Gestión de riesgos de seguridad en ACME

GALVÁN, Gabriela

G. Galván

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

ACME, is a Mexican Company dedicated to marketing high value solutions based on technology information services, with market knowledge for more than 15 years of experience. It has ISO9001 certification, for the delivery of IT services and solutions in the Mexican market. The objective of the present work is to know the level of risk to which the organization is exposed by information security risks for the delivery of Managed Services and based on the analysis determine the necessary controls to mitigate the risk to which the organization is exposed to ensure the value of the company and the projected growth for this group of services based on ISO / IEC 27005 (Information security risk management).

2 Introducción

El uso de las tecnologías de la información (TI) se ha intensificado en las organizaciones independiente de la naturaleza y actividad de las mismas, estás se encuentran en constante evolución adaptándose a las nuevas necesidades de las organizaciones y así mismo dando lugar a otras relacionadas con su operación diaria. Adicionalmente su masificación las han convertido en blanco de ataques; los riesgos asociados a estas se intensifican y transforman y por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información que las organizaciones quieren proteger.

Derivado del crecimiento en el ofrecimiento de Servicios Administrados en el mercado de Mexicano, ACME identifica la necesidad de fortalecer la tecnología, procesos, procedimientos y el recurso humano especializado de TI para la entrega de este grupo de servicios. La estrategia de la organización es iniciar con una evaluación para conocer el nivel de riesgos de seguridad al que está expuesta para poder determinar los controles necesarios que permitan mitigar el riesgo y de esta forma asegurar el valor de la empresa y el crecimiento proyectado para el grupo de Servicios Administrados con base en ISO/IEC 27005 (Information security risk management).

El resultado del presente trabajo mostrará las áreas de oportunidad para una mejor gestión de riesgos de seguridad en la organización que permita que la entrega de Servicios Administrados cumpla con los estándares de calidad necesarios para asegurar el crecimiento del 20% en el próximo año que permita que la empresa fortalezca su posición en el mercado mexicano.

2.1 Metodología

Alineación ISO27005 con modelo PHVA

La metodología para el presente análisis se alinea con el modelo PHVA con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua siguiendo el esquema presentado a continuación:

Planificar. Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.

Hacer. Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos.

Verificar. Evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados.

Actuar. Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimientos de los indicadores que fueran establecidos desde la planificación.

Como se mencionó anteriormente, la metodología a usar tiene su base en ISO 27005 e ISO 31000, dado su enfoque en gestión de riesgos y siendo parte de los estándares de la familia ISO fue posible establecer una alineación con el l modelo PHVA (Tabla 2).

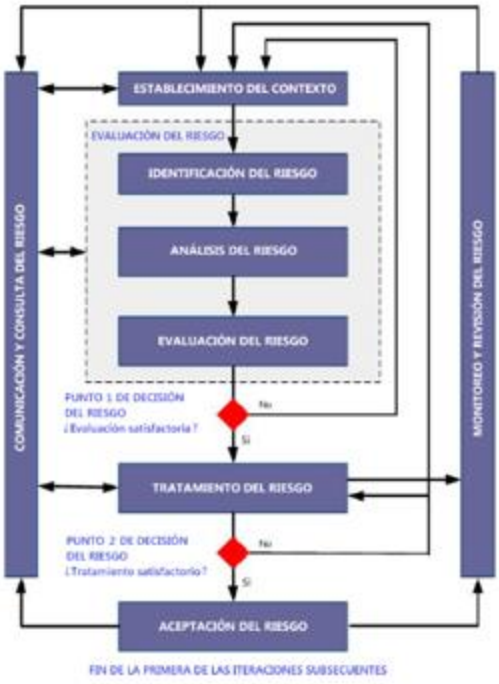
Tabla 2 Alineación de estándar ISO 27005 con modelo PHVA

PHVA	ISO 27005	
Planear	Definir plan de gestión de riesgos	
	Establecimiento del contexto	
	Valoración Riesgo	Identificación del riesgo
		Estimación del riesgo
		Evaluación del riesgo
	Desarrollar el plan de tratamiento del riesgo	
	Aceptación del riesgo	
Hacer	Implementar el plan de tratamiento	
	Implementar plan de comunicación del riesgo	
Verificar	Monitoreo y revisión del riesgo	
Actuar	Mantener y mejorar el proceso de gestión	

La metodología sigue los pasos del proceso de gestión de riesgos de acuerdo a ISO 27005, la cual contempla las siguientes etapas (Figura 2).

- Establecimiento de plan de comunicación interno y externo
- Definición del contexto organizacional
- Evaluación de riesgos
- Tratamiento de riesgos
- Monitoreo y revisión de riesgos

Figura 2 Proceso de Gestión de Riesgos ISO 27005



2.2 Plan de Comunicación

Establecimiento de plan de comunicación interno y externo

El plan de comunicación se debe realizar a nivel interno (áreas de la organización, empleados, directivos, socios) y externo (clientes, proveedores, entes reguladores, todos los anteriores si así se requiere), teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el debido informe de los avances del proceso y todo aquello que se considere necesario.

El plan de comunicación debe crear conciencia en seguridad, si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información de soporte al análisis y colaborar en la planificación del proceso de gestión de riesgos.

El plan de comunicación propuesto se compone de acciones de comunicación desde el inicio de la implementación hasta su cierre y durante la operación del esquema de gestión (Tabla 2.1).

Tabla 2.1 Plan de comunicación

Etapa	Tema	Objetivo	Periodicidad	Audiencia	Medio	Responsable
Inicio Implementación	Presentación esquema Gestión de Riesgos Seguridad	1. Entendimiento esquema de riesgos 2. Entendimiento conceptos riesgos 3. Beneficios gestión de riesgos 4. Presentación organigrama del proyecto de implementación	Una vez al inicio	Personal Interno Proveedores	Presentación Banner	Gerente Seguridad
Durante Implementación	Campaña de Concientización	1. Sensibilizar a colaboradores sobre los diferentes problemas asociados a los riesgos de seguridad y su inadecuada gestión. 2.Difundir los beneficios de la Gestión Integral de Riesgos de Seguridad para lograr que la organización se involucre en sus diferentes etapas de implementación. 3. Fomentar prácticas para minimizar los riesgos de seguridad 4. Promover la detección de riesgos de seguridad 5. Dar visibilidad de los hallazgos y soluciones, así como los beneficios adquiridos	Mensual	Personal Interno Proveedores	Presentación Correos Talleres	Gerente Seguridad Gerentes de área
	Presentación avance	1. Informar sobre el estado de la implementación 2. Informar sobre los entregables comprometidos 3. Informar atrasos, riesgos o situaciones destacables 4. Informar compromisos siguiente periodo 5. Obtener retroalimentación y mantener la participación de todos los involucrados en la organización 6. Establecer acciones preventivas / correctivas necesarias	Quincenal	Equipo Implementación	Presentación	Gerente Seguridad
Final Implementación	Presentación Cierre de Implementación	1. Informar cumplimiento de los objetivos de la implementación 2. Formalizar esquema final de Gestión de Riesgos de Seguridad 3. Formalizar inicio de operación	Una vez al cierre	Personal Interno Proveedores	Presentación	Gerente Seguridad
Durante Operación	Presentación indicadores	1. Informar a la dirección del desempeño del esquema de gestión necesarias 2. Determinar acciones preventivas o correctivas	Semestral	Dirección Equipo Seguridad	Presentación	Gerente Seguridad

2.3 Definición del contexto organizacional

Misión

Ser el referente mexicano para los productos de consultoría y servicios de alto valor agregando en las TIC´s que genere un sistema sustentable, apreciado entre nuestros clientes, colaboradores, proveedores y accionistas.

Visión

Transformar la industria de los proveedores de soluciones en las Tecnologías de Información y Comunicaciones (TIC´s), a través de una propuesta diferenciada, en función de la sinergia entre las estrategias de negocio de los clientes, su innovación y la oferta tecnológica.

Filosofía

Leer oportunamente los cambios en la industria, en el mercado y en los clientes, para poder adecuar el mejor portafolio de soluciones y competencias que permitan a nuestro ecosistema desarrollarse económicamente.”

Política de Calidad

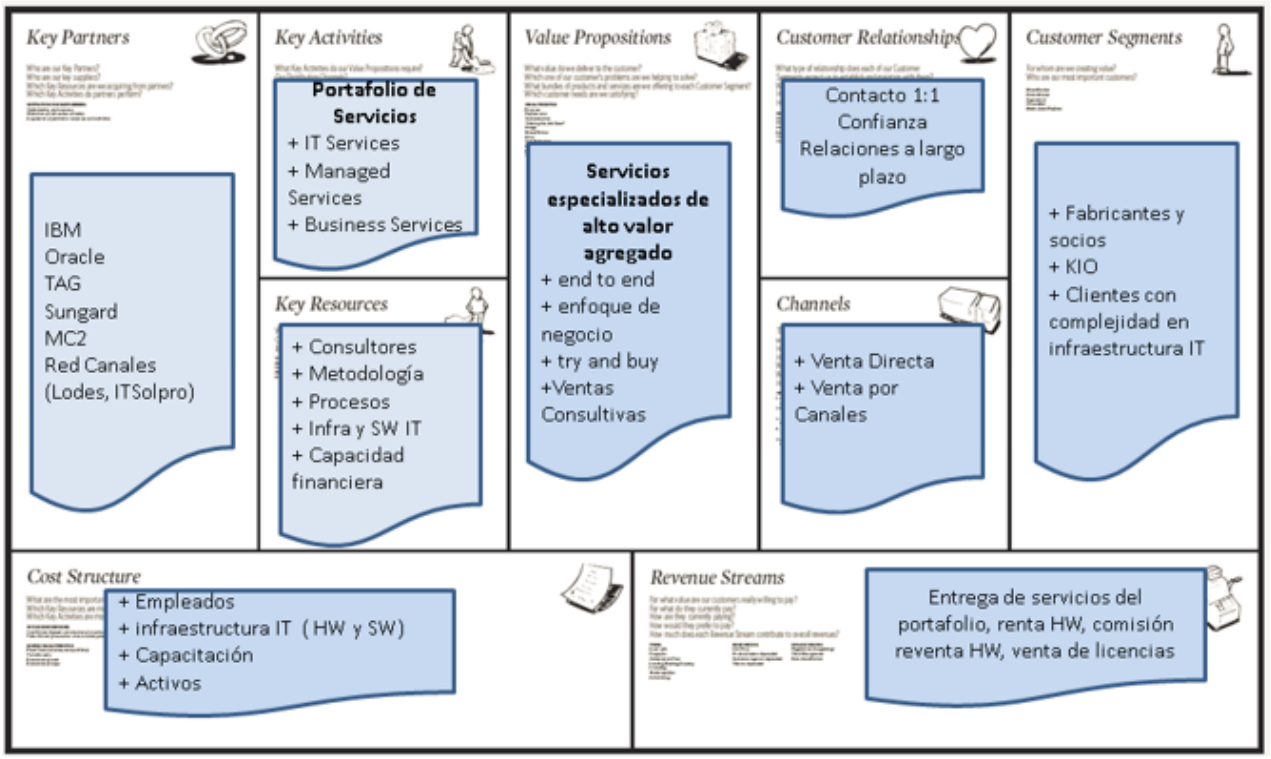
Asegurar, que mediante nuestras soluciones, las Tecnologías de la Información y Comunicación coadyuven al logro de las estrategias de negocio de nuestros clientes sin perder de vista la mejora continua de nuestro Sistema de Gestión de Calidad.

Modelo de Negocio

ACME genera ingresos y utilidades mediante servicios especializados en TI que resuelven los problemas de negocio de sus clientes. Típicamente ACME apoya reduciendo el costo operacional o permitiendo la habilitación de nuevas capacidades que generen ingresos en el negocio de los clientes.

Los servicios de ACME permiten a los clientes optimizar su ambiente de TI a través de la eficiencia, la flexibilidad y la productividad, al mismo tiempo que se genera reducción de costos.

Tabla 2.2



Clientes Objetivo. Se cubren clientes principalmente en las industrias de Servicios Financieros, Distribución y Productos de Consumo. Tienen como característica principal una infraestructura de TI compleja y por lo mismo, el valor de la inversión en estos activos es muy grande.

Portafolio de Servicios

ACME cuenta con un portafolio dinámico, sólido y actual que incluye soluciones de corto y largo plazo, con soluciones relevantes del mercado y un enfoque de ahorro y calidad con foco en servicios administrados.

El portafolio cuenta con 3 grandes pilares; IT Services, Managed Services y Business Services, las cuales son soportadas en su implementación por metodologías y mejores prácticas de las TICs , al igual que múltiples especialidades donde se garantiza que se cuenta con certificaciones en todas ellas.

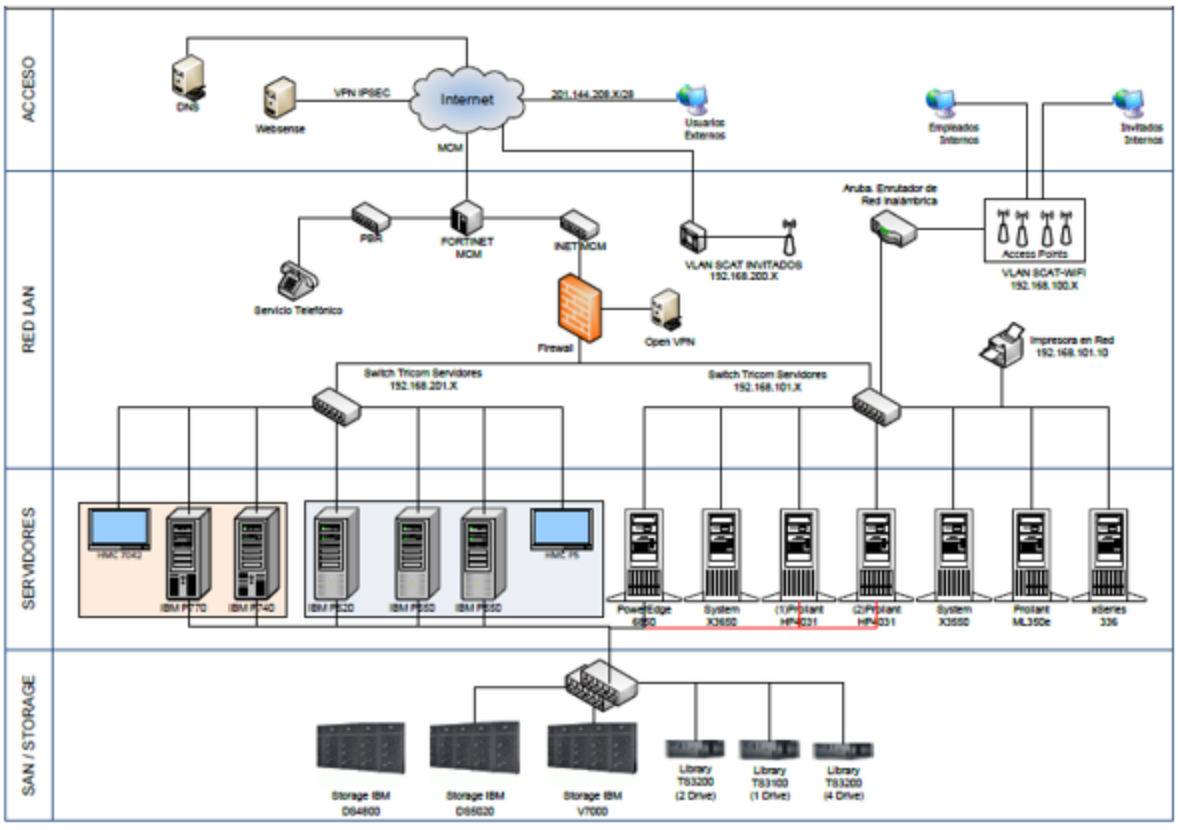
El alcance de este análisis se limita al grupo de Servicios Administrados que forma parte del pilar de "Managed Services que se muestra en la Figura 2.1.

