FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

APLICACIÓN DE NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN PARA SYSTEMS SUPPORT & SERVICES S.A.

PRESENTADA POR

MAURO LUIS VENTO MEZA

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2014

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

APLICACIÓN DE NORMATIVAS DE SEGURIDAD DE LA INFORMACION PARA SYSTEMS SUPPORT & SERVICES S.A.

TESIS

PARA OPTAR EL GRADO DE INGENIERO EN COMPUTACIÓN Y SISTEMAS

PRESENTADO POR:

VENTO MEZA, MAURO LUIS

LIMA, PERÚ

2014

Dedicatoria

A mis padres, Mauro y Amelia y a mi hermana Amelia a quienes debo el estar hoy en estas instancias y a mis profesores, que con sus enseñanzas y recomendaciones me guiaron en el logro de este trabajo.

Agradecimiento

A Dios, por haberme dado la vida y haberme permitido tener el éxito que hoy en día tengo, a mi familia que hizo posible cumplir una meta trazada años atrás, a mis asesores por sus buenas recomendaciones y su apoyo constante en los avance, al Ing. Pineda por el apoyo en este trabajo brindándome la información requerida y finalmente a los Ingenieros Figueroa y Villena por su incondicional apoyo en esta investigación.

ÍNDICE

LISTA DE TABLAS

Página

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

La presente tesis está centrada en la aplicación de las normativas para el diseño y ejecución de un Sistema de Gestión de Seguridad de Información, con lo cual se podrá tener un control y monitoreo adecuado de las políticas de seguridad de la información, a fin de proteger la información relevante para la organización, además de gestionar los riesgos de manera idónea y mitigar las falencias.

En esta investigación se desarrolló una metodología aplicada con la que se realizó la captura de información, para el análisis de la información, con la cual se va a poder realizar un diagnóstico, asignar la prioridad y determinar cuál es la brecha existentes en el área de sistemas y los riesgos a los que están expuestos los activos de la organización, y finalmente poder plantear e implementar la solución.

Como resultado, se consiguió implementar un cuerpo normativo, con el cual se pretende controlar y prevenir futuras incidencias, garantizando de esta manera la integridad, confiabilidad de la información y mantenerla disponible. Además, se logró culminar satisfactoriamente las fases de desarrollo del proyecto, entregables adecuados y establecidos por las metodologías Familia ISO 27000 y COBIT 5.0.

Palabras Claves: Familia ISO 27000, COBIT 5.0, Sistema de Gestión de Seguridad de Información.

ABSTRACT

This project is about implementation of the regulations for the design and implementation of a Management System of Information Security, which may have an appropriate control and monitoring policies information security, to protect information relevant to the organization, and manage risks in an appropriate way and mitigate weaknesses.

In this research applied research with the data capture was performed to analyze the information, which will be able to make a diagnosis, prioritized and determine the existing gap developed the area of systems and the risks they are exposed to the assets of the organization, and finally to raise and deploy the solution.

As a result, it was possible to implement a regulatory body, which is intended to control and prevent future incidents, thereby ensuring the integrity, reliability of information and keep it available. In addition, he managed to successfully finish the project development phases, deliverables and appropriate methodologies established by ISO 27000 Family and COBIT 5.0.

Keywords: ISO 27000 family, *COBIT 5.0*, Management System of Information Security.

INTRODUCCIÓN

La seguridad de la información es hoy en día una de las ramas más importantes en la informática no solo por proveer protección de los activos tecnológicos y la información almacenada, sino porque además, es una herramienta en las que las empresas se apoyan para poder obtener ventaja competitiva respecto de las demás empresas del mismo rubro que día a día compiten para poder esta ventaja y posicionarse en el mercado.

En muchos casos las empresas tienden a enfocarse más en generar valor que en cuidar los medios que les permiten obtener este valor, estando así propensas a una fuga de información de la cual sus competidores podrían hacer uso y obtener un mayor posicionamiento.

Con la finalidad de contribuir con la compañía con la continuidad del negocio, se realizó esta investigación, la cual consiste en la aplicación de normativas de seguridad de la información, mediante las cuales se van a plantear controles de seguridad para preservar esta información delicada.

La presente investigación está dividida en cuatro capítulos, que a continuación se detallaran:

En el primer capítulo se describen los antecedentes, que son investigaciones a fines a esta con lo cual se podrá tener una idea del campo de investigación al que se quiere entrar, las bases teóricas que se van a poner en práctica en esta investigación y los términos básicos que se empelan en la investigación.

En el segundo capítulo se hace mención a los materiales y herramientas utilizados para la investigación y los métodos, que en este caso son las normativas y estándares de seguridad de la información.

En el tercer capítulo se detallas cuáles fueron las pruebas y resultados obtenidos en esta investigación con el fin de evidenciar que la solución planteada fue la correcta.

En el capítulo final se discute sobre el tema para hacer el comparativo de la situación de la empresa antes de aplicar la solución n y el después de aplicarla, así como que aplicaciones puede tener a futuro dicha solución planteada.

1. Definición del Problema

Todas las empresas se rigen a las normativas y políticas establecidas, pero no todos los miembros del personal lo cumplen, nos encontramos que este problema principal se resume en las deficiencias presentadas por la empresa en el control de seguridad de la seguridad de su información, y la carencia de una gestión de riesgos adecuada en dicha empresa que impide que se pueda identificar vulnerabilidades, así como cuantificarlas y priorizarlas, por ende tomar medidas de acción que permitan subsanar estas falencias.

Este descuido ocasiona que la información relevante para el negocio este expuesta a personas no autorizadas para un fin indebido, otro riesgo seria la pérdida de la información y por ende que la organización tenga una desventaja competitiva con respecto a sus competidores.

1.1. Problema

Ineficiente control en la seguridad de la información y la gestión de riesgos en Systems Support & Services S.A.

2. Objetivos

2.1. Objetivo General

- Optimizar la gestión de seguridad de la información en la empresa,

2.2. Objetivos Específicos

- Identificar amenazas y vulnerabilidades existentes en la empresa.
- Realizar un análisis de riesgos de los activos de la empresa.
- Mapear los riesgos de activos.
- Asignar controles asociados a los riesgos identificados.

- Validar que la efectividad de controles de la seguridad de la información funcionen a un 70%.
- Concientizar al 70% del personal de la empresa sobre los riesgos a los que están expuestos los activos.

3. Justificación

3.1. Justificación teórica

Con esta investigación se pretende reforzar los conocimientos adquiridos en la parte teórica referido a lo que es seguridad de la información y en los estándares de seguridad como las COBIT, así como en la como la familia ISO 27000.

En esta investigación se optó por COBIT, debido a que es un estándar que integra otros estándares, como por ejemplo, PMBOK, ITIL,ISO 27002, entre otros, está orientado a procesos, además COBIT es fuerte en controles y métricas de TI, mientras que la ISO 27000 tiene su fortaleza principal en los controles de seguridad.

3.2. Justificación práctica

Tomando como base lo expuesto en la justificación teórica, se busca plasmar toda la teoría adquirida en una situación real para conocer como las organizaciones actúan para poder mitigar las falencias identificadas, de tal manera que se pueda garantizar la integridad, confiabilidad y disponibilidad de la información, así como monitorear y prevenir incidencias para evitar que la información delicada se vea afectada.

Además, los beneficios de contar con una metodología son que esta permitirá realizar una planeación y organización adecuada, así como reducir riesgos y costos.

3.3. Justificación tecnológica

Como resultado del incremento de la dependencia de las organizaciones respecto a la tecnología para el manejo de su información y del incremento de interconectividad la información cada vez está más expuesta a una variedad más amplia y sofisticada de amenazas y vulnerabilidades. Estas amenazas pueden ser internas, externas, premeditadas, accidentales, etc.

Por ello se busca con este proyecto aplicar normativas a fin de proteger los recursos tecnológicos con los que cuenta la empresa y asegurar el mantenimiento preventivo y correctivo a nivel de recursos de tecnologías de información.

3.4. Justificación económica

Los grandes y diferentes volúmenes de información que se manejan en la compañía constituyen un activo de gran importancia que actualmente no se protege con la prudencia necesaria ni con las medidas formales que técnicamente se deben tener en cuenta.

La aplicación de esta normativa permitirá proteger la información de los clientes de tal manera que se evite que la lista de clientes caiga en manos de la competencia o desaparezca, lo cual ocasionaría daño a la marca y pérdida de confianza de los accionistas, costos por multas y por notificación a los afectados así como la suspensión de servicio y pérdida de clientes e ingresos.

CAPÍTULO I
MARCO TEÓRICO

1.1. Antecedentes

Antes de la aparición de las primeras redes de computadores, prácticamente toda la información sensible de una organización se guardaba en un formato físico: Bodegas repletas de grandes archivadores y toneladas de papeles eran los encargados de guardar los datos y la contabilidad de una empresa. Pero con la aparición de la computación y el auge de las redes, la información comenzó a digitalizarse de una manera impresionante, y una bodega llena de archivadores con datos de una cartera de clientes ahora podía resumirse al contenido de un disco duro de un equipo que podría ocupar menos de un metro cuadrado de superficie. Este avance en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de la información, trajo consigo un nuevo problema al mundo de la informática: La información en formato digital, es más fácil de transportar, por lo que las posibilidades de hurtarla o alterarla no son latentes.

Systems Support & Services S.A, empresa integradora de tecnología fue fundada el 18 de Agosto de 1989 por el ingeniero Luis Reátegui Sánchez. En la actualidad, la empresa, cuenta con más de 400 clientes para los cuales tiene destinados a aun equipo de profesionales que en su mayor parte se dedican a la atención y servicio 80% de los cuales están dedicados al área de soporte, servicios y comercial y un 20% a las áreas de soporte administrativo, ambas dispuestas a ofrecer un servicio de alta calidad.

Algunas investigaciones relacionadas al tema se mencionan a continuación:

La tesis de Aliaga (2013) sobre el Diseño de un sistema de gestión de seguridad de información para un instituto educativo, y la investigación de Lahuara (2007) acerca de la Metodología para desarrollar un plan de Seguridad de Información demostraron que la información es el activo más importante en una organización y que cualquier empresa que no cuente con un adecuado SGSI, está en desventaja con respecto a las demás empresas del mismo rubro.

Precisamente, la tesis de Sánchez (2010) sobre Normativa e Inducción en Seguridad de información para el grupo Telefónica del Perú , la cual explicó sobre la importancia de concienciar al personal sobre la importancia de proteger la información que administra la organización de personas no autorizadas, así como de minimizar la pérdida o fuga de datos.

1.2. Bases Teóricas

1.2.1. Gestión de riesgos

Areitio (2008) dice:

La gestión de riesgos es el proceso total de identificar, controlar y eliminar o minimizar los eventos inciertos que puedan afectar a los recursos en una unidad de negocio. En la práctica, existen dos enfoques básicos a la hora de realizar un completo análisis de riesgos, uno cualitativo y el otro cuantitativo, siendo el primero de uso muy común en la actualidad, debido a que es más sencillo e intuitivo que el cuantitativo, ya que implica datos complejos o datos difíciles de estimar. La gestión del riesgo integra las técnicas de análisis de riesgos, análisis de beneficios, selección de mecanismos, implementación, verificación, evaluación de la seguridad de las salvaguardas y revisión de la seguridad global. (Pp.54-55).

La *IT Governance Institute (2009) sostiene:*

El apetito de riesgo se puede definir en la práctica en términos de combinaciones de la frecuencia y la magnitud de un riesgo. El apetito de riesgo puede y va a ser diferente entre las organizaciones ya que no existe una norma absoluta o una norma de lo que constituye un riesgo aceptable e inaceptable. (p.17).

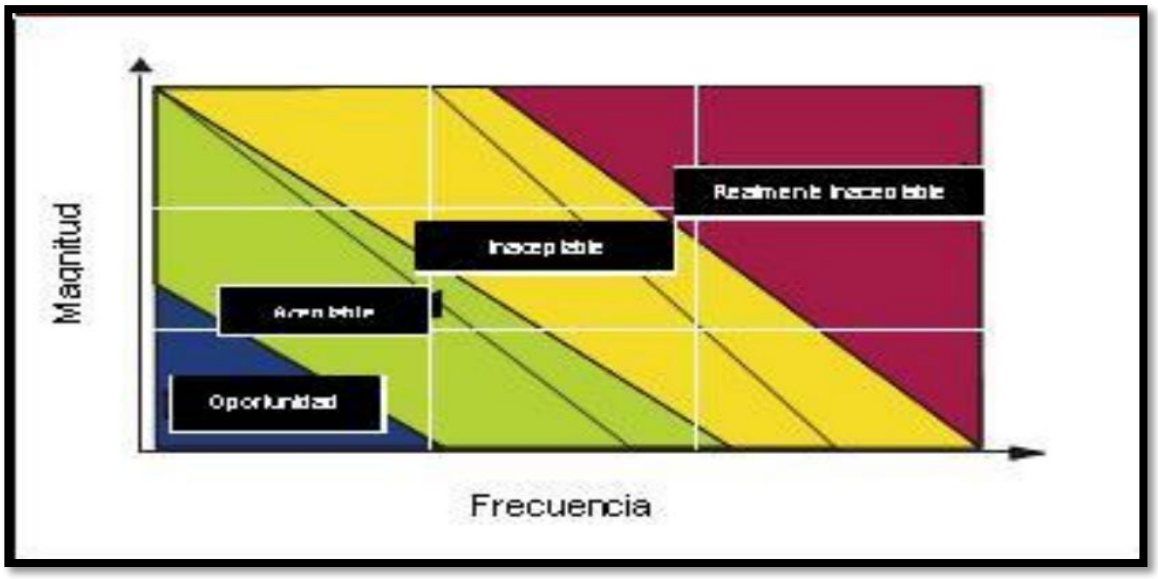


Figura 1: Mapa de Riesgos **Fuente: IT Governance Institute (2009).*RISK IT basado en COBIT. USA: ISACA*, p.17**

1.2.2. Sistema de Gestión de Seguridad de Información(SGSI)

Areitio (2008) establece:

Es parte del sistema global, basado en el enfoque de riesgos del negocio y que establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información. El SGSI incluye la estructura organizacional, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y recursos. (p.200).

1.2.3. Familia ISO 27000

Merino y Cañizares (2011) establecieron:

La serie de normas ISO 27000 se han reservado específicamente por la ISO en materia de seguridad de la información. Esto, por supuesto, se alinea con una serie de otros temas, como la ISO 9000 (gestión de calidad) e ISO 14000 (gestión medioambiental). (p.66)

1.2.4. ISO/IEC 27001 - Sistema de Gestión de la Seguridad de la Información

Merino (2011) sostiene:

"La norma/estándar UNE ISO/IEC 27001 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y Salvaguarda de la información. El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Planificar-Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés ***PDCA (Plan-DO-Check-Act)*** (similar a la más extendida y reconocida norma ISO 9001). (p.68).

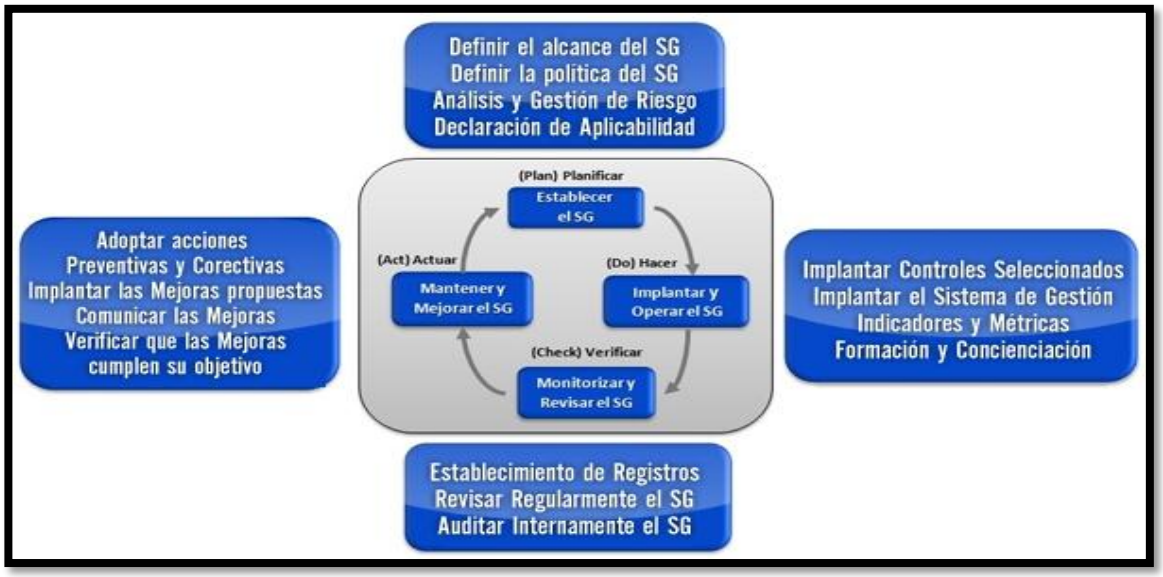


Figura 2: Fases y tareas del ciclo PDCA **Fuente**: Web Site GConsulting Compliance

1.2.5. ISO/IEC 27002 - Técnicas de seguridad - Código de conducta para los controles de seguridad de la información

Merino (2011) sostiene:

La ISO/IEC 27002 es una guía de buenas prácticas en las que se describen los objetivos de control y controles recomendables en cuanto a la seguridad de la información. (p.70).

1.2.6. Normativa COBIT 5.0

La IT Governance Institute (2012) sostiene:

En el 2012 se desarrolló la versión COBIT 5 para el gobierno y la gestión de las TI de la empresa. Además de estar orientado a la gestión, auditoria de sistemas, control y seguridad COBIT 5 ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos (p.13).

COBIT está dividido en 4 dominios, estos son:

- **Planear y Organizar (PO)**

  Estrategias y Tácticas, identifica la manera en que las TI contribuya de la mejor manera a los objetivos del negocio.

- **Adquirir e Implementar (AI)**

  Identificar las soluciones, desarrollo, cambios y mantenimiento de los sistemas existentes.

- **Entregar y Dar Soporte (DS)**

  Incluye la prestación del servicio, administración de seguridad, soporte a los usuarios, etc.

- **Monitorear y Evaluar (ME)**

  Monitoreo de forma periódica en cuanto a calidad y cumplimiento de los requerimientos de control y cubre la administración del desempeño.

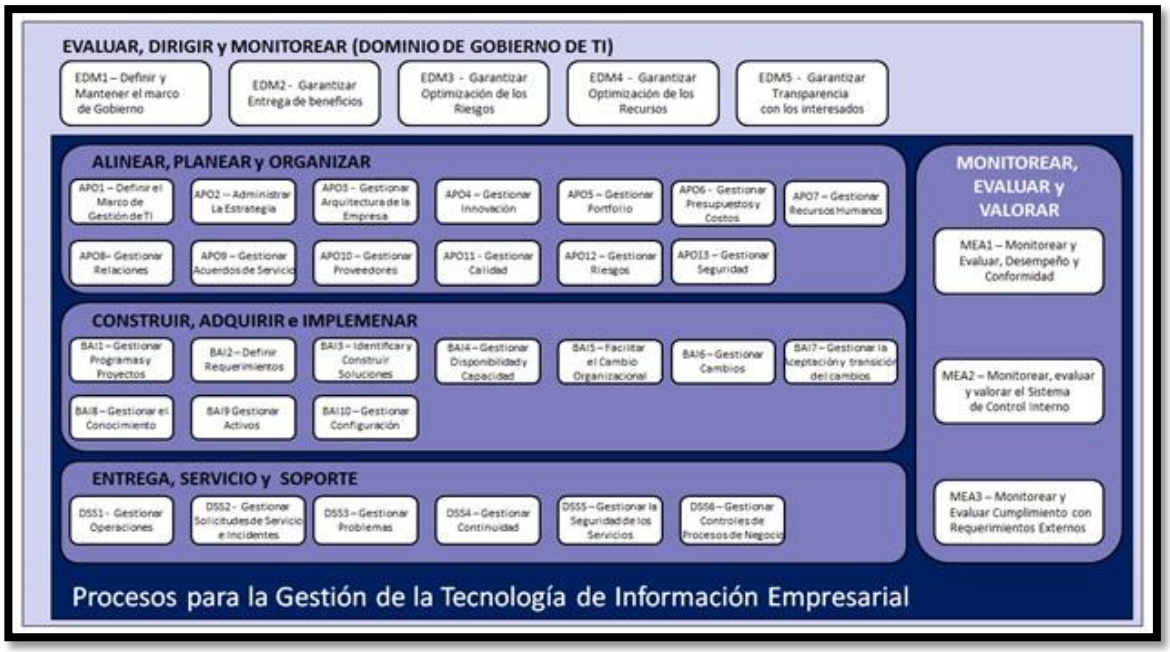


Figura 3: Dominios de COBIT 5.0 **Fuente**: IT Governance Institute (2012) COBIT 5.0. USA: ISACA, p.33

Los principios de COBIT 5 son los que a continuación se puede ver en la figura2:

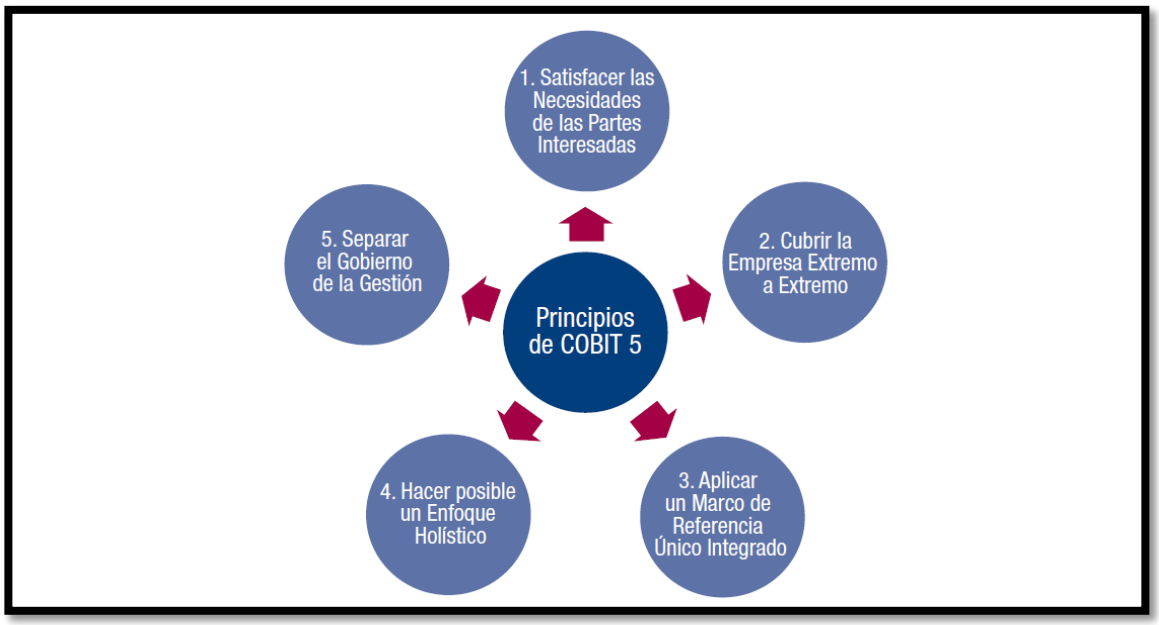


Figura 4: Principios de COBIT 5.0 **Fuente:** IT Governance Institute (2012) *COBIT 5.0*. USA: ISACA, p.13

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Este principio está enfocado a la creación de valor con la finalidad de mantener el equilibrio entre la realización de beneficios y la optimización de los riesgos y recursos, esto se consigue mediante procesos y catalizadores para permitir crear este valor.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, esto significa que cubre todas las funciones y procesos dentro de la empresa, COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin.

Principio 3: Aplicar un Marco de Referencia único integrado

COBIT 5, se alinea con otros estándares y marcos de tal manera que pueda hacer la función de marco de trabajo principal para el gobierno y gestión de TI's en la empresa.

Principio 4: Hacer Posible un Enfoque Holístico

COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores: Principios, Políticas y Marcos de Trabajo, Procesos, Estructuras Organizativas, Cultura, Ética y Comportamiento, Información, Servicios, Infraestructuras y Aplicaciones, Personas, Habilidades y Competencias.

Principio 5: Separar el Gobierno de la Gestión

COBIT 5 establece una división entre sus procesos, separándolos en dos área, una es el área de gobierno de la empresa y la otra es el área de gestión de la empresa.

Finalmente, COBIT 5 nos introduce una cascada de objetivos la cual permite definir las prioridades para la implementación, mejora y aseguramiento del gobierno de TI basada en los objetivos de negocio de la organización y el posible riesgo al que este expuesta. Principalmente, la cascada de objetivos:

Define los objetivos más relevantes y tangibles en varios niveles de responsabilidad.

Permite extraer la información más relevante del conocimiento base de COBIT 5 para su inclusión en proyectos específicos.

Identifica y comunica claramente como los habilitadores son importantes para alcanzar los objetivos organizacionales.

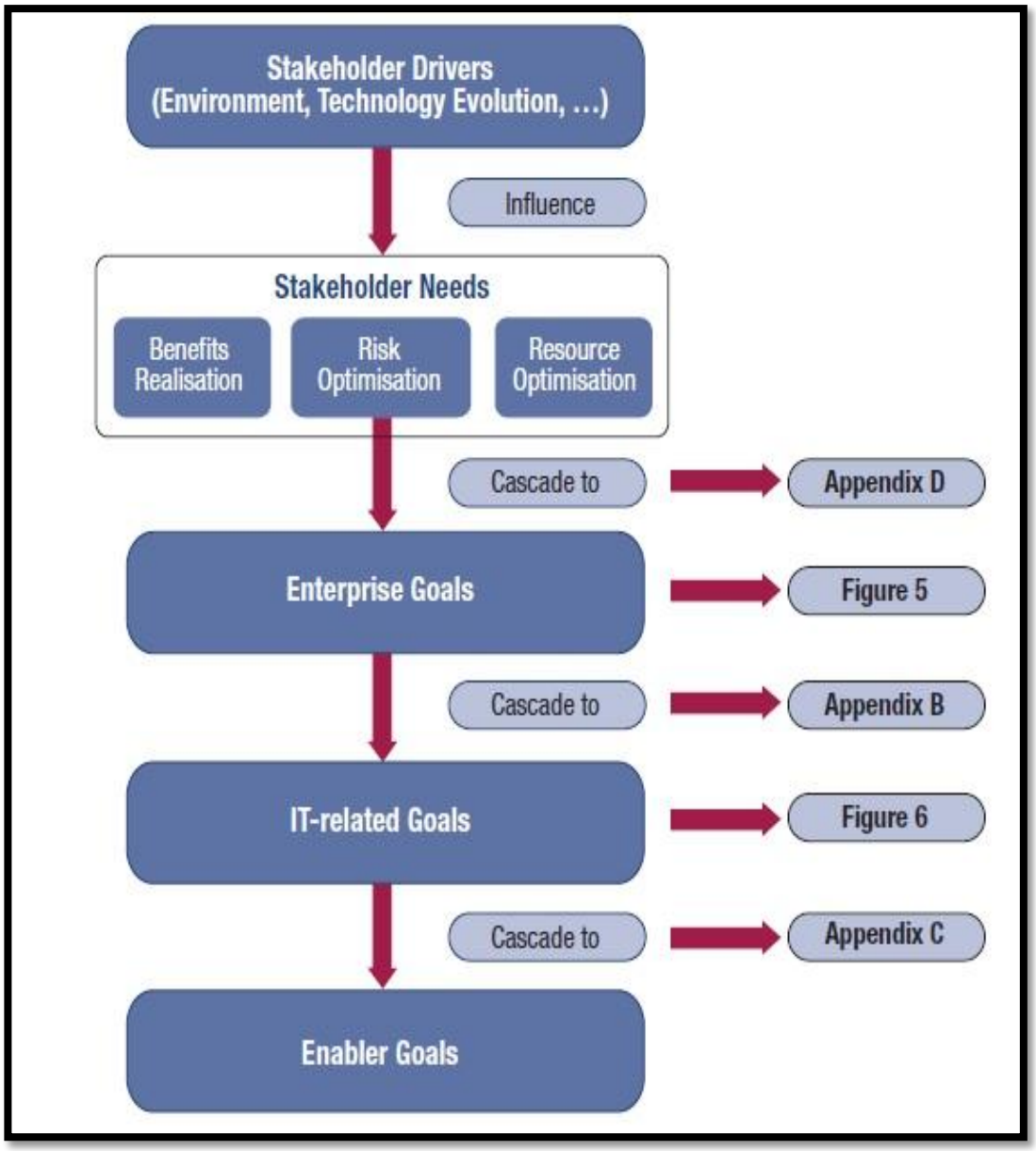


Figura 5: Cascada de objetivos de COBIT **Fuente**: IT Governance Institute (2012) *COBIT 5.0*. USA: ISACA, p.18

1.3. Términos Básicos

Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

Activos

Es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección.

Amenaza

Una condición o situación desfavorable para el proyecto, conjunto de circunstancias negativas, conjunto de eventos negativos, riesgo que si se hace realidad tendrá un impacto negativo en un objetivo del proyecto, o posibilidad de cambios negativos. Cualquier circunstancia o evento que pueda explotar, intencionadamente o no, una vulnerabilidad especifica de un sistema de información.

Apetito de riesgo

Es el nivel de riesgo que una empresa está dispuesta a soportar.

Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora. Un ataque activo es aquello que implica la intrusión directa en el tráfico de red a través de la transmisión, modificación o la reproducción de paquetes.

Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene. Ataque pasivo, es esencialmente un ataque al escuchar en la q el atacante escucha (captura) del tráfico de red, pero no modifica los paquetes o inserta nuevos paquetes en el flujo del tráfico. Los ataques pasivos son sigilosos en la naturaleza y son por lo tanto difíciles de detectar por los administradores que supervisan la seguridad de sus sistemas de redes.

Autentificación

Proceso de verificar la identidad del usuario, estableciendo una sesión por medio de una clave.

Confidencialidad

Significa que la información está protegida frente a accesos no autorizados. La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Control

La palabra control proviene del termino francés *contrôle* y significa comprobación, inspección, fiscalización o intervención. También puede hacer referencia al dominio, mando y preponderancia, o a la regulación sobre un sistema.

Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

Golpe (Breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Impacto

Es la consecuencia que tiene la materialización de una amenaza sobre un activo, sobre un sistema de información y comunicaciones sobre una organización. Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

Integridad de datos

Precisión, oportunidad y relevancia de los datos en un contexto.

Plan de seguridad

Conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.

Políticas de gestión de seguridad de la información

Están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización.

Política de seguridad

Declaración de intenciones de alto nivel que cubre la necesidad de los sistemas informáticos y que proporcionan las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Procedimiento de seguridad

Es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por la organización.

Riesgos

Los riesgos son eventos o condiciones inciertas que, si se produce tiene un efecto positivo o negativo en los objetivos de un proyecto. Es la estimación el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Seguridad

Estar protegido de una amenaza o pérdida, protección de algo que puede dañar, intencionalmente o de otra manera. Es el proceso consistente en mantener un nivel aceptable de riesgo percibido. Además el proceso de seguridad gira en torno a 4 pasos: Estimación, protección, detección y respuesta.

Seguridad Lógica

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. La seguridad lógica se complementa con la seguridad física.

Seguridad Física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informativo, para proteger el hardware de amenazas físicas. Esta también se complementa con la seguridad lógica.

Seguridad de la información

Este concepto está relacionado a la prevención de la confidencialidad, integridad y disponibilidad de la información, además, también pueden estar involucradas otras propiedades como la intensidad, responsabilidad, no-repudio y confiabilidad.

Seguridad informática

Podríamos definirla como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Vulnerabilidad

Cualquier debilidad o falta de control que aumente la probabilidad de que se materialice una de las amenazas a las que están expuestos los activos o elementos del sistema e información y comunicaciones.

La vulnerabilidad representa las a debilidades que permiten que una amenaza lo explote. Ausencia o debilidad de una salvaguarda que mitiga el riesgo, lo cual es condición que tiene el potencial de aumentar la frecuencia de ocurrencia, el impacto o factor de exposición, o ambos, del riesgo. El análisis consiste en identificar estas ausencias o debilidades.

CAPÍTULO II
METODOLOGÍA

2.1. Material

A continuación se aprecia en la siguiente tabla los recursos del proyecto.

Tabla 1: Listado de recursos

RECURSO	DESCRIPCION
Hardware	Laptop
	Multifuncionales
	Impresoras laser
	Servidores
Software	Microsoft Office 2010
	Sistema Operativo Windows 7
	Zotero
	Violet UML
R.R.H.H.	Gerente de soluciones de infraestructura
	Jefe de sistemas
	Gerente de Proyectos
	Jefe de Proyectos
	Coordinador de seguridad y calidad

Fuente: Elaboración propia

2.2. Métodos

2.2.1. Metodología de desarrollo

Para este proyecto se decidió por trabajar con la normativa ISO/IEC 27001:2013 y COBIT 5. Para el caso de la ISO 27001, por ser prácticamente un estándar a nivel mundial y tener mayor reconocimiento en las organizaciones.

En el caso de COBIT5, se optó por esta metodología para fines de poder medir el desempeño de la solución que se pretende implantar y el análisis de riesgos.

Además, la ISO es una de las tantas normativas que se puede integrar con COBIT, ya que este último es la base de todas las metodologías.

Finalmente, se utilizara la metodología PMBOK del PMI para la gestión del proyecto.

2.3. Desarrollo de la investigación

Para el desarrollo de esta solución se utilizó la normativa de seguridad de información ISO/IEC 27001:2013, 27002:2013 y COBIT 5.0

Previamente se dará inicio al proyecto y una vez realizadas todas las fases del PDCA se dará por culminado el proyecto. A continuación se detallará la aplicación de dicho modelo al proyecto:

2.3.1. Establecimiento del SGSI

Este es la etapa inicial, en la cual se va a definir el proyecto en sí, empezando por definir el área donde se va a trabajar, siendo esta el área de sistemas, para ello se elaboró el documento Acta de constitución del proyecto (Ver ANEXO 1), mediante el cual se formalizará el inicio de dicho proyecto en la empresa, además se va a elaborar el Alcance (Ver ANEXO 2).

2.3.2. Planeación del SGSI

Una vez definida el área de trabajo y formalizado el inicio del proyecto se procede a ajustar los plazos y definir las actividades a realizar, elaborando el cronograma de actividades (Ver ANEXO 7), en el cual se definirán las actividades y tareas. También se establecerán pautas de gestión interna del proyecto, en cuanto a organización, gestión de recursos profesionales y técnicos, división de tareas a realizar, reuniones, captura de datos, identificación de riesgos y gestión de incidencias, entre otros.

Primero se recolecta información mediante cuestionarios (Ver ANEXO 9), los cuales van a servir para poder recopilar la información necesaria para poder hacer el análisis respectivo.

Posteriormente se procede a realizar un análisis de brecha o gap análisis, para poder tener una panorama de cuál es la situación actual en la que se encuentra la empresa en temas de seguridad de la información. A continuación se puede apreciar un ejemplo de dicho análisis, usando uno de los dominios que posee la metodología.

Primero se usa los niveles de madurez que establece la ISO 27001, esto nos va a permitir medir la madurez de la empresa en cuanto a seguridad de datos de tal manera que se pueda saber cuál es la situación. Primero se aprecia el cuadro de estados, el cual muestra la descripción exacta de cada nivel y cuál es su equivalente en porcentajes.

Tabla 2: Cuadro de estados de capacidad.

CUADRO DE ESTADOS DE NIVELES DE MADUREZ			
REPRESENTACION A COLORES	**VALOR DE LA MEDICION**	**NIVEL**	**DESCRIPCION**
	100%	Optimizado	Se centra en la mejora continua de los procesos.
	80%	Gestionado y Medible	Usando medidas de campo, la dirección puede controlar empíricamente la eficiencia y efectividad de los salvaguardas, los procesos son cuantificados.
	60%	Definido/Establecido	Se despliegan y se gestionan las salvaguardas. Las oportunidades de sobrevivir son altas, pero siempre queda el factor de no planificación.
	40%	Repetible	Los éxitos son repetibles, pero no hay plan para los incidentes.
	20%	Inicial	Existen salvaguardas, pero no se gestionan.
	0%	Nulo	No existe salvaguarda implementada.

Fuente: Merino Bada C, (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001*.Madrid: FC editorial, p.51.

Una vez descrito los niveles de madurez con los que se van a hacer las mediciones, se realiza el análisis de brecha pre, para efectos de mostrar el procedimiento se usara una parte del cuadro, en el ANEXO 11 se puede apreciar la matriz completa.

Tabla 3: Formato del GAP Análisis

	SITUACION ACTUAL	CONTROL	ANALISIS DE BRECHA PRE	
DOMINIO DE LA NORMATIVA				
	La empresa SSS			
ID CONTROL	Brechas identificadas		Controles que deben implementarse para mitigar dichas brechas.	Nivel de madurez de la empresa en este dominio.

Fuente: Barrantes Porras, C y Hugo Herrera J. (2012). *Diseño e Implementación de un Sistema de Gestiona de Seguridad de la Información en procesos tecnológicos.* Lima: Universidad San Martin de Porres, pp.105-109.

Una vez recolectada la información, esta debe ser analizada, pero antes de ello se procederá con identificar los activos con los que cuenta la empresa. Como se puede apreciar cada activo es categorizado, dependiendo de si se trata de una persona, un recurso físico o lógico, además de su descripción, también se les asigna un impacto, este último ítem representa que tan perjudicial puede ser para la empresa si perdiera alguno de estos activos o si alguno de estos fuera afectado por alguna anomalía, en otras palabras, que tanto le afecta a la empresa el perder dichos activos. Teniendo identificados dichos activos se procede a listar las posibles amenazas que podrían dañar los activos, de igual manera categorizándolos, describiéndolos y añadiéndoles una probabilidad de ocurrencia, siendo la mayor la más factible, de igual manera como en el gap análisis. En la siguiente tabla se puede apreciar lo expresado en el párrafo anterior.

En los anexos se podrá ubicar la tabla completa (Listado de activos) y tener un mayor detalle, a continuación apreciaremos un el formato de dicho documento. Ver ANEXO 11.

Tabla 4: Formato de la lista de activos

ID	DEFINICION DEL ACTIVO	CRITERIOS DE VALORIZACION			VALOR TOTAL	CRITICIDAD
		INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD		

Fuente: Merino Bada C, (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001.* Madrid: FC editorial, p.106

A continuación, la siguiente tabla detalla el rango de valores que se puede obtener, asociados a un nivel de criticidad específico. Cabe señal que es la misma organización la que define sus niveles de criticidad en lo que a activos se refiere.

Tabla 5: Lecturas de los niveles críticos

VALOR	CRITICIDAD
0	NINGUNO
1 A 3	BAJO
4 A 6	MEDIO
7 A 10	ALTO

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, p.40.

2.3.2.1. Mapa de Riesgos

Para en análisis de riesgos, se elaboró la siguiente matriz de calor, en la cual tengo como variables el impacto que sufriría el negocio con las anomalías que se puedan encontrar, así como el impacto de que este afecte al negocio, teniendo ambas variables hacemos una conjunción y en base a eso obtenemos como resultado la categoría de riesgos, como podemos apreciar a continuación en la Tabla 6.

A esta matriz se le conoce como matriz de calor porque en teoría los riesgos elevados, que son representados por el color rojo queman, es decir, causan un daño de gran magnitud en los activos de información y a menor nivel de riesgo menor nivel de calor hasta llegar al nivel más bajo, el cual está representado por el color verde.

Tabla 6: Mapa de riesgo

PROBABILIDAD		RARO 1	IMPROBABLE 2	POSIBLE 3	MUY PROBABLE 4	CASI CIERTO 5
IMPACTO	CATASTRÓFICO 5	Aceptable 5	Elevado 10	Elevado 15	Inaceptable 20	Inaceptable 25
	MAYOR 4	Bajo 4	Aceptable 8	Elevado 12	Elevado 16	Inaceptable 20
	MODERADO 3	Bajo 3	Aceptable 6	Aceptable 9	Elevado 12	Elevado 15
	MENOR 2	Bajo 2	Bajo 4	Aceptable 6	Aceptable 8	Elevado 10
	INSIGNIFICANTE 1	Bajo 1	Bajo 2	Bajo 3	Bajo 4	Aceptable 5

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, pp.46-47.

Ahora se describe la probabilidad que los activos se vean afectados por dichas anomalías como se puede apreciar en la Tabla 7.

Tabla 7: Probabilidades de que se vea afectado los activos.

PROBABILIDAD QUE AFECTE	INTERPRETACION
CASI CERTERO	ES CASI SEGURO QUE LA AMENAZA AFECTARÁ A LA VULNERABILIDAD
MUY PROBABLE	ES MUY PROBABLE QUE LA AMENAZA AFECTARÁ A LA VULNERABILIDAD
POSIBLE	ES POSIBLE QUE LA AMENAZA AFECTARÁ A LA VULNERABILIDAD
IMPROBABLE	ES IMPROBABLE QUE LA AMENAZA AFECTARÁ A LA VULNERABILIDAD
RARO	ES IMPENSABLE QUE LA AMENAZA AFECTARÁ A LA VULNERABILIDAD

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, pp.47-48

De igual manera hacemos lo mismo para el impacto de negocio, como se aprecia en la Tabla 8.

Tabla 8: Impacto de las amenazas

IMPACTO EN EL NEGOCIO	INTERPRETACION
CATASTROFICO	AFECTARÁ POR MAS DE UNA SEMANA LAS OPERACIONES DE LA EMPRESA
MAYOR	AFECTARÁ HASTA 72 H LAS OPERACIONES DE LA EMPRESA
MODERADO	AFECTARÁ HASTA 24 H LAS OPERACIONES DE LA EMPRESA
MENOR	AFECTARÁ HASTA 6 H LAS OPERACIONES DE LA EMPRESA
INSIGNIFICANTE	EFECTO NULO O MUY PEQUEÑO SOBRE LAS OPERACIONES DE LA EMPRESA

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, pp.47-48

Una vez planteado el mapa de riesgos, categorizando los impactos y probabilidades de ocurrencia de dichos riesgos, el siguiente paso es elaborar la Matriz de Riesgos, en dicha matriz asignamos un identificador al riesgo, describimos el activo, describimos la vulnerabilidad y el riesgo al que está expuesto, aplicando la conjunción mencionada anteriormente en el mapa de riesgos con la cual obtenemos el nivel de riesgos, observemos la Tabla 9 para entender el procedimiento, teniendo una determinada amenaza(A1, A2, A3,A4). Ver el ANEXO 14 se muestra la tabla completa, para un mejor entendimiento,

para efectos de la explicación y desarrollo del capítulo se muestra una parte de la tabla, que es la que se está apreciando en la siguiente tabla.

Tabla 9: Matriz de riesgos.

MATRIZ DE RIESGOS			
AMENAZA	**PROBABILIDAD QUE LA AMENAZA EXPLOTE LA VULNERABILIDAD**	**IMPACTO ESTIMADO EN LA EMPRESA**	**NIVEL DE RIESGO**
A1	RARO	INSIGNIFICANTE	BAJO
A2	POSIBLE	MODERADO	ACEPTABLE
A3	MUY PROBABLE	MAYOR	ELEVADO
A4	CASI CIERTO	CATASTROFICO	INACEPTABLE

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, p.48.

2.3.2.2. Controles para el tratamiento de riesgos

Para empezar se definió controles respecto a las políticas de seguridad que la entidad busca establecer para alcanzar el nivel de seguridad deseado, para efectos de explicar el procedimiento se seleccionó dos de los controles, ver en el ANEXO 16 la tabla completa. Cabe resaltar que todos estos controles o políticas contribuyen a la mitigación de todos los riesgos identificados y, en su mayoría, deberán ser desarrollados y promovidos por la Alta Gerencia de la empresa. Estos controles y políticas de seguridad son los siguientes:

Tabla 10: Controles para la mitigación de riesgos

CLAUSULA	CATEGORIA DE SEGURIDAD	NOMBRE DEL CONTROL	DESCRIPCIÓN	RIESGOS A CONTROLAR	ADAPTACION A LA EMPRESA
Políticas de seguridad	Políticas de seguridad de información.	Documentar las políticas de seguridad de información.	Debe crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad.	TODOS	Se deberá crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad.
		Revisión de las políticas de seguridad de información.	Los documentos de política de seguridad de información debieran ser aprobados por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.	TODOS	La gerencia deberá aprobar por la gerencia, publicar y comunicar a todos los empleados y las partes externas relevantes los documentos de las políticas de seguridad de información.
Seguridad en R.R.H.H.	Seguridad durante el desempeño de las funciones.	Concientización y formación sobre la seguridad de la información.	Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.	R1, R4, R6, R11, R16, R20, R22, R26, R28, R32, R34,R38, R40, R50, R53, R100, R101, R102, R103, R104, R105,R106,R107,R108, R109, R110, R111, R112, R113	Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, pp.57-59.

Identificados los controles se procede a preparar un plan de acción para mitigar las falencias, en el siguiente cuadro de se tiene un planteamiento de dicho plan.

Objetivos

Tabla 11: Objetivos por acción

ACCIONES	OBJETIVO(PRINCIPAL/OPERATIVO)	RESPONSABLE	PLAZO DE EJECUCION	PRIORIDAD
Acciones a realizar.	Objetivo de la acción.	Responsable de ejecutar la acción.	Duración de la ejecución de la acción.	Prioridad de la acción**.**

Fuente: Merino Bada C, (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001.* Madrid*:* FC editorial, p.169

Planificación de acciones

Tabla 12: Planificación de acciones

OBJETIVOS	ACCIONES	RESPONBASILIDADES (QUIEN?)	RESULTADO ESPERADO
Objetivo de la acción.	Acciones a realizar.	Responsable de ejecutar la acción.	Resultado que se espera obtener de esta acción.

Fuente: Merino Bada C, (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001.* Madrid*:* FC editorial, p.170

2.3.2.3. Mapeo de los controles con COBIT 5.0

En este punto se identificarán los objetivos corporativos que COBIT 5 propone, relacionados a los objetivos de negocio de Systems Support & Services S.A. Luego, se procederá a relacionar las metas de TI asociadas a dichos objetivos organizacionales y, a continuación, se identificará los procesos habilitadores que dan soporte al cumplimiento de dichas metas de TI. Todo este mapeo sigue el esquema de la “Cascada de Objetivos" que propone COBIT 5 (figura 5).

Finalmente, se comparará y evaluará los procesos habilitadores finales con los controles para el tratamiento de los riesgos que se establecieron en el punto anterior.

Cabe recordar que COBIT 5 se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer. Asimismo, la audiencia objetivo es la alta gerencia, en conjunto con los demás gerentes de las demás áreas. Mientras que los controles que propone la ISO 27002, tienen un mayor grado de detalle, siendo enfocados a la parte de la implementación de dichos controles dentro de la organización. Habiendo dado una mayor luz al enfoque de cada marco y/o norma, se procede a realizar el mