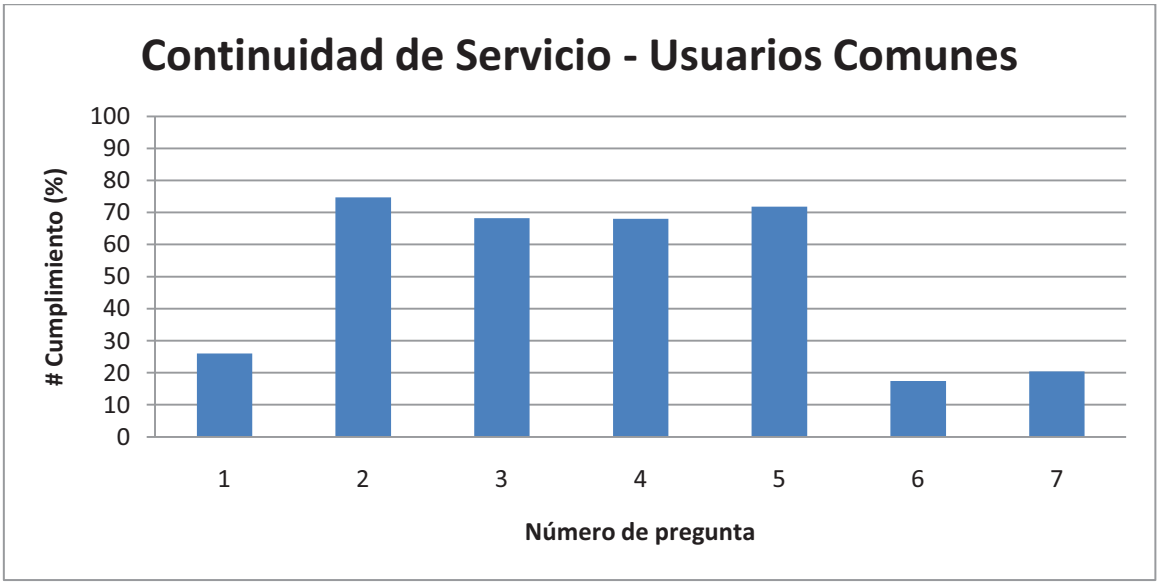

Figura 3-20: Gráfico de Cumplimiento - Gestión de Continuidad de Servicio para Usuarios Comunes

3.4.2.3 Recomendaciones

La mejor forma de enfrentar emergencias, es actuar con procedimientos prediseñados para cada tipo de situación. El orden ayuda a que la emergencia no se mantenga por un largo tiempo en la empresa. Actualmente, según el ítem 1 "¿Ha sido notificado que procedimientos seguir en caso de emergencias, tales

como el corte de energía eléctrica?" sólo el 26% de los usuarios afirma que se encuentra preparado para enfrentar emergencias. El DDS debe analizar cuáles pueden ser las amenazas con mayor probabilidad de ocurrencia y para estas realizar talleres de capacitación para los usuarios.

Según los usuarios la empresa tuvo un 17.45% de efectividad para enfrentar el inicio de la crisis de energía, esto relativo al ítem 6 de la encuesta "Cuando empezaron los cortes de Energía Eléctrica ¿Por cuánto tiempo afectó dicha emergencia, el normal desempeño de su trabajo?". Y una efectividad en el ítem 7 "Durante la época de Cortes de Suministro Eléctrico. Diariamente ¿Por cuánto tiempo se vio afectado el normal desempeño de su trabajo?" de 20.41% cuando ya se conocía la planificación de los racionamientos de energía.

La insatisfacción notada en los usuarios debe ser contrarrestada con campañas de formación de procedimientos a seguir en caso de emergencia.

3.4.3 GESTIÓN DE CAMBIOS

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿En caso de la necesidad de un cambio de software o hardware su solicitud es receptada por el DDS?	78,00	75,00	66,67	**73,22**	**0,27**
2	¿Es notificado cuándo se realizará un cambio que afecte a su entorno de trabajo?	76,00	61,11	63,33	**66,81**	**0,33**
3	¿En general los cambios realizados por el DDS tienen como objetivo innovación y mejoramiento?	98,00	80,56	86,67	**88,41**	**0,12**
4	¿En general los cambios realizados por el DDS tienen como objetivo correcciones?	16,00	27,78	23,33	**22,37**	**0,78**
5	¿Habitualmente los cambios realizados por el DDS lo han satisfecho?	74,00	66,67	80,00	**73,56**	**0,26**
6	¿Tiene la oportunidad de calificar su nivel de satisfacción respecto a un cambio realizado por el DDS?	36,00	30,56	30,00	**32,19**	**0,68**
7	En promedio semanalmente ¿qué porcentaje de los cambios realizados lo han satisfecho?	71,20	70,00	57,33	**66,18**	**0,34**
8	En promedio semanalmente de los cambios realizados, cuántos no le han sido notificados y han afectado el desenvolvimiento normal de su trabajo?	88,80	77,78	78,67	**81,75**	**0,18**
					#Cumpl Promedio	**63,06**

Tabla 3-41: Porcentaje de Cumplimiento - Gestión de Cambios para Usuarios Comunes

3.4.3.1 Estados de Indicadores de Gestión de Cambios

De la Tabla 3-42 se establece que del total, el 25 % tiene un GC Bajo, es decir los usuarios comunes consideran que los cambios realizados por el DDS tienen la tendencia a sólo realizarse por correcciones, además no poseen una forma de calificar la satisfacción con respecto a los cambios realizados.

Otro 25% es Moderado Moderado, es decir que los usuarios se sienten medianamente satisfechos respecto a: porcentaje de cambios que han sido satisfactorios, así como las notificaciones que debería hacer el DDS cuando va a realizar un cambio.

Así mismo el 25% es Moderado Alto, es decir los usuarios comunes se sienten satisfechos respecto a la apertura del DDS a recibir solicitudes de cambios.

Finalmente como Alto el 25%, implica que en promedio a la semana se produce un cambio que ha afectado el trabajo normal de los usuarios comunes y se reconoce que sí existen cambios para los cuáles su orientación es innovación y mejoramiento.

En promedio el manejo de cambios de parte del DDS, es calificado como medianamente satisfactorio según los usuarios comunes.

N.	#Cumplimiento	GC
4	22,37	B
6	32,19	B
7	66,18	MM
2	66,81	MM
1	73,22	MA
5	73,56	MA
8	81,75	A
3	88,41	A

Tabla 3-42: Grado de Confianza - Gestión de Cambios para Usuarios Comunes

3.4.3.2 Gráfico de Cumplimiento de Gestión de Cambios

La Figura 3-21, muestra que por debajo de 50 de cumplimiento resaltan la tendencia a realizar cambios sólo con el objetivo de corregir y la falta de un método para calificar el nivel de satisfacción. Como la mejor calificada se observa a los objetivos de innovación y mejoramiento que presenta el DDS.

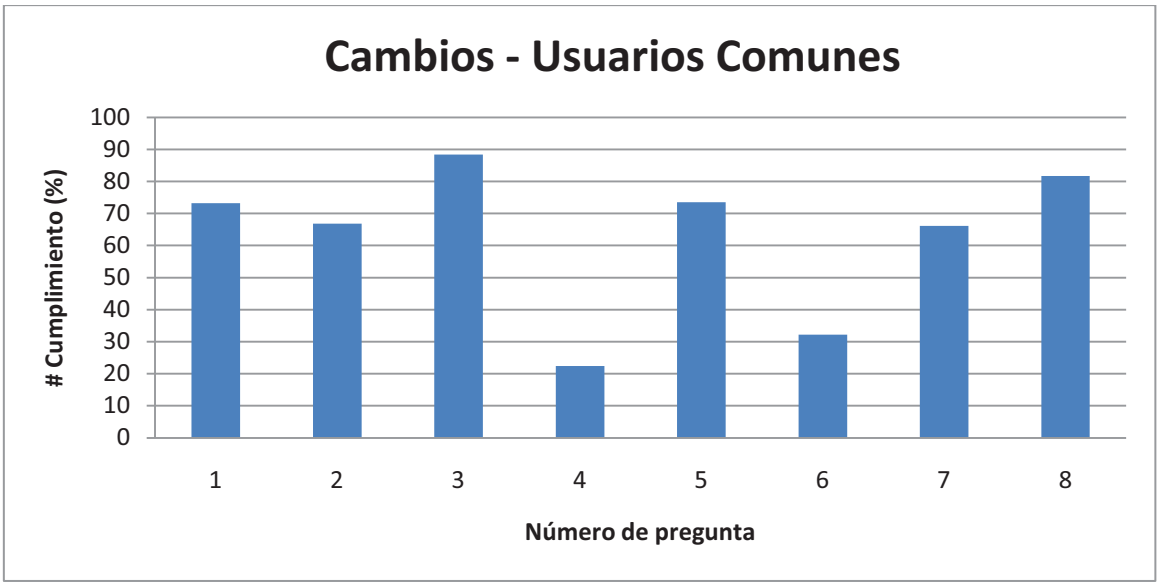

Figura 3-21: Gráfico de Cumplimiento - Gestión de Cambios para Usuarios Comunes

3.4.3.3 Recomendaciones

Según los usuarios obtenido del ítem 4 de la encuesta "¿En general los cambios realizados por el DDS tienen como objetivo correcciones?", la tendencia a realizar cambios para correcciones de parte del DDS es del 77.63%, este porcentaje debe ser reducido para que en lo posible los cambios tiendan sólo al mejoramiento de la empresa.

La calificación del nivel de satisfacción de los usuarios con respecto a los cambios realizados por el DDS tiene una efectividad del 32.19%, según el numeral 6 de la encueta "¿Tiene la oportunidad de calificar su nivel de satisfacción respecto a un cambio realizado por el DDS?" es importante elevar este indicador para recibir la retroalimentación de los usuarios que ayudarán a mejorar la calidad de los cambios realizados por el equipo de tecnología.

3.4.4 GESTIÓN DE CONFIGURACIONES

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿En general las configuraciones realizadas por el DDS se realizan de forma metódica y ordenadamente?	76,00	80,56	67,86	**74,80**	**0,25**
				#Cumpl Promedio	**74,80**	

Tabla 3-43: Porcentaje de Cumplimiento - Gestión de Configuraciones para Usuarios Comunes

3.4.4.1 Estados de Indicadores de Gestión de Configuraciones

Con respecto a las Configuraciones realizadas por el DDS, según la Tabla 3-44, indica que su único indicador tiene un GC Moderado Alto, es decir los usuarios comunes consideran que las configuraciones realizadas por el DDS se realizan satisfactoriamente tomando en cuenta el método y el orden.

En promedio los usuarios comunes consideran que la Gestión de Configuraciones tiene un desempeño satisfactorio.

N.	#Cumplimiento	GC
1	74,80	MA

Tabla 3-44: Grado de Confianza - Gestión de Configuraciones para Usuarios Comunes

3.4.4.2 Gráfico de Cumplimiento de Gestión de Configuraciones

La Figura 3-22, muestra que las configuraciones realizadas de forma metódica y ordenada de parte del DDS según los usuarios comunes tiene un cumplimiento cercano a 70.

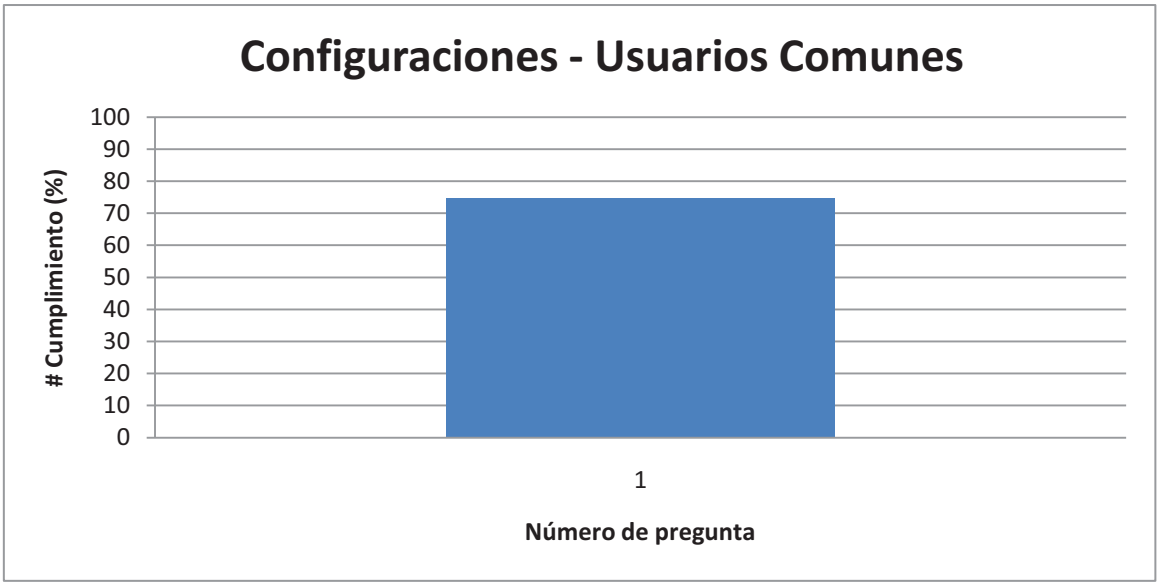

Figura 3-22: Gráfico de Cumplimiento - Gestión de Configuraciones para Usuarios Comunes

3.4.4.3 Recomendaciones

La Gestión de Configuraciones para Usuarios Comunes no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.4.5 GESTIÓN DE INCIDENTES

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿Los incidentes tecnológicos afectan con frecuencia el normal desempeño de su trabajo?	48,00	58,33	36,67	**47,67**	**0,52**
2	¿Cree que los recursos tecnológicos que le han sido asignados se ajustan a sus necesidades laborales?	80,00	66,67	66,67	**71,11**	**0,29**
3	¿Cree que la tecnología usada en la empresa ha evolucionado de forma continua para mejorar el servicio ofrecido?	76,00	83,33	76,67	**78,67**	**0,21**
4	¿Son atendidas las sugerencias hechas al DDS para mejorar el servicio que se apoya en la tecnología?	74,00	72,22	63,33	**69,85**	**0,30**
5	¿Recibe cursos o entrenamientos cuando existe la necesidad de manejar nuevos programas informáticos?	38,00	44,44	26,67	**36,37**	**0,64**
6	¿En general el tiempo de solución a los incidentes de parte del DDS ha sido satisfactorio?	78,00	69,44	63,33	**70,26**	**0,30**
7	¿Se repiten con frecuencia incidentes específicos?	76,00	75,00	53,33	**68,11**	**0,32**
8	Método de Gestión de incidentes.	39,33	39,81	11,67	**30,27**	**0,70**
9	¿Tiene la oportunidad de calificar el servicio recibido de parte del DDS?	16,00	11,11	13,33	**13,48**	**0,87**
10	¿En general cuánto tiempo le toma al DDS solucionar un incidente?	75,20	83,89	72,67	**77,25**	**0,23**
11	¿Cuál sería la calificación general para el DDS respecto a resolución de incidentes?	68,00	66,67	63,33	**66,00**	**0,34**
12	¿Cuál es la frecuencia de ocurrencia de incidentes con Programas de ofimática en su labor cotidiana?	66,00	91,67	63,33	**73,67**	**0,26**
13	¿Cuál es la frecuencia que se den incidentes que impliquen falla física de su Computadora, en su labor cotidiana?	88,00	91,67	70,00	**83,22**	**0,17**
14	¿En qué frecuencia su trabajo normal se ve afectado por Virus informáticos?	82,00	88,89	66,67	**79,19**	**0,21**
15	¿En qué frecuencia su trabajo normal se ve afectado por problemas de Internet?	84,00	72,22	66,67	**74,30**	**0,26**
16	¿Con qué frecuencia su trabajo normal se ve afectado por problemas con el Sistema de la Empresa?	84,00	69,44	66,67	**73,37**	**0,27**

17	¿Con qué frecuencia su trabajo normal se ve afectado por problemas con el Correo Electrónico Corporativo?	88,00	72,22	76,67	**78,96**	**0,21**
					#Cumpl Promedio	**53,98**

Tabla 3-45: Porcentaje de Cumplimiento - Gestión de Incidentes para Usuarios Comunes

3.4.5.1 Estados de Indicadores de Gestión de Incidentes

Según la Tabla 3-46, el 23,5% de los indicadores tienen un GC Bajo, es decir los usuarios no poseen una vía para calificar al DDS respecto al servicio de soporte de incidentes, no es satisfactoria la gestión de sus incidentes, ni la capacitación cuando se trata de manejar nuevos programas informáticos, además los usuarios comunes colocan como frecuentes a los incidentes tecnológicos que afectan la normalidad de su trabajo.

El 5,9% es Moderado Moderado, es decir los usuarios se encuentran medianamente satisfechos con el buen mantenimiento que implica que no se den fallas físicas de los computadores.

El 41,2% Moderado Alto, implica que los usuarios comunes están satisfechos con: que no existe frecuencia de incidentes específicos, la recepción de sugerencias hechas al DDS, el tiempo de solución a incidentes de parte del DDS, los recursos tecnológicos se ajustan a las necesidades de los usuarios comunes, baja frecuencia de problemas con el sistema de la empresa, con programas de ofimática o de Internet.

Finalmente el 29,4% es Alto, esto implica que los usuarios perciben que los incidentes se resuelve en alrededor de 30 minutos, la tecnología ha evolucionado en la empresa de manera muy satisfactoria y las fallas con respecto a correo electrónico, problemas con virus informáticos o fallas físicas de los computadores no son frecuentes.

En promedio los usuarios comunes calificaron a la Gestión de Incidentes como no satisfactoria.

N.	#Cumplimiento	GC
9	13,48	B
8	30,27	B
5	36,37	B
1	47,67	B
13	66,00	MM
7	68,11	MA
4	69,85	MA
6	70,26	MA
2	71,11	MA
16	73,37	MA
12	73,67	MA
15	74,30	MA

10	77,25	A
3	78,67	A
17	78,96	A
14	79,19	A
13	83,22	A

Tabla 3-46: Grado de Confianza - Gestión de Incidentes para Usuarios Comunes

3.4.5.2 Gráfico de Cumplimiento de Gestión de Incidentes

La figura 3-23, muestra que en general el manejo de incidentes de parte del DDS son bien calificados por los usuarios comunes con excepción de: Alta frecuencia de incidentes, cursos respecto a programas informáticos, registro formal de incidentes y falta de un método para calificar la satisfacción del servicio recibido, que tienen un cumplimiento menor a 50.

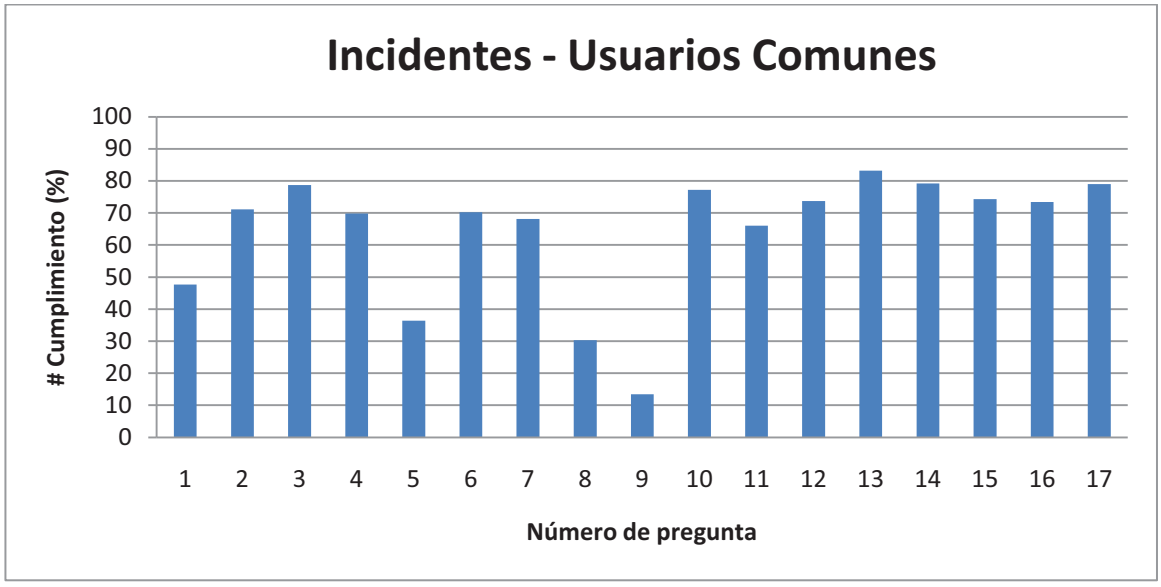

Figura 3-23: Gráfico de Cumplimiento - Gestión de Incidentes para Usuarios Comunes

3.4.5.3 Recomendaciones

Según el ítem 1 "¿Los incidentes tecnológicos afectan con frecuencia el normal desempeño de su trabajo?" de la encuesta realizada la solución de incidentes de parte del DDS tiene una efectividad menor al 50%, en las sucursales de Quito, Cuenca y Manta. El equipo de tecnología debe verificar cuáles son los indicadores insatisfechos, rediseñar el manejo de incidentes y verificar que los usuarios ya no se vean afectados con frecuencia por incidentes tecnológicos.

Los usuarios perciben que no existe un adecuado manejo de incidentes, según el numeral 8 de la encuesta “Método de Gestión de incidentes”, debido a falencias encontradas en: registro automático en incidentes, solución rápida vía telefónica y falta de un identificador que se relacione con su incidente.
La efectividad de gestión de incidentes al presente de parte del DDS es del 30.27%, tomando en cuenta las falencias mencionadas. La gerencia debe mejorar las prácticas de gestión y elevar este indicador.

Los usuarios deben tener la oportunidad de calificar el servicio recibido respecto a incidentes para mejorar continuamente la calidad de resolución. Los usuarios que al presente califican de alguna manera el servicio a nivel nacional llega al 13.48%, según el ítem 9 de la encuesta “¿Tiene la oportunidad de calificar el servicio recibido de parte del DDS?”.