Figura 2.1 Detalle por grupo de servicios

2.4 Análisis de Riesgos

Alcance

Figura 2.2 Infraestructura involucrada para el alcance del análisis



Evaluación de Riesgos

En la etapa de evaluación de riesgos se identifican los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestos. Se tomaron en cuenta los activos relevantes, señalando los daños que pueden implicar las amenazas, la determinación de las probabilidades e impactos.

Para los activos y escenarios de riesgos identificados se valoraron los siguientes elementos:

- Consecuencia
- Dificultad de acceso al activo
- Confidencialidad
- Integridad
- Disponibilidad
- Explotación de la amenaza
- Control implementado
- Reporte de la amenaza

El resultado de las valoraciones arrojó el nivel de riesgo inicial y riesgo residual para cada escenario de riesgo.

Tabla 2.3 Riesgos del SITE

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
1	SITE	Robo o daño intencionado de equipos que puede afectar la disponibilidad de los servicios	Falta de control de acceso al site para personal interno o ajeno a la empresa	BAJO	ALTO	BAJO	PARCIAL	NINGUNA	PARCIAL	DISPONIBILIDAD	NO PROBADA	PERMANENTE	NO CONFIRMADO	53.66%	17.52%
2		Daño parcial o total de equipo en caso de un incendio	Falta de sistema de incendios (Extintores)	BAJO	ALTO	ALTO	COMPLETA	NINGUNA	COMPLETA	DISPONIBILIDAD	NO PROBADA	NINGUNO	NO CONFIRMADO	68.01%	35.30%
3		Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad	Falta de mantenimiento al sistema de aire acondicionado	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
4		Indisponibilidad del servicio por Falta de energía	Insuficiencia del Power Supply por fallas en baterías para soportar más de 7 min el suministro de energía	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	82.91%	82.91%
5		Indisponibilidad del servicio por fallas en cableado	Falta de un cableado estructurado de quipos	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%
6		Acumulación de polvo u otros residuos que dañan los componentes de la infraestructura	Falta de limpieza periódica	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.94%	19.86%

Tabla 2.4 Riesgos hardware general

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
7	HARDWARE GENERAL	Falla del equipo que puede afectar la disponibilidad de los servicios	Falta de póliza de mantenimiento y soporte	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
8		Caída de ambientes críticos	Falta de esquema de alta disponibilidad para ambientes críticos	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
9		Obsolescencia tecnológica	Falta de plan de renovación de tecnología para asegurar el buen desempeño de los ambientes	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%
10		Perdida o mal manejo de información en desecho de equipos	Falta de control en eliminación de desechos	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PRUEBA DE CONCEPTO	PERMANENTE	IDENTIFICADO	13.58%	13.58%

Tabla 2.5 Riesgos de acceso y servidores

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
11	ACCESO DNS (Nube) Websense (Nube) Internet	Problemas de acceso en cambios de IP's	Accesos Hardcoded	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	59.96%	48.74%
12		Dependencia de internet para otorgar servicios	Punto único de falla en ISP (Internet)	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
13	SERVIDORES Equipos Power Equipos X (Vmware,Linux yWindows)	Vencimiento equipos en comodato	Ambientes productivos de clientes se encuentran instalados en equipos prestados y no hay equipos propios para migrar ambientes	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PRUEBA DE CONCEPTO	NINGUNO	IDENTIFICADO	59.96%	49.49%
14		Deficiencia en la operación	Falta de capacidad de equipos	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%

Tabla 2.6 Riesgos de red y almacenamiento/biblioteca

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
15	RED Switches de LAN	Empleados y clientes no pueden acceder a los ambientes	Punto único de falla Firewall	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
16			Punto único de falla en Switches LAN	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
17	ALMACENAMIENTO/BIBLIOTECA Storage V7000 Storage DS5020 Bibliotecas IBM TS3200, TS3100 Switches de SAN	Incumplimiento RTO y RPO, posible perdida de información	Incapacidad para poder realizar los respaldos comprometidos por falta de cintas LTO4	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	82.91%	78.38%

Tabla 2.7 Riesgos de software

ID	Activo	Amenaza	Vulnerabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
18	SOFTWARE	Errores o fallas del software (Mal funcionamiento)	Falta de control de cambios	MEDIO	BAJO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.13%	28.28%
19		Errores de uso	Falta de documentación o actualización para operación de los sistemas y servicios	ALTO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	60.75%	60.75%
20			Asignación incorrecta de accesos	MEDIO	BAJO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	42.50%	42.50%
21			Configuración incorrecta	MEDIO	BAJO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	NO CONFIRMADO	25.00%	25.00%
22		Pérdida de versiones de respaldos	Falta de políticas de respaldo adecuada	ALTO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	60.75%	60.75%
23		Problemas de no licenciamiento adecuada de software	Falta de control en descarga de software	MEDIO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	INMEDIATO	CONFIRMADO	31.75%	31.56%

Tabla 2.8 Riesgos del personal

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
24	PERSONAL	Incumplimiento en los SLA's de cliente	Falta de atención a clientes por ausencia del personal	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.94%	19.86%
25		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Procedimientos de redutamiento inadecuados	MEDIO	MEDIO	ALTO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	41.63%	29.16%
26			Capacitación inadecuada	MEDIO	MEDIO	ALTO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	41.63%	29.16%
27		Robo de documentos o medios de almacenamiento	Trabajo no supervisado de proveedores	MEDIO	MEDIO	ALTO	PARCIAL	NINGUNA	NINGUNA	CONFIDENCIALIDAD	PROBADA	PERMANENTE	CONFIRMADO	33.31%	27.08%

Tabla 2.9 Riesgos de administración – 1a parte

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
28	ADMINISTRACION	Abuso de derechos, robo, eliminación y/o modificación de información	Falta de procedimientos registro y cancelación de usuarios	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	PERMANENTE	CONFIRMADO	76.50%	76.50%
29			Falta de previsiones referentes a seguridad en contratos con clientes, proveedores y empleados	MEDIO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	FUNCIONAL	NINGUNO	IDENTIFICADO	45.00%	45.00%
30		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Falta de auditorias regulares (supervisión)	MEDIO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	45.00%	45.00%
31			Falta de monitoreo de operaciones	MEDIO	ALTO	N/A	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	45.00%	45.00%
32			Falta de actualización de procedimientos operativos	ALTO	MEDIO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	42.50%	42.50%

Tabla 2.10 Riesgos de administración – 2a parte

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
33	ADMINISTRACION	Pérdida parcial o total del Site	Falta de plan de continuidad	ALTO	ALTO	N/A	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
34		Perdida de evidencia	Falta de logs de operadores y administradores	ALTO	ALTO	N/A	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
35		Modificación no autorizada, no intencional de la información y mal uso de los activos de información	Falta de clasificación de la información	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
36			Falta de definición de responsabilidad de seguridad en perfiles de puestos	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
37			Falta de segregación de funciones	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%

Resumen Evaluación de Riesgos

La valoración de riesgos en su conjunto muestra que el nivel de riesgo inicial de la organización no cumple con la tolerancia al riesgo establecido del 30%, el 62% de los escenarios son de riesgo MUY ALTO y un 32% con riesgo ALTO, es decir el 94% de los riesgos están fuera del limite establecido, en promedio el nivel de riesgo es del 58% (Figura 5).

El riesgo residual muestra una ligera mejora bajando a 75% los riesgos arriba del limite establecido con un promedio del 53% (Tabla 2.11).

Tabla 2.11 Resumen evaluación de riesgos

TIPO RIESGO	RANGO	RIESGO INICIAL		RIESGO RESIDUAL	
		Cant	%	Cant	%
Verde (Riesgo BAJO)	0-10%	0	0	0	0
Azul (Riesgo MEDIO)	11-30%	2	5%	9	24%
Amarillo (Riesgo ALTO)	31-50%	12	32%	9	24%
Rojo (Riesgo MUY ALTO)	51-100%	23	62%	19	51%
		37	100%	37	100%
Promedio			58%		53%

La organización establece que la prioridad del tratamiento de riesgos es la siguiente (Tabla 2.12).

Tabla 2.12 Prioridad tratamiento de riesgos

PRIORIDAD	NIVEL RIESGO	FECHA COMPROMISO
1	Rojo (Riesgo MUY ALTO)	mar-17
2	Amarillo (Riesgo ALTO)	jun-17
3	Azul (Riesgo MEDIO)	sep-17

Tratamiento de Riesgos

Como parte del tratamiento se definen las posibles acciones a seguir sobre los riesgos y de acuerdo a la prioridad establecida se determinan los beneficios, responsables, recursos, fechas compromiso e inversión requerida considerando las restricciones de presupuesto.

Los tratamientos recomendados deben incluir un análisis costo-beneficio (incluyendo costos de implementación y mantenimiento), sin embargo por falta de tiempo no se incluyen en este trabajo, sólo se especifica si se requiere inversión pero no se indica el monto de dicha inversión.
Los tratamientos propuestos se listan a continuación:

Tabla 2.13 Tratamiento riesgos del SITE

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
1	SITE	Robo o daño intencionado de equipos que puede afectar la disponibilidad de los servicios	Falta de control de acceso al site para personal interno o ajeno a la empresa	1. Cerradura en entrada al SITE 2. Autorización de acceso con asignando de un gafete 3. Bitácora de accesos (Nombre, fecha, motivo, hora entrada y salida)	Migrar infraestructura a un Data Center que cumpla con los componentes indispensables que aseguren un desempeño optimo de los equipos, así como prevenir la pérdida, daño, robo o comprometer la disponibilidad de los sistemas y servicios.	1. Seguridad sobre los equipos 2. Menor inversión por pagos mensuales que renovar SITE propio 3. Instalaciones bajo las mejores prácticas (espacio, aire acondicionado, sistema incendios, cableado, limpieza) que aseguren el óptimo funcionamiento de los equipos 4. Mejor servicio a clientes 5. Asegurar el cumplimiento de los SLA's comprometidos	Director de Operaciones	Personal Interno Proveedor	31-mar-17	Pago mensual de servicios	28.76%
2		Daño parcial o total de equipo en caso de un incendio	Falta de sistema de incendios (Extintores)								28.76%
3		Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad	Falta de mantenimiento al sistema de aire acondicionado								23.67%
4		Indisponibilidad del servicio por Falta de energía	Insuficiencia del Power Supply por fallas en baterías para soportar más de 7 min el suministro de energía								49.84%
5		Indisponibilidad del servicio por fallas en cableado	Falta de un cableado estructurado de quipos								38.94%
6		Acumulación de polvo u otros residuos que dañan los componentes de la infraestructura	Falta de limpieza periódica	Una vez a la semana, personal técnico ayuda y supervisa al personal de limpieza para el aseo del SITE							19.86%

Tabla 2.14 Tratamiento riesgos de hardware general

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
7	HARDWARE GENERAL	Falla del equipo que puede afectar la disponibilidad de los servicios	Falta de póliza de mantenimiento y soporte		Contratación póliza de mantenimiento y soporte para asegurar el desempeño optimo de los equipos y soporte en caso de contingencias que permita minimizar el impacto en la disponibilidad de los sistemas y servicios	1. Mejor servicio a clientes 2. Asegurar optimo desempeño de los equipos 3. Asegurar el cumplimiento de los SLA's comprometidos	Director Operaciones	Personal Interno Proveedor	31-mar-17	Pago mensual de servicios	58.99%
8		Caída de ambientes críticos	Falta de esquema de alta disponibilidad para ambientes críticos		Implementación de esquemas de alta disponibilidad en ambientes críticos que permita cumplir los SLA´s comprometidos	1. Mejor servicio a clientes 2. Asegurar el cumplimiento de los SLA's comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra de HW y SW	23.67%
9		Obsolescencia tecnológica	Falta de plan de renovación de tecnología para asegurar el buen desempeño de los ambientes		No hay presupuesto, la organización asume el riesgo. Se integrará presupuesto en el 2018						59.96%
10		Perdida o mal manejo de información en desecho de equipos	Falta de control en eliminación de desechos	Definición procedimiento ante el SGC (Sistema de Gestión de Calidad) para eliminación de desechos considerando el manejo adecuado de la información		1. Asegurar el resguardo de la información para no comprometer la confidencialidad, integridad y disponibilidad					13.50%

Tabla 2.15 Tratamiento riesgos acceso y servidores

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
11	ACCESO DNS (Nube) Websense (Nube) Internet	Problemas de acceso en cambios de IP's	Accesos Hardcoded	Cambiar configuración de clientes VPN softcoded y realizar la migración de clientes		1. Asegurar el acceso a los sistemas y servicios durante mantenimiento de IP's para no impactar disponibilidad de servicios					23.67%
12		Dependencia de internet para otorgar servicios	Punto único de falla en ISP (Internet)		No hay presupuesto, la organización asume el riesgo. Se integrará presupuesto en el 2018						28.84%
13	SERVIDORES Equipos Power Equipos X (Vmware,Linux y Windows)	Vencimiento equipos en comodato	Ambientes productivos de clientes se encuentran instalados en equipos prestados y no hay equipos propios para migrar ambientes		Compra de equipo para reemplazo equipos en comodato para migrar a equipo propio y asegurar la disponibilidad de los servicios	1. Asegurar operación de ambientes productivos 2. Asegurar el cumplimiento de los SLA's comprometidos	Director Operaciones	Personal Interno	30-jun-17	Compra HW y SW	23.67%
14		Deficiencia en la operación	Falta de capacidad de equipos		Realizar análisis de capacidades y proyecciones de los requisitos futuros para determinar los requisitos de capacidad que garanticen el desempeño optimo de los equipos	1. Mejor desempeño en sistemas y servicios 2. Asegurar el cumplimiento de los SLA's comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	23.67%

Tabla 2.16 Tratamiento riesgos red y almacenamiento/biblioteca

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
15	**RED Switches de LAN**	Empleados y clientes no pueden acceder a los ambientes	Punto único de falla Firewall		Implementar redundancia en firewall que asegure el accesos a los sistemas y servicios	1. Eliminar punto único de falla 2. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	28.04%
16			Punto único de falla en Switches LAN		Implementar redundancia en swithes LAN que asegure el acceso a los sistemas y servicios	1. Eliminar punto único de falla 2. Asegurar operación de sistemas y servicios de acuerdo a los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	28.04%
17	**ALMACENAMIENTO/BIBLIOTECA Storage V7000 Storage DS5020 Bibliotecas IBM TS3200, TS3100 Switches de SAN**	Incumplimiento RTO y RPO, posible perdida de información	Incapacidad para poder realizar los respaldos comprometidos por falta de cintas LTO4	Compra de cintas LTO4		1. Asegurar cumplimiento de RTO y RPO comprometidos					22.58%

Tabla 2.17 Tratamiento riesgos de software

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
18	**SOFTWARE**	Errores o fallas del software (Mal funcionamiento)	Falta de control de cambios	Creación procedimiento de control de cambios		1. Mejorar servicio por errores o fallas del SW 2. Asegurar el cumplimiento de los SLA´s comprometidos					28.28%
19		Errores de uso	Falta de documentación o actualización para operación de los sistemas y servicios		Creación o actualización de documentación de operación	1. Minimizar errores en la operación 2. Asegurar el cumplimiento de los SLA´s comprometidos	Gerente Área	Personal Interno	31-mar-17	N/A	24.21%
20			Asignación incorrecta de accesos		Creación de procedimientos para asignación de accesos por roles ante el SGC	1. Asegurar asignación correcta de accesos 2. Salvaguardar la integridad, confidencialidad y disponibilidad de la información	Gerente SGC	Personal Interno	30-jun-17	N/A	7.58%
21			Configuración incorrecta								25.00%
22		Pérdida de versiones de respaldos	Falta de políticas de respaldo adecuada		Implementar TSM para asegurar que los respaldos d e la información, software e imágenes de sistemas se realizan regularmente de acuerdo con la política de respaldos acordada	1. Asegurar la disponibilidad de respaldos 2. Asegurar el cumplimiento de los SLA´s comprometidos	Gerente Infraestructura	Personal Interno	31-mar-17	N/A	21.53%
23		Problemas de no licenciamiento adecuada de software	Falta de control en descarga de software	Restricción de descarga de SW		1. Asegurar que la descarga de SW s cumpla con el licenciamiento adecuado para no poner en riesgo la operación de sistemas y servicios					13.45%

Tabla 2.18 Tratamiento riesgos del personal

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
25	**PERSONAL**	Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Procedimientos de redutamiento inadecuados	Cambio a procedimiento de redutamiento para incluir examen práctico y segunda entrevista por otro gerente además del gerente de área		1. Asegurar un mejor redutamiento de personal 2. Minimizar las penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s					29.16%
26			Capacitación inadecuada	Creación de política de no asignar a un recurso a un actividad hasta que haya realizado la tarea con supervisión del gerente y este confirme que cumple con la competencia requerida		1. Asegurar que los recursos cumplen con las competencias requeridas para la operación 2. Minimizar las penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s					29.16%
27		Robo de documentos o medios de almacenamiento	Trabajo no supervisado de proveedores	Política de custodiar en todo momento a proveedores además de asegurar la autorización del gerente de área		1. Asegurar que el trabajo de proveedores sea supervisado para evitar robo de documentos o medios de almacenamiento					27.08%

Tabla 2.19 Tratamiento riesgos de administración – 1ra parte

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
28	ADMINISTRACION	Abuso de derechos, robo, eliminación y/o modificación de información	Falta de procedimientos registro y cancelación de usuarios	Cambios en procedimiento para el ingreso y salida de personal incluyendo la validación del alta y cancelación de usuarios por el gerente responsable		1. Asegurar que el alta de usuarios corresponde a las funciones que va a desempeñar y que a la salida se revoquen todos los accesos para salvaguardar la información de abuso de					13.50%
29			Falta de previsiones referentes a seguridad en contratos con clientes, proveedores y empleados		1.Definir políticas de seguridad de la información e integrar en los acuerdos contractuales con clientes, proveedores y empleados las responsabilidades para seguridad de la información	1. Garantizar la protección de la información que sea accesible por los clientes, proveedores y empleados	Director de Operaciones	Personal Interno	30-jun-17	N/A	13.50%
30		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Falta de auditorias regulares (supervisión)		Definir procedimientos para realizar auditorias con el objetivo de minimizar las interrupciones a los sistemas y servicios	1. Asegurar que se identifican las mejoras necesarias para minimizar las interrupciones de sistemas y servicios	Gerente SGC	Personal Interno	30-jun-17	N/A	13.50%
31			Falta de monitoreo de operaciones		Implementar herramientas, procesos y procedimientos que informen el estado de las operaciones para tomar las acciones necesarias para minimizar las fallas en la	1. Contar con la información suficiente para tomar las acciones de mejora que minimicen las interrupciones de sistemas y servicios	Gerente de Operaciones	Personal Interno	30-jun-17	Compra HW y SW	13.50%
32			Falta de actualización de procedimientos operativos		Revisión y actualización de procedimientos operativos por cada gerente de área	1. Operación eficiente que se vea reflejada en una buena atención a clientes	Gerentes de área	Personal Interno	30-jun-17	N/A	7.50%

Tabla 2.10 Tratamiento riesgos de administración – 2da parte

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
33	ADMINISTRACION	Pérdida parcial o total del Site	Falta de plan de continuidad		Definir, implementar y mantener procesos, procedimientos y controles para garantizar la continuidad durante una situación adversa que asegure el cumplimiento de los SLA´s	1. Asegurar la continuidad del servicio que permita cumplir los SLA´s comprometidos en una situación de emergencia	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
34		Perdida de evidencia	Falta de logs de operadores y administradores		Definir los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información de evidencia	1.Garantizar que se cuenta con procesos definidos para contar con evidencia que soporte la administración de incidentes en las operaciones	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
35		Modificación no autorizada, no intencional de la información y mal uso de los activos de información	Falta de clasificación de la información		Definir esquema de clasificación para implementar un apropiado conjunto de procedimientos para la clasificación y etiquetado de la información	1. Asegurar que la información reciba un apropiado nivel de protección de acuerdo con su importancia para la organización	Director de Operaciones Gerentes de área	Personal Interno	31-mar-17	N/A	13.50%
36			Falta de definición de responsabilidad de seguridad en perfiles de puestos		Definir todas las responsabilidades de la seguridad de la información y asignarse en perfiles de puesto	1. Asegurara la conciencia en empleados sobre sus responsabilidades de seguridad de la información para minimizar incidentes en la operación	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
37			Falta de segregación de funciones		Definir tareas en conflicto y áreas de responsabilidad que deben segregarse para reducir la modificación no autorizada, no intencional o mal uso de los activos de la organización	1. Reducir las oportunidades de mal uso de la información	Director de Operaciones Gerentes de área	Personal Interno	31-mar-17	N/A	13.50%

Resumen Tratamiento de riesgos

Se realizó la valoración de los riesgos asumiendo que las acciones de tratamiento se lleven a cabo con el objetivo de determinar si las acciones de tratamiento establecidas darán como resultado el cumplimiento del nivel de riesgo autorizado por la organización, el nuevo riesgo residual calculado muestra que la organización asume 2 riesgos arriba del 30% por restricciones de presupuesto, el 84% de los riesgos se mantienen dentro del límite establecido, de manera global el nivel de riesgo promedio del 24% permitirá que la organización cumpla con sus objetivos de crecimiento definidos para el año 2017 (Figura 2.2).

Tabla 2.11 Tratamiento riesgos del SITE

TIPO RIESGO	RANGO	RIESGO INICIAL		RIESGO RESIDUAL		RIESGO RESIDUAL CALCULADO	
		Cant	%	Cant	%	Cant	%
Verde (Riesgo BAJO)	0-10%	0	0	0	0	2	5%
Azul (Riesgo MEDIO)	11-30%	2	5%	9	24%	31	84%
Amarillo (Riesgo	31-50%	12	32%	9	24%	2	5%
Rojo (Riesgo MUY	51-100%	23	62%	19	51%	2	5%
		37	100%	37	100%	37	100%
Promedio			58%		53%		24%

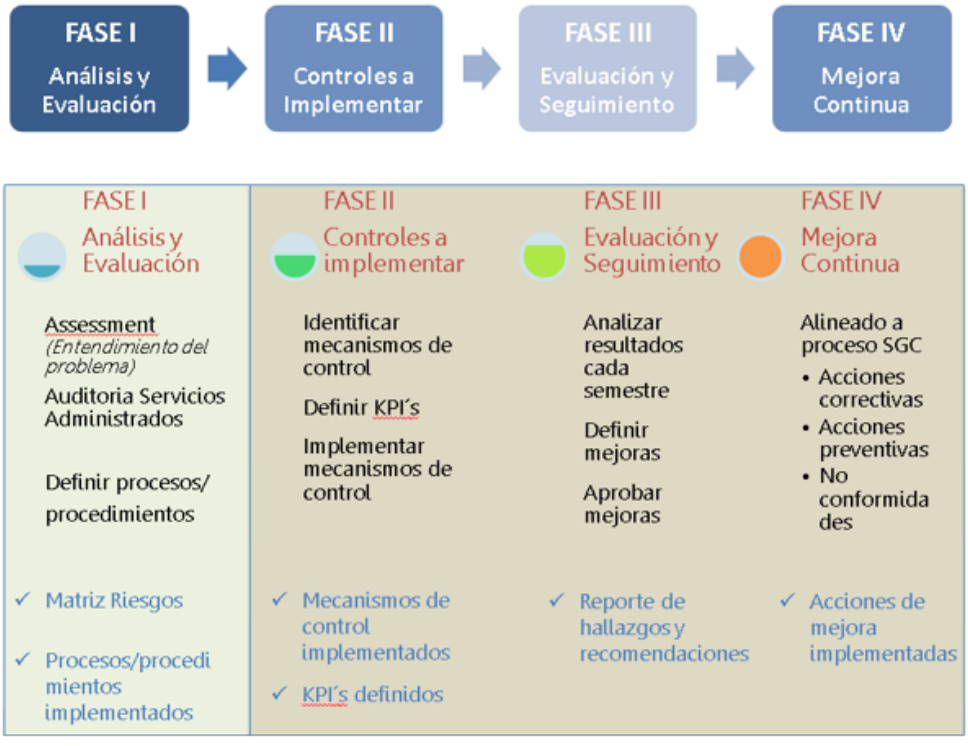
Monitoreo y Mejora Continua del Proceso de Gestión

Es una decisión de la dirección formalizar el análisis de riesgos en la organización, como primera etapa el alcance será el análisis de riesgos para la entrega de Servicios Administrados y paulatinamente se implementará para todos los servicios en la organización.

Con el monitoreo y la mejora continua se busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos. También, permitirá agregar al análisis riesgos nuevos que puedan aparecer luego de la definición de los planes teniendo en cuenta posibles cambios internos y externos

La implementación se realizará con la siguiente metodología de trabajo, para cada fase se realizarán actividades específicas y se generarán entregables. El seguimiento se realizará de forma semestral.

Figura 2.2 Actividades y entregables por fase



2.5 Conclusiones

Es irrefutable los beneficios de un análisis de riesgos de seguridad, el análisis y los hallazgos del presente trabajo son la base de cambios importantes en la organización, se concluye que los principales ejes de atención para lograr una implementación exitosa son:

- Compromiso de la dirección
- Formalizar la función de gestión de riesgos
- Construir un sistema para la gestión de riesgos
- Permear en la organización que la gestión de riesgos de seguridad se vea como una herramienta para ser más competitivos y no de cumplimiento
- Mejorar con el tiempo los procesos con controles efectivos
- Mostrar resultados semestralmente

Si bien esta implementación supone un importante consumo de recursos y un gran desafío, también se considera que los beneficios de tener una mayor comprensión de las fuentes de riesgos y el nivel de exposición permitirá que la empresa de pasos firmes hacia una mejora continua, disminuyendo la incertidumbre en el logro de los objetivos estratégicos de la organización y de esa forma se asegure su competitividad y rentabilidad para permanecer en el mercado.

2.6 Referencias

ISO (International Standard Organization). (2011). Gestión del riesgo – Principios directrices. Estándar de Seguridad ISO 31000.

ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

NIST (National Institute of Standards and Technology). (2002). NIST SP 800-30. Guía de Gestión de riesgo para sistemas de tecnología de la Información – Recomendaciones del Instituto Nacional de Estándares y Tecnología.

Ramírez Castro, Alexandra. (2012). Desarrollo de una metodología para la gestión del riesgo tecnológico a partir de ISO 31000 e ISO 27005 - Tesis de grado para optar como Ingeniera de sistemas, Proyecto curricular de ingeniería de sistemas, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Orientación acerca del enfoque basado en procesos para los sistemas de gestión de la calidad. (Mayo 2001). Recuperado de http://www.iram.com.ar/Documentos/Certificacion/Sistemas/ISO9000_2000/procesos.pdf.