Diagnosticar y asesorar la implementación de un sistema sgsi que permita controlar y gestionar todos los procesos relacionados con la información.

Elaborado por:

Bernal lópez walter adolfo

Universidad nacional abierta y a distancia
Cead José Acevedo y Gómez
Especialización en gestión de proyectos
Bogotá d.c.,
2014

Diagnosticar y asesorar la implementación de un sistema sgsi que permita controlar y gestionar todos los procesos relacionados con la información.

Bernal lópez walter adolfo

Trabajo de grado para optar el título de especialista en gestión de proyectos

Director
Forero barón luis alejandro

Universidad nacional abierta y a distancia
Cead José Acevedo y Gómez
Especialización en gestión de proyectos
Bogotá d.c.,
2014

Nota de aceptación

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del Jurado

_____

Firma del jurado

Bogotá D.C Diciembre 2014

AGRADECIMIENTOS

A Dios por darme la sabiduría, paciencia, tolerancia y perseverancia necesaria para la elaboración y cumplimiento de esta nueva etapa en mi vida y bendecirme con la posibilidad de caminar a su lado.

A mi familia por darme su apoyo incondicional, por creer en mis capacidades y ayudarme siempre a pesar de los obstáculos.

A la Universidad Abierta y a Distancia (UNAD) por permitirme ser parte de sus estudiantes y abrirme las puertas a desarrollar nuevas habilidades y progresar profesionalmente.

DEDICATORIAS

A Dios

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi familia

Por su motivación para la culminación mis estudios profesionales. Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA FIGURAS

Pág.

INTRODUCCIÓN

La información es el activo más importante que poseen las PYMES, por ende se deben identificar y crear técnicas que la aseguren más allá de la seguridad física. Estas técnicas permitirán brindar seguridad lógica que consiste en aplicaciones y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas. Por medio del ciclo PHVA y el modelo SGSI nos permitirá definir reglas, procedimientos, acciones y sensibilizar a los usuarios con los problemas ligados con la seguridad de los sistemas informáticos.

El método espiral nos permitirá garantizar el funcionamiento de nuestro Sistema de Gestión, orientado al ciclo de vida del proyecto el cual requiere una constante evaluación en todas sus fases.

Actualmente la empresa TRANSPACK LTDA no conoce el valor de los activos que posee, aunque la información está organizada el desarrollo del proyecto permitirá llevar control y gestión orientados al mejoramiento continuo.

Con el fin de generar un valor agregado, se realizará un diagnostico con la asesoría necesaria para implementar un nuevo sistema de gestión de seguridad de la información.

RESUMEN

La situación actual de nuestro país demuestra una alta tendencia hacia la tecnología, por ende algunas personas inescrupulosas crean estrategias para obtener beneficios de la inocencia y falta de aseguramiento de la información.

La seguridad debe mejorar de forma continua con el fin de satisfacer las necesidades básicas del mercado y al mismo tiempo mitigar futuros fraudes, chantajes, robos etc.

1. ANTECEDENTES DEL PROBLEMA

1.1. Importancia de la investigación

Los avances tecnológicos impulsan la competitividad en nuestro país, afortunadamente contamos con la infraestructura y elementos necesarios para garantizar nuestro aprendizaje, sin embargo debemos cuidar nuestra información personal y laboral.

La información es el activo más importante por ende debemos compartir la información con personas específicas y debemos utilizar móviles, computadores, portátiles y dispositivos conocidos.

Por medio de un diagnóstico y la asesoría correspondiente el sistema de gestión propuesto minimizará las brechas de seguridad de la información.

Es necesario conocer los defectos y a las fortalezas del área informática con el fin de aprobar las propuestas orientadas al mejoramiento continuo o la inversión en infraestructura tecnológica.

El departamento de sistemas no debe trabajar con base en incidentes, es necesario revisar y obtener los indicadores con el fin de identificar los problemas que impiden a los usuarios realizar su trabajo en los tiempos establecidos.

Un Sistema documental permite evidenciar las falencias y proponer mejoras orientadas a mitigar o mejorar los servicios de la Empresa.

1.2. Formulación del Problema

Las decisiones se deben basar en indicadores, estadísticas, incidentes y requerimientos sin esta información las inversiones realizadas pueden generar pérdidas.

Los directivos y personal administrativo deben ser conscientes de las políticas y procedimientos necesarios para minimizar las vulnerabilidades y amenazas, finalmente la seguridad de la información debe ser una asignatura obligatoria con el fin de garantizar un mejoramiento continuo.

Síntomas y causas

La Empresa TRANSPACK se interesa por obtener más ingresos sacrificando sus activos y exponiendo la seguridad de la información.

Pronóstico

Los empleados y personal ajeno tienen la capacidad de extraer información, por ende se perderá la integridad y confidencialidad.

Presentación de alternativas

Asesorar en la implementación de políticas, planes de Contingencia y planes de recuperación ante desastres con el fin de mejorar e invertir en infraestructura tecnológica orientada al control de acceso de la información.

1.3. Sistematización del Problema

¿Qué políticas y estrategias se debe implementar con el fin de mitigar los posibles riesgos informáticos a futuro?

¿La gestión documental del departamento de sistemas es una base para las decisiones en seguridad de la información?

¿Cuáles son las estrategias para garantizar el cumplimiento de las políticas y procedimientos establecidos?

1.4. Objetivos

Objetivo general

Diagnosticar y asesorar la implementación de un sistema de SGSI que permita controlar y gestionar todos los procesos relacionados con la información de la Empresa TRANSPACK LTDA.

Objetivos específicos

- Realizar un diagnóstico y una asesoría orientada al mejoramiento de las políticas y procedimientos basados con el SGSI.

- Analizar e Identificar las fortalezas y debilidades de la gestión de la información.

- Proponer mejoras orientadas a buenas prácticas.

1.5. Justificación

Actualmente los empleados no conocen los procedimientos necesarios para garantizar la continuidad de sus actividades, las instrucciones de los directivos y del departamento de sistemas no son coherentes.

Las evidencias para tomar las decisiones son basadas en supuestos y las soluciones son temporales, finalmente los empelados usan indebidamente los computadores, portátiles e información de la empresa.

El proyecto se hace necesario implementarlo para mejorar la seguridad de la información, tener un control de las actividades que se realizan en la empresa y minimizar los posibles riesgos. Basándonos en el ciclo PHVA este proyecto se encargará de diagnosticar y asesorar la implementación de un Sistema de gestión de seguridad de la información de la empresa TRANSPACK LTDA; es necesario recordar que la información es el activo más importante de una Empresa, por ende la disponibilidad, integridad y confidencial deben ser los pilares principales.

Por medio del ciclo PHVA y un Sistema de Gestión de Seguridad de la Información lograremos mejorar nuestra seguridad, brindando mayor satisfacción a los directivos, realizando seguimiento y control desde el momento en que se crean los procesos.

Justificación teórica

El conjunto de políticas creadas para mejorar la administración de la información debe ser conocido y cumplido por todos los Empleados y Directivos, debido a que el SGSI es un sistema orientado al mejoramiento continuo basado en el ciclo PHVA.

Justificación Metodológica

El Enfoque que utilizaremos en el proyecto será el método Espiral: Es una evolución de método clásico en cascada (Waterfall, top-down) y se considera un método de desarrollo incremental. Este tipo de metodología equivale al de cascada, pero en él se permite el manejo de varias etapas con el objetivo de flexibilizar y compensar el tiempo de desarrollo total y alcanzar resultados funcionales en etapas tempranas. Está considerada como un método rápido y eficiente.

Justificación práctica

Los problemas e inconvenientes tecnológicos afectaran a una empresa en la medida que las políticas estén implementadas y monitoreadas, una excelente gestión garantizará confidencialidad, disponibilidad e integridad.

1.6. Alcances y límites de la investigación

- Alcance: Diagnosticar y asesorar la correcta implementación de un SGSI enfocado al control de acceso a la información.

- Límites: Las políticas, procedimientos y cambios propuestos están sujetas a la aprobación de los Directivos de la compañía.

2. MARCO DE REFERENCIAL

2.1. Marco Teórico

Un sistema de gestión de la seguridad de la información es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, por medio del ciclo PHVA se identificaran las necesidades y metas de la empresa, luego se generaran las estrategias necesarias para mitigar las falencias del sistema, finalmente se realizará un verificación del cumplimiento de los procedimientos establecidos con el fin de cambiar la estrategia o mantenerla.

2.2. Marco legal

2.2.1. Ciclo PHVA

La utilización continua del PHVA nos brinda una solución que realmente nos permite mantener la competitividad de nuestros productos y servicios, mejorar la calidad, reduce los costos, mejora la productividad, reduce los precios, aumenta la participación de mercado, supervivencia de la empresa, provee nuevos puestos de trabajo, aumenta la rentabilidad de la empresa.

Planear

Es establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

- Identificar servicios.
- Identificar clientes.
- Identificar requerimientos de los clientes.
- Trasladar los requerimientos del cliente a especificaciones.
- Identificar los pasos claves del proceso (diagrama de flujo).
- Identificar y seleccionar los parámetros de medición.
- Determinar la capacidad del proceso.
- Identificar con quien compararse (benchmarks) (5.1 de ISO 9004).

Hacer

- Implementación de los procesos.
- Identificar oportunidades de mejora
- Desarrollo del plan piloto
- Implementar las mejoras

Verificar

Realizar el seguimiento, medir los procesos y los productos contra las políticas, los objetivos y los requisitos del producto e informar sobre los resultados.

Actuar

Tomar acciones para mejorar continuamente el desarrollo de los procesos.

- Institucionalizar la mejora y/o volver al paso de Hacer

2.2.2. Aplicando el PHVA en la implementación de un sistema de gestión de la calidad en una empresa de servicios, tenemos:

La definición de la red de procesos, la política de calidad y los objetivos, se define el Representante de Gerencia, y el aseguramiento de los procesos. En el Hacer se hace la implementación de lo definido en la planeación, es decir, toda la organización se alinea de acuerdo a las definiciones, se conforman equipos de trabajo para que documenten los procesos con el enfoque de PHVA y con una metodología definida. En el Verificar, se aplica el subproceso de Revisiones de Gerencia y Auditorías internas de Calidad.

En el Actuar, se aplica el subproceso de Acciones correctivas, preventivas y planes de mejoramiento como consecuencia de unos informes de auditorías, adicionalmente se aplica la metodología para análisis y solución de problemas a aquellos subprocesos que necesitan un mejoramiento continuo para luego incorporarlos en los subprocesos y convertirlos nuevamente como parte del día a día.

No es posible realizar con calidad una actividad, proceso, producto o servicio, si se viola alguno de los pasos del ciclo.

Podría decirse que la metodología PHVA no da lugar a fisuras en cuanto su propósito: se define una meta y dejándose llevar por la sabiduría contenida en cada etapa, se llega a cumplirla quitando del camino los obstáculos (no conformidades) que se interpongan, ya sean humanos, materiales o financieros. Si el objetivo es realista y considera las variables del entorno, entonces siguiendo la estrategia del Ciclo de la Calidad, la probabilidad de éxito es mayor. No debe olvidarse que en cada paso habrá que realizar acciones tácticas y operativas para seguir adelante con dominio[1].

---

1. *http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/*

2.3. Normatividad SGSI

Es una norma internacional que ofrece recomendación para la gestión de la seguridad de la información enfocada en el inicio, implantación o mantenimiento de la seguridad en una organización. La seguridad de la información se define con la preservación de:

Confidencialidad: aseguración de la privacidad de la información de la organización.
Integridad: garantía del estado original de los datos.
Disponibilidad: Acceso cuando sea requerido por los usuarios.
No repudio: Estadísticas de la acciones realizadas por el personal autorizado.

El objetivo de la norma ISO 27002 es proporcionar una base para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Esta norma establece 10 dominios de control que cubre por completo la gestión de seguridad de la información:

Política de seguridad: dirige y da soporte a la gestión de la seguridad de la información

Aspectos organizativos para la seguridad: gestiona la seguridad de la información dentro de la organización; mantiene la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros y mantiene la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

Clasificación y control de activos: mantiene una protección adecuada sobre los activos de la organización y asegura un nivel de protección adecuado a los activos de la información.

Seguridad ligada al personal: reduce el riesgo de los errores humanos, robos, fraudes o mal uso de la instalación y los servicios; asegura que los usuarios son conscientes de las amenazas y riesgo en el ámbito de la seguridad de la información, y que están preparados para sostener las políticas de seguridad de la organización y minimiza los daños provocados por incidencias de seguridad y por el mal funcionamiento controlándolo y aprendiendo de ellos.

Seguridad física y del entorno: evita el acceso no autorizado, daños e interferencias contra los locales y la información de la organización; evita perdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización y previene las exposiciones a riesgos y a robos de la información y de recursos de tratamiento de información.

Gestión de comunicación y operaciones: asegura la operación correcta y segura de los recursos de tratamiento de la información; minimiza el riesgo de fallos en el sistema; protege la integridad del software y de la información; mantiene la integridad y la disponibilidad de los servicios de tratamiento de información y de comunicación; asegura la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo; evita daño a los activos e interrupciones de actividades de la organización y previene la perdida, modificación o mal uso de la información intercambiada entre organizaciones.

Control de acceso: controla los accesos a la información; evita acceso no autorizado a los sistemas de información; protege los servicios en red; evita acceso no autorizado a ordenadores; evita el acceso no autorizado a la información contenida en el sistema; detecta actividades no autorizadas y garantiza la seguridad de la información cuando se usan dispositivos de información móvil o teletrabajo.

Desarrollo y mantenimiento de sistema: afirma que la seguridad está incluida dentro de los sistemas de información; evita perdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones; protege la confidencialidad, integridad y autenticidad de la información; asegura que los proyectos de Tecnologías de la Información y las actividades complementarias son llevadas a cabo de una forma segura y mantiene la seguridad del software y la información de la aplicación del sistema.

Gestión de continuidad del negocio: reacciona a la interrupción de actividades del negocio y protege sus procesos críticos frente a grandes fallos o desastres.

Conformidad con la legislación: evita el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad; garantiza la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma y maximiza la efectividad y minimiza la interferencia de o desde el proceso de auditoría del sistema.[2]

2.4. Marco espacial

Este proyecto se realizará en la ciudad de Bogotá, donde se investigará el proceso de gestión de la información que tiene la empresa *TRANSPACK LTDA*, con la ayuda de la UNAD que será gestora y facilitadora con el fin de garantizar el funcionamiento adecuado del mismo.

2.5. Marco temporal

El presente proyecto se auditara y gestionara con base en la información correspondiente a los meses Agosto – Septiembre 2014.

2.http://seguridadinformaticaufps.wikispaces.com/NORMATIVIDAD+SGSI

2.6. Hipótesis de trabajo.

Por medio del presente proyecto es necesario identificar e informar de las falencias e inconvenientes de seguridad de la empresa TRANSPACK LTDA, finalmente se debe diagnosticar y asesorar en la implementación de un sistema de gestión de seguridad de la información el cual mitigará los riesgos basados en políticas, procedimientos.

2.7. Variables

Definición conceptual de variables

- Tiempo: es un factor el cual se debe gestionar por medio de cronogramas de trabajo, se debe presentar informe de avance, auditoria y recomendaciones necesarias.

- Costos: Con el fin de implementar un Sistema de Gestión es necesario identificar los costos y la posible inversión realizada.

- Recursos: Cuantas personas estarán disponibles para gestionar y supervisar el sistema de gestión.

Definición operacional de variables

- Diagnóstico: Una empresa es un sistema abierto el cual tiene interacción con otros sistemas, por medio de un diagnostico se identificará la entropía de las actividades y procesos con el fin de proponer nuevas estrategias.

- Informes e Indicadores: Los informes e indicadores enviados a los directivos de la empresa deben informar el plan de trabajo, costos e inversión necesaria, recursos utilizados y beneficios obtenidos a corto, mediano y largo plazo.
- Asesoría y socialización del sistema de gestión, los directivos y empleados deben conocer las políticas, cambios tecnológicos y cambios organizacionales orientados a un mejoramiento continuo.

3. MARCO METODOLÓGICO

3.1. Tipo de estudio.

Investigación Exploratoria

Por medio de una entrevista y observación se logrará recolectar datos, con el fin de crear un marco teórico y epistemológico lo suficientemente fuerte como para determinar qué factores son relevantes al problema y por lo tanto deben ser investigados.

Es necesario conocer los procedimientos actuales y el objeto social de la empresa, las políticas del SGSI y el ciclo PHVA deben ir orientadas a la misión y visión de la empresa.

Investigación Descriptiva

Debemos basarnos en los conceptos o variables y medir cada una de ellas independientemente de las otras, con el fin, precisamente, de describirlas.

Las actividades de los empleados y directivos deben integrarse con el fin de crear las políticas necesarias para una empresa y no para departamentos por separado.

Investigación Explicativa.

Los estudios realizados pretenden conducir a un sentido de comprensión o entendimiento de las actividades realizadas de la empresa, pero es necesario identificar las necesidades de un empleado vs las necesidades de la empresa, como investigador debo interpretar y recomendar las políticas necesarias con el fin de mitigar riesgos.

3.2. Método Espiral

Análisis de requerimientos: Durante esta etapa se estudia detalladamente los requerimientos que cada objetivo conlleva. Aquí establecen todos los detalles funcionales deseados.

Diseño del sistema: Con los datos de la etapa anterior, se diseña el sistema teniendo en cuenta las actividades y responsabilidades de cada usuario.

Etapas de construcción: recomendaciones para implementar un sistema de gestión.