Los usuarios comunes califican a la capacitación para el manejo de nuevos programas informáticos, como no satisfactoria con un cumplimiento de 36%. Por esto se recomienda planificar cursos para el personal en las herramientas tecnológicas que usan a diario o que se hayan adquirido recientemente, para las cuales no se ha organizado una capacitación formal. Esta información fue adquirida del ítem 5 de la encuesta “¿Recibe cursos o entrenamientos cuando existe la necesidad de manejar nuevos programas informáticos?”.

3.4.6 GESTIÓN DE PROBLEMAS

N.	PREGUNTAS	UIO	GYE	CUENCA-MANTA	#Cumplimiento	Prob. de Amenaza
1	¿Su incidente trata de ser generalmente resuelto inmediatamente para restablecer sus actividades laborales	96,00	91,67	73,33	**87,00**	**0,13**
2	¿Incidentes que ya han ocurrido antes son resueltos con mayor rapidez?	96,00	77,78	76,67	**83,48**	**0,17**
					#Cumpl Promedio	**85,24**

Tabla 3-47: Porcentaje de Cumplimiento - Gestión de Problemas para Usuarios Comunes

3.4.6.1 Estados de Indicadores de Gestión de Problemas

Según la Tabla 3-48, se muestra que el 100 % de indicadores tienen un GC Alto, es decir que los usuarios comunes reconocen que el DDS hace una diferenciación de prioridades para solucionar problemas e incidentes, dando como resultado que las actividades laborales sean restablecidas inmediatamente. Además los usuarios comunes ven que el DDS ha hecho un estudio de los problemas que han causado ciertos incidentes, provocando que incidentes ya ocurridos se solucionen con mayor rapidez.

N.	#Cumplimiento	GC
2	83,48	A
1	87,00	A

Tabla 3-48: Grado de Confianza - Gestión de Problemas para Usuarios Comunes

3.4.6.2 Gráfico de Cumplimiento de Gestión de Problemas

Según la Figura 3-24, se determina que sus dos indicadores tienen un cumplimiento mayor a 80, es decir los Usuarios Comunes perciben que sus incidentes tratan de ser resueltos inmediatamente y se resuelven con mayor rapidez incidentes ya ocurridos.

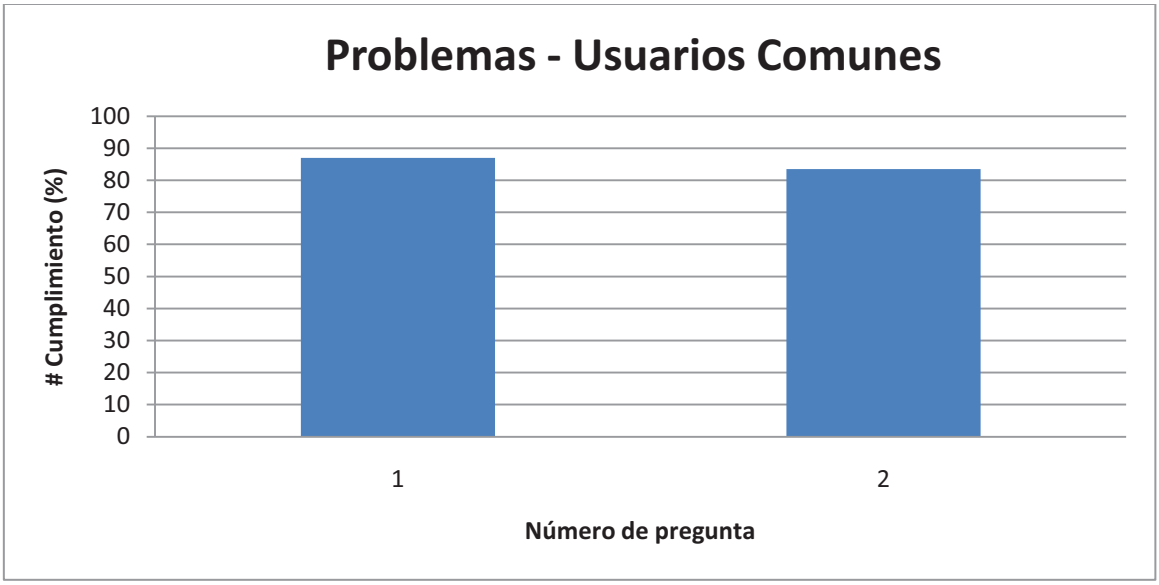

Figura 3-24: Gráfico de Cumplimiento - Gestión de Problemas para Usuarios Comunes

3.4.6.3 Recomendaciones

La Gestión de Problemas para Usuarios Comunes no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.5 PUNTOS DE VENTA SOAT

El grupo de Puntos de Venta SOAT presenta los siguientes resultados, con respecto al Porcentaje de Cumplimiento. El detalle de las encuestas aplicadas a los puntos de venta SOAT, con sus respectivos totales para cada pregunta, de respuesta cerrada o de métricas, puede ser encontrado en el Anexo 2-5, del capítulo 2.

3.5.1 GESTIÓN DE NIVEL DE SERVICIO

N.	PREGUNTAS	PTOS. DE VENTA	#Cumplimiento	Prob. de Amenaza
1	¿Se siente satisfecho con la calidad del servicio del sistema de Seguros de Alianza?	82,56	**82,56**	**0,17**
2	¿Se siente satisfecho con la calidad del servicio de Soporte Técnico de Alianza?	87,21	**87,21**	**0,13**
		#Cumpl Promedio	**84,88**	

Tabla 3-49: Porcentaje de Cumplimiento - Gestión de Nivel de Servicio para Puntos de Venta SOAT

3.5.1.1 Estados de Indicadores de Nivel de Servicio

La Tabla 3-50, muestra que el grupo Puntos de Venta SOAT tiene todos sus indicadores de Gestión de Nivel de Servicio con GC Alto, es decir los Puntos de Venta SOAT encuentran muy satisfactoria la calidad de sistema de seguros así como el soporte técnico.

En promedio según los Puntos de Venta SOAT, la Gestión de Nivel de Servicio se la realiza de forma muy satisfactoria.

N.	#Cumplimiento	GC
1	82,56	A
2	87,21	A

Tabla 3-50: Grado de Confianza - Gestión de Nivel de Servicio para Puntos de Venta SOAT

3.5.1.2 Gráfico de Cumplimiento de Gestión de Nivel de Servicio

En la Figura 3-25, se aprecia que según el grupo de Puntos de Venta SOAT, existe una satisfacción mayor a 80/100 respecto al Sistema SOAT y al soporte Técnico que brinda Alianza.

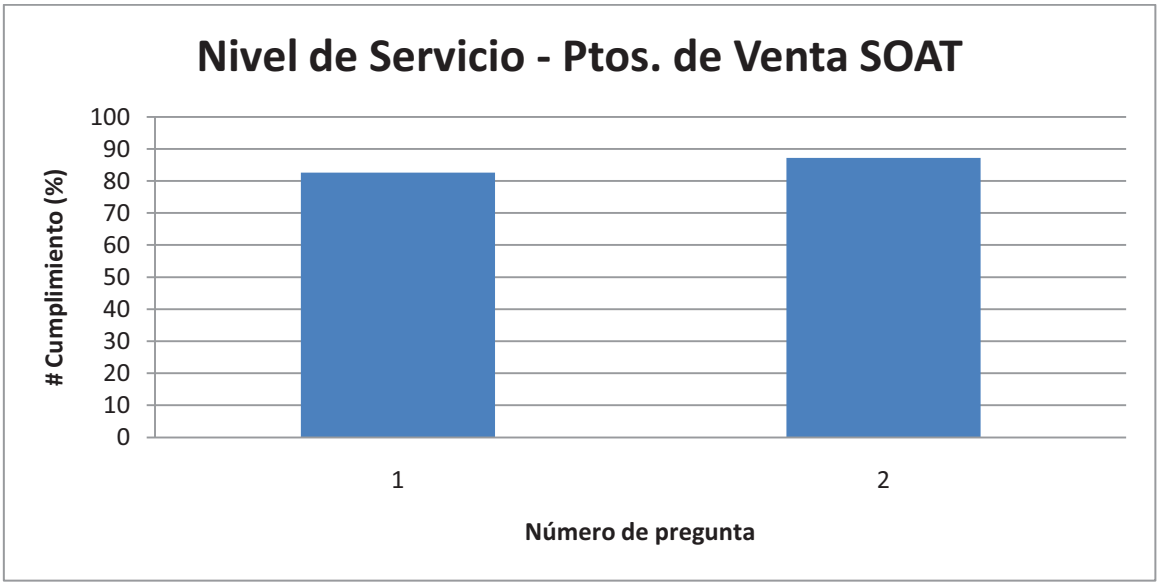

Figura 3-25: Gráfico de Cumplimiento - Gestión de Nivel de Servicio para Puntos de Venta SOAT

3.5.1.3 Recomendaciones

La Gestión de Nivel de Servicio para Puntos de Venta SOAT no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.5.2 GESTIÓN DE CONTINUIDAD DE SERVICIO

N.	PREGUNTAS	PTOS. DE VENTA	#Cumplimiento	Prob. de Amenaza
1	¿Ha sido notificado que procedimientos seguir en caso de emergencias, tales como el corte de energía eléctrica?, de parte de Alianza.	11,63	**11,63**	**0,88**
2	Disponibilidad del Sistema de SOAT.	49,13	**49,13**	**0,51**
		#Cumpl Promedio	**30,38**	

Tabla 3-51: Porcentaje de Cumplimiento - Gestión de Continuidad de Servicio para Puntos de Venta SOAT

3.5.2.1 Estados de Indicadores de Gestión de Continuidad de Servicio

Según la Tabla 3-52, se concluye que todos sus indicadores tienen un GC Bajo, es decir los Puntos de Venta SOAT no han sido informados de parte de Alianza de cómo proceder ante emergencias como el corte de suministro eléctrico, ya que esto implica que el sistema informático no podrá ser usado. Además este grupo de usuarios califica como no satisfactoria la disponibilidad que presenta actualmente el sistema SOAT.

En promedio la Gestión de Continuidad de Servicio realizada por Alianza, es calificada por los Puntos de Venta SOAT como no satisfactoria.

N.	#Cumplimiento	GC
1	11,63	B
2	49,13	B

Tabla 3-52: Grado de Confianza - Gestión de Continuidad de Servicio para Puntos de Venta SOAT

3.5.2.2 Gráfico de Cumplimiento de Gestión de Continuidad de Servicio

La figura 3-26, muestra que tanto la preparación frente a emergencias de parte de los Puntos de Venta SOAT y la disponibilidad percibida del Sistema está por debajo de un cumplimiento de 50.

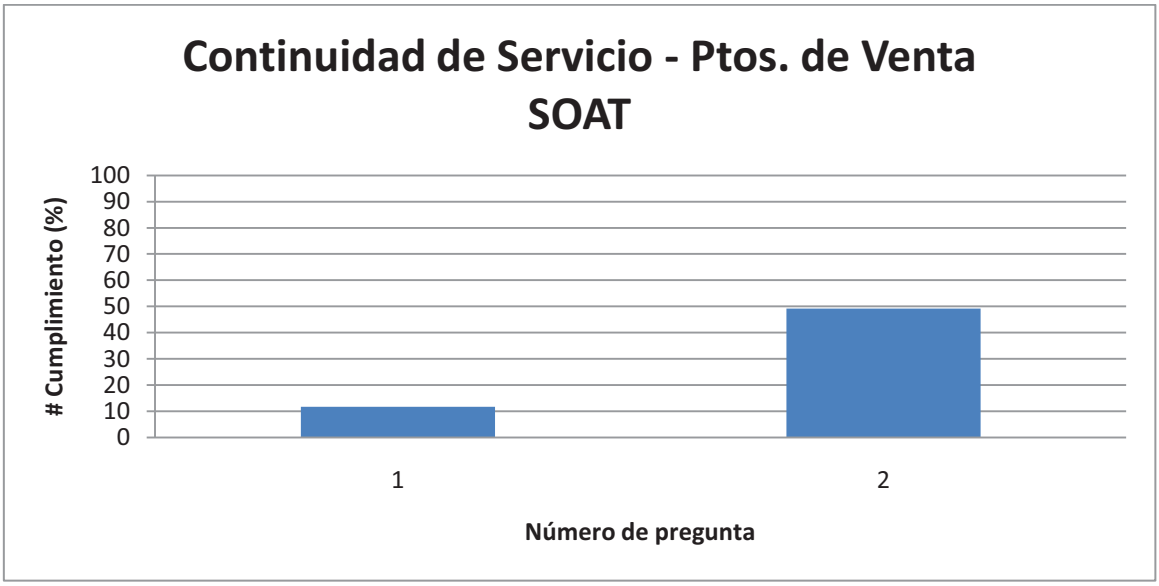

Figura 3-26: Gráfico de Cumplimiento - Gestión de Continuidad de Servicio para Puntos de Venta SOAT

3.5.2.3 Recomendaciones

Los usuarios en los Puntos de Venta SOAT, al igual que los usuarios internos de la empresa, en su mayoría (88.37%) no conocen que procedimientos seguir en caso de emergencias, según el ítem 1 de la encuesta "¿Ha sido notificado que procedimientos seguir en caso de emergencias, tales como el corte de energía eléctrica?, de parte de Alianza."

El DDS de Alianza, debe tomar en cuenta estos usuarios también para su capacitación en contra de eventos críticos.

Según el numeral 2 de la encuesta "Disponibilidad del Sistema de SOAT", en promedio el 50.87% de los usuarios en los Puntos de venta SOAT, sufren de caída del sistema por más de 3 horas a la semana. El equipo de Tecnología debe verificar en qué sucursales suceden la mayoría de problemas para dar solución y elevar el nivel de disponibilidad del Sistema de Seguros.

3.5.3 GESTIÓN DE CAMBIOS

N.	PREGUNTAS	PTOS. DE VENTA	#Cumplimiento	Prob. de Amenaza
1	¿En caso de la necesidad de un cambio para emisión de SOAT su solicitud es receptada por Alianza?	93,02	**93,02**	**0,07**
2	¿Es notificado cuándo se realizará un cambio que afecte a su entorno de trabajo con el SOAT?	52,33	**52,33**	**0,48**
3	¿Habitualmente los cambios realizados por Alianza lo han satisfecho?	81,40	**81,40**	**0,19**
		#Cumpl Promedio	**72,67**	

Tabla 3-53: Porcentaje de Cumplimiento - Gestión de Cambios para Puntos de Venta SOAT

3.5.3.1 Estados de Indicadores de Gestión de Cambios

Según la Tabla 3-54, el 33,3 % de sus indicadores posee un GC Moderado Bajo, es decir la notificación de cambios sobre el sistema SOAT, para que no afecte las actividades de los usuarios Puntos de Venta SOAT, es calificada por estos como no satisfactoria. El 66,6 % restante es Alto, lo que implica que los cambios realizados por Alianza son calificados como muy satisfactorios por los Puntos de Venta SOAT, así como la predisposición de Alianza para recibir solicitudes de cambios.

En promedio la Gestión de Cambios realizada por Alianza, es calificada como satisfactoria según los Puntos de Venta SOAT.

N.	#Cumplimiento	GC
2	52,33	MB
3	81,40	A
1	93,02	A

Tabla 3-54: Grado de Confianza - Gestión de Cambios para Puntos de Venta SOAT

3.5.3.2 Gráfico de Cumplimiento de Gestión de Cambios

La Figura 3-27, muestra indicadores con niveles superiores a 80 de cumplimiento son: apertura a recepción de cambios de parte de Alianza, y satisfacción de cambios realizados. Con cerca del 50 de cumplimiento y el más bajo indicador dentro de Gestión de Cambios, se encuentra la notificación de cuándo se realizará un cambio que pueda afectar el trabajo del usuario.

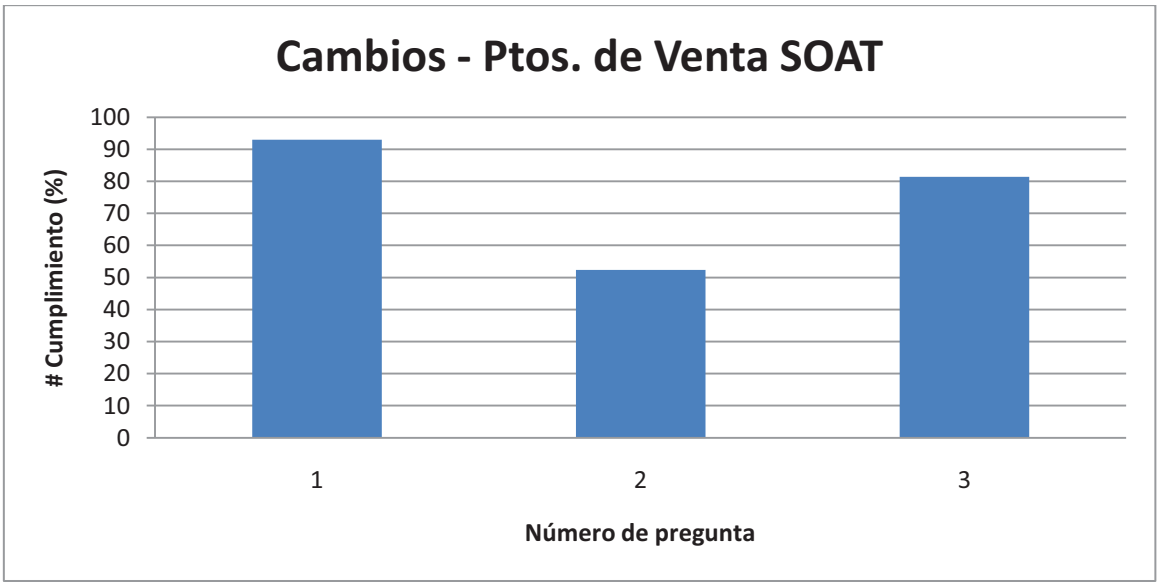

Figura 3-27: Gráfico de Cumplimiento - Gestión de Cambios para Puntos de Venta SOAT

3.5.3.3 Recomendaciones

La Gestión de Cambios para Puntos de Venta SOAT no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.5.4 GESTIÓN DE INCIDENTES

N.	PREGUNTAS	PTOS. DE VENTA	#Cumplimiento	Prob. de Amenaza
1	¿Son atendidas las sugerencias hechas a Alianza para mejorar el servicio de SOAT?	90,698	**90,70**	**0,09**
2	¿Recibe cursos o entrenamientos cuando existe la necesidad de manejar cambios del sistema SOAT?	74,42	**74,42**	**0,26**
3	¿En general el tiempo de solución a los incidentes de parte de Alianza ha sido satisfactorio?	86,05	**86,05**	**0,14**
4	¿Se repiten con frecuencia incidentes específicos?	65,12	**65,12**	**0,35**
5	Tiempo para dar solución a un incidente.	77,21	**77,21**	**0,23**
6	¿Cuál sería la calificación general para Alianza respecto a resolución de incidentes?	86,05	**86,05**	**0,14**
7	¿Con qué frecuencia su trabajo normal se ve afectado por problemas con el Sistema de SOAT?	93,02	**93,02**	**0,07**
		#Cumpl Promedio	**81,79**	

Tabla 3-55: Porcentaje de Cumplimiento - Gestión de Incidentes para Puntos de Venta SOAT

3.5.4.1 Estados de Indicadores de Gestión de Incidentes

La Tabla 3-56, muestra que el 14,3% de los indicadores tienen un GC Moderado Moderado, esto significa que se hace un estudio medianamente satisfactorio de los incidentes, porque existen incidentes específicos que se repiten medianamente.

De igual forma hay un 14,3% que es Moderado Alto, lo cual significa que los usuarios de los Puntos de Venta SOAT califican como satisfactorios los cursos y entrenamientos realizados por Alianza, que son necesarios cuando existe un cambio en el sistema SOAT.

Finalmente existe un 71,4 % con nivel Alto, lo que implica que ha sido muy satisfactorio: el tiempo de solución de incidentes, la atención de sugerencias para mejorar el servicio de SOAT, la frecuencia mínima de problemas con el sistema SOAT.

En promedio la Gestión de Incidentes realizada por Alianza es calificada como muy satisfactoria, según los Puntos de Venta SOAT.

N.	#Cumplimiento	GC
4	65,12	MM
2	74,42	MA
3	86,05	A
6	86,05	A
5	77,21	A
1	90,70	A
7	93,02	A

Tabla 3-56: Grado de Confianza - Gestión de Incidentes para Puntos de Venta SOAT

3.5.4.2 Gráfico de Cumplimiento de Gestión de Incidentes

Según la Figura 3-28, se observa que la Gestión de Incidentes de parte de Alianza según los Puntos de Venta SOAT, es bastante favorable con un cumplimiento de todos los indicadores mayor a 60. Donde su indicador más bajo se refiere a frecuencia de incidentes específicos, y el mejor calificado es la baja tasa de errores con el Sistema SOAT.

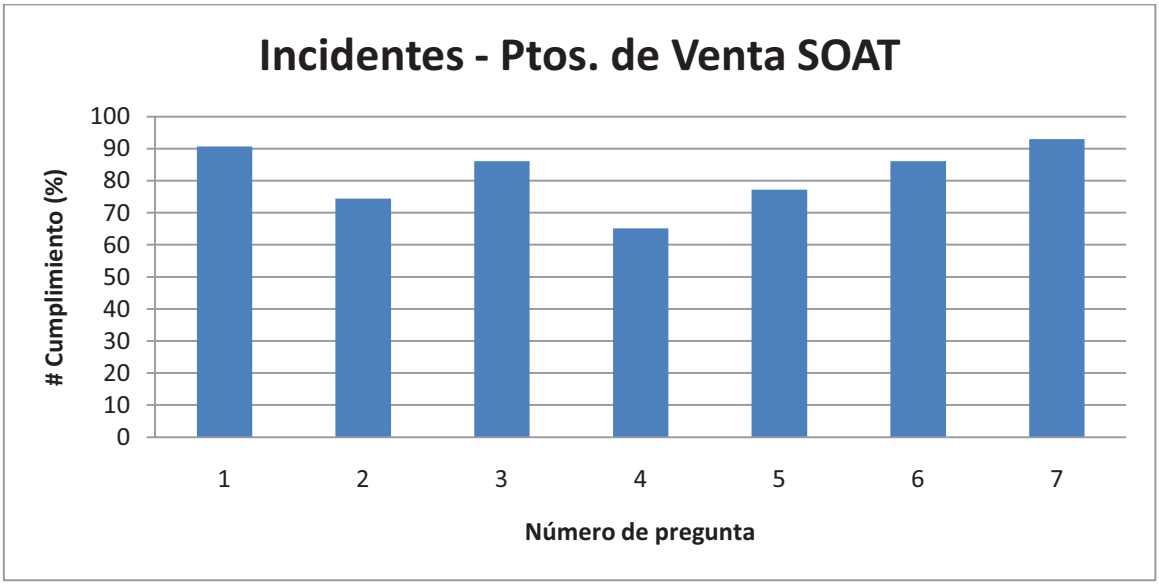

Figura 3-28: Gráfico de Cumplimiento - Gestión de Incidentes para Puntos de Venta SOAT

3.5.4.3 Recomendaciones

La Gestión de Incidentes para Puntos de Venta SOAT no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.5.5 GESTIÓN DE PROBLEMAS

N.	PREGUNTAS	PTOS. DE VENTA	# Cumplimiento	Prob de Amenaza
1	¿Su incidente trata de ser generalmente resuelto inmediatamente para restablecer sus actividades laborales?	90,70	**90,70**	**0,09**
2	¿Incidentes que ya han ocurrido antes son resueltos con mayor rapidez?	94,19	**94,19**	**0,06**
			#Cumpl Promedio	**92,44**

Tabla 3-57: Porcentaje de Cumplimiento - Gestión de Problemas para Puntos de Venta SOAT

3.5.5.1 Estados de Indicadores de Gestión de Problemas

La Tabla 3-58, muestra que el 100% de sus indicadores poseen un GC Alto o muy satisfactorio, lo que implica que los usuarios de los Puntos de Venta SOAT, reconocen que el DDS hace una diferenciación de prioridades para solucionar problemas e incidentes, dando como resultado que las actividades laborales sean restablecidas inmediatamente. Además este grupo de usuarios, ve que el DDS ha hecho un estudio de los problemas que han causado ciertos incidentes, provocando que incidentes ya ocurridos se solucionen con mayor rapidez.

N.	#Cumplimiento	GC
1	90,70	A
2	94,19	A

Tabla 3-58: Grado de Confianza - Gestión de Problemas para Puntos de Venta SOAT

3.5.5.2 Gráfico de Cumplimiento de Gestión de Problemas

La Figura 3-29, resalta que sus dos ítems tienen un cumplimiento mayor a 90, es decir los Puntos de Venta SOAT perciben que sus incidentes tratan de ser resueltos inmediatamente y se resuelven con mayor rapidez incidentes ya ocurridos.

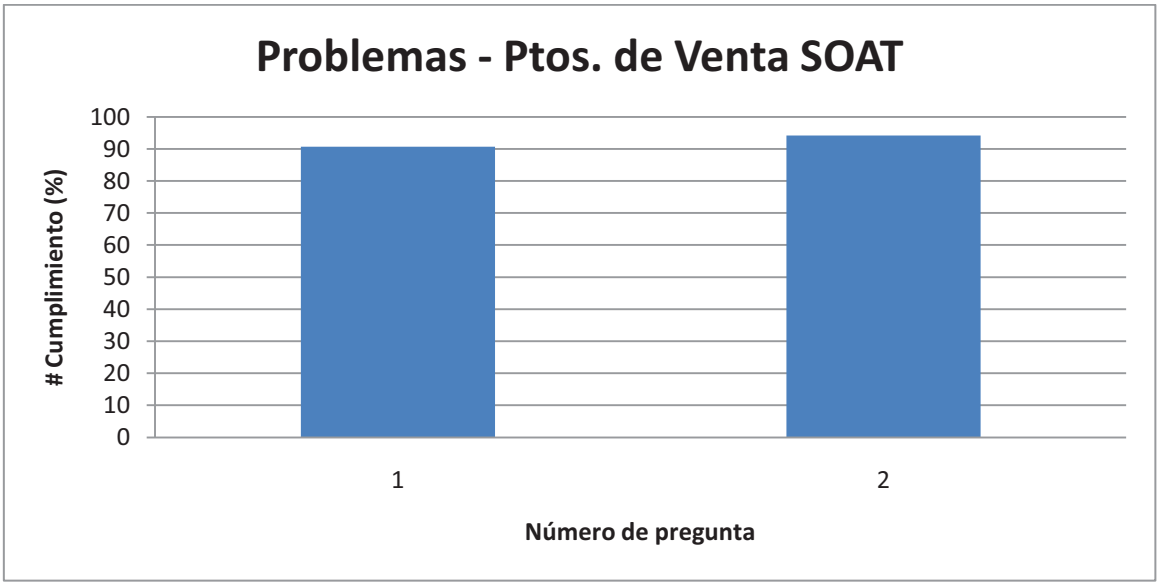

Figura 3-29: Gráfico de Cumplimiento - Gestión de Problemas para Puntos de Venta SOAT

3.5.5.3 Recomendaciones

La Gestión de Problemas para Puntos de Venta SOAT no posee indicadores con GC Bajo, por lo tanto no se registran sugerencias.

3.6 ANÁLISIS DE RIESGOS

A continuación se presentan las tablas con los resultados del Análisis de Riesgos, para todos los involucrados. Para conocer el origen de los impactos insertados, se elaboró un ejemplo con los análisis realizados para llegar a la matriz de impactos, ver Anexo 3-1.

3.6.1 EJECUTIVOS[40]

El grupo de Ejecutivos presenta los siguientes resultados, con respecto al Análisis de Riesgos.

3.6.1.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.	3	3	1	2	3	2,4	1,00	2,40
2	No entrega de documentación formal que informe los servicios que provee el DDS.	3	3	1	2	3	2,4	1,00	2,40
3	Baja calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.	4	4	1	4	4	3,4	0,00	0,00
4	Falta de apoyo a proyectos que mejoren el nivel de servicio que provee el DDS.	5	4	1	4	5	3,8	0,00	0,00
5	Falta de cumplimiento de la calidad del Servicio de Sistema Empresarial	4	5	2	4	4	3,8	0,00	0,00
6	Falta de cumplimiento de la calidad del Servicio de Internet	4	5	2	4	4	3,8	0,17	0,63
7	Falta de cumplimiento de la calidad del Servicio de Correo	4	5	2	4	4	3,8	0,17	0,63
8	Falta de cumplimiento de la calidad del Servicio de Videoconferencia	3	3	1	3	2	2,4	0,50	1,20

[40] Los niveles de impacto fueron analizados en conjunto con la Ejecutiva de Cuenta Paola Pérez.

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
9	Falta de cumplimiento de la calidad del Servicio de Soporte	4	4	1	4	4	3,4	0,00	0,00
10	Falta de cumplimiento de la calidad del Servicio de Asesoría	4	4	1	4	4	3,4	0,00	0,00
11	Falta de cumplimiento de la calidad del Servicio de Capacitación	4	4	1	3	3	3,0	0,25	0,75
12	Falta de cumplimiento de la calidad del Servicio de Desarrollo	4	4	1	4	4	3,4	0,00	0,00
13	Falta de cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros	3	4	1	3	3	2,8	0,50	1,40
								PROMEDIO	**0,724**

Tabla 3-59: Resultados Matriz de Riesgos - Gestión de Nivel de Servicio para Ejecutivos

3.6.1.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apoyo para el desarrollo de planes de contingencia que aseguren la continuidad del servicio en épocas de emergencia.	5	5	4	4	5	4,6	0,00	0,00
2	Falta de preparación frente la emergencias de corte de suministro eléctrico	5	5	2	4	5	4,2	0,16	0,70
3	Falta de preparación frente la emergencias de corte de Internet	5	5	2	4	5	4,2	1,00	4,20
4	Falta de preparación frente a emergencias de virus	4	4	1	3	4	3,2	0,50	1,60
5	Tiempo extendido en estado de emergencia por corte de suministro eléctrico.	5	5	2	5	5	4,4	0,94	4,13

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
6	Tiempo extendido en estado de emergencia por corte de Internet.	5	5	2	5	5	4,4	0,94	4,13
7	Tiempo extendido en estado de emergencia por virus.	4	4	1	3	4	3,2	0,94	3,00
8	Falta de disponibilidad del Sistema de Seguros.	5	5	3	5	5	4,6	0,00	0,00
								PROMEDIO	**2,219**

Tabla 3-60: Resultados Matriz de Riesgos - Gestión de Continuidad de Servicio para Ejecutivos

3.6.1.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios de software o hardware de parte del DDS.	5	5	2	4	4	4,0	0,00	0,00
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.	5	5	2	5	5	4,0	0,00	0,00
3	Baja frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.	4	3	2	4	4	3,4	0,00	0,00
4	Alta frecuencia de cambios realizados por el DDS que tengan como objetivo modificaciones o correcciones.	4	4	2	4	4	3,6	0,00	0,00
5	Bajo Nivel de satisfacción de los cambios realizados por el DDS.	4	4	2	4	4	3,6	0,00	0,00
6	Falta de método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.	3	3	2	2	3	2,6	1,00	2,60
7	Falta de indicadores que muestren el éxito en la implementación de cambios de parte del DDS a lo largo del 2009.	4	3	2	2	4	3,0	1,00	3,00
8	Bajo porcentaje de cambios implementados frente a los solicitados	3	3	2	3	3	2,8	0,00	0,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
9	Número elevado de cambios que no le han sido notificados y han afectado el desenvolvimiento normal de su trabajo	5	5	2	5	5	4,4	0,00	0,00
								PROMEDIO	**0,622**

Tabla 3-61: Resultados Matriz de Riesgos - Gestión de Cambios para Ejecutivos

3.6.1.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No realización de configuraciones de forma metódica y ordenadamente por el DDS .	4	4	2	4	4	3,6	1,00	3,60
2	Falta de apoyo a proyectos que tengan como objetivo la automatización de configuración de equipos.	5	4	1	4	4	3,6	0,00	0,00
								PROMEDIO	**1,800**

Tabla 3-62: Resultados Matriz de Riesgos - Gestión de Configuraciones para Ejecutivos

3.6.1.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apoyo a proyectos que mejoren el servicio prestado por las tecnologías de Información.	5	4	1	4	5	3,8	0,00	0,00
2	Falta de un método de Gestión de incidentes.	4	4	2	3	4	3,4	0,53	1,81
3	Falta de notificación de posibles amenazas tecnológicas.	4	3	1	2	3	2,6	0,33	0,87
4	Alta frecuencia de incidentes que afectan el normal desempeño de su trabajo.	5	5	2	5	5	4,4	0,33	1,47

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
5	Falta de satisfacción de los recursos tecnológicos asignados.	4	3	1	2	2	2,4	0,50	1,20
6	Falta de evolución de la tecnología en la empresa.	4	3	1	2	3	2,6	0,00	0,00
7	Falta de apertura del DDS para recibir sugerencias.	4	4	2	3	4	3,4	0,00	0,00
8	Falta de capacitación a los usuarios de parte del DDS.	4	4	2	4	4	3,6	0,17	0,60
9	No satisfacción del usuario frente al tiempo de solución de incidentes.	4	3	2	4	4	3,4	0,00	0,00
10	Alta frecuencia de incidentes específicos.	4	4	2	4	4	3,6	0,17	0,60
11	Falta de método de calificación del servicio recibido de parte del DDS.	3	2	1	2	3	2,2	1,00	2,20
12	Tiempo prolongado para dar solución a un incidente	4	4	3	4	4	3,8	0,00	0,00
13	Baja calificación general para el DDS respecto a resolución de incidentes.	4	4	1	4	4	3,4	0,00	0,00
								PROMEDIO	**0,673**

Tabla 3-63: Resultados Matriz de Riesgos - Gestión de Incidentes para Ejecutivos

3.6.1.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.	5	5	2	5	5	4,4	0,00	0,00
2	Falta de apoyo a desarrollar un equipo especialista para resolver problemas de TI.	3	3	1	2	3	2,4	0,00	0,00
3	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.	5	5	2	5	5	4,4	0,00	0,00
								PROMEDIO	**0,000**

Tabla 3-64: Resultados Matriz de Riesgos - Gestión de Problemas para Ejecutivos

3.6.2 GERENTE DE SISTEMAS[41]

El grupo de Gerente de Sistemas presenta los siguientes resultados, con respecto al Análisis de Riesgos.

3.6.2.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de monitoreo del Servicio de Internet recibido	5	2	1	2	5	3,0	0,50	1,50
2	Falta de monitoreo del Servicio de Internet suministrado	5	2	1	2	5	3,0	0,50	1,50
3	Falta de monitoreo de enlaces WAN	5	2	1	2	5	3,0	0,50	1,50
4	Falta de historial del servicio de Internet recibido.	5	2	1	2	5	3,0	1,00	3,00
5	Falta de historial de la calidad de enlaces WAN.	5	2	1	2	5	3,0	1,00	3,00
6	Falta de historial de la calidad de los servicios suministrados.	5	3	1	2	5	3,2	1,00	3,20
7	Falta de Contratos formales de nivel de servicio.	5	4	1	2	5	3,4	0,30	1,12
8	No especificación del nivel de servicio para los usuarios de la red corporativa.	5	4	1	2	5	3,4	1,00	3,40
9	No Identificación de necesidades para implementar un servicio.	5	5	1	2	5	3,6	0,00	0,00
10	Falta de Indicadores para identificar desempeño de proveedores de tecnología.	5	3	1	2	5	3,2	1,00	3,20
11	Vía de comunicación con proveedores externos, no efectiva.	5	4	1	2	5	3,4	0,50	1,70
12	Vía de comunicación entre los usuarios y el DDS, no efectiva.	5	4	1	2	5	3,4	0,50	1,70
13	Falta de Mejoramiento de servicios basados en monitoreo.	4	4	1	2	4	3,0	1,00	3,00
14	Baja disponibilidad de los servicios que provee el DDS.	5	4	1	2	5	3,4	0,00	0,00
15	Falta de monitoreo de nivel de calidad de los servicios que provee el DDS.	5	4	1	2	5	3,4	1,00	3,40

[41] Los niveles de impacto fueron analizados en conjunto con el Gerente de Sistemas Ing. Pablo Herrera.

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
16	Bajo cumplimiento del Nivel de Servicio de servicios suministrados.	5	4	1	2	5	3,4	1,00	3,40
17	Falta de monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.	5	4	1	2	5	3,4	1,00	3,40
18	Falta de un encargado para manejar los niveles de servicio de la organización.	4	4	1	2	4	3,0	1,00	3,00
19	No deficnición formal de la calidad de los servicios que provee el DDS.	4	4	1	2	4	3,0	1,00	3,00
20	No conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.	3	2	1	2	3	2,2	1,00	2,20
21	Falta de revisión de los niveles de servicio de lo suministrado y de proveedores externos.	5	4	1	2	5	3,4	1,00	3,40
								PROMEDIO	**2,363**

Tabla 3-65: Resultados Matriz de Riesgos - Gestión de Nivel de Servicio para Gerente de Sistemas

3.6.2.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.	5	4	2	2	5	3,6	0,50	1,80
2	Falta de desarrollado formal de planes de respuesta ante una emergencia.	5	4	2	2	5	3,6	0,50	1,80
3	Falta de desarrollado de un plan en caso de falla para equipos o sistemas.	5	4	2	2	5	3,6	0,50	1,80
4	Falta de un lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.	5	4	2	2	5	3,6	0,50	1,80
5	Falta de evaluación de planes de respuesta ante emergencias o recuperación antes de ser puestos en marcha.	5	4	2	2	5	3,6	0,50	1,80
6	No revisión de los planes de emergencia ya desarrollados.	5	4	2	2	5	3,6	0,25	0,90

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
7	Falta de entrenamiento del DDS para utilizar correctamente los planes de emergencia.	5	4	2	2	5	3,6	0,50	1,80
8	Falta de análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización.	5	4	2	2	5	3,6	1,00	3,60
9	Tiempo prolongado en solución de catátrofes.	5	4	4	4	5	4,4	1,00	4,40
								PROMEDIO	**2,189**

Tabla 3-66: Resultados Matriz de Riesgos - Gestión de Continuidad de Servicio para Gerente de Sistemas

3.6.2.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de revisión a los últimos cambios realizados para solucionar incidentes.	4	2	1	2	4	2,6	0,50	1,30
2	Falta de análisis de riegos sobre las implicaciones que podría producir un cambio propuesto.	5	2	1	2	5	3,0	1,00	3,00
3	No tomar en cuenta los posibles incidentes que producirá la ejecución del cambio.	5	3	1	2	5	3,2	0,00	0,00
4	Baja frecuencia de cambios realizados que tengan como objetivo innovación y mejoramiento.	4	2	1	2	4	2,6	0,00	0,00
5	Alta frecuencia de cambios realizados que tengan como objetivo modificaciones o correcciones.	4	3	1	3	4	3,0	1,00	3,00
6	Independencia entre manejo de cambios y configuraciones.	5	2	1	2	4	2,8	1,00	2,80
7	No definir las ventajas de realizar el cambio en cada petición.	4	2	1	2	4	2,6	1,00	2,60
8	No coordinar cada cambio con los departamentos que serán afectados.	5	3	1	3	5	3,4	0,00	0,00
9	La planificación de un cambio no es pública ni notificada al personal de la organización.	4	2	1	2	4	2,6	0,50	1,30

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
10	No registro de todos los cambios realizados sobre un dispositivo específico.	5	2	1	2	4	2,8	1,00	2,80
11	No existencia de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.	5	2	1	2	5	3,0	1,00	3,00
12	No registro de cada detalle del ciclo de vida del cambio.	4	2	1	2	4	2,6	1,00	2,60
13	No registro del manejo de cambios en el sistema de manejo de configuraciones.	5	2	1	2	4	2,8	1,00	2,80
14	Falta de un filtro de condiciones predeterminadas antes de la aprobación de un cambio.	5	2	1	2	5	3,0	0,50	1,50
15	No identificación de los recursos necesarios antes de la realización de un cambio.	5	3	1	2	5	3,2	0,50	1,60
16	Falta de evaluación al finalizar el ciclo de un proceso de cambio.	5	2	1	2	5	3,0	0,50	1,50
17	Registro como un pedido de cambio a los cambios estándar de rutina.	4	2	1	2	5	2,8	0,50	1,40
18	No registro del responsable de la petición de cambio.	5	3	1	2	4	3,0	0,50	1,50
19	No identificación de la razón para realizar el cambio.	5	3	1	2	5	3,2	0,50	1,60
20	No existencia de recalificación de pedido de cambios en caso de ser negados en primera instancia.	4	2	1	2	4	2,6	1,00	2,60
21	Falta de análisis financiero durante la planeación de un cambio.	5	3	1	2	5	3,2	1,00	3,20
22	No realización de pruebas piloto antes de la implementación de un cambio.	5	3	1	2	5	3,2	0,50	1,60
23	No comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.	5	2	1	2	5	3,0	0,50	1,50
24	No comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.	5	3	1	3	4	3,2	0,00	0,00
25	No registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.	5	2	1	2	5	3,0	0,00	0,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
26	No comprobación de cumplimiento de costos al finalizar la implementación de un cambio.	5	2	1	3	5	3,2	1,00	3,20
27	No comprobación del cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.	5	2	1	3	5	3,2	0,50	1,60
28	Falta de documentación del proceso de evaluación post implementación de cambios.	5	2	1	2	5	3,0	1,00	3,00
29	El encargado de la administración de problemas no participa en la administración de cambios.	5	2	1	2	5	3,0	0,50	1,50
30	El encargado de la administración de incidentes participa en la administración de cambios.	3	2	1	2	3	2,2	0,50	1,10
31	Bajo número de cambios solicitados registrados automáticamente.	4	2	1	2	4	2,6	1,00	2,60
32	Bajo número de cambios realizados frente a los solicitados.	4	3	1	3	4	3,0	0,00	0,00
33	Alto número de cambios realizados con carácter de emergencia frente al total de realizados.	5	3	1	3	5	3,4	0,50	1,70
34	Alto número de cambios realizados sin éxito frente al total de realizados.	5	4	1	4	5	3,8	0,60	2,28
35	Falta de identificación de mejoras en servicios gracias a la realización de cambios.	5	2	1	2	5	3,0	1,00	3,00
36	Falta de un método para registro de Cambios.	5	2	1	2	5	3,0	0,75	2,25
								PROMEDIO	**1,818**

Tabla 3-67: Resultados Matriz de Riesgos - Gestión de Cambios para Gerente de Sistemas

3.6.2.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.	5	2	1	1	5	2,8	1,00	2,80

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
2	Registro no apropiado de los cambios en el manejo de configuraciones de parte del encargado.	5	2	1	1	5	2,8	0,00	0,00
3	Falta de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.	4	2	1	1	4	2,4	0,00	0,00
4	Falta de documentación de cada equipo configurable con sus características propias.	4	2	1	1	4	2,4	1,00	2,40
5	Falta de levantamiento de procesos para recuperación de desastres de cada equipo configurable.	5	2	1	1	5	2,8	1,00	2,80
6	Falta de cálculo del nivel de perjuicio que puede causar la falta de o falla de cada equipo configurable.	4	2	1	1	4	2,4	1,00	2,40
7	Falta de acceso a todo el ciclo de vida de configuraciones de un equipo específico.	4	2	1	1	4	2,4	1,00	2,40
8	No registro de cada equipo configurable con su estado actual.	5	2	1	1	5	2,8	1,00	2,80
9	Ninigún registro de cada equipo configurable posee atributos que lo relacionen con manejo de cambios, problemas e incidentes.	4	2	1	1	4	2,4	1,00	2,40
10	No toma en cuenta los datos del manejo de configuraciones para el desarrollo de software de la organización.	5	3	1	1	5	3,0	1,00	3,00
11	Falta de relación de manejo de configuraciones con el manejo de cambios.	5	2	1	1	4	2,6	1,00	2,60
12	No documentación de los detalles de verificación al cierre de una configuración.	5	2	1	1	5	2,8	1,00	2,80
13	Falta de un responsable o ejecutor para cada configuración registrada.	5	2	1	1	5	2,8	1,00	2,80
14	No realización de una planificación previa a la implementación de una configuración.	5	3	1	1	5	3,0	1,00	3,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
15	Falta de control del correcto funcionamiento al finalizar la configuración de un ítem.	5	3	1	1	5	3,0	1,00	3,00
16	Falta de evaluación antes del registro de cada configuración.	5	2	1	1	5	2,8	1,00	2,80
17	Falta de identificación concreta de los ítems configurables para cada configuración registrada.	5	3	1	1	5	3,0	1,00	3,00
18	No registro de versión de cada ítem configurable.	4	2	1	1	4	2,4	1,00	2,40
19	Bajo número de configuraciones realizadas frente a las solicitadas.	4	3	1	3	4	3,0	1,00	3,00
20	Falta de un método de registro de Configuraciones.	5	2	1	1	5	2,8	1,00	2,80
21	Alto número de configuraciones realizadas sin éxito frente al total de realizadas.	5	4	1	4	5	3,8	x	x
22	Alto número de configuraciones realizadas sin autorización.	5	4	1	4	5	3,8	x	x
23	Alto número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.	5	3	1	3	5	3,4	x	x
24	No identificación de servicios que han tenido mejora gracias a configuraciones en la organización.	5	2	1	1	5	2,8	x	x
								PROMEDIO	**2,460**

Tabla 3-68: Resultados Matriz de Riesgos - Gestión de Configuraciones para Gerente de Sistemas

3.6.2.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No toma en cuenta personal que de soporte (resuelva incidentes), cuando existen proyectos no cotidianos.	5	3	1	2	5	3,2	0,50	1,60

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
2	No utiliza un escalamiento de solución para resolver incidentes de usuario.	5	2	1	1	5	2,8	0,50	1,40
3	Falta de conocimiento del estado actual de incidentes abiertos.	5	2	1	2	5	3,0	0,50	1,50
4	Falta de conocimiento del número de incidentes que se encuentran abiertos.	5	2	1	1	5	2,8	0,00	0,00
5	Falta de conocimiento de quién es el responsable de la solución y cierre de un incidente abierto.	5	2	1	2	5	3,0	0,50	1,50
6	Falta de conocimiento de quienes son los usuarios que mantienen incidentes sin resolver.	5	2	1	2	5	3,0	0,00	0,00
7	Falta de conocimiento de tiempo de respuesta y solución para un incidente específico.	4	2	1	1	4	2,4	0,00	0,00
8	Falta de acceso a la bitácora de cambios que se relacionan con un incidente específico.	4	2	1	1	4	2,4	1,00	2,40
9	No proveer un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.	5	3	1	2	5	3,2	0,00	0,00
10	No informar al usuario sobre el escalamiento de su incidente.	4	2	1	1	4	2,4	1,00	2,40
11	No informar al usuario sobre el cierre del incidente.	4	2	1	1	4	2,4	0,50	1,20
12	No agrupación de incidentes por su naturaleza.	4	2	1	1	4	2,4	1,00	2,40
13	No agrupación de incidentes por su solución tipo.	4	2	1	1	4	2,4	1,00	2,40
14	No resolución de incidentes tomando en cuenta un banco de soluciones.	5	2	1	1	5	2,8	0,50	1,40
15	Falta de respaldos de la configuración del sistema y equipos para realizar una restauración al estado anterior de los mismos.	5	2	1	1	5	2,8	0,50	1,40
16	Falta de registro de los detalles del cierre de incidentes.	5	2	1	1	5	2,8	0,50	1,40
17	No registro de los niveles de satisfacción del usuario luego del cierre de un incidente.	4	2	1	1	4	2,4	1,00	2,40

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
18	Falta de un lineamiento específico para que los usuarios realicen un pedido de servicio.	5	2	1	1	5	2,8	0,00	0,00
19	No identificación de los incidentes críticos para su empresa.	5	3	1	1	5	3,0	0,50	1,50
20	No poseer procesos de manejo propios para cada incidente crítico.	5	3	1	1	5	3,0	0,50	1,50
21	No registrar de cada incidente abierto el nombre del técnico que lo recibió.	5	2	1	1	5	2,8	1,00	2,80
22	Tiempo prolongado en resolver incidentes.	5	3	1	2	5	3,2	0,00	0,00
23	Baja frecuencia en la realización de actualizaciones de software.	4	2	1	1	4	2,4	0,00	0,00
24	Baja frecuencia en la realización de actualizaciones de hardware.	4	2	1	1	4	2,4	0,00	0,00
25	Bajo porcentaje de incidentes que se han resuelto en el tiempo esperado.	5	3	1	2	5	3,2	0,50	1,60
26	Alto porcentaje de incidentes que han sido reabiertos del total en un periodo específico.	4	3	1	2	4	2,8	0,05	0,14
27	Bajo porcentaje de incidentes resueltos sin la necesidad de una visita.	3	2	1	1	3	2,0	0,10	0,20
28	Falta de Método para registro de Incidentes.	5	2	1	1	5	2,8	0,70	1,96
								PROMEDIO	**1,182**

Tabla 3-69: Resultados Matriz de Riesgos - Gestión de Incidentes para Gerente de Sistemas

3.6.2.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No diferenciación entre problemas e incidentes.	5	2	1	2	4	2,8	0,50	1,40
2	No tomar en cuenta como base para la resolución de incidentes, la administración de problemas.	5	2	1	2	4	2,8	1,00	2,80
3	Resolución de problemas antes de los incidentes en su organización.	5	3	1	3	4	3,2	1,00	3,20

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
4	No usar como apoyo a la continuidad del servicio el manejo de problemas.	5	2	1	2	5	3,0	0,00	0,00
5	No existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.	5	2	1	2	4	2,8	1,00	2,80
6	No poseer un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT.	4	2	1	2	4	2,6	1,00	2,60
7	No mantener la infraestructura de comunicaciones sincronizada en tiempo con un reloj interno directamente del servidor NTP de la compañía.	4	2	1	2	4	2,6	0,00	0,00
8	No identificación concreta de las entradas para el proceso de resolución de problemas.	5	2	1	2	5	3,0	1,00	3,00
9	No registro de las salidas del proceso de resolución de problemas.	5	2	1	2	5	3,0	1,00	3,00
10	No apoyo de la resolución de problemas en la base de datos de administración de problemas.	5	2	1	2	4	2,8	1,00	2,80
11	Falta de conocimiento de los problemas cerrados en un periodo de tiempo específico.	5	2	1	3	5	3,2	1,00	3,20
12	Falta de conocimiento concreto del estado de un problema.	5	2	1	3	5	3,2	0,00	0,00
13	Mala coordinación entre administración de problemas y la de cambios.	5	2	1	3	5	3,2	0,00	0,00
14	Objetivos no diferenciados entre problemas e incidentes.	5	2	1	2	4	2,8	0,50	1,40
15	Falta de personal designado para investigación especializada de problemas.	4	2	1	2	4	2,6	1,00	2,60
16	No registro de la o las acciones intuitivas que han mitigado un problema.	5	2	1	2	5	3,0	1,00	3,00
17	Cierre del problema cuando ejecuta una acción intuitiva que atenúa el problema.	5	3	1	3	5	3,4	0,50	1,70
18	No registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.	5	2	1	2	5	3,0	0,50	1,50
19	Soluciona problemas sin apoyo en la base de datos de errores conocidos.	5	3	1	2	4	3,0	1,00	3,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
20	Falta de revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.	5	3	1	3	5	3,4	0,50	1,70
21	Falta de revisión de los procedimientos erróneos, luego del suceso de un error crítico.	5	3	1	3	5	3,4	0,50	1,70
22	Falta de revisión de que se puede mejorar en el futuro, luego del suceso de un error crítico.	5	3	1	3	5	3,4	0,50	1,70
23	Falta de análisis de qué se puede hacer para que no suceda otra vez un suceso de un error crítico, luego de sucedido.	5	3	1	3	5	3,4	0,50	1,70
24	Falta de análisis si la responsabilidad del hecho era de una empresa proveedora de servicios, luego del suceso de un error crítico.	5	2	1	2	5	3,0	0,50	1,50
25	Falta de acciones inmediantas en caso de que un problema crítico sea responsabilidad de una empresa proveedora.	5	2	1	2	5	3,0	0,00	0,00
26	Falta de registro de datos de retroalimentación respecto a problemas críticos.	5	2	1	2	5	3,0	1,00	3,00
27	Falta de Método para registro de problemas.	5	2	1	2	5	3,0	0,75	2,25
28	Bajo número de problemas resueltos frente a los registrados.	5	5	2	4	5	4,2	0,15	0,63
29	Bajo porcentaje de problemas que se han resuelto en el tiempo esperado.	5	5	3	4	5	4,4	0,88	3,88
30	Alta tendencia a que se incrementen los problemas críticos.	5	5	4	4	5	4,6	0,00	0,00
								PROMEDIO	**1,869**

Tabla 3-70: Resultados Matriz de Riesgos - Gestión de Problemas para Gerente de Sistemas

3.6.3 OPERADOR DEL DEPARTAMENTO DE SISTEMAS[42]

El grupo de Operador del DDS presenta los siguientes resultados, con respecto al Análisis de Riesgos.

3.6.3.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de historial del servicio de Internet	5	2	1	2	5	3,0	0,67	2,00
2	Falta de Indicadores para identificar desempeño de proveedores de tecnología.	5	3	1	2	5	3,2	0,67	2,13
3	Falta de conocimiento del nivel de servicio que los usuarios de la organización deben recibir.	5	4	1	2	5	3,4	0,67	2,27
4	Vía de comunicación con proveedores externos, no efectiva.	5	4	1	2	5	3,4	1,00	3,40
5	Vía de comunicación entre los usuarios y el DDS, no efectiva.	5	4	1	2	5	3,4	0,33	1,13
6	Falta de conocimiento de qué servicios ofrece el DDS a la organización	4	4	1	2	4	3,0	0,33	1,00
7	Falta de monitoreo de nivel de calidad de los servicios que se reciben de proveedores externos.	5	4	1	2	5	3,4	0,48	1,63
8	Falta de monitoreo de nivel de calidad de los servicios que provee el DDS.	5	4	1	2	5	3,4	0,67	2,27
9	No deficnición formal de la calidad de los servicios que provee el DDS.	4	4	1	2	4	3,0	1,00	3,00
10	No conocimiento del nivel de satisfacción del usuario respecto a los servicios que provee el DDS.	3	2	1	2	3	2,2	0,83	1,83
								Promedio	**2,066**

Tabla 3-71: Resultados Matriz de Riesgos - Gestión de Nivel de Servicio para Operadores del DDS

[42] Los niveles de impacto fueron analizados en conjunto con el Gerente de Sistemas Ing. Pablo Herrera y el Operario del DDS Ing. Juan Guamba.

3.6.3.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.	5	4	2	2	5	3,6	1,00	3,60
2	Falta de entrenamiento del DDS para utilizar correctamente los planes de emergencia.	5	4	2	2	5	3,6	X	X
3	Falta de desarrollado de un plan en caso de falla para equipos o sistemas.	5	4	2	2	5	3,6	0,78	2,80
4	Falta de un lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.	5	4	2	2	5	3,6	0,67	2,40
5	Tiempo prolongado en solución de catástrofes.	5	4	4	4	5	4,4	0,96	4,22
								Promedio	**3,254**

Tabla 3-72: Resultados Matriz de Riesgos - Gestión de Continuidad de Servicio para Operadores del DDS

3.6.3.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de revisión a los últimos cambios realizados para solucionar incidentes.	4	2	1	2	4	2,6	0,17	0,43
2	No registro de cambios que se realizaron sobre un dispositivo específico.	5	2	1	2	4	2,8	0,33	0,93
3	No tomar en cuenta los posibles incidentes que producirá la ejecución del cambio.	5	3	1	2	5	3,2	0,33	1,07
4	Baja frecuencia de cambios realizados que tengan como objetivo innovación y mejoramiento.	4	2	1	2	4	2,6	0,17	0,43
5	Alta frecuencia de cambios realizados que tengan como objetivo modificaciones o correcciones.	4	3	1	3	4	3,0	0,50	1,50
6	No existencia de procesos modelos para afrontar cambios que se repiten o son comunes para la organización.	5	2	1	2	5	3,0	0,67	2,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
7	No identificación de los recursos necesarios antes de la realización de un cambio.	5	3	1	2	5	3,2	0,50	1,60
8	Falta de evaluación al finalizar el ciclo de un proceso de cambio.	5	2	1	2	5	3,0	0,33	1,00
9	No identificación de la razón para realizar el cambio.	5	3	1	2	5	3,2	0,33	1,07
10	No realización de pruebas piloto antes de la implementación de un cambio.	5	3	1	2	5	3,2	0,17	0,53
11	No comprobación de cumplimiento de objetivos al finalizar la implementación de un cambio.	5	2	1	2	5	3,0	0,17	0,50
12	No comprobación de la satisfacción de los involucrados al finalizar la implementación de un cambio.	5	3	1	3	4	3,2	0,00	0,00
13	No registro de los eventos no planificados que tuvieron efectos negativos sobre la organización al finalizar la implementación de un cambio.	5	2	1	2	5	3,0	0,83	2,50
14	No comprobación del cumplimiento de tiempos de ejecución al finalizar la implementación de un cambio.	5	2	1	3	5	3,2	0,83	2,67
15	Falta de un método para registro de Cambios.	5	2	1	2	5	3,0	0,79	2,38
16	Bajo número de cambios realizados frente a los solicitados.	4	3	1	3	4	3,0	0,13	0,40
17	Bajo número de cambios solicitados registrados.	4	2	1	2	4	2,6	0,20	0,52
18	Alto número de cambios realizados sin éxito frente al total de realizados.	5	4	1	4	5	3,8	0,00	0,00
19	Alto número de cambios realizados con carácter de emergencia frente al total de realizados.	5	3	1	3	5	3,4	0,17	0,57
20	Falta de identificación de mejoras en servicios gracias a la realización de cambios.	5	2	1	2	5	3,0	0,50	1,50
								Promedio	**1,080**

Tabla 3-73: Resultados Matriz de Riesgos - Gestión de Cambios para Operadores del DDS

3.6.3.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de una bitácora actualizada con la información de la infraestructura de comunicaciones de la organización.	5	2	1	1	5	2,8	0,33	0,93
2	Registro no apropiado de los cambios en el manejo de configuraciones.	5	2	1	1	5	2,8	0,00	0,00
3	Falta de un mapa con la topología de los elementos configurables de la infraestructura de comunicaciones de la compañía.	4	2	1	1	4	2,4	0,67	1,60
4	Falta de levantamiento de procesos para recuperación de desastres de cada equipo configurable.	5	2	1	1	5	2,8	0,67	1,87
5	Falta de acceso a todo el ciclo de vida de configuraciones de un equipo específico.	4	2	1	1	4	2,4	0,67	1,60
6	No registro de cada equipo configurable con su estado actual.	5	2	1	1	5	2,8	0,83	2,33
7	No toma en cuenta los datos del manejo de configuraciones para el desarrollo de software de la organización.	5	3	1	1	5	3,0	0,50	1,50
8	No documentación de los detalles de verificación al cierre de una configuración.	5	2	1	1	5	2,8	0,50	1,40
9	Falta de un un responsable o ejecutor para cada configuración registrada.	5	2	1	1	5	2,8	0,83	2,33
10	No realización de una planificación previa a la implementación de una configuración.	5	3	1	1	5	3,0	0,17	0,50
11	Falta de control del correcto funcionamiento al finalizar la configuración de un ítem.	5	3	1	1	5	3,0	0,00	0,00
12	Falta de identificación concreta de los ítems configurables para cada configuración registrada.	5	3	1	1	5	3,0	0,50	1,50
13	Alto número de configuraciones realizadas sin éxito frente al total de realizadas.	5	4	1	4	5	3,8	0,00	0,00
14	Alto número de configuraciones realizadas sin autorización.	5	4	1	4	5	3,8	0,00	0,00

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
15	Alto número de configuraciones realizadas con carácter de emergencia frente al total de realizadas.	5	3	1	3	5	3,4	0,15	0,51
16	No identificación de servicios que han tenido mejora gracias a configuraciones en la organización.	5	2	1	1	5	2,8	0,50	1,40
								Promedio	**1,092**

Tabla 3-74: Resultados Matriz de Riesgos - Gestión de Configuraciones para Operadores del DDS

3.6.3.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No utiliza un escalamiento de solución para resolver incidentes de usuario.	5	2	1	1	5	2,8	0,50	1,40
2	Falta de conocimiento de quién es el responsable de la solución y cierre de un incidente abierto.	5	2	1	2	5	3,0	0,67	2,00
3	Falta de conocimiento de quienes son los usuarios que mantienen incidentes sin resolver.	5	2	1	2	5	3,0	0,50	1,50
4	Falta de conocimiento de tiempo de respuesta y solución para un incidente específico.	4	2	1	1	4	2,4	0,67	1,60
5	Falta de acceso a la bitácora de cambios que se relacionan con un incidente específico.	4	2	1	1	4	2,4	1,00	2,40
6	No proveer un soporte inicial rápido para solución del incidente sin la identificación del problema que lo causó.	5	3	1	2	5	3,2	0,83	2,67
7	No informar al usuario sobre el escalamiento de su incidente.	4	2	1	1	4	2,4	0,33	0,80
8	No informar al usuario sobre el cierre del incidente.	4	2	1	1	4	2,4	0,50	1,20
9	No agrupación de incidentes por su naturaleza.	4	2	1	1	4	2,4	1,00	2,40
10	No agrupación de incidentes por su solución tipo.	4	2	1	1	4	2,4	1,00	2,40

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
11	No resolución de incidentes tomando en cuenta un banco de soluciones.	5	2	1	1	5	2,8	0,83	2,33
12	No registro de los niveles de satisfacción del usuario luego del cierre de un incidente.	4	2	1	1	4	2,4	0,83	2,00
13	No registro del técnico que cierra el incidente.	5	2	1	2	5	3,0	0,83	2,50
14	Tiempo prolongado en resolver incidentes.	5	3	1	2	5	3,2	0,00	0,00
15	Baja frecuencia en la realización de actualizaciones de software.	4	2	1	1	4	2,4	0,00	0,00
16	Baja frecuencia en la realización de actualizaciones de hardware.	4	2	1	1	4	2,4	0,27	0,64
17	Falta de Método para registro de Incidentes.	5	2	1	1	5	2,8	0,82	2,29
								Promedio	**1,670**

Tabla 3-75: Resultados Matriz de Riesgos - Gestión de Incidentes para Operadores del DDS

3.6.3.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No diferenciación entre problemas e incidentes.	5	2	1	2	4	2,8	0,50	1,40
2	Resolución de problemas antes de los incidentes en su organización.	5	3	1	3	4	3,2	1,00	3,20
3	No existencia de reuniones de apoyo para mejoramiento como por ejemplo para proponer actualizaciones o identificación de vulnerabilidades.	5	2	1	2	4	2,8	0,33	0,93
4	No poseer un servidor de Logs centralizado para registro de la actividad de la infraestructura de IT.	4	2	1	2	4	2,6	0,83	2,17
5	No apoyo de la resolución de problemas en la base de datos de administración de problemas.	5	2	1	2	4	2,8	0,50	1,40

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
6	Falta de personal designado para investigación especializada de problemas.	4	2	1	2	4	2,6	0,67	1,73
7	No registro de la o las acciones intuitivas que han mitigado un problema.	5	2	1	2	5	3,0	0,50	1,50
8	Cierre del problema cuando ejecuta una acción intuitiva que atenúa el problema.	5	3	1	3	5	3,4	0,33	1,13
9	No registro en la base de datos de errores conocidos al finalizar el diagnóstico de un problema.	5	2	1	2	5	3,0	0,67	2,00
10	Soluciona problemas sin apoyo en la base de datos de errores conocidos.	5	3	1	2	4	3,0	0,83	2,50
11	Falta de revisión de las tareas que se realizaron correctamente, luego del suceso de un error crítico.	5	3	1	3	5	3,4	0,33	1,13
12	Falta de revisión de los procedimientos erróneos, luego del suceso de un error crítico.	5	3	1	3	5	3,4	0,33	1,13
13	Falta de análisis de qué se puede hacer para que no suceda otra vez un suceso de un error crítico, luego de sucedido.	5	3	1	3	5	3,4	0,17	0,57
14	No registro adecuado de problemas.	5	2	1	2	5	3,0	1,00	3,00
15	Bajo número de problemas resueltos frente a los registrados.	5	3	1	3	5	3,4	0,14	0,48
16	Bajo porcentaje de problemas que se han resuelto en el tiempo esperado.	5	2	1	2	5	3,0	0,56	1,69
17	Alta tendencia a que se incrementen los problemas críticos.	5	3	1	3	5	3,4	0,00	0,00
								Promedio	**1,528**

Tabla 3-76: Resultados Matriz de Riesgos - Gestión de Problemas para Operadores del DDS

3.6.4 USUARIOS COMUNES[43]

El grupo de Usuarios Comunes presenta los siguientes resultados, con respecto al Análisis de Riesgos.

3.6.4.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de conocimiento del nivel de calidad de los servicios que debe recibir de parte del DDS.	3	3	1	2	3	2,4	0,55	1,31
2	No entrega de documentación formal que informe los servicios que provee el DDS.	3	3	1	2	3	2,4	0,93	2,24
3	Baja calidad de servicio que recibe del DDS en comparación con sus necesidades laborales.	4	4	1	4	4	3,4	0,40	1,35
4	Falta de cumplimiento de la calidad del Servicio de Sistema Empresarial.	4	5	2	4	4	3,8	0,35	1,32
5	Falta de cumplimiento de la calidad del Servicio de Internet.	4	5	2	4	4	3,8	0,52	1,97
6	Falta de cumplimiento de la calidad del Servicio de Correo.	4	5	2	4	4	3,8	0,27	1,02
7	Falta de cumplimiento de la calidad del Servicio de Soporte.	4	4	1	4	4	3,4	0,35	1,19
8	Falta de cumplimiento de la calidad del Servicio de Capacitación.	4	4	1	3	3	3,0	0,71	2,13
9	Falta de cumplimiento de la calidad del Servicio de Reportes del Sistema de Seguros.	3	4	1	3	3	2,8	0,39	1,09
								PROMEDIO	**1,513**

Tabla 3-77: Resultados Matriz de Riesgos - Gestión de Nivel de Servicio para Usuarios Comunes

[43] Los niveles de impacto fueron analizados en conjunto con la Ejecutiva de Cuenta Paola Pérez.

3.6.4.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de preparación frente la emergencias como corte de suministro eléctrico.	5	5	2	4	5	4,2	0,74	3,11
2	Tiempo extendido en estado de emergencia por virus.	4	4	1	3	4	3,2	0,25	0,81
3	Falta de disponibilidad del Sistema de Seguros.	5	5	3	5	5	4,6	0,32	1,46
4	Tiempo extendido en estado de emergencia por corte de Internet.	5	5	2	5	5	4,4	0,32	1,41
5	Tiempo extendido en estado de emergencia por corte de Correo Electrónico.	5	5	2	5	5	4,4	0,28	1,24
6	Falta de preparación frente la emergencias de corte de suministro eléctrico.	5	5	2	4	5	4,2	0,83	3,47
7	Tiempo extendido en estado de emergencia por corte de suministro eléctrico.	5	5	2	5	5	4,4	0,80	3,50
								PROMEDIO	**2,141**

Tabla 3-78: Resultados Matriz de Riesgos - Gestión de Continuidad de Servicio para Usuarios Comunes

3.6.4.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios de software o hardware de parte del DDS.	5	5	2	4	4	4,0	0,27	1,07
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo.	5	5	2	5	5	4,4	0,33	1,46
3	Baja frecuencia de cambios realizados por el DDS que tengan como objetivo innovación y mejoramiento.	4	3	2	4	4	3,4	0,12	0,39

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
4	Alta frecuencia de cambios realizados por el DDS que tengan como objetivo modificaciones o correcciones.	4	4	2	4	4	3,6	0,78	2,79
5	Bajo Nivel de satisfacción de los cambios realizados por el DDS.	4	4	2	4	4	3,6	0,26	0,95
6	Falta de método de calificación del nivel de satisfacción respecto a un cambio realizado por el DDS.	3	3	2	2	3	2,6	0,68	1,76
7	Bajo porcentaje de cambios que han sido satisfechos frente a los solicitados.	3	3	2	3	3	2,8	0,34	0,95
8	Número elevado de cambios que no le han sido notificados y han afectado el desenvolvimiento normal de su trabajo.	5	5	2	5	5	4,4	0,18	0,80
								PROMEDIO	**1,273**

Tabla 3-79: Resultados Matriz de Riesgos - Gestión de Cambios para Usuarios Comunes

3.6.4.4 Gestión de Configuraciones

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No realización de configuraciones de forma metódica y ordenadamente por el DDS.	4	4	2	4	4	3,6	0,25	0,91
								PROMEDIO	**0,907**

Tabla 3-80: Resultados Matriz de Riesgos - Gestión de Configuraciones para Usuarios Comunes

3.6.4.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Alta frecuencia de incidentes que afectan el normal desempeño de su trabajo.	5	5	2	5	5	4,4	0,52	2,30
2	Falta de satisfacción de los recursos tecnológicos asignados.	4	3	1	2	2	2,4	0,29	0,69
3	Falta de evolución de la tecnología en la empresa.	4	3	1	2	3	2,6	0,21	0,55
4	Falta de apertura del DDS para recibir sugerencias.	4	4	2	3	4	3,4	0,30	1,03
5	Falta de capacitación a los usuarios de parte del DDS.	4	4	2	4	4	3,6	0,64	2,29
6	No satisfacción del usuario frente al tiempo de solución de incidentes.	4	3	2	4	4	3,4	0,30	1,01
7	Alta frecuencia de incidentes específicos.	4	4	2	4	4	3,6	0,32	1,15
8	Falta de un método de Gestión de incidentes.	4	4	2	3	4	3,4	0,70	2,37
9	Falta de método de calificación del servicio recibido de parte del DDS.	3	2	1	2	3	2,2	0,87	1,90
10	Tiempo prolongado para dar solución a un incidente.	4	4	3	4	4	3,8	0,23	0,86
11	Baja calificación general para el Dto. de Sistemas respecto a resolución de incidentes.	4	4	1	4	4	3,4	0,34	1,16
12	Alta frecuencia de incidentes con Programas de Ofimática.	4	4	1	3	4	3,2	0,26	0,84
13	Alta frecuencia de incidentes de Falla Física de su computador.	5	5	1	5	5	4,2	0,17	0,70
14	Alta frecuencia de incidentes de virus.	5	5	2	3	5	4,0	0,21	0,83
15	Alta frecuencia de incidentes de Internet.	5	5	2	5	5	4,4	0,26	1,13
16	Alta frecuencia de incidentes con Sistema de la empresa.	5	5	4	5	5	4,8	0,27	1,28

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
17	Alta frecuencia de incidentes con el Correo Electrónico Corporativo.	5	5	2	5	5	4,4	0,21	0,93
								PROMEDIO	**1,237**

Tabla 3-81: Resultados Matriz de Riesgos - Gestión de Incidentes para Usuarios Comunes

3.6.4.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.	5	5	2	5	5	4,4	0,13	0,57
2	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.	5	5	2	5	5	4,4	0,17	0,73
								PROMEDIO	**0,649**

Tabla 3-82: Resultados Matriz de Riesgos - Gestión de Problemas para Usuarios Comunes

3.6.5 PUNTOS DE VENTA SOAT[44]

El grupo de Puntos de Venta SOAT presenta los siguientes resultados, con respecto al Análisis de Riesgos.

3.6.5.1 Gestión de Nivel de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de cumplimiento de la calidad del Servicio del Sistema de SOAT.	5	5	5	5	5	5,0	0,17	0,87
2	Falta de cumplimiento de la calidad del Servicio de Soporte Técnico.	5	5	4	5	5	4,8	0,13	0,61
								PROMEDIO	**0,743**

Tabla 3-83: Resultados Matriz de Riesgos en Gestión de Nivel de Servicio para Puntos de Venta SOAT

[44] Los niveles de impacto fueron analizados en conjunto con la Ejecutiva de Cuenta Paola Pérez.

3.6.5.2 Gestión de Continuidad de Servicio

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de preparación frente la emergencias como corte de suministro eléctrico.	5	5	3	5	5	4,6	0,88	4,07
2	Baja disponibilidad del Sistema de SOAT.	5	5	3	5	5	4,6	0,51	2,34
								PROMEDIO	**3,203**

Tabla 3-84: Resultados Matriz de Riesgos para Gestión de Continuidad de Servicio en Puntos de Venta SOAT

3.6.5.3 Gestión de Cambios

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	No recepción de cambios para emisión de SOAT de parte de Alianza.	5	5	2	4	5	4,2	0,07	0,29
2	Falta de notificación de cuándo se realizará un cambio que afecte a su entorno de trabajo con el SOAT.	5	5	3	4	5	4,4	0,48	2,10
3	Bajo Nivel de satisfacción de los cambios realizados por Alianza.	5	5	3	4	5	4,4	0,19	0,82
								PROMEDIO	**1,070**

Tabla 3-85: Resultados Matriz de Riesgos para Gestión de Cambios en Puntos de Venta SOAT

3.6.5.4 Gestión de Configuraciones

No existen registros referentes al Manejo de Configuraciones para el grupo Puntos de Venta SOAT.

3.6.5.5 Gestión de Incidentes

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de apertura de Aianza para recibir sugerencias.	4	4	2	4	4	3,6	0,09	0,33
2	Falta de capacitación a los usuarios de parte de Alianza.	5	5	2	4	5	4,2	0,26	1,07
3	No satisfacción del usuario frente al tiempo de solución de incidentes.	5	5	2	4	5	4,2	0,14	0,59
4	Alta frecuencia de incidentes específicos.	5	5	3	4	5	4,4	0,35	1,53
5	Tiempo prolongado para dar solución a un incidente.	5	5	2	4	5	4,2	0,23	0,96
6	Baja calificación general para Alianza respecto a resolución de incidentes.	5	5	2	4	5	4,2	0,14	0,59
7	Alta frecuencia de incidentes con el Sistema SOAT.	5	5	5	5	5	5,0	0,07	0,35
								PROMEDIO	**0,775**

Tabla 3-86: Resultados Matriz de Riesgos para Gestión de Incidentes en Puntos de Venta SOAT

3.6.5.6 Gestión de Problemas

ITEM	AMENAZA	Impacto Resultados	Impacto Operaciones	Impacto Regulatorio	Impacto Reputación	Impacto Económico	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de urgencia para restablecer sus actividades laborales inmediatamente.	5	5	4	4	5	4,6	0,09	0,43
2	Falta de rapidez en resolución de incidentes que ya han sucedido anteriormente.	5	5	4	5	5	4,8	0,06	0,28
								PROMEDIO	**0,353**

Tabla 3-87: Resultados Matriz de Riesgos para Gestión de Problemas en Puntos de Venta SOAT

3.6.6 CALCULO DE RIESGO PROMEDIO POR PROCESO ITIL

	GRUPOS					
PROCESO	EJECUTIVOS	GERENTE DE SISTEMAS	OPERADOR DEL DDS	USUARIOS COMUNES	PUNTOS DE VENTA	**PROMEDIO**
GESTIÓN DE NIVEL DE SERVICIO	0,724	2,363	2,066	1,513	0,743	1,482
GESTIÓN DE CONTINUIDAD DE SERVICIO	2,219	2,189	3,254	2,141	3,203	2,601
GESTIÓN DE CAMBIOS	0,622	1,818	1,080	1,273	1,070	1,172
GESTIÓN DE CONFIGURACIONES	1,800	2,460	1,092	0,907	x	1,565
GESTIÓN DE INCIDENTES	0,673	1,182	1,670	1,237	0,775	1,107
GESTIÓN DE PROBLEMAS	0,000	1,869	1,528	0,649	0,353	0,880

Tabla 3-88: Resultados Riesgo Promedio por Proceso ITIL

Según la tabla 3-88, se aprecia que para:

Gestión de Nivel de Servicio

Los Ejecutivos aprecian un riesgo muy bajo, en la calidad de los servicios que gestiona el DDS. Por otro lado según lo evaluado a la Gerencia de Sistemas se tiene un riesgo bajo igual que para los Operadores de Sistemas. Los usuarios comunes perciben un mayor riesgo que los Ejecutivos (tiende a ser bajo), debido a que cuando hay un incidente, la prioridad la tienen los Ejecutivos en lugar de los Usuarios Comunes, pero como diferencia sólo tienen un escalón, por lo que se considera un riesgo similar. Finalmente se ve que el riesgo de una mala gestión de la calidad para los Puntos de Venta SOAT, es muy bajo y están en similares condiciones que los Ejecutivos, es decir en su mayoría están bien tratados y no representan un riesgo peligroso para la empresa. De estos, el ítem con mayor riesgo son las actividades que no se gestionan de forma adecuada en la Gerencia de Sistemas. En promedio la Gestión de Nivel de Servicio tiene un riesgo entre muy bajo y bajo.

Gestión de Continuidad de Servicio

Los Ejecutivos muestran un riesgo entre bajo y medio con tendencia a bajo, es decir que esta gestión a pesar sus problemas, se han podido solucionar para que no se conviertan en críticos. La Gerencia de Sistemas también tiene un riesgo entre bajo y medio menor que el de los Ejecutivos, esto debido a que en el momento de crisis han sido manejados de tal forma que no se vuelvan críticos. Por el contrario el Operador del DDS tiene un riesgo entre medio y alto tendiente a medio, esto se refiere a que los miembros de este grupo han manejado crisis que no se han vuelto catástrofes, pero a la vez se sienten preocupados por que la empresa no tiene preparación como planes establecidos para enfrentar una crisis. Los usuarios comunes tienen un riesgo entre bajo y medio con tendencia a bajo, esto implica que han notado el suceso de catástrofes, pero han buscado la manera de seguir con sus labores y por ejemplo en el caso de la crisis eléctrica han determinado que al ser un problema nacional, se tenía que acostumbrar a este nuevo ritmo de trabajo. Por otro lado clientes finales como los Puntos de Venta SOAT, presentan un riesgo entre medio y alto con tendencia a ser medio, debido a que ellos al ser clientes y no empleados pagan por un servicio que Alianza les debe suministrar, por la crisis energética del 2009, ellos pudieron constatar que Alianza no se encontraba preparada para enfrentar este tipo de crisis, porque en algunas sucursales no existía una continua disponibilidad del Sistema SOAT.

En promedio la Gestión de Continuidad de Servicio tiene un riesgo entre bajo y medio, con tendencia a ser medio.

Gestión de Cambios

La gestión que se dan a los cambios cuando implican TI, desde el punto de vista de los Ejecutivos es baja, principalmente porque los Ejecutivos tienden a ser notificados cuando hay la planificación de un cambio que afecte a su trabajo. Según los aspectos evaluados a la Gerencia de Sistemas se concluye que presentan un riesgo entre muy bajo y bajo, con tendencia a ser bajo, esto porque este grupo representado por el Ing. Pablo Herrera tiende a cumplir con todas las solicitudes de cambio realizadas. El Operador de Sistemas presenta un riesgo muy bajo en su evaluación de cómo procede ante cambios, esto debido a que

tienen la política de comprobar la satisfacción de los involucrados luego de implementar un cambio, así como su tendencia a realizar cambios con éxito. Los usuarios comunes presentan un riesgo entre muy bajo y bajo, con tendencia a bajo, esto debido a que como para los Ejecutivos este grupo tiende a ser notificado cuando el DDS tiene planificado un cambio que podría afectar el trabajo normal de los usuarios. Finalmente el grupo de Puntos de Venta SOAT, presenta un riesgo bajo, esto principalmente porque Alianza representados por los Ejecutivos de Cuenta que a su vez son respaldados por el DDS, tienen la apertura adecuada para receptar las solicitudes de cambio que necesitarían los Puntos de Venta SOAT a nivel nacional.

En promedio la Gestión de Cambios, tiene un riesgo entre muy bajo y bajo con tendencia a bajo.

Gestión de Configuraciones

Los Ejecutivos representados por la Ing. Elizabeth Vallejo, califican un riesgo entre muy bajo y bajo, principalmente porque hay la predisposición para apoyar proyectos que tengan como objetivo la mejora de procesos de configuración. El Gerente de Sistemas según su evaluación da como resultado un riego entre bajo y medio con tendencia a medio esto debido a que: no se toma en cuenta el dato de los equipos para desarrollar software, no se planifica generalmente una configuración, falta de control de funcionamiento luego de una configuración, y bajo número de configuraciones realizadas frente a solicitadas. El Operador del DDS, luego de su evaluación presenta un riesgo bajo, principalmente por su tendencia a realizar configuraciones con éxito y la política de siempre realizar configuraciones con autorización. Los Usuarios Comunes califican a la Gestión de Configuraciones con un riesgo bajo, esto porque antes los usuarios el DDS tiende realizar configuraciones de forma metódica y ordenada. Para los Puntos de Venta no se aplica esta encuesta.

En promedio la Gestión de Configuraciones tiene un riesgo entre muy bajo y bajo con tendencia a bajo.

Gestión de Incidentes

Los Ejecutivos presentan un riesgo bajo con respecto a Gestión de Incidentes, debido principalmente a que este grupo se siente satisfecho a la forma en que el DDS los ha asesorado cuando tienen un incidentes que implican el uso de la tecnología. El Gerente de Sistemas luego de ser evaluado en la forma de gestionar incidentes, se concluye que posee un riesgo entre muy bajo y bajo con tendencia a bajo, esto debido a que se tiene la política de atención inmediata a los internos y externos para restituirle el servicio afecto lo más pronto posible. El Operador del DDS luego de su evaluación presenta un riesgo entre muy bajo y bajo con tendencia a bajo, la diferencia con la Gerencia de Sistemas se da básicamente porque el DDS no posee un lineamiento formal de cómo proceder para el proceso de un incidente y la falta de soluciones tipo para reducir tiempos de respuesta ante incidentes comunes. Los Usuarios comunes califican a la Gestión de Incidentes con un riesgo entre muy bajo y bajo, con tendencia a bajo, si bien es similar el riesgo con los Ejecutivos, en los Usuarios Comunes se da un riesgo mayor por la diferencia de prioridad de atención que se le da a un grupo y a otro, además también influye la falta de capacitación de los usuarios para el manejo de tecnología. Finalmente los Puntos de Venta SOAT, presentan un riesgo muy bajo, similar al de los Ejecutivos pero mayor, es decir que la atención de los incidentes para este grupo se da en parte de forma satisfactoria, porque los usuarios reconocen que el sistema es bastante robusto.

En promedio la Gestión de Incidentes tiene un riesgo entre muy bajo y bajo, con tendencia a bajo.

Gestión de Problemas

La evaluación que dan los Ejecutivos a la Gestión de Problemas tiene un riesgo nulo, principalmente porque: primero los Ejecutivos tienen la predisposición de apoyar la generación de un grupo que resuelva problemas, notan que hay urgencia en restablecer el servicio que fue afectado y finalmente porque eventos negativos que han sucedido anteriormente se resuelven con mayor rapidez. La evaluación para el Gerente de Sistemas respecto a la Gestión de Problemas tiene un riesgo que está entre muy bajo y bajo, con tendencia a bajo, a pesar de que no representa un riesgo peligroso, sus mayores riesgos se dan por la falta de una

política de registro y la no clara diferenciación entre problemas e incidentes. La gestión evaluada a los Operadores del DDS produjo un riesgo similar al presentado para la Gerencia de Sistemas es decir entre muy bajo y bajo pero con tendencia a ser bajo, esto dice que existen falencias en la administración pero que para los usuarios no es perceptible, los problemas que presenta son similares a los de la Gerencia de Sistemas. Los Usuarios Comunes presentan un riesgo muy bajo, por el hecho de que las falencias de gestión del DDS, no son visibles, la diferencia entre este grupo y los Ejecutivos es que, como ya se mociono los Ejecutivos por su cargo poseen una prioridad más alta para resolver sus incidentes. Finalmente para los Puntos de Venta SOAT, la Gestión de Problemas posee un riesgo muy bajo, esto de la misma manera porque la urgencia que demuestra Alianza para restablecer el servicio con falla y la resolución de incidentes que ya han sucedió anteriormente en un tiempo más corto, aplacan las falencias de los procesos de la Gestión de Problemas que son específicos del DDS.
En promedio la Gestión de Problemas presenta un riesgo muy bajo.

Según los resultados obtenidos se concluye que el proceso ITIL con mayor riesgo para la empresa es la Gestión de Continuidad de Servicio y el con menos riesgo la Gestión de Problemas.

3.7 INFORME EJECUTIVO

El informe ejecutivo es un resumen de la investigación donde se presentan los resultados obtenidos, este puede ser encontrado en el Anexo 3-2.

CAPÍTULO IV: DESARROLLO DE LA SOLUCIÓN DE GESTIÓN PARA EL EVENTO MÁS CRÍTICO

El presente capítulo detalla las recomendaciones ITIL para el proceso ITIL reconocido como el más crítico.

4.1 ANTECEDENTES

En vista de los resultados obtenidos en el Análisis de Riesgos, se llega a la conclusión que el dominio ITIL con mayor riesgo es la Gestión de Continuidad de Servicio, con un valor de 2,601. De esta manera este ítem se convierte en el más crítico para la empresa y para el cual se desarrollará un plan modelo según las recomendaciones de ITIL V3.

A continuación se presenta un cuadro con los valores de riesgo que cada dominio ITIL alcanzó:

4.1.1 RIESGO ALCANZADO POR CADA DOMINIO ITIL.

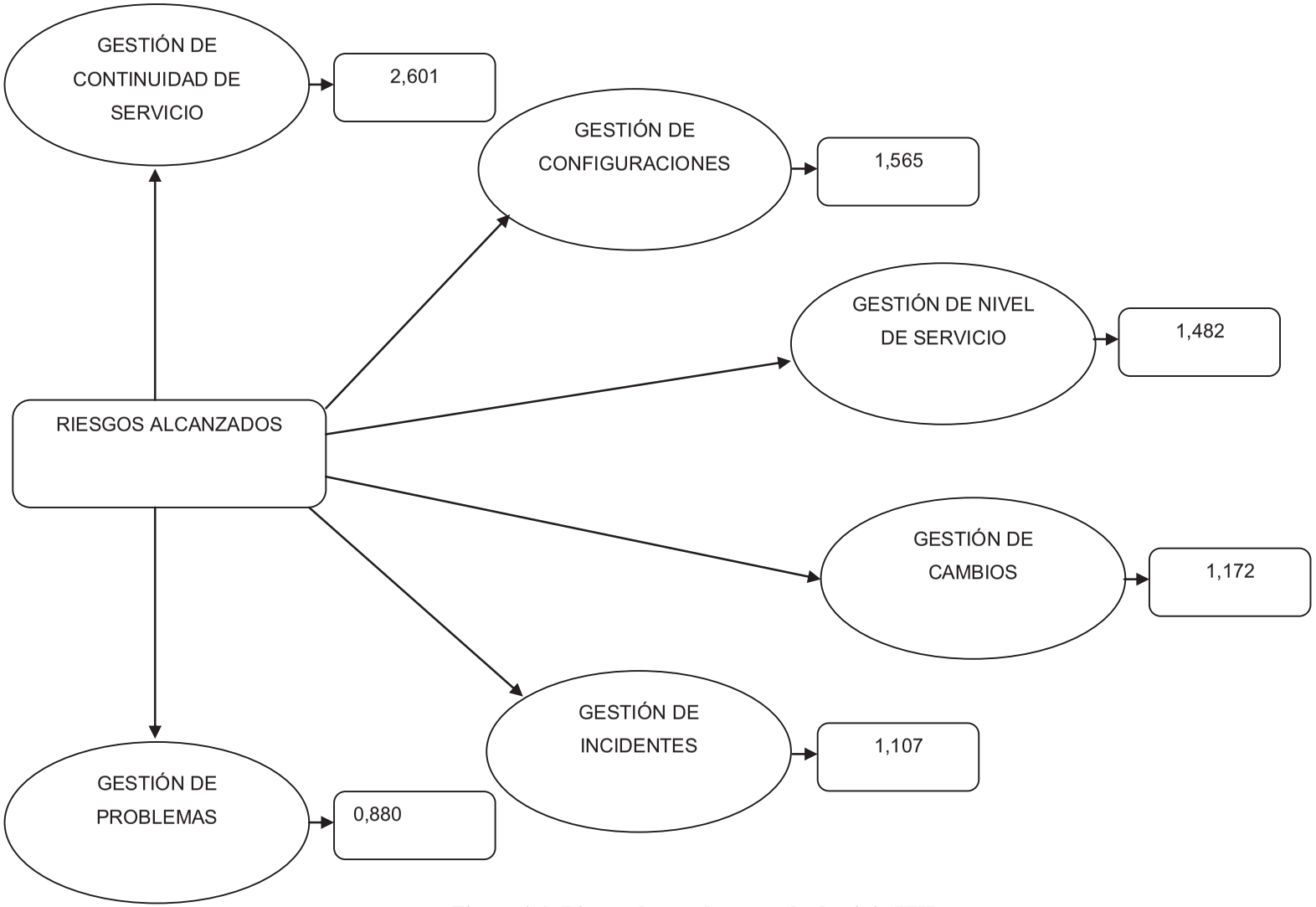

Figura 4-1: Riesgo alcanzado por cada dominio ITIL

4.2 DETALLE DE LA SOLUCIÓN

La solución se basa en las actividades sugeridas por ITIL, tomando en cuenta la situación actual de Alianza CIA de Seguros y Reaseguros S.A.
El dominio de ITIL Manejo de Continuidad de Servicio, se encuentra detallado en el libro de Diseño de Servicio, en este punto de planificación se debe especificar la respuesta que se espera de un servicio ante cierto comportamiento del medio, es decir la capacidad de reacción ante eventos fortuitos como crisis o emergencias.

4.2.1 ESTADO ACTUAL DEL MANEJO DE CONTINUIDAD DE SERVICIO EN ALIANZA CIA. DE SEGUROS Y REASEGUROS S.A.

Del Análisis de Riesgos realizado en el capítulo 3 del dominio Continuidad de Servicio, se deben tomar en cuenta los indicadores de Riesgo Medio[45], es decir los mayores a 2,5 como lo sugieren los lineamientos de Auditoría Interna de la EPN[46]. En este contexto un indicador es reconocido como de relevancia, cuando es mayor o igual al valor de riesgo Medio de la escala general. A continuación se detallan estos valores, para cada tipo de usuario.

[45] Nomenclatura usada en la escala de MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, ver Anexo 2-7.
[46] Referencia de la entrevista con Patricia Pérez, Auditor Interno 2 de la EPN, 10 años de experiencia.

4.2.1.1 Ejecutivos

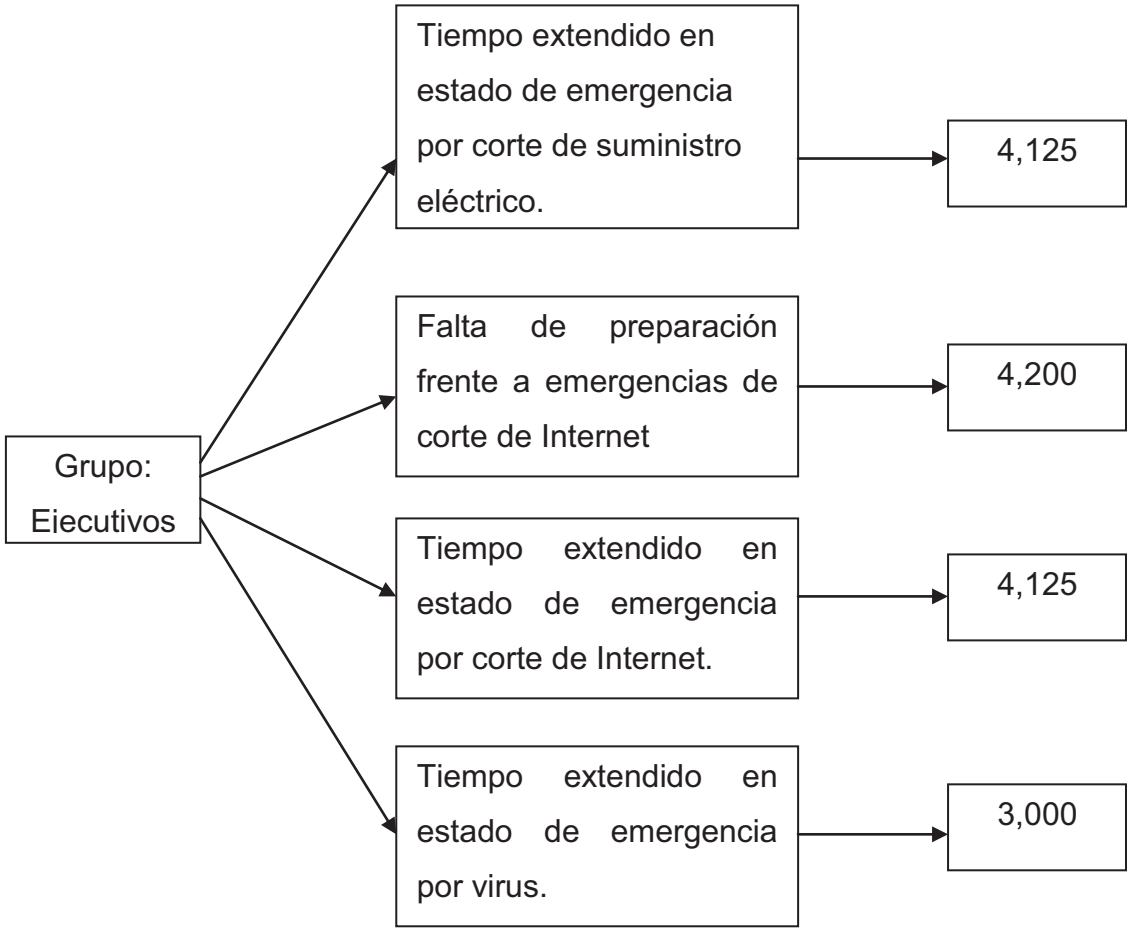

Figura 4-1: Riesgos relevantes en Continuidad de Servicio para Ejecutivos

4.2.1.2 Gerente de Sistemas

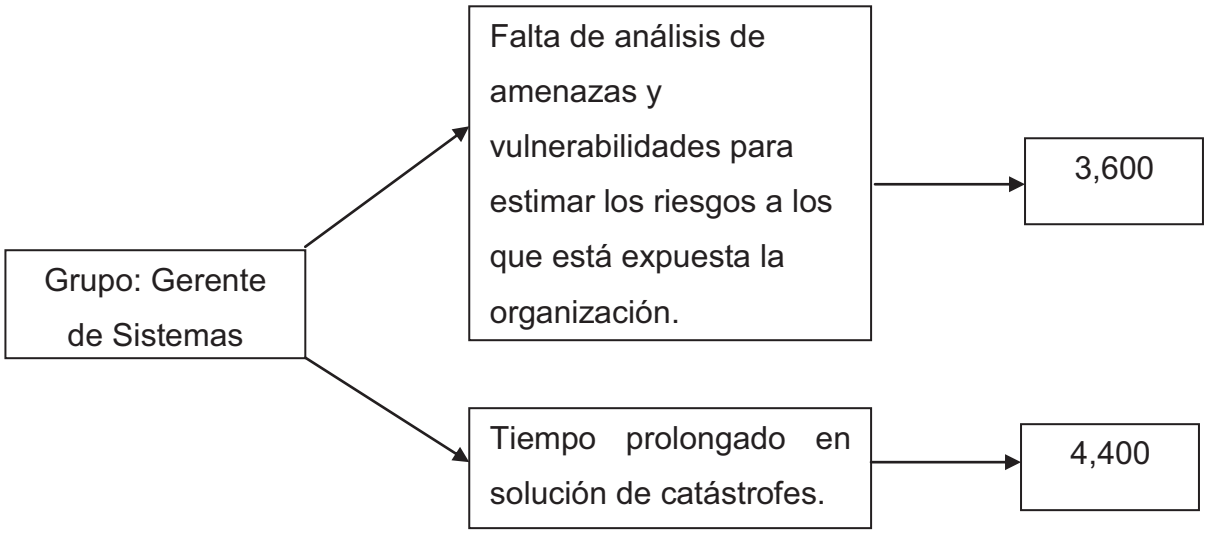

Figura 4-2: Riesgos relevantes en Continuidad de Servicio para Gerente de Sistemas

4.2.1.3 Operador del DDS

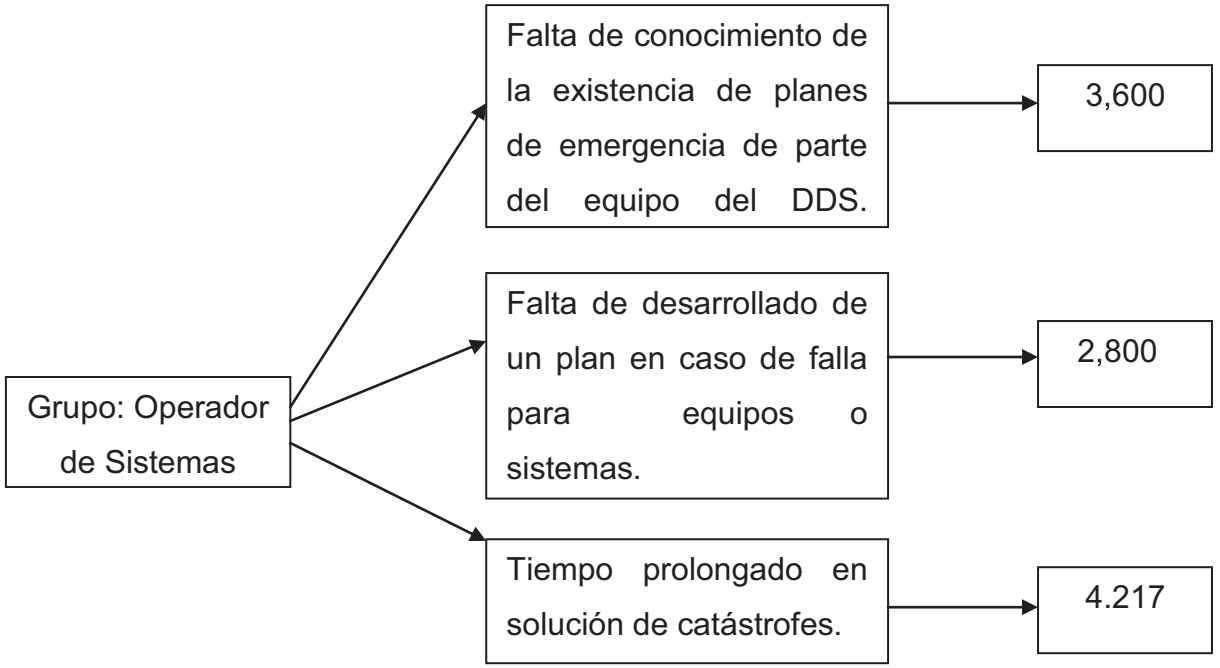

Figura 4-3: Riesgos relevantes en Continuidad de Servicio para Operador de Sistemas

4.2.1.4 Usuarios Comunes

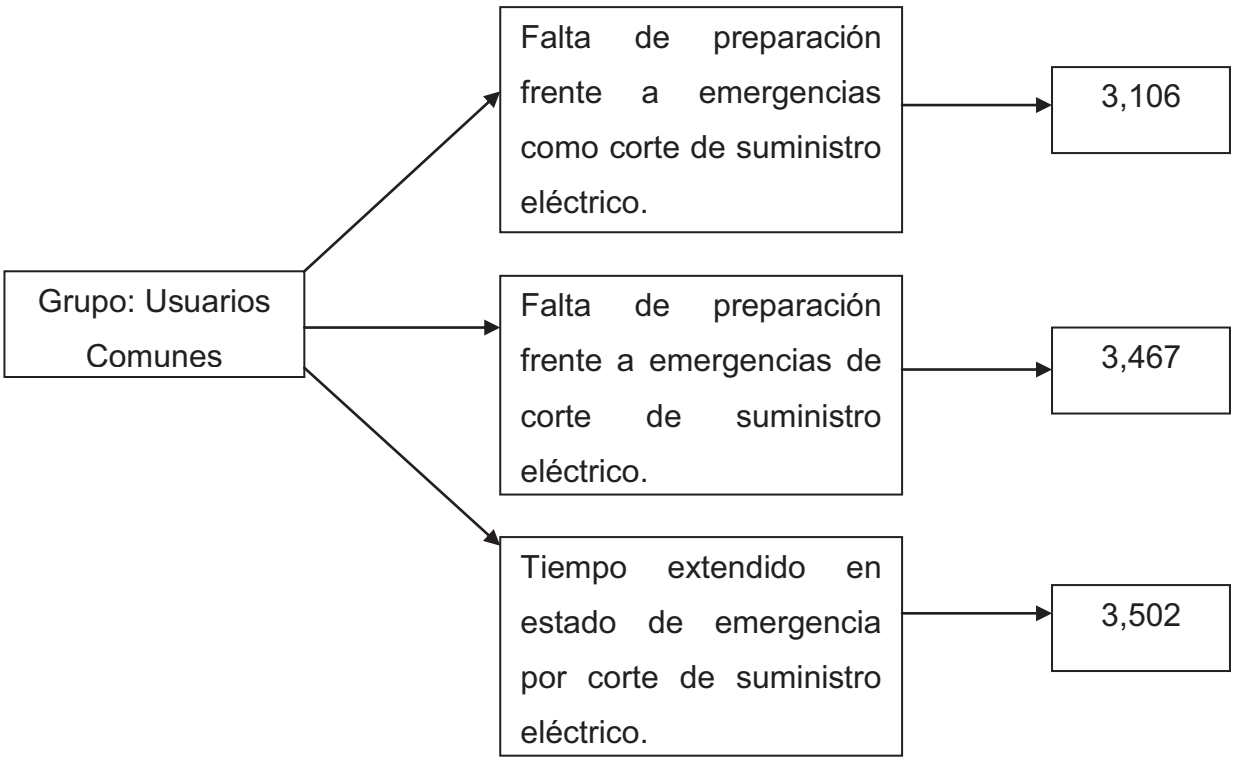

Figura 4-4: Riesgos relevantes en Continuidad de Servicio para Usuarios Comunes

4.2.1.5 Puntos de venta SOAT

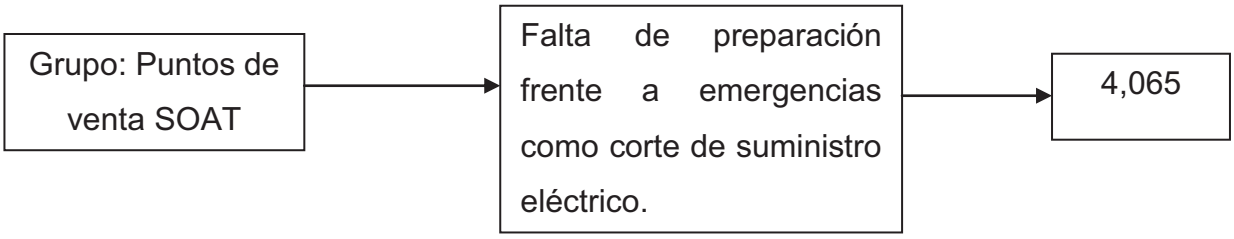

Figura 4-5: Riesgos relevantes en Continuidad de Servicio para Puntos de Venta SOAT

4.2.2 ACTIVIDADES PARA MANEJO DE CONTINUIDAD DE SERVICIO

4.2.2.1 Inicio

Cubre todas las actividades que ayudan al entendimiento de continuidad para el negocio, se recomienda desarrollar lo siguiente:

4.2.2.1.1 Establecimiento de políticas para el plan

Nombra el motivo de la gestión y objetivos, por ejemplo como objetivo se puede mencionar:

- Contar con varios planes que aseguren la continuidad de servicios para Alianza CIA de Seguros y Reaseguros S.A.
- Mantener los planes para Gestión de Continuidad de acuerdo, a la realidad cambiante de Alianza CIA de Seguros y Reaseguros S.A.
- Capacitar constantemente al personal para el correcto uso de procedimientos en contra de catástrofes y nuevas amenazas.

4.2.2.1.2 Términos de referencia y alcance

Implanta responsabilidades sobre el personal de toda la empresa (Análisis de Riesgos e Impacto) e identificar áreas de relevancia.

En el caso de Alianza, la responsabilidad de dirigir la tendrá el Gerente de Sistemas Ing. Pablo Herrera. Para apoyar en el desarrollo de la región Sierra del país estarán los técnicos Juan Guamba y Patricio León, en la región Costa el Ing. Juan Cevallos.

Con respecto a las áreas importantes, se mencionan a las siguientes, tomando como base la información obtenida de la compañía:

- Sistema de Seguros.
- Servicio de Internet.
- Enlaces WAN dedicados.
- Correo Electrónico.
- Soporte a los usuarios.

4.2.2.1.3 Asignar recursos

El establecimiento de la continuidad del negocio requiere recursos representativos, tanto en la parte monetaria como humana. En esta primera etapa de familiarización del personal con ITIL, se deben tener en cuenta recursos para

capacitación y consultores externos que ayudarían a realizar el análisis de gestión con mayor rapidez.
Además la gerencia debe tomar en consideración, qué recursos necesita para mantener los procesos de gestión en el futuro sin ayuda externa.

4.2.2.1.4 Definir la organización del proyecto y la estructura de control

Los proyectos de continuidad son potencialmente complejos, por esto deben estar bien organizados y controlados de ahí que se recomienda el uso de estándares de planificación metodológicos, como PRINCE2[47] o PMBOK[48], ver Anexo 4-1.
PMBOK es un estándar desarrollado por el PMI[49] de origen en los Estados Unidos, que se enfoca en proporcionar el cuerpo de conocimiento necesario para la gerencia de proyectos. Por otro lado PRINCE2 se desarrolló por la OGC[50] del Reino Unido, dando prioridad a la práctica más que la enseñanza lo que le da un enfoque a tener más probabilidades de éxito en el desarrollo de proyectos.

4.2.2.1.5 Aprobación de proyecto y planes de calidad

Los planes ayudan a que el proyecto sea controlado y la calidad asegura que lo suministrado tenga un buen desempeño.
En el caso de Alianza CIA de Seguros y Reaseguros S.A., la aprobación se manejará entre el Gerente de Sistemas y el Presidente de la compañía.

4.2.2.2 Requerimientos y Estrategia

Los requisitos para la continuidad del servicio son un componente crítico, puesto que de esto depende el correcto desenvolvimiento de la empresa ante fallas o catástrofes. Si el análisis es incorrecto se pueden dar graves consecuencias en la efectividad del Manejo de Continuidad del Servicio.

---

[47] **PR**ojects **IN C**ontrolled **E**nvironments
[48] Project Management Body of Knowledge
[49] Project Management Institute
[50] Office of Government Commerce

4.2.2.2.1 Requerimientos

En esta sección se debe desarrollar lo siguiente:

- Análisis de Impacto en el Negocio

Cuantifica el nivel de impacto que tendría para la empresa que un servicio deje de funcionar.
Los niveles de impacto son una escala de referencia, con la cual se identifica si un impacto es alto o bajo. Como referencia para la presente investigación se usó el análisis mediante tablas que se establece en MAGERIT versión 2[51], realizada por el Ministerio de Administraciones Públicas de España.
En este tipo de análisis se pueden utilizar varios tipos de impactos, como por ejemplo en el realizado para los dominios de ITIL en el capítulo 2 por el autor, se tomo en cuenta a: Resultados, Operaciones, Regulatorio, Reputación y Económico. Con ellos se calcula un promedio que ayuda a obtener un impacto ponderado para cada servicio.
Así al final se obtendrán los servicios principales que mueven a la compañía, los mismos que deben tener prioridades diferentes según la necesidad y se convierten en una entrada principal para el proceso de Nivel de Servicio.
Es útil conocer la opinión de representantes antiguos y jóvenes de diferentes áreas, así como de supervisores respecto a su punto de vista con los niveles de impacto, cada uno tendrá una contribución valiosa a la hora de producir la estrategia global.

- Evaluación de riesgos

El segundo requerimiento es analizar la posibilidad de que un desastre ocurra, tomando en cuenta las amenazas que se relacionan con éste. Así se denotarán las vulnerabilidades de la organización. Aquí se podría usar una metodología estándar como M_o_R[52], la misma que realiza un perfil de los riesgos

[51] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, ver Anexo 2-7.
[52] Management of Risk

encontrados, identificando los aceptables y no aceptables. Con esta información se pueden establecer las medidas a ser tomadas para la reducción de riesgos, ya sea bajando el impacto o la probabilidad de ocurrencia. Además sugiere la realización de un listado de cada riesgo con las causas que lo podrían provocar.
Por ejemplo si se pone en consideración el perfil de riesgos de Continuidad de Servicio para el Gerente de Sistemas, se tendría lo siguiente:

ITEM	AMENAZA	Impacto	Probabilidad de Amenaza	Riesgo	Est. de Riesgo
1	Falta de conocimiento de la existencia de planes de emergencia de parte del equipo del DDS.	3,6	0,5	1,8	B
2	Falta de desarrollado formal de planes de respuesta ante una emergencia.	3,6	0,5	1,8	B
3	Falta de desarrollado de un plan en caso de falla para equipos o sistemas.	3,6	0,5	1,8	B
4	Falta de un lineamiento formal, de cómo proceder para la recuperación al estado anterior de servicios.	3,6	0,5	1,8	B
5	Falta de evaluación de planes de respuesta ante emergencias o recuperación antes de ser puestos en marcha.	3,6	0,5	1,8	B
6	No revisión de los planes de emergencia ya desarrollados.	3,6	0,25	0,9	MB
7	Falta de entrenamiento del DDS para utilizar correctamente los planes de emergencia.	3,6	0,5	1,8	B
8	Falta de análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización.	3,6	1	3,6	A
9	Tiempo prolongado en solución de catástrofes.	4,4	1	4,4	A

Considerando la escala de MAGERIT.

MB	1
B	2
M	3
A	4
MA	5

Donde se identifica que los ítems de alto riesgo son: la Falta de análisis de amenazas y vulnerabilidades para estimar los riesgos a los que está expuesta la organización y el tiempo prolongado en solución de catástrofes.

4.2.2.2.2 Estrategia

Para que la empresa Alianza CIA de Seguros y Reaseguros S.A. sea la mejor compañía de seguros del país se propone ofrecer alta disponibilidad para los servicios que provee, para esto se sigue con el análisis de requerimientos, la documentación de las medidas para reducción de riesgos y las opciones de recuperación para dar soporte al negocio.

Por ejemplo como medidas para reducción de riesgos para el "Tiempo prolongado en solución de catástrofes, se debe empezar por analizar las zonas de mayor impacto para la organización y luego generar planes de contingencia en caso de ocurrencia de los mismos. Los planes propuestos a la vez deberían ser evaluados para confirmar su efectividad. Con estas medidas ya se estaría reduciendo el nivel de riesgo.

Por otro lado las opciones de recuperación se refieren directamente con el tiempo de restitución del servicio. De acuerdo al análisis de impacto la organización debe identificar qué operaciones pueden esperar más o menos tiempo.

Por ejemplo si falla un disco del arreglo en el equipo AS400 donde se aloja el Sistema de Seguros, este debe tener en espejo otro que lo sustituya de inmediato para que no exista pérdida de datos o información corrupta. Al momento en que las transacciones del sistema no se puedan realizar, se está parando el principal servicio de la empresa, por esto la opción de recuperación debe ser inmediata.

4.2.2.3 Implementación

Una vez que la estrategia ha sido aprobada, los Planes de Continuidad del Servicio de TI necesitan ser producidos simultáneamente con los Planes de Continuidad del Negocio.

Pasos para implementación:

4.2.2.3.1 Organización y Planificación de la implementación

Implica la coordinación de la implementación.

4.2.2.3.2 Implementación de soluciones en espera

Representan los procesos listos a ser implementados ante fallas.

4.2.2.3.3 Desarrollar Planes de Recuperación

Se refiere a demostrar la efectividad de las opciones de recuperación que se sugieren en las soluciones en espera.

4.2.2.3.4 Implementación de medidas para reducción de riesgos

Significa hacer efectivas las medidas para reducir riesgos, es decir comprar los equipos necesarios, hacer configuraciones o actualizar la infraestructura tecnológica.

4.2.2.3.5 Desarrollo de Procedimientos

Aquí se escriben los manuales que van a ser utilizados por los técnicos que van a enfrentar las crisis en la empresa. Esta etapa además debe incluir la capacitación del personal a que proceda de forma correcta con los métodos diseñados.

4.2.2.3.6 Evaluación inicial

Una vez implementados, una parte crítica de los Planes de Continuidad es la evaluación de los mismos. Existen 4 tipos de pruebas que pueden ser realizadas:

- Simuladas: Por ejemplo un esquema de red puede ser simulado con la ayuda de software como Cisco Packet Tracer, o un ambiente de infraestructura se lo puede generar con el programa de virtualización, VMWare.

- Completas: Este tipo de prueba se refiere a realizar todos los procesos a los que la tecnología debe responder, estimados en el diseño de equipos de redes

o servidores. Es importante usar el mismo modelo de equipos que se usarán en producción para la evaluación.

- Parciales: Estas evaluaciones como lo dice su nombre sólo toman una parte de la tecnología a ser evaluada, por ejemplo una prueba parcial del SAEW[53] sería sólo realizar experimentos con el módulo de Matrículas sin tomar en cuenta los restantes del sistema.

- Para escenarios específicos: Esta prueba consiste en provocar una falla específica a la que tiene que responder la tecnología a ser evaluada. Por ejemplo cuando se realiza un RAID 1 en un chasis de almacenamiento entre dos discos, para probar el funcionamiento se simula la avería de un disco sacándolo en caliente, si la redundancia ha sido configurada correctamente el sistema seguirá funcionando sin ningún problema.

4.2.2.4 Operación en Producción

La presente etapa, consiste en lo siguiente:

4.2.2.4.1 Educación, concienciación y entrenamiento

Este ítem corre por parte del departamento de Tecnología para poner a todo el personal pendiente y preparado, para poder proceder correctamente con los planes de continuidad.

4.2.2.4.2 Revisión

Revisiones regulares de todos los entregables del Manejo de Continuidad del Servicio para confirmar que se mantienen disponibles y actualizados.

[53] Sistema de Administración Estudiantil Web

4.2.2.4.3 Evaluación

Se debe realizar una evaluación regular para mantener controlados los elementos críticos de la estrategia, por lo menos mensualmente. Todos los planes deben ser evaluados luego de cada cambio importante en el negocio. Los respaldos y la recuperación de los servicios debe ser monitoreada y evaluada para asegurar que cuando sean necesitadas durante un incidente, operen como es requerido.

4.2.2.4.4 Manejo de Cambios

El proceso de manejo de Cambios debe asegurar que todos los cambios sean evaluados respecto a su posible impacto en los planes de Manejo de Continuidad del Servicio de TI. Si los cambios planificados afectan a los planes de continuidad, entonces el plan debe ser actualizado antes de implementar el cambio y debería ser puesto a prueba como parte de la evaluación del cambio.

4.2.2.5 Invocación

La invocación es la última prueba de planes de Continuidad del negocio y Continuidad de los Servicios de TI. Si todo el trabajo preparatorio se ha completado exitosamente, con planes desarrollados y probados, entonces una invocación a los planes de Continuidad del Negocio debe ser un proceso continuo y directo, pero si los planes no han sido previamente evaluados, se podrían esperar fallas.

4.3 EJEMPLO DE UN PLAN ESPECÍFICO PARA UN SERVICIO DE ALIANZA

Con el fin de dar un ejemplo más específico de cómo aplicar las actividades para el Manejo de Continuidad de Servicio, se eligió un servicio y se aplicaron dichas normativas. El ejemplo puede ser encontrado en el Anexo 4-2.

CAPÍTULO V: ANÁLISIS DE COSTOS DE LA SOLUCIÓN DE GESTIÓN AL EVENTO MÁS CRÍTICO

En el presente capítulo se detallan las propuestas de costos para la implementación del proyecto que tiene como objetivo la mejora del evento más crítico, respecto a la Gestión de Tecnologías de Información. En Alianza CIA. de Seguros y Reaseguros S.A. el plan de mejora se lo realizará para la Gestión de Continuidad de Servicio.

Las actividades necesarias para la implementación del Plan de Gestión de Continuidad de Servicio implica la ejecución de tres tareas globales descritas en el capítulo 4: Inicio[54], Requerimientos y Estrategia[55] e Implementación[56].

Los costos para el evento más crítico comprenderán todo lo referente a capacitación y tiempo del personal interno y externo, necesario para trabajar en el proyecto.

Un curso de ITIL V3 para el gerente y los operarios del DDS es necesario para que asimilen los conceptos y ventajas de ITIL. Una vez cumplida dicha tarea inicial podrán avanzar con el procedimiento recomendado por el estándar.

Como referencia para la capacitación se toma la propuesta hecha por la empresa New Horizons.[57], la misma que consta de 24 horas de clase, distribuidas en 8 horas cada día por 3 días.

[54] El detalle se encuentra en el punto 4.2.2.1 del capítulo 4.
[55] El detalle se encuentra en el punto 4.2.2.2 del capítulo 4.
[56] El detalle se encuentra en el punto 4.2.2.3 del capítulo 4.
[57] Ver Anexo 5-1, Propuesta de New Horizons.

5.1 PROPUESTAS PARA DAR SOLUCIÓN DE GESTIÓN AL EVENTO MÁS CRÍTICO

En base a las posibles necesidades de la compañía y las ofertas del mercado se han elaborado tres propuestas para la implementación del plan de solución.

5.1.1 ALTERNATIVA 1: PERSONAL INTERNO

En esta propuesta sólo trabajará el personal del DDS[58], con la excepción de la etapa inicial donde recibirán un curso de capacitación, de un instructor externo.

Con referencia a la predisposición de la Gerencia de Sistemas para la realización del proyecto, se acordó que el personal estaría en capacidad de dedicar 2 horas diarias de las 8 para el desarrollo del proyecto. Por tal razón las horas para esta actividad se las realizará dentro de sus horas laborales normales y no se tomarán en cuenta como costo del proyecto.

[58] El DDS está formado por el Gerente, Operador 1 y 2 de Quito, y Operador de Guayaquil.

5.1.1.1 Cuadro con tareas, tiempos, participantes y costos

				Horas	Días	Gerente	Op.1 - UIO	Op.2 - UIO	Op. - GYE	PRESIDENTE	COSTO (USD)
1	TAREA GLOBAL:	CURSO									
		SUBTAREAS:	Capacitación al personal de la empresa con ITIL V3	24	3	X	X	X	X		$2.568,00
2	TAREA GLOBAL:	INICIO									
		SUBTAREAS:	Establecer políticas (motivo de la gestión, objetivos)	16	8	X	X	X	X		-
			Términos de referencia y alcance (responsables y areas de relevancia)	24	12	X	X	X	X		-
			Asignar recursos	8	4	X	X				-
			Definir la organización del proyecto y la estructura de control	40	20	X	X				-
			Aprobación de proyecto y planes de calidad	8	7	X				X	-
3	TAREA GLOBAL:	REQUERIMIENTOS Y ESTRATEGIA									
		SUBTAREAS:	Análisis de Impacto del Negocio	40	20	X	X				-
			Evaluación de Riesgos	24	12	X	X				-
			Documentación de medidas para reducción de riesgos requeridas	16	8	X	X	X	X		-
			Opciones de Recuperación	24	12	X	X	X	X		-
4	TAREA GLOBAL:	IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD									
		SUBTAREAS:	Organización y Planificación de la implementación	40	20	X	X				-
			Implementación de soluciones en espera	24	12	X	X				-
			Desarrollar Planes de Recuperación	40	20	X	X				-
			Implementación de medidas para reducción de riesgos	16	8	X	X	X	X		-
			Desarrollo de Procedimientos (8h escribir)	24	12	X	X				-
			Desarrollo de Procedimientos (8 capacitacion)	16	8	X	X	X	X		-
			Evaluación inicial	24	12	X	X	X	X		-
			TOTAL	**408**	**198**						**$2.568,00**

Tabla 5-1: Cuadro de Costos para Alternativa 1: Personal Interno

5.1.1.2 Cuadro de Costo Final

COSTO TOTAL	
ITEM	**COSTO (USD)**
CURSO	$ 2.568,00
PERSONAL	$ 0
CONSULTOR	$ 0
TOTAL	$ 2.568,00

Tabla 5-2: Cuadro de Costo Final para Alternativa 1: Personal Interno

El costo total para la Alternativa 1 es: $2.568,00

Donde:

Las tareas globales y subtareas representan el proceso recomendado por ITIL para la Gestión de Continuidad de Servicio. Además todas las tareas globales y subtareas de cada una se realizarán de forma secuencial.

Horas[59]**:** Constituyen el tiempo necesario en horas para realizar cada actividad.
Días: Con la excepción de la tarea global Curso y la subtarea de la tarea global inicio "Aprobación de proyecto y planes de calidad", los días para toda tarea se la calcula como la división para dos de las horas, considerando que cada día se trabajarán dos horas para el proyecto.
X: Significa que el involucrado participa en la realización de la tarea.
Costo: Cantidad monetaria que implica la realización de cada atarea.
Gerente: Está representado por el Gerente de Sistemas, Ing. Pablo Herrera.
Op.1 – UIO: Identificación para el Ing. Juan Carlos Guamba, Operador del DDS en Alianza con 10 años de experiencia.
Op.2 – UIO: Representa al Operador del DDS Ing. Patricio León, el mismo que cuenta con 2 años de experiencia en la empresa.
Op.1 – GYE: Identifica al Ing. Juan Carlos Cevallos técnico de Guayaquil.

[59] Tiempos sugeridos por experto en Auditoría Ec. Andrés López, experiencia de 10 años en Gerencia y Administración de Sistemas en proyectos de *Business Continuity Plan, Disaster Recovery Plan.*

Ventajas:

Cuando el equipo de Sistemas realiza el plan de Continuidad por sí mismo, aprende y aporta con su conocimiento para el desarrollo de los procesos, esto hace que tanto el Gerente como los Operarios conozcan a profundidad como se ha estado manejando la empresa y qué medidas se deben tomar para mejorar.
Además con esta propuesta ponen en práctica el curso de Gestión de Tecnologías según ITIL.

Al realizar el plan sin personal externo se ahorra el uso de un consultor, o de una persona extra para trabajar en el departamento.

Desventajas:

Se necesita que los involucrados aporten con tiempo que generalmente lo destinaban para otras actividades, como programar o dar soporte a los usuarios de la empresa.

Con la participación de sólo personal interno, el proyecto tiende a tener una duración de casi 10 meses, por el contrario contratando otra persona para soporte el tiempo sería menor.

5.1.2 ALTERNATIVA 2: PERSONAL INTERNO CON TÉCNICO TEMPORAL

La presente propuesta se desarrolla con las mismas bases de la primera, la diferencia se da en que el personal en lugar de dedicarse dos horas al proyecto se dedicará cuatro horas diarias, es decir la mitad de tiempo de su horario normal.

Se determinó que el umbral para dar paso a la contratación de una persona adicional, inicia cuando el personal del DDS empieza a dedicar más de dos horas al día para el proyecto de continuidad. Si las 4 personas del equipo de Tecnología empiezan a dedicarse 3 horas diarias en primera instancia, sabiendo que dos eran adecuadas para no afectar sus actividades diarias. La hora que no pueden cubrir

las cuatro personas se multiplica por cuatro y da como resultado cuatro horas diarias que en conjunto no se cubrirán, en este caso se necesitaría el apoyo de una persona a medio tiempo. De ahí que con la sugerencia de trabajar cuatro horas en el proyecto se necesitaría un técnico adicional a tiempo completo, generalmente para dar soporte a los usuarios de la compañía.

El empleado debe tener un perfil alto para el trabajo temporal en Alianza, de esta manera logrará acoplarse sin problemas en las actividades de gestión para: Apliance Kypus, Servidor de Antivirus McAfee, AS/400, Servidor de Active Directory en Windows Server 2003, mantenimiento preventivo y correctivo de computadores y soporte de escritorio.

5.1.2.1 Cuadro con tareas, tiempos, participantes y costos

				Horas	Días	Gerente	Op.1 - UIO	Op.2 - UIO	Op. - GYE	PRESIDENTE	COSTO (USD)
1	TAREA GLOBAL:	CURSO									
		SUBTAREAS:	Capacitación al personal de la empresa con ITIL V3	24	3	X	X	X	X		$2568,00
2	TAREA GLOBAL:	INICIO									
		SUBTAREAS:	Establecer políticas (motivo de la gestión, objetivos)	16	4	X	X	X	X		-
			Términos de referencia y alcance (responsables y areas de relevancia)	24	6	X	X	X	X		-
			Asignar recursos	8	2	X	X				-
			Definir la organización del proyecto y la estructura de control	40	10	X	X				-
			Aprobación de proyecto y planes de calidad	8	7	X				X	-
3	TAREA GLOBAL:	REQUERIMIENTOS Y ESTRATEGIA									
		SUBTAREAS:	Análisis de Impacto del Negocio	40	10	X	X				-
			Evaluación de Riesgos	24	6	X	X				-
			Documentación de medidas para reducción de riesgos requeridas	16	4	X	X	X	X		-
			Opciones de Recuperación	24	6	X	X	X	X		-
4	TAREA GLOBAL:	IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD									
		SUBTAREAS:	Organización y Planificación de la implementación	40	10	X	X				-
			Implementación de soluciones en espera	24	6	X	X				-
			Desarrollar Planes de Recuperación	40	10	X	X				-
			Implementación de medidas para reducción de riesgos	16	4	X	X	X	X		-
			Desarrollo de Procedimientos (8h escribir)	24	6	X	X				-
			Desarrollo de Procedimientos (8 capacitacion)	16	4	X	X	X	X		-
			Evaluación inicial	24	6	X	X	X	X		-
			TOTAL	**408**	**104**						**$2568,00**

Tabla 5-3: Cuadro de Costos para Alternativa 2: Personal Interno con Técnico Temporal

5.1.2.2 Cuadro de Costo Final

COSTO TOTAL	
ITEM	**COSTO (USD)**
CURSO	$ 2.568,00
PERSONAL EXTERNO	$ 3.600,00
CONSULTOR	$ 0
TOTAL	$ 6.168,00

Tabla 5-4: Cuadro de Costo Final para Alternativa 2: Personal Interno con Técnico Temporal

El costo total para la Alternativa 2 es: $6.168,00

Donde:

Las tareas globales y subtareas representan el proceso recomendado por ITIL para la Gestión de Continuidad de Servicio. Además todas las tareas globales y subtareas de cada una se realizarán de forma secuencial.

Horas[60]**:** Constituyen el tiempo necesario en horas para realizar cada actividad.
Días: Con la excepción de la tarea global Curso y la subtarea de la tarea global inicio "Aprobación de proyecto y planes de calidad", los días para toda tarea se la calcula como la división para cuatro de las horas, considerando que cada día se trabajarán cuatro horas para el proyecto.
X: Significa que el involucrado participa en la realización de la tarea.
Costo: Cantidad monetaria que implica la realización de cada atarea.
Gerente: Está representado por el Gerente de Sistemas, Ing. Pablo Herrera.
Op.1 – UIO: Identificación para el Ing. Juan Carlos Guamba, Operador del DDS en Alianza con 10 años de experiencia.
Op.2 – UIO: Representa al Operador del DDS Ing. Patricio León, el mismo que cuenta con 2 años de experiencia en la empresa.
Op.1 – GYE: Identifica al Ing. Juan Carlos Cevallos técnico de Guayaquil.

[60] Tiempos sugeridos por experto en Auditoría Ec. Andrés López, experiencia de 10 años en Gerencia y Administración de Sistemas en proyectos de *Business Continuity Plan, Disaster Recovery Plan.*

PERSONAL EXTERNO: El cálculo de este costo se realiza en base a dos parámetros, sueldo mensual del técnico temporal y tiempo a ser contratado.
El sueldo mensual para un técnico con el perfil necesario es de $600, 00[61] y el tiempo en meses de duración del proyecto se calcula:

Donde:

Se toma en cuenta que los días de trabajo a la semana son 5 y las semanas del mes son 4.

Entonces:

Lo que se le aproxima a 6 meses.

El costo de Personal externo se los realiza con la ecuación:

Entonces:

Ventajas:

Se aplican las mismas ventajas que se refieren a realizar las actividades por cuenta del personal del DDS detalladas en la alternativa uno.
A esto se suma que al permitir que el personal se dedique más tiempo a la realización del proyecto, disminuye el tiempo para realizar el proyecto a casi 6 meses.

[61] Información obtenida de la Gerencia de Sistemas, Ing. Pablo Herrera.

Desventajas:

El costo del plan de Gestión de Continuidad se incrementa a $ 6.168,00. Puede llegar a ser complicada la administración del tiempo de cada miembro del DDS.

5.1.3 ALTERNATIVA 3: PERSONAL INTERNO CON CONSULTOR

La presente propuesta, sugiere realizar las actividades mencionadas en las alternativas uno y dos, pero con la ayuda de un consultor externo. Básicamente el consultor tiene la misión de realizar las actividades de dirección que en las alternativas anteriores las tenía el gerente, con esto las horas de gerencia se verán disminuidas a la mitad.

Las horas diarias de trabajo para el proyecto serán de dos diarias, si bien el consultor dirige la implementación del proyecto, necesita horas de discusión con el grupo de trabajo.

El consultor a ser contratado debe tener experiencia en desarrollar Planes de Gestión de Continuidad del Negocio, así como un alto conocimiento en software y hardware.

5.1.3.1 Cuadro con tareas, tiempos, participantes y costos

1	TAREA GLOBAL:	CURSO		Horas	Días	Consultor	Gerente	Op.1 – UIO	Op.2 – UIO	Op. – GYE	PRESIDENTE	COSTO (USD)
		SUBTAREAS:	Capacitación al personal de la empresa con ITIL V3	24	3		X	X	X	X		$2.568,00
2	TAREA GLOBAL:	INICIO										
		SUBTAREAS:	Establecer políticas (motivo de la gestión, objetivos)	16	8	X	X	X	X	X		$560,00
			Términos de referencia y alcance (responsables y areas de relevancia)	24	12	X	X	X	X	X		$840,00
			Asignar recursos	8	2	X	X	X				$280,00
			Definir la organización del proyecto y la estructura de control	40	10	X	X	X				$1.400,00
			Aprobación de proyecto y planes de calidad	8	7		X				X	$0,00
3	TAREA GLOBAL:	REQUERIMIENTOS Y ESTRATEGIA										
		SUBTAREAS:	Análisis de Impacto del Negocio	40	10	X	X	X				$1.400,00
			Evaluación de Riesgos	24	6	X	X	X				$840,00
			Documentación de medidas para reducción de riesgos requeridas	16	8	X	X	X	X	X		$560,00
			Opciones de Recuperación	24	12	X	X	X	X	X		$840,00

4	TAREA GLOBAL:	IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD									
	SUBTAREAS:	Organización y Planificación de la implementación	40	10	X	X	X				$1.400,00
		Implementación de soluciones en espera	24	6	X	X	X				$840,00
		Desarrollar Planes de Recuperación	40	10	X	X	X				$1.400,00
		Implementación de medidas para reducción de riesgos	16	8	X	X	X	X	X		$560,00
		Desarrollo de Procedimientos (8h escribir)	24	6	X	X	X				$840,00
		Desarrollo de Procedimientos (8 capacitacion)	16	8	X	X	X	X	X		$560,00
		Evaluación inicial	24	12	X	X	X	X	X		$840,00
		TOTAL	**408**	**138**							**$15.728,00**

Tabla 5-5: Cuadro de Costos para Alternativa 3: Personal Interno con Consultor

5.1.3.2 Cuadro de Costo Final

COSTO TOTAL	
ITEM	**COSTO (USD)**
CURSO	$ 2.568,00
CONSULTOR	$ 13.160,00
DESC. GERENCIA[62]	$ 2.535,38
TOTAL	$ 13.192,62

Tabla 5-6: Cuadro de Costo Final para Alternativa 3: Personal Interno con Consultor

El costo total para la Alternativa 3 es: $13.192,62

[62] Ver ventajas de alternativa 3.

Donde:

Las tareas globales y subtareas representan el proceso recomendado por ITIL para la Gestión de Continuidad de Servicio. Además todas las tareas globales y subtareas de cada una se realizarán de forma secuencial.

Horas[63]**:** Constituyen el tiempo necesario en horas para realizar cada actividad.

Días: Con la excepción de la tarea global Curso y la subtarea de la tarea global inicio "Aprobación de proyecto y planes de calidad", los días para las tareas que realizan Consultor, Gerente y todos los operadores se la calcula como la división para dos de las horas, considerando que cada día se trabajarían dos horas. Por el contrario si la tarea es realizada sólo por el Consultor, Gerente y un operario, se trabajarán 4 horas diarias, donde el consultor trabajará 2 horas con el operario y 2 horas con el Gerente.

X: Significa que el involucrado participa en la realización de la tarea.

Costo: Cantidad monetaria que implica la realización de cada atarea.

Gerente: Está representado por el Gerente de Sistemas, Ing. Pablo Herrera.

Op.1 – UIO: Identificación para el Ing. Juan Carlos Guamba, Operador del DDS en Alianza con 10 años de experiencia.

Op.2 – UIO: Representa al Operador del DDS Ing. Patricio León, el mismo que cuenta con 2 años de experiencia en la empresa.

Op.1 – GYE: Identifica al Ing. Juan Carlos Cevallos técnico de Guayaquil.

CONSULTOR: El cálculo de este costo se realiza en base a dos parámetros, el valor hora del consultor y tiempo a ser contratado.

Entonces:

[63] Tiempos sugeridos por experto en Auditoría Ec. Andrés López, experiencia de 10 años en Gerencia y Administración de Sistemas en proyectos de *Business Continuity Plan, Disaster Recovery Plan.*

El valor hora para un consultor con el perfil necesario es de $35,00[64] y el tiempo en horas de consultoría viene de:

Entonces:

El costo del consultor es:

Ventajas:

La principal ventaja es la disminución de horas que destinará el Gerente de Sistemas en comparación a las dos alternativas anteriores, en la presente alternativa las horas de trabajo de la gerencia para el proyecto se reducirán a la mitad.

El cálculo monetario que la empresa gana al no dar horas del Gerente de Sistemas para la realización del Plan de Gestión de Continuidad de Servicio, es el siguiente:

Donde:

[64] Información obtenida del experto en Auditoría Ec. Andrés López, basado en su experiencia con la empresa InSoft.

Entonces el ahorro en dinero de parte de la Gerencia de Sistemas es de $ 2.535,38.

Otra ventaja es el apoyo del Consultor con su experiencia para realizar el proyecto, lo que permite reducir las fallas que generalmente se dan por falta de conocimiento del estándar y de su aplicación.

Desventajas:

La desventaja al contratar a un Consultor se da en que el personal no adquiere experiencia en realizar el trabajo, mientras que al realizarlo sin apoyo externo incentiva a estudiar y familiarizarse más con el estándar.

5.2 COMPARACIÓN ENTRE PROPUESTAS PARA DAR SOLUCIÓN AL EVENTO MÁS CRÍTICO

	Alternativa 1 Personal interno	**Alternativa 2** Personal interno con técnico temporal	**Alternativa 3** Personal interno con consultor
Curso ITIL V3	Si	Si	Si
Tiempo diario al proyecto de Operadores del DDS	2 horas	4 horas	2 horas
Tiempo diario al proyecto del Gerente del DDS	2 horas	4 horas	1 hora
Participantes	Instructor ITIL V3 Gerente del DDS Operador 1 UIO Operador 2 UIO Operador GYE Presidente de Alianza	Instructor ITIL V3 Gerente del DDS Operador 1 UIO Operador 2 UIO Operador GYE Presidente de Alianza Empleado temporal	Instructor ITIL V3 Gerente del DDS Operador 1 UIO Operador 2 UIO Operador GYE Presidente de Alianza Consultor
Costo	$ 2.568,00	$ 6.168,00	$ 13.192,62
Duración del proyecto	198 días	104 días	138 días

Tabla 5-6: Comparativa entre propuestas para dar solución al evento más crítico.

5.2.1 COMENTARIO

- En común todas las alternativas 1, 2 y 3, tienen el curso de ITIL V3 como su primera etapa. Además las tres alternativas poseen las mismas actividades, con el mismo número de horas de duración. Las tres alternativas poseen las mismas actividades encabezadas por el curso ITIL porque tienen la misma estructura, lo que cambia es modo de participación de los involucrados.

- El tiempo diario que ofrecen los Operadores del DDS, a la elaboración del proyecto es de dos horas diarias para las alternativas 1 y 2, debido a que en estas alternativas no existe la participación de un técnico temporal que ayude a resolver dificultades de soporte técnico, sin la ayuda de esta persona no se pueden incrementar las horas diarias de los Operadores del DDS. En la alternativa dos como existe la participación de un empleado temporal, las horas diarias que los Operadores del DDS pueden aportar para la elaboración del proyecto se incrementan a 4 horas.

- El tiempo diario que ofrece el Gerente de Sistemas, para la alternativa 1 es de dos horas diarias, puesto que debe aportar en iguales condiciones que los Operadores del DDS, lo mismo se aplica para la alternativa 2, pero ahora los dos grupos deben aportar con 4 horas diarias de su trabajo para el proyecto. En la alternativa 3 se da la diferencia por el ingreso de un consultor externo, mismo que a más de asesorar a la empresa, trata de alivianar la carga que tendría el Gerente del DDS a la mitad, en comparación con las otras dos alternativas, por esto la hora diaria promedio del gerente se reduce a 1, mientras que los operadores deben aportar con las dos establecidas.

- En las tres alternativas se cuenta con la participación de: Instructor ITIL V3, Gerente del DDS, Operador 1 UIO, Operador 2 UIO, Operador GYE y Presidente de Alianza. Para la alternativa dos, puesto que se trata de incrementar las horas que se dediquen al proyecto se incluye la participación de un empleado temporal. En la tercera se adiciona la participación de un consultor, mismo que justifica su participación en primer lugar para ayudar al

desarrollo del proyecto puesto que los miembros del DDS no tienen experiencia en la elaboración de este tipo de proyecto, pero además para aliviar la carga de trabajo que implica la elaboración del plan de continuidad para el Gerente de Sistemas.

- El costo de cada alternativa se relaciona directamente con los participantes de cada una. Es así que la primera alternativa es la más barata porque no adiciona personal externo, con la excepción del instructor de ITIL que se incluye en todas las alternativas, sólo se trabaja con la Gerencia de Sistemas, Operadores del DDS y presidente de la empresa. La segunda alternativa tiene un costo intermedio por implicar la contratación de un empleado temporal. Finalmente la tercera y más cara alternativa, tiene este costo porque requiere la contratación de un consultor externo que va a asesorar en todo el desarrollo del proyecto.

- La duración del proyecto, depende de igual forma de sus participantes, la primera alternativa es la más larga porque sólo usa personal interno, la segunda es la más corta dado que un empleado temporal ayudará con las labores cotidianas de soporte, se pueden incrementar las horas de colaboración diarias de los miembros del DDS, esto provoca que se elabore más rápido el proyecto. La tercera alternativa es intermedia en relación a la duración del proyecto debido a que si bien un auditor externo colaborará en el asesoramiento, las horas diarias destinadas para los miembros del DDS serán las mismas, con excepción de la Gerencia de Sistemas que disminuye su carga a la mitad.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

El diseño de la investigación de ITIL para Alianza CIA. de Seguros y Reaseguros S.A. tomando en cuenta los procesos Gestión de: Nivel de Servicio, Continuidad de Servicio, Cambios, Configuraciones, Incidentes y Problemas, puede ser utilizada como base para analizar puntos críticos en compañías similares, el aporte en este caso será la disminución de tiempo para el análisis.

La implementación de ITIL requiere el apoyo de no solamente el grupo de tecnología de la empresa, por el contrario de todos sus miembros. De ahí que el estudio se debe realizar individualizado para cada grupo identificado de la empresa.

Gracias a la experiencia del DDS en el manejo de: Sistema de Seguros, equipo Kypus y enlaces WAN, nombrando a los principales, los ejecutivos califican con un grado de confianza alto a la calidad de servicios de tecnología a pesar de que el equipo de Sistemas de Alianza no defina formalmente los servicios con la calidad respectiva que se proveen a los usuarios internos de la compañía. Por esto el impacto en la reputación al no realizar un catálogo de servicios es baja pero a lo largo del tiempo con respecto al impacto en resultados se determina que la definición correcta de los servicios ayuda a que estos sean explotados en toda su potencialidad.

Para el grupo de Usuarios Comunes tampoco no se les ha sido presentado los servicios de tecnología pero tienen una percepción Moderada de la calidad recibida del Sistema de Seguros y Correo, mismos que son los principales para ellos, esta afirmación dice que los usuarios aceptan que existe una calidad media con la cual se puede trabajar.

Finalmente para los Puntos de Venta SOAT, si bien no conocen como los otros dos grupos nombrados formalmente los servicios de TI, ellos los tienen bien identificados y con un GC Alto.

Al analizar los tres grupos de usuarios se concluye que el DDS da un nivel de prioridad alta a los Ejecutivos por su importancia y a los Puntos de Venta SOAT, por ser usuarios externos que son fuente de todos los potenciales clientes del sector. Y una prioridad un poco más moderada a los usuarios que se encuentran dentro de la empresa por su contacto más directo con el departamento de tecnología y la posibilidad de adaptarse sin problemas a los recursos disponibles.

La eficiencia de los planes de contingencia para enfrentar emergencias sólo se comprueban al enfrentar una crisis. De la misma manera aparecen las falencias o los planes no existentes cuando se da un evento negativo inesperado. Al presente tanto los usuarios internos (Ejecutivos y Usuarios Comunes) como externos (Puntos de Venta SOAT) no tienen conocimiento de cómo proceder ante crisis debido a que la Gerencia de Sistemas y sus Operadores no han realizado un análisis de vulnerabilidades por lo que no se ha desarrollado planes formales para enfrentar eventos que provoquen corte de servicios vitales para la empresa como: Sistema de Seguros e Internet. El problema fue conocido por toda la organización cuando empezaron los cortes de energía eléctrica en el año 2009, debido a la falta de mantenimiento de la planta eléctrica lo que provocó que la sucursal de Quito responsable de mantener disponibles todos los servicios, incluido el Sistema de Seguros, permaneció en funcionamiento intermitente o anormal por cerca de 24 horas según Marcelo Galeano subgerente de la compañía. Este problema provocó pérdidas para la empresa que pudieron ser evitadas al implementar planes de salvaguarda que si bien tienen una inversión en tiempo y recursos ayudarían a que no existan cortes de servicio nacionales de las 7 sucursales.

Según los resultados de la encuesta referente a Gestión de Cambios se concluye que los cambios realizados en general cumplen con las expectativas de los usuarios internos y externos de la compañía. Esto indica que tanto el Gerente de Sistemas como los Operadores saben panificar, para conseguir éxito en la

implementación de cambios, además de al final comprobar la satisfacción de los involucrados. El punto negativo esta en que no se hace una documentación formal del inicio, progreso y cierre de un cambio, ni tampoco se ha elaborado un método para que el beneficiado evalúe el trabajo realizado. Si bien esto no influye aparentemente en la ejecución de cambios este ordenamiento tendría una repercusión a largo plazo en impacto de resultados y económico.

La Gestión de Configuraciones al ser una actividad interna del DDS, para los Ejecutivos y Usuarios Comunes no es muy perceptible la buena o mala gestión. Por esto se da que mientras Elizabeth Vallejo Gerente Financiera y jefe inmediato del DDS indica que no han sido presentados procesos formales para realizar configuración de equipos y se asume que no se utiliza un método ordenado y metódico. Por otro lado los Usuarios Comunes afirman un GC Moderado Alto para configuraciones realizadas de forma metódica y ordenada. Entonces los grupos de Gerente y Operadores del DDS son los más indicados para evaluar los procesos de Gestión de Configuraciones, aquí es donde se identificó que las falencias están en el deficiente registro de configuraciones sobre equipos así como de características de los mismos.

La Gestión de Incidentes reflejada en la solución de los mismos de parte del DDS, tiene una calificación positiva según los Ejecutivos, Usuarios Comunes y Puntos de Venta SOAT, a pesar de que no existe un lineamiento para que los usuarios registren sus incidentes formalmente o tengan la posibilidad de calificar el servicio. Este caso se da porque tanto Gerente como Operadores del DDS tienen como objetivo tratar de solucionar el incidente lo más pronto posible, así como el informar al usuario sobre el avance en el proceso de cierre de su incidente.

Tomando en cuenta que la visión de Alianza CIA de Seguros y Reaseguros S.A. es “Liderar el mercado de seguros ecuatoriano”, se concluye que su principal servicio tecnológico es el Sistema Integrado de Seguros, de la mano con este van los enlaces dedicados entre Quito y las sucursales del resto del país, así como el servidor de transacciones para el Sistema SOAT. Estos servicios son críticos y al

no mantener planes de emergencia para ellos se corre el riesgo de incumplir con los objetivos de la empresa.

El proceso sugerido por el autor basado en ITIL para manejar de forma adecuada la Gestión de Nivel de Servicio, reconocido como proceso crítico consta de cinco actividades, pero para el presupuesto de implementación sólo se incluyeron las actividades de Inicio, Requerimientos - Estrategia y finalmente de Implementación, las actividades Operación en Producción e Invocación no se las tomó en cuenta, por ser tareas post implementación.

Luego del estudio del desempeño que ha tenido Alianza con respecto al estándar ITIL, y al darse como descubierta la criticidad de la gestión de Continuidad de Servicio se concluye que a pesar de que cuando surgían los problemas como el caso del generador eléctrico en tiempo de estiaje, se solucionaban cuando ocurrían, no se lo estaba remediando por completo e incluso no se generaba un plan ni se identificaban las amenazas. La solución está en seguir un proceso ordenado que ayude a evaluar si se hace bien o mal y además que se acople a los demás procesos de la empresa, aquí esta es la importancia en usar un estándar como ITIL, el mismo que da lineamientos de cómo proceder para gestionar la tecnología y alertar cuando un problema está próximo a causar un incidente o luego una catástrofe.

6.2 RECOMENDACIONES

Al definir la organización del proyecto y la estructura de control para el Plan de Gestión de Continuidad de Servicio, se recomienda usar el estándar PMBOK en la parte inicial para enseñar y dar todos los conocimientos necesarios al personal acerca de gestión de proyectos. Luego para la implementación y manejo se recomienda usar PRINCE2 por su enfoque en mejorar las probabilidades de éxito en el desarrollo de proyectos.

El DDS debería aprovechar el apoyo que existe de parte de los ejecutivos de Alianza, para implementar mejoras en Gestión de: Nivel de Servicio, Continuidad

de Servicio, Configuraciones, Incidentes y Problemas. Según las encuestas realizadas todos los ejecutivos calificaron con una predisposición de apoyo del 100 %.

Las prioridades establecidas actualmente con referencia al Nivel de Servicio de parte del DDS deben ser establecidas con la misma tendencia para mantener la satisfacción de Ejecutivos y Puntos de Venta SOAT, pero revisar necesidades de Usuarios Comunes para elevar su satisfacción moderada y prevenir que por falta de apoyo tecnológico exista deficiencia laboral.

El proceso ITIL crítico para la Alianza CIA de Seguros y Reaseguros S.A. es la Gestión de Continuidad de Servicio, por esto se debe por lo menos hacer un análisis de vulnerabilidades tomando en cuenta los objetivos del negocio, y para los eventos críticos encontrados formalizar planes de contingencia para bajar el riesgo de la amenaza: baja disponibilidad del Sistema de Seguros, que podrían sufrir sus clientes por un tiempo prolongado.

La Gestión de Cambios es recomendable mantenerla con el buen nivel de satisfacción que reflejan los Ejecutivos, Usuario Comunes y Puntos de Venta SOAT, pero se debe mejorar la forma de comunicar a los posibles afectados que un servicio dado puede ser suspendido debido a las tareas necesarias para completar un cambio. La planificación debe tomar especial cuidado con los Puntos de Venta SOAT, dado que una falla en el sistema no anunciada puede ocasionar insatisfacción en sus clientes y la futura migración hacia la competencia.

Se recomienda llevar un registro actualizado de configuraciones realizadas sobre todos los equipos de la infraestructura tecnológica, esto ayudará a resolver con mayor eficiencia incidentes y reducir el tiempo que la organización tenga que permanecer en estado de emergencia.

La Gestión de Incidentes en Alianza CIA de Seguros y Reaseguros S.A. se debe formalizar usando un método que automatice los pedidos de los usuarios. Caso contrario por más que exista la predisposición de resolver inmediatamente de

parte de la Gerencia y los Operadores del DDS, no se darán abasto a los pedidos que se pueden generar de más de 100 usuarios internos distribuidos en 7 sucursales además de 400 Puntos de Venta SOAT a nivel nacional.

Se recomienda que tanto Gerencia y Operadores del DDS se familiaricen con la diferencia entre problemas e incidentes, para que manejen como prioridad la resolución de incidentes antes de la investigación para solucionar problemas. Actualmente esta diferenciación se la realiza parcialmente en los dos grupos.

Es recomendable integrar en el proceso de Requerimientos y Estrategia segundo punto de las actividades para el manejo de Continuidad de Servicio sugeridas en el capítulo 4, los servicios primordiales detectados: Sistema de Seguros Integrado, Enlaces Dedicados entre Sucursales, Servicio de Internet, Correo Electrónico y Soporte a los Usuarios.

La actividad de Inicio sugerida para Gestionar el Proceso crítico ITIL de Alianza, se recomienda que sea con la participación de todos los miembros del DDS, debido a que cada uno puede aportar con ideas valiosas según su experiencia y actividades diarias, a pesar de que se elija la opción de utilizar un consultor externo, esta persona sólo guiará la reunión y recomendará lo mejor basado en lo expuesto por los miembros internos de la empresa.

Para las empresas del sector público se recomienda el uso del estándar ITIL con el fin de dar orden a los procesos de gestión en la Unidad de Tecnología de Información. Esto ayudará a mejorar su desempeño en los lineamientos normados por la Contraloría General del Estado[65] de: Organización informática, Segregación de funciones, Plan informático estratégico de tecnología, Políticas y procedimientos, Administración de proyectos tecnológicos, Desarrollo y adquisición de software aplicativo, Adquisiciones de infraestructura tecnológica, Mantenimiento y control de la infraestructura tecnológica, Seguridad de tecnología de información, Plan de contingencias, Administración de soporte de tecnología

[65] Obtenido del Acuerdo N° 039-CG, Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos.

de información, Monitoreo y evaluación de los procesos y servicios, Sitio web servicios de internet e intranet, Capacitación informática y Comité informático.

BIBLIOGRAFÍA

LIBROS:

- Randy A. Ateinberg & Robin Yearsley, ITIL Design Guidelines, OGC, 2007.
    - Part 1-ITIL Service Strategy.
    - Part 2-ITIL Service Design.
    - Part 3-ITIL Service Transition.
    - Part 4-ITIL Service Operation.
    - Part 5-ITIL Continual Service Improvement.

- Menken Ivanka, ITIL factsheets, the art of service, 2007.

- Ronald Walpole, Raymond Myers, Sharon Myers, Keying Ye. Probabilidad y Estadística para Ingeniería y ciencias. PRENTICE HALL. 8 Ed. 2007.

- Contraloría General del Estado, Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, Acuerdo N° 039-CG, Registro Oficial, Quito, 14 de diciembre de 2009.

DIRECCIONES ELECTRÓNICAS:

- http://www.itil-officialsite.com/home/home.asp.
    - Fecha de acceso: 15/01/10.
- http://www.best-management-practice.com/IT-Service-Management-ITIL/?trackid=002094.
    - Fecha de acceso: 15/01/10.

- http://www.isoiec20000certification.com/about/whatis.asp.
    - Fecha de acceso: 20/12/09.
- http://www.iso.org/iso/catalogue_detail?csnumber=41332.
    - Fecha de acceso: 20/12/09.
- http://www.iso.org/iso/home.htm.
    - Fecha de acceso: 20/12/09.