Test y evaluación: En esta etapa se realiza un test del módulo completo así como su evaluación frente al estudio de requerimientos. En muchos casos en es esta etapa los usuarios finales participan de manera activa aportando información decisiva para la usabilidad del sistema.[3]

---

3. http://www.acertasoftware.com/mspiral.html

3.3. Instrumentos a utilizar

Con el fin de diagnosticar y asesorar el sistema de SGSI es necesario entrevistar y tabular la información recolectada del departamento de sistemas de la empresa TRANSPACK LTDA.

3.4. Contenido

3.4.1. Alcance y Limites

- Las oportunidades de mejora se implementarán de acuerdo a la respectiva aprobación de los Directivos.

- Asesorar en el control de acceso a la información de la Empresa.

- Sensibilizar a los Directivos y Empleados.

3.4.2. Diagnóstico Inicial

1. ¿Conoce que computadores, servidores, dispositivos móviles y dispositivos extraíbles tiene la información de la empresa?

Actualmente no se conoce todos los dispositivos que pueden tener información sensible de la Empresa, es necesario que los directivos de la Empresa aprendan a reconocer el valor que puede ofrecer el Departamento de Sistemas.

Con el fin de guardar, asegurar y clasificar la información es indispensable almacenar la información de la Empresa en dispositivos autorizados y en un lugar de confianza externo a las instalaciones de la Empresa.

2. ¿La información más sensible se encuentra centralizada en los servidores de la empresa?

Actualmente la Empresa cuenta con un servidor externo de antivirus, sin embargo debemos tener en cuenta que el tamaño o número de empleados no es directamente proporcional al número de servidores.

Todas las empresas deben tener mínimo un servidor en producción con su respectivo servidor de respaldo, adicionalmente la información no debe estar en todos los computadores y dispositivos, es imperativo almacenar la información en un solo servidor y realizar Backup diarios de forma Incremental y un backup full mensual.

Es necesario determinar el número de backup que deseo almacenar y seleccionar un lugar adecuado para su respectivo almacenamiento.

3. ¿Tiene un cronograma de backup?

Se recomienda realizar backup todos los días de la información de la empresa y realizar mínimo un backup full al mes.

4. ¿Tiene contingencia en caso de pérdida o robo de información?

Se recomienda crear políticas de acceso a la información con el fin de mantener la confidencialidad e integridad de la información, sin embargo para mantener la disponibilidad de la información es necesario realizar backup y almacenar fuera de las instalaciones.

5. ¿Tiene monitoreado y restringido el software que se utilizan en los computadores y/o portátiles de la empresa?

Actualmente el Departamento de sistemas realiza una gestión excelente, los equipos y portátiles de la empresa tiene el software necesario para ejecutar sus funciones.

Se recomienda implementar el software OCS Inventory (está publicado bajo la licencia GNU General Public License, version 2.0, GNU GPLv2) para gestionar los activos y programas instalados en la empresa.

6. ¿Existe una consola que garantice la gestión del antivirus?.

La empresa cuenta con una consola de antivirus web, lo cual permite administrar los posibles inconvenientes de virus, spam, spyware, etc. En los equipos desde cualquier lugar del mundo.

Se recomienda actualizar las bases de datos a diario y ejecutar mínimo un escaneo al mes para cada equipo.

7. ¿Existe un plan de contingencia en caso de posibles fallas de los sistemas?

El plan de contingencia actual es:

- Computadores, Laptop e Impresoras: En caso de fallas o inconvenientes de hardware se solicitará a un proveedor externo el arrendamiento de un computador, portátil o impresora por el tiempo necesario mientras repara la falla.

Aunque la contingencia mencionada anteriormente es excelente se recomienda implementar las siguientes recomendaciones:

- Solicitar y alquilar un canal de internet secundario con otro proveedor diferente al actual, con el fin de garantizar alta disponibilidad de Conectividad a Internet.
- Se recomienda tener los servicios de un proveedor o persona que administre, gestione las conexiones eléctricas, datos, voz de la empresa.
- En caso de presentar fallas o daños en dispositivos LAN (Router, Switch, etc.), se recomienda comprar con un proveedor las partes afectadas en el menor tiempo posible.
- Se recomienda comprar un servidor en el cual se almacene la información de la Empresa de acuerdo a un plan de backup establecido (Backup Diario Incremental y mínimo un Backup Full Mensual).
- Se recomienda guardar los backup de la Empresa en un lugar diferente a las instalaciones actuales.

8. ¿Existe un plan de recuperación de desastres en caso de posibles fallas de la infraestructura?

El plan de recuperación ante desastres es:

- Computadores, Laptop e Impresoras: En caso de pérdida o daño total de hardware se solicitará a un proveedor externo el arrendamiento de un computador, portátil o impresora por el tiempo necesario mientras se compra su respectivo reemplazo.

Aunque el plan de recuperación ante desastres mencionado anteriormente es excelente se recomienda implementar las siguientes recomendaciones:

- Se recomienda restaurar el backup de la información en un computador, portátil o servidor rentado con el fin de continuar con la operación diaria de la empresa.

- En caso de problemas eléctricos en la Empresa se debe reestablecer el servicio por medio de un proveedor o persona que administre, gestione las conexiones eléctricas, datos, voz.
- Se recomienda asegurar los activos e infraestructura de la Empresa con el fin de minimizar el impacto de las pérdidas materiales.

9. ¿Los empleados y directivos conoce los procedimientos y gestión del departamento de sistemas?

El departamento de sistemas realiza capacitaciones, inducciones a todo el personal de la Empresa con el fin de notificar los cambios o proyectos. Se recomienda realizar capacitaciones al personal antiguo una vez al mes.

10. ¿Existen formatos de mantenimiento, monitoreo, checklist y/o indicadores de gestión?

Actualmente no existen formatos, informes e indicadores de gestión en la cual se pueda identificar los puntos débiles y/o fortalezas de la empresa.

Se recomienda crear formatos, políticas e informes de gestión mensual.

11. ¿Tiene inventario de Hardware y software?

El inventario de hardware y software se encuentra en un archivo de Excel, sin embargo se recomienda implementar el software OCS Inventory (está publicado bajo la licencia GNU General Public License, version 2.0, GNU GPLv2) para gestionar los activos y programas instalados en la empresa.

3.4.3. Sistema Actual

Tabla1. DOFA Sistema Actual

	Fortalezas	**Debilidades**
Oportunidades	El personal de sistemas tiene la experiencia necesaria para garantizar el óptimo funcionamiento de la infraestructura y servicios.	Se debe realizar presupuesto e invertir en tecnología basado en informes, estadísticas, incidentes y requerimientos.
Amenazas	➢ Revisar y optimizar la gestión de proveedores externos. ➢ Obtener herramientas necesarias para garantizar los planes de contingencia y planes de recuperación de desastres	Se deben crear y cumplir las políticas aprobadas por la Dirección y el Departamento de Sistemas orientadas al mejoramiento continuo.

Fuente: Autor

3.4.4. Infraestructura

Tabla2. Activos Infraestructura

#	Activo	Cantidad	Función
1	Modem	1	Dispositivo encargado de la comunicación con internet.
2	Router	1	Dispositivo que permite la comunicación de la red interna con el internet.
3	Access Point	1	Permite a los equipos y portátiles de la red conectarse sin cables hacia la red interna e internet.
4	Switch	1	Permite a los equipos y portátiles de la red conectarse con la red interna e internet.

5	Impresoras	3	Permite a los equipos y portátiles imprimir documentos.
6	Portátil	2	Equipo móvil liviano que permite trabajar al usuario desde cualquier lugar.
7	Computadores	11	Equipo fijo que permite trabajar al usuario.
8	Servidor	1	Servidor ubicado fuera de la red el cual permite administrar el antivirus de la red.

Fuente: Autor

3.4.5. Servicios indispensables para la infraestructura.

Información

El activo más importante de la empresa debe estar disponible para realizar consultas en cualquier momento y lugar.

Software Contable

La información histórica permite tomar nuevas decisiones orientadas a mejorar las estrategias comerciales y financieras.

Internet

La interacción por medio del internet permite mejoras las relaciones comerciales y garantizar una oportuna atención a proveedores y clientes.

4. METODOLOGÍA SGSI

Con el fin de realizar una óptima asesoría, es necesario evaluar constantemente los procesos realizados por el área de TI, adicionalmente la estrategia generada debe garantizar el funcionamiento adecuado de los sistemas sin afectar la seguridad de la información.

Por medio del ciclo PHVA podemos implementar un sistema SGSI debido a que es una herramienta orientada al mejoramiento continuo, los cuatro procesos Planear, Hacer, Verificar y Actuar garantizan orden y calidad.

Las ventajas de implementar un sistema basado en el ciclo PHVA son:

- Se concentra el esfuerzo en ámbitos organizativos y de procedimientos puntuales Consiguen mejoras en un corto plazo y resultados visibles.

- Si existe reducción de productos defectuosos, trae como consecuencia una reducción en los costos, como resultado de un consumo menor de materias primas.

- Incrementa la productividad y dirige a la organización hacia la competitividad, lo cual es de vital importancia para las actuales organizaciones.

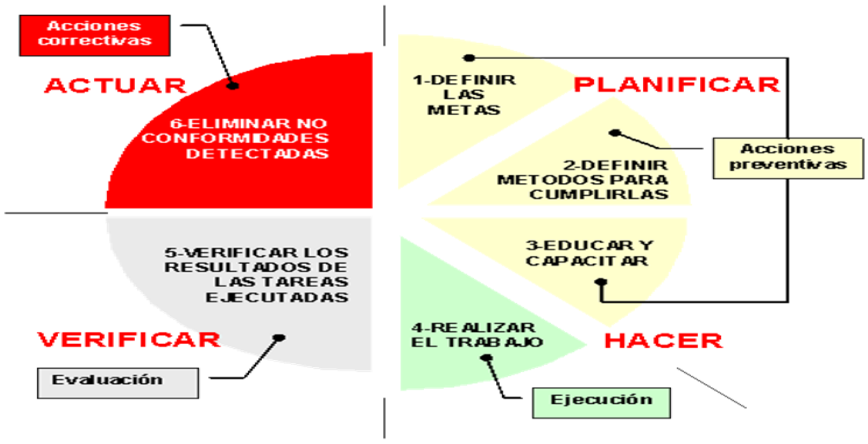
- Contribuye a la adaptación de los procesos a los avances tecnológicos.

- Permite eliminar procesos repetitivos[4].

---

4. http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

Figura1. PHVA



Fuente: Autor

4.1. Planear

Con el fin de establecer los objetivos y procesos necesarios para obtener resultados, es necesario identificar las necesidades de la empresa y generar un plan de trabajo el cual permita mejorar los procedimientos actuales.

4.1.1. Planear – Servicios

Soporte a Infraestructura.

El departamento de sistemas tiene la experiencia necesaria para:

- Mantener
- Estabilizar
- Actualizar las aplicaciones, servidores, computadores, equipos activos.

Soporte a Usuarios Finales.

Los requerimientos presentados por los usuarios se deben clasificar y atender según el impacto y la clasificación del incidente o requerimiento.

Monitorear y Auditar servicios.

Los requerimientos e incidentes presentados deben atenderse de forma proactiva basado en un cronograma de actividades.

Es necesario realizar monitoreo a la infraestructura de forma continua con el fin de identificar posibles fallas y mitigarlas.

Optimizar Procesos.

Los procesos y tareas realizadas a diario deben ser auditados con el fin de verificar y establecer mejores alternativas encaminadas al mejoramiento continuo.

4.1.2. Planear – Clientes

Todo el personal de la Empresa es considerado como parte fundamental, sin embargo los requerimientos e incidentes se deben categorizar y atender de acuerdo al impacto generado.

4.1.3. Planear - Metas

Mantener en óptimas condiciones la infraestructura.

- Se debe realizar mantenimiento de Hardware a las estaciones de trabajo 3 veces al año.
- Se debe realizar mantenimiento de Hardware 2 veces al año a los servidores, la actividad se debe realizar fuera del horario laboral.

Monitorear constantemente los servicios.

- Se debe realizar un checklist de los servicios todos los días a primera hora.

Minimizar el tiempo de respuesta ante posibles fallas de los servicios.

- Se debe categorizar las fallas y atender los requerimientos e incidentes de acuerdo a su impacto.

Planes de contingencia

Con el fin de mantener la Integridad, confidencialidad y la disponibilidad es necesario tener en cuenta:

- La información:
  - ✓ La información de la compañía debe estar almacenada en un servidor principal, se recomienda realizar un backup diario incremental y un Backup full mensual.

- ✓ El backup debe realizarse en un servidor externo o disco duro externo.
- ✓ El backup no debe permanecer más de un día en la Empresa.
- ✓ En caso de utilizar discos duros externos se recomienda tener más de un disco.
- ✓ La información debe segmentarse por año y por departamento.
- ✓ La información de años anteriores debe quedar con permisos de solo lectura.

- Los servicios

  - ✓ Se debe clasificar los servicios de acuerdo a su importancia.
  - ✓ Todos los servicios deben tener un respaldo.

- Hardware necesario para trabajar

  - ✓ Se recomienda mantener activo el soporte en sitio de los respectivos proveedores de hardware.
  - ✓ Todos los equipos activos deben tener un respaldo, en caso de fallas se debe reparar, cambiar partes.
  - ✓ Se recomienda rentar equipos, servidores, impresoras en caso de ser necesario con el fin de no afectar la operación.

Plan de recuperación de desastres

En caso de presentar fallas en la infraestructura se recomienda habilitar un servicio el cual nos garantice la continuidad del negocio, por ende se recomienda:

- Mantener los backups en un lugar seguro fuera de la Empresa con el fin de restaurarlos en otro computador, portátil o servidor.

- Configurar los servicios críticos de la Empresa en un servidor en la Nube, o servicios de arrendamiento de DataCenter, etc.
- Solicitar apoyo de proveedores externos para reparaciones en la infraestructura.
- Asegurar activos e infraestructura con el fin de minimizar el impacto material.
- Capacitar constantemente a los usuarios con respecto a la posible conectividad desde sus puestos de trabajo o desde sus casas.

Políticas

- Se debe garantizar que los computadores tengan las aplicaciones estrictamente necesarias.
- Se debe garantizar que los usuarios naveguen a sitios web permitidos de acuerdo a su perfil
- Se debe prohibir la extracción de la información de la Empresa
- Se debe monitorear que los usuarios tengan acceso solo a cierta parte de la información de la empresa.
- Se debe monitorear los archivos almacenados por los usuarios.
- Se debe solicitar mantenimientos externos para el cableado estructurado, locativo y eléctrico.
- Se debe programar mantenimiento de Hardware y software a los computadores, portátiles y servidores de la empresa.
- Se debe evitar el acceso, manipulación y control a cualquier dispositivo de la red, cada usuario se debe hacer responsable de sus herramientas de trabajo.
- Se debe realizar la inducción correspondiente a cada usuario, mínimo una vez al mes.
- Se debe capacitar a cada usuario de acuerdo a sus necesidades o cambios en la infraestructura.

- Se deben asignar permisos específicos por usuarios, cada archivo y/o carpeta debe tener permisos de lectura y/o de escritura de acuerdo al perfil y departamento de cada usuario.
- Se deben bloquear dispositivos que permitan extraer información de los computadores y portátiles de la Empresa, por ejemplo Memorias USB, CD's, DVD's, etc.
- Todos los equipos de la red deben tener el antivirus corporativo.
- Cada usuario debe tener las respectivas actas de entrega por cada activo utilizado en la red.

4.1.4. Requerimientos e Incidentes

Con el fin de brindar la mejor asesoría y soporte respectivo es necesario identificar si el caso reportado por un usuario es un requerimiento o incidente.

- Requerimiento: Solicitud del cliente para optimizar o revisar un proceso.

- Incidente: Es un obstáculo el cual le impide al usuario realizar sus funciones.

Teniendo en cuenta lo anterior los casos se categorizan de acuerdo a su nivel de complejidad e impacto para la empresa.

Tabla 3. Incidentes

#	Tipo de Caso	Nivel	Observaciones
1	Conectividad Internet	1	Acceso a sitios web como Bancos, envió y recepción de correos
2	Virus informáticos	1	Se debe verificar los archivos infectados y mitigar/eliminar el virus

3	Programa Contable	1	El software contable debe tener una disponibilidad del 99%
4	Acceso a la información	1	El activo más importante de la empresa, se deben asignar permisos de acuerdo al perfil de cada usuario.
5	Problemas de Impresión	2	En caso de presentarse fallas en las impresoras, es necesario garantizar la impresión de los documentos de acuerdo a su necesidad.
6	Fallas con las estaciones de trabajo	2	Se debe asignar un computador/portátil temporal al usuario afectado mientras se revisa la falla.

Fuente: Autor

Tabla4. Requerimientos

#	Tipo de Caso	Nivel	Observaciones
1	Mantenimiento de Hardware	2	El mantenimiento de hardware es programado y autorizado según cronograma del área de sistemas (3 veces al año).
2	Mantenimiento de Software	2	Actualizaciones, eliminación de temporales e inconvenientes menores (3 veces al año).
3	Cambio de Puesto de trabajo	2	Ubicación de equipos o impresoras debe ser programada por el área de sistemas.
4	Cotizaciones o Nuevos Proyectos	3	Los proyectos y/o cotizaciones deben ser evaluados con respecto a las posibles ventajas a corto, mediano y largo plazo.
5	Documentación de procedimientos y checklist	1	Se deben realizar test diarios con su respectiva documentación, adicionalmente los procedimientos y tareas fundamentales se debe documentar y actualizar constantemente.

Fuente: Autor

4.1.5. Tratamiento del Riesgo por parte del departamento de Sistemas

Plataformas y comunicaciones

Se ejecutarán los siguientes procedimientos:

Tabla5. Plataforma tecnológica, redes y comunicaciones

ISO 27002			
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Revisar checklist relativo al monitoreo de la red y Analizar las bitácoras de problemas a diario.	12. Seguridad Operativa	12.4. Registro de Actividad y Supervisión	12.4.1 Registro y gestión de eventos de actividad.
Verificar los mecanismos de comunicación y acceso a los datos de la red desde el punto de vista de disponibilidad.	9. Control de Acceso	9.1 Requisitos de negocio para el control de accesos	9.1.2. Control de acceso a las redes y servicios asociados.
Mantener, Supervisar y monitorear el hardware y software existentes e identificar la necesidad de renovar tecnología.	8. Gestión de Activos	8.1 Responsabilidad sobre los activos	8.1.3 Uso Aceptable de los activos.

Fuente: Autor

Evaluación de seguridades y procedimientos de continuidad

Se ejecutarán los siguientes procedimientos:

Tabla 6. Seguridades: físicas, lógicas y de comunicaciones

ISO 27002			
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar las políticas y procedimientos de seguridad vigentes.	5.Politicas de Seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.2. Revisión de las políticas para la seguridad de la información.
Revisar la seguridad lógica implantada en los servidores, así como los parámetros de seguridad relativos a las claves de acceso, utilizando la herramienta de software específicas para cada plataforma Esto comprende, entre otros: – Tipo y longitud mínima y máxima de las claves de acceso. – Manejo de claves de acceso históricas. – Administración de claves de acceso por servicio.	9. Control de Accesos	9.4. Control de Acceso a sistemas y aplicaciones	9.4.1. Restricción del acceso a la información.
			9.4.2. Procedimientos seguros de inicio de sesión.
			9.4.3. Gestión de contraseñas de usuario
			9.4.4 Uso de Herramientas de administración de Sistemas
			9.4.5. Control de acceso al código

			fuente de los programas.
Revisar las seguridades de accesos remotos (VPN, internet, intranet, Conexión Remota, etc.).	13. Seguridad en las telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.2. Mecanismos de seguridad asociados a servicios de red
Evaluar los mecanismos de protección antivirus.	12. Seguridad operativa	12.6. Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas.
Evaluar mecanismos de seguridad física existentes.	11. Seguridad Física y Ambiental	11.1. Áreas Seguras	11.1.4. Protección contra las amenazas externas y ambientales.

Fuente: Autor

Tabla 7. Plan de contingencias y Recuperación ante desastres

ISO 27002			
Procedimiento	**Dominio**	**Código**	**Objetivo de Control**
Evaluar estrategia de recuperación de información en caso de eliminación y o daños de hardware.	17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	17.2 Redundancias	17.2.1. Disponibilidad de instalaciones para el procesamiento de la información.

Evaluar la estrategia de recuperación, infraestructura tecnológica y las facilidades para la continuidad del procesamiento.	17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	17.1. Continuidad de la seguridad de la información.	17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Evaluar los procedimientos de recuperación y operación durante la emergencia, tomando en cuenta: responsables, actualización, pruebas periódicas, metodología para la determinación de los procedimientos.	17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	17.1. Continuidad de la seguridad de la información.	17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Fuente: Autor

4.2. Hacer

Después de planear los procedimientos necesarios para garantizar la estabilidad del sistema, es necesario ejecutar las actividades y/o procesos de acuerdo a lo planeado.

4.2.1. Educar y Capacitar

Se deben realizar capacitaciones en las siguientes ocasiones:

- Cuando ingresa una persona nueva
- Se debe programar capacitaciones de acuerdo a las necesidades de cada usuario.

- Se debe programar una capacitación una vez al mes con el fin de socializar políticas, planes de contingencia y plan de recuperación ante desastres.

Figura2. Formato Capacitaciones Versión 0.

FR-CAP-V00	
FORMATO DE CAPACITACIONES Y/O ASISTENCIAS A REUNIÓN	

Fecha		Hora	
Capacitador			
Tema			

Nombre Completo	Cargo	Firma

Observaciones:

Fuente: Autor.

4.2.2. Monitoreo.

- Los servicios más importantes se deben verificar a diario y se recomienda tener en cuenta las observaciones con el fin de mitigar o transferir la falla.

- Es importante diligenciar el formato FR-MON Versión 0 a primera hora del día.

- Las UPS que deben funcionar sin problemas son donde están conectados los servidores, en una empresa se puede permitir daños totales y/o parciales en impresoras, equipos, switch, router, etc. La UPS que protege el activo más importante de la Empresa debe contar con una disponibilidad de servicio del 100%.

- La conexión a internet se ha convertido en un servicio importante para todas las personas, se utiliza para comunicación, información e investigación. Si una empresa no puede enviar correos o no se puede comunicar con sus clientes la rentabilidad puede disminuir considerablemente.

- Los dispositivos que permiten la conectividad LAN como Switch, Router, Access Point, etc. Garantizan comodidad al usuario desde su puesto de trabajo.

- La información del software contable debe mantener la seguridad, disponibilidad e integridad necesaria para extraer y consultar información histórica y actual, en algunas ocasiones se puede permitir fallas temporales o mantenimiento programados, sin embargo la disponibilidad de la aplicación debe mantenerse superior al 90%.

- Los archivos, informes y documentos de la Empresa deben permanecer en un servidor con las restricciones necesarias para los usuarios.

- Por medio del antivirus podemos mantener la integridad de la información, es necesario verificar los posibles virus en nuestra red y eliminarlos a tiempo.

- Aunque el servicio de telefonía ha evolucionado, es necesario garantizar la atención a nuestros clientes.

Figura3. Formato de Monitoreo Versión 0

FR-MON-V00	
FORMATO DE MONITOREO DIARIO	

Fecha		**Hora**	

Revisado por	

UPS Servidores	**Observaciones**
Verificar Estado de la UPS	
Conectividad WAN	**Observaciones**
Verificar Velocidad Canal	
Verificar ingreso a internet	
Enviar Correo a cuenta Externa	
Recibir Correo de una cuenta Externa	
Conectividad LAN	**Observaciones**
Verificar Dispositivos LAN	
Software Contable	**Observaciones**
Verificar Ingreso a Software Contable	
Realizar Prueba de Impresión	
Revisar Backup realizado	
Acceso a Documentación	**Observaciones**
Ingresar a las carpetas compartidas	
Revisar Backup realizado	
Antivirus	**Observaciones**
Verificar Estado de los equipos	
Actualizar Base de Datos de Antivirus	
Telefonía	**Observaciones**
Llamada a extensión interna	
Llamada externa	

Observaciones:

Fuente: Autor

4.2.3. Hojas de Vida

- Todos los equipos de la Empresa deben tener su hoja de vida de forma digital, es imperativo para auditorias.

- Es necesario identificar el software y las licencias instaladas en cada equipo.

- Se debe asignar permisos a los usuarios responsables de manejar cada equipo y/o dispositivo.

- Es necesario conocer el funcionamiento de los aplicativos así mismo los puertos necesarios para garantizar la conectividad y funcionamiento.

- El Backup de la información debe ser programado de acuerdo a su uso, se debe almacenar la configuración de los equipos y la información corporativa.

- Se debe garantizar que cada equipo tenga instalado un antivirus y el software necesario para cada área de la Empresa.

Figura4. Formato Hoja de Vida Versión 0

Código: FR-HV-00

HOJA DE VIDA EQUIPOS

INFORMACIÓN GENERAL			
FECHA DE INGRESO:		MODELO DEL EQUIPO:	
FACTURA NÚMERO:		PROCESADOR	
FECHA DE FACTURA:		MEMORIA RAM:	
ROLE A DESEMPEÑAR:		UNIDAD DVD:	
NOMBRE DEL EQUIPO:		DISCOS DUROS:	
NÚMERO SERIE EQUIPO:		RAID:	
GARANTÍA DEL EQUIPO:		PARTICIONES:	
SISTEMA OPERATIVO:		BACKUP ARCHIVOS	
MARCA EQUIPO:		BACKUP CONFIG APLICACIONES	
OBSERVACIONES:			

ADQUISICIÓN DE APLICATIVOS Y/O LICENCIAS			
APLICACIONES / SOFTWARE	CONTACTO / TELÉFONO	GARANTÍA SOPORTE	LICENCIA No

TARJETAS DE RED INSTALADAS			
TARJETA DE RED NO.1			
DIRECCIÓN IP:		DIRECCIÓN FÍSICA:	
PUERTA DE ENLACE:		DNS PRIMARIO:	
DNS SECUNDARIO:			

USUARIOS		
NOMBRE USUARIO	NOMBRE FUNCIONARIO RESPONSABLE	OBJETIVO DEL ACCESO

ACTIVIDADES / MANTENIMIENTOS		
NOMBRE USUARIO	NOMBRE FUNCIONARIO RESPONSABLE	DESCRIPCIÓN ACTIVIDAD / FECHA

Fuente: Autor

4.2.4. Entrada y Salida de Equipos

- Se debe identificar la fecha en las que ingresa o sale un equipo de la oficina.

- Es necesario verificar la hoja de vida de cada equipo con el fin de realizar backup de la información.

- En caso de cambiar el equipo o revisar de hardware fuera de la oficina es necesario que el equipo no tenga información (se debe realizar backup antes de aprobar la salida del equipo).

- Después de verificar las sugerencias anteriores se puede aprobar la salida o ingreso de un equipo o dispositivo.

Figura5. Formato Entrada y Salida de Equipos Versión 0

FR-ENS-00					
FORMATO ENTRADA Y/O SALIDA DE EQUIPOS					
Fecha				Hora	
Descripción		Activo	Marca	Modelo	Serie
Entrada	Salida				
Observaciones					
Entrega	Nombre		Recibe	Nombre	
	Firma			Firma	

Fuente: Autor

4.2.5. Soporte Categorizar requerimientos e incidentes y solucionarlos en los tiempos óptimos

- Realizar Mantenimientos de Hardware - 3 veces al año.

- Realizar Mantenimientos de Software - 3 veces al año.

- Con el fin de atender los casos en orden se debe diligenciar el formato FR-SOP Versión 0.

- Es necesario recordar que los incidentes se revisan primero, los requerimientos son oportunidades de mejora.

Figura6. Formato de Soporte y Mantenimiento Versión 0

FR-SOP-V00									
FORMATO DE SOPORTE Y MANTENIMIENTO									
Realizado por									
fecha	**Descripción del requerimiento**								
Marque con una X									
Requrimiento		**Incidente**		**Nivel Caso**			**Impacto Usuarios**		
SI	NO	SI	NO	1	2	3	<2	<10	masivo
Estado Caso			**Solución Caso**						
Abierto	Cerrado	Pendiente	Observaciones						

Fuente: Autor

4.2.6. Políticas

- El eslabón más débil en la seguridad es el usuario, por ende se deben crear políticas basados en requerimientos realizados por Directivos o inconformidades.

- El cumplimiento de las políticas es obligatorio y no deben existir excepciones.

Figura7. Formato Políticas Versión 0

Código: FR-POL-00		
FECHA DE CREACIÓN	POLÍTICA No	

INTRODUCCIÓN

(Breve Resumen de la política a implementar y su necesidad).

OBJETIVOS

(Mínimo 3).

ALCANCE

(Límites de la política a implementar).

PROCEDIMIENTO

(Actividades necesarias para garantizar el cumplimiento de la política).

POLÍTICAS

(Descripción específica de la política).

Fuente: Autor

4.2.7. BCP Ejecutar planes de contingencia de acuerdo a la metodología planteada

- Las fallas parciales se pueden generar en cualquier empresa, pero la continuidad de nuestras actividades debe permanecer intacta.

- Los planes de continuidad aplican a Computadores, portátiles, equipos e información

- Se debe realizar un plan de contingencia para cada actividad indispensable.

Figura8. Formato Plan de Continuidad del Negocio Versión 0

Código: FR-BCP-00	
PLAN DE CONTINUIDAD DEL NEGOCIO	

PROCESO:

1. **OBJETIVO:** (Descripción general de la contingencia para garantizar la continuidad del negocio).

2. **DESCRIPCION GENERAL DEL PROCESO:** (Identificar los Funcionarios encargados de activar el Plan de Continuidad del negocio).

3. **ALCANCE:** (Límite necesario para garantizar el desarrollo de las actividades).

4. **PROCEDIMIENTOS**

   (Actividades necesarias con el fin de activar la contingencia, identificar personas encargadas de cada actividad).

5. **ESCENARIOS DE FALLA:**
   (Describir las situaciones específicas en las cuales se activa el plan de continuidad del negocio).

6. **CONSIDERACIONES:** (Identificar los requisitos mínimos para activar la contingencia)

Fuente: Autor

4.2.8. DRP Ejecutar planes de recuperación de desastres de acuerdo a la metodología planteada

- Las fallas ocasionadas por la naturaleza o por errores humanos se pueden generar en cualquier empresa, pero la continuidad de nuestras actividades debe permanecer intacta mediante procedimientos aprobados por los Directivos de la Empresa.

- Los planes de recuperación ante desastres aplican a la Infraestructura e información

- Se debe realizar un plan de recuperación ante desastres para cada actividad indispensable

Figura9. Formato Plan de Recuperación ante Desastres Versión 0

Código: FR-BCP-00	
PLAN DE RECUPERACIÓN ANTE DESASTRES	

PROCESO:

1. **OBJETIVO:** (Descripción general del Plan de Recuperación ante Desastres).
2. **DESCRIPCION GENERAL DEL PROCESO:** (Identificar los Funcionarios encargados de activar el Plan de Recuperación ante Desastres).
3. **ALCANCE:** (Límite necesario para garantizar el desarrollo de las actividades).
4. **PROCEDIMIENTOS**

   (Actividades necesarias con el fin de activar el Plan de Recuperación ante Desastres, identificar personas encargadas de cada actividad).
5. **ESCENARIOS DE FALLA:**
   (Describir las situaciones específicas en las cuales se activa el Plan de Recuperación ante Desastres).
6. **CONSIDERACIONES:** (Identificar los requisitos mínimos para activar el Plan de Recuperación ante Desastres).

Fuente: Autor

4.3. Verificar

Debemos evaluar y tabular la información con el fin de identificar las posibles fallas y aciertos basados en la Planeación.

- Los formatos, políticas y planes deben estar diligenciados con el fin de tabular la información y generar indicadores mensuales.

- Se debe verificar el cumplimiento de las políticas aprobadas por los Directivos de la Empresa.
- Se debe actualizar o revisar una vez al mes los Planes de Continuidad del negocio y Planes de recuperación ante desastres.
- Se debe verificar el estado de los casos, su clasificación y su concurrencia con el fin de generar nuevas políticas y planes.
- Verificar estabilidad de los servicios, equipos, etc.
- Verificar permisos y accesos a la información en la red o de forma remota.

4.3.1. Tabulación, indicadores de gestión

El departamento de TI debe gestionar, administrar e innovar con el fin de mantener la seguridad de la información, El objetivo del departamento de TI es minimizar el número de incidentes y requerimientos generados por los usuarios.

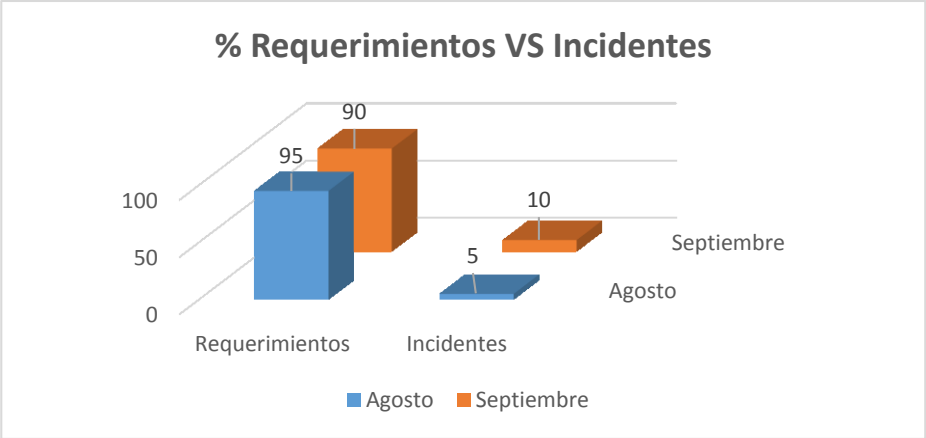
Por medio de políticas, planes, procedimientos y capacitaciones podemos minimizar recursos, tiempo y costos empleados por el departamento de TI, es necesario recordar que los Empleados y Directivos deben acoplarse con el fin de garantizar el correcto funcionamiento de los sistemas orientado al aseguramiento de la información.

Con el fin de tomar decisiones es necesario revisar las estadísticas de servicio y de atención al cliente por parte del departamento de sistemas, las siguientes graficas permiten evidenciar las actividades realizadas por el Departamento de TI.

GESTIÓN E INDICADORES SEPTIEMBRE 2014

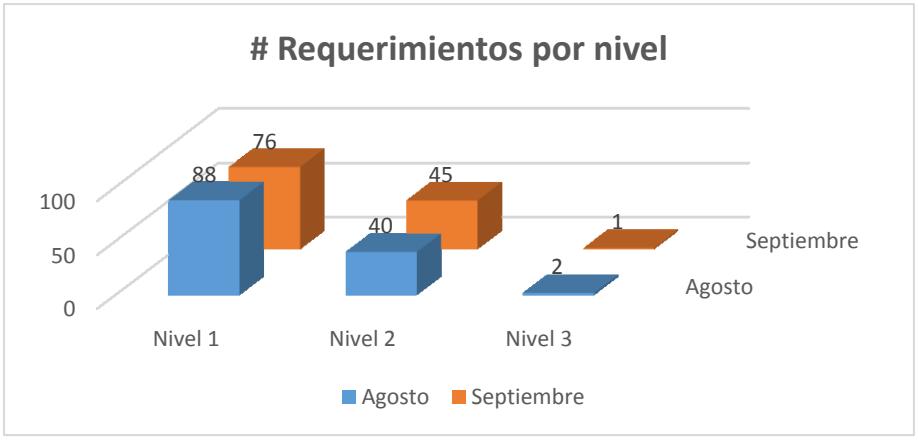
1. Requerimientos VS Incidentes atendidos en el mes

Mes	Requerimientos	Incidentes
Agosto	95	5
Septiembre	90	10



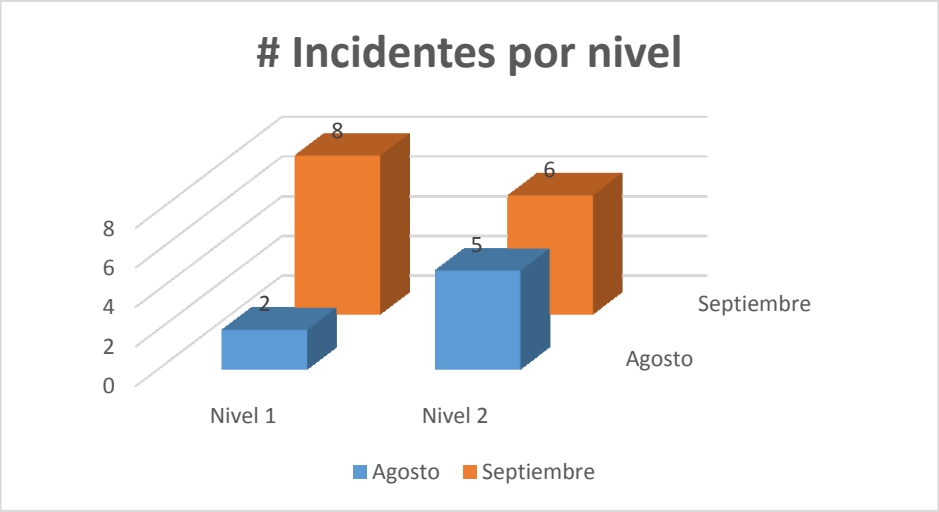
2. Requerimientos por nivel atendidos en el mes

Mes	Nivel 1	Nivel 2	Nivel 3	Total
Agosto	88	40	2	130
Septiembre	76	45	1	122



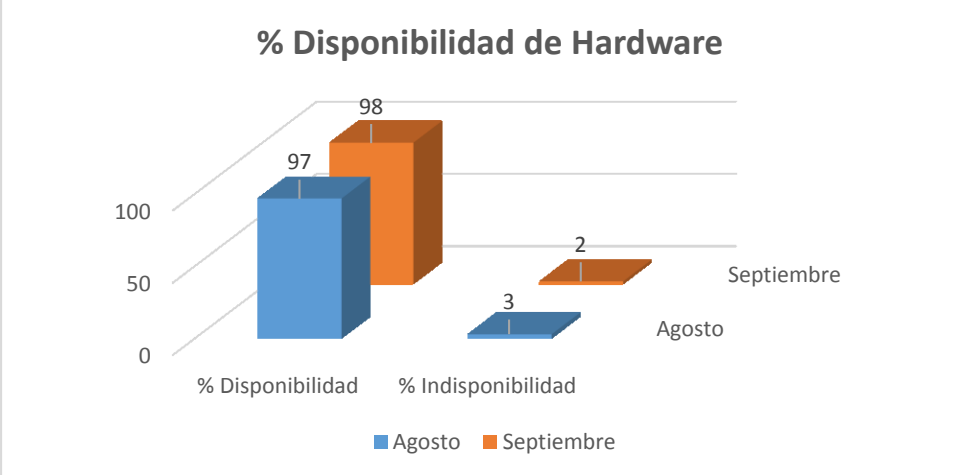
3. Incidentes por nivel atendidos en el mes

Mes	Nivel 1	Nivel 2	Total
Agosto	2	5	7
Septiembre	8	6	14



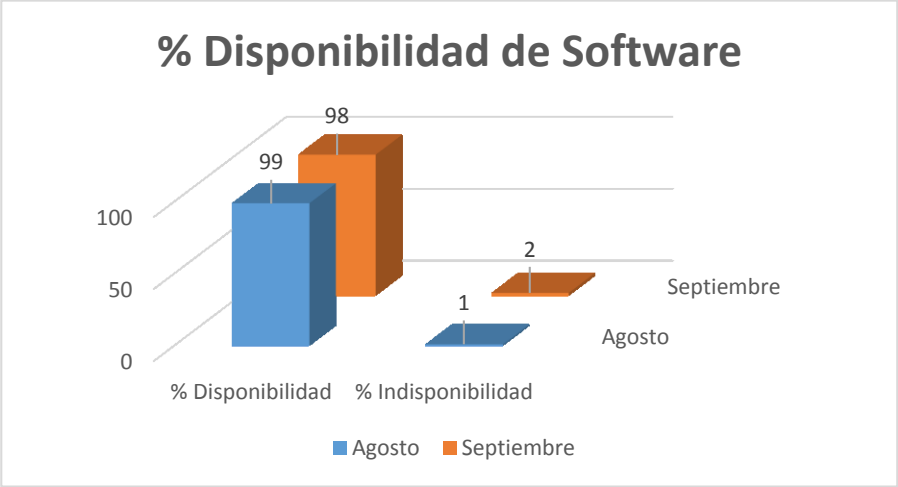
4. Disponibilidad de Hardware

Mes	% Disponibilidad	% Indisponibilidad
Agosto	97	3
Septiembre	98	2



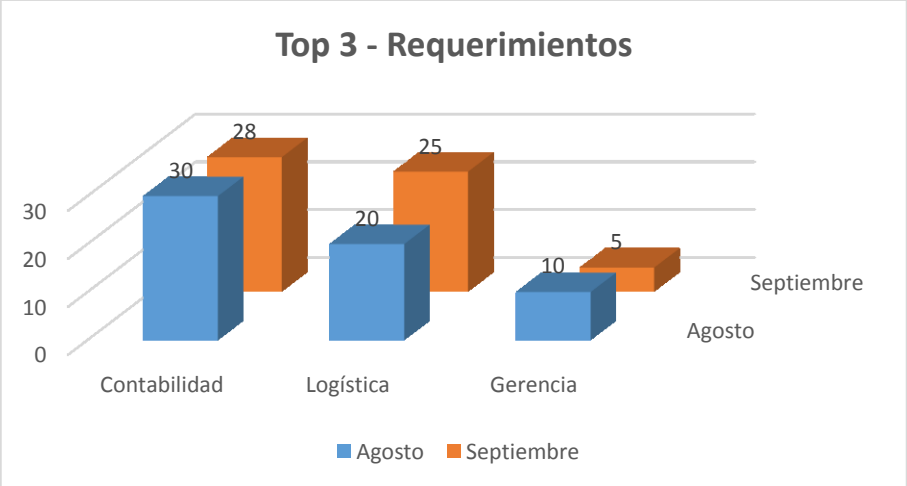
5. Disponibilidad de Software

Mes	% Disponibilidad	% Indisponibilidad
Agosto	99	1
Septiembre	98	2



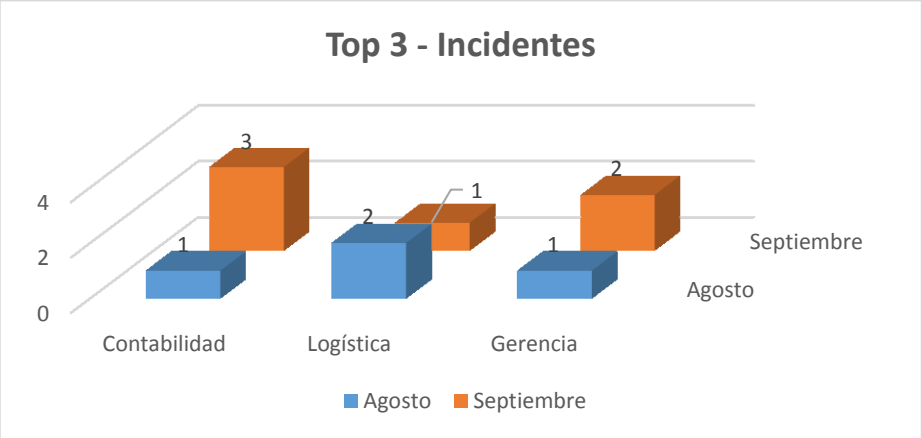
6. Departamentos - Top 3 de Requerimientos

Mes	Contabilidad	Logística	Gerencia
Agosto	30	20	10
Septiembre	28	25	5



7. Departamentos - Top 3 de Incidentes

Mes	Contabilidad	Logística	Gerencia
Agosto	1	2	1
Septiembre	3	1	2



4.4. Actuar

Con el fin de eliminar No Conformidades y optimizar la estrategia del negocio es necesario mejorar los procedimientos actuales y mantener un excelente nivel de servicio, finalmente los siguientes puntos pueden hacer diferencia orientado al departamento de TI hacia el mejoramiento continuo:

Usuarios

- Concientizar a los usuarios mediante capacitaciones.
- De acuerdo a las quejas e inconvenientes presentados cada mes se debe mejorar los métodos usados actualmente.
- De acuerdo a las quejas e inconvenientes presentados cada mes se debe definir nuevas políticas, procedimientos y planes.

Directivos

- Se debe socializar con los Directivos de la Empresa con el fin de crear nuevas políticas y modificaras en caso de ser necesarios.
- Se debe socializar con los Directivos de la Empresa los Planes de Continuidad del Negocio y modificarlo si es necesario.
- Se debe socializar con los Directivos de la Empresa los Planes de recuperación ante desastres y modificarlo si es necesario.

Infraestructura

- Conocer e informar la vida útil de los equipos, dispositivos, infraestructura, etc.
- Proponer nuevos proyectos encargados de mejorar los procedimientos a actividades realizadas a diario.
- Minimizar costos y tiempo requerido en nuestras actividades.

5. ASPECTOS ADMINISTRATIVOS

5.1. Recursos Humanos

Tabla 9. Costo Recursos

N°	Nombre	Cant	Und	Tiempo	Valor $	Origen	Costo $
1	**Ingeniero de Sistemas - Asesor**	**1**	**Hora**	**64 Horas / Mes**	**$200.000**	**Outsourcing**	**$200.000**
2	**Técnico en Sistemas – Persona Operativa**	**1**	**Hora**	**160 Horas / Mes**	**$750.000**	**Contrato**	**$750.000**

Fuente: Autor

5.2. Recursos Físicos Propuestos

Tabla 10. Costo Hardware

N°	Nombre	Cant	Und	Tiempo	Valor $	Origen	Costo $
1	Servidor Power Edge T320 Garantía Pro 5 años	**1**	**Unidad**	**5 Años**	**$7.000.000**	**Activo**	**$7.000.000**

Fuente: Autor

5.3. Recursos Financieros Propuestos

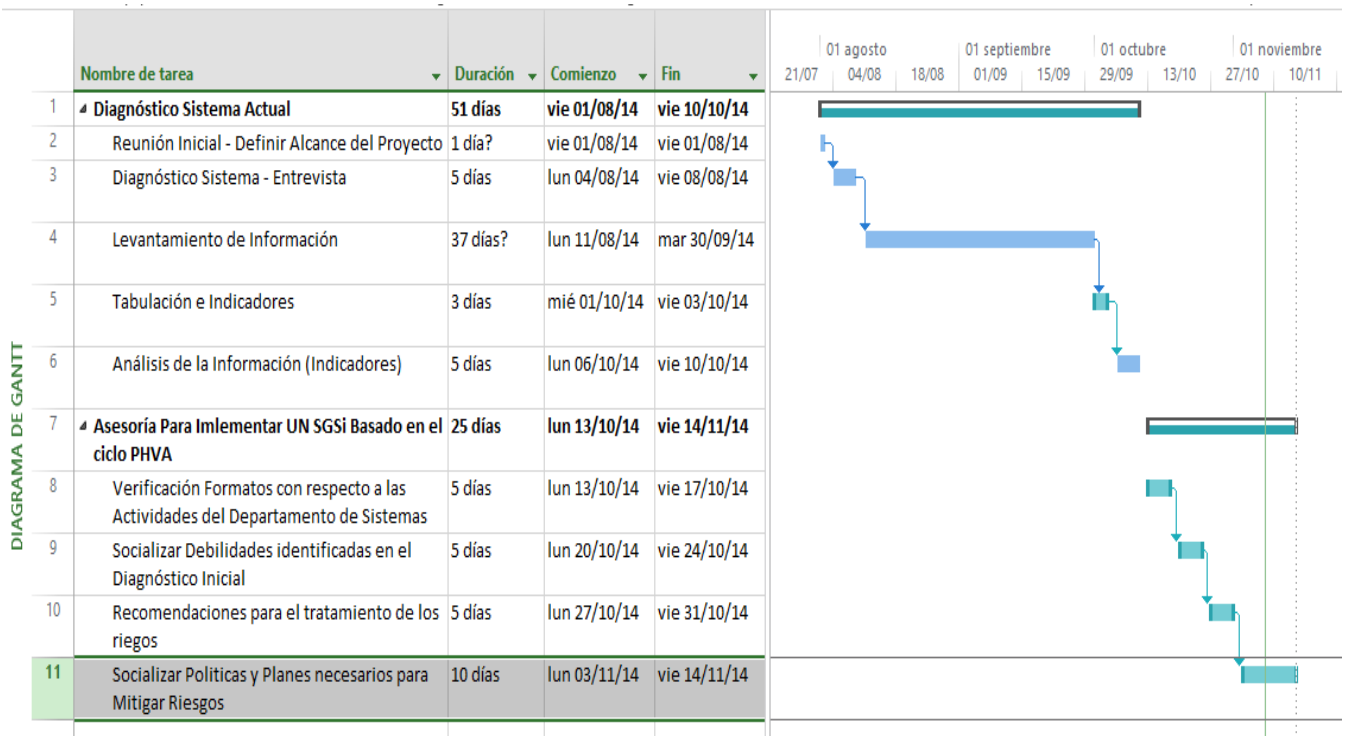
Tabla 11. Costo Software Backup

N°	Nombre	Cant	Und	Tiempo	Valor $	Origen	Costo $
1	Dropbox para Empresas – Software para almacenar archivos	**1**	**Mes**	**Mes**	**USD 15**	**Alquiler**	**USD 15**

Fuente: Autor

5.4. Cronograma de Actividades.

Figura11. Diagrama de Gantt



	Nombre de tarea	Duración	Comienzo	Fin
1	**Diagnóstico Sistema Actual**	**51 días**	**vie 01/08/14**	**vie 10/10/14**
2	Reunión Inicial - Definir Alcance del Proyecto	1 día?	vie 01/08/14	vie 01/08/14
3	Diagnóstico Sistema - Entrevista	5 días	lun 04/08/14	vie 08/08/14
4	Levantamiento de Información	37 días?	lun 11/08/14	mar 30/09/14
5	Tabulación e Indicadores	3 días	mié 01/10/14	vie 03/10/14
6	Análisis de la Información (Indicadores)	5 días	lun 06/10/14	vie 10/10/14
7	**Asesoría Para Imlementar UN SGSi Basado en el ciclo PHVA**	**25 días**	**lun 13/10/14**	**vie 14/11/14**
8	Verificación Formatos con respecto a las Actividades del Departamento de Sistemas	5 días	lun 13/10/14	vie 17/10/14
9	Socializar Debilidades identificadas en el Diagnóstico Inicial	5 días	lun 20/10/14	vie 24/10/14
10	Recomendaciones para el tratamiento de los riegos	5 días	lun 27/10/14	vie 31/10/14
11	Socializar Politicas y Planes necesarios para Mitigar Riesgos	10 días	lun 03/11/14	vie 14/11/14

Fuente: Autor

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Después de aplicar la metodología en espiral se obtuvo un planteamiento inicial el cual permitirá llevar y administrar la infraestructura de la Empresa orientada al control de acceso a la información.

- Los requerimientos del cliente permitieron recomendar políticas y planes a nivel corporativo.

- Las funciones del Departamento de TI deben orientarse al mejoramiento continuo con el fin de mitigar e identificar nuevas falencias de la gestión realizada.

- Los requerimientos e incidentes generados en la Empresa TRANSPACK deben ser atendidos en menor tiempo posible, por medio de una base de conocimiento.

- El ciclo PHVA permite gestionar las estrategias basadas en un Sistema de gestión de Seguridad de la Información con el fin de asegurar el acceso a la información.

- Las falencias identificadas en el Sistema de Gestión de la Seguridad de la información deben ser tratadas por medio de políticas basadas en ISO 27002.

6.2. Recomendaciones

- La información de la Empresa Transpack es el activo más importante por ende un Plan de continuidad de negocio garantizará la disponibilidad del 100% de la infraestructura orientada al acceso a de la información.

- Los riegos naturales son inevitables para la Empresa, no se puede estimar su impacto y el momento en que pueda ocurrir, es recomendable crear y diseñar planes de recuperación ante desastres con el fin de garantizar la disponibilidad de la información y la capacidad de la empresa de continuar con sus operaciones a pesar de riesgos inminentes.

REFERENCIAS

El ciclo PHVA planear-hacer-verificar-actuar. Disponible en internet: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

Normatividad SGSI. Disponible en internet: http://seguridadinformaticaufps.wikispaces.com/normatividad+sgsi

Metodología de desarrollo en espiral. Disponible en internet: http://www.acertasoftware.com/mspiral.html

Aprenda a blindarse contra los 'hackers'. Disponible en internet: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-blindarse-de-los-hackers/14462677

Sistema de gestión de seguridad de la información ISO/IEC 27001. Disponible en internet: http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039-iso-iec-27001-es-260412.pdf

Normas APA 2014. Disponible en internet: http://normasapa.com/2014/descargar-plantilla-en-word-de-tesis-con-normas-apa-2014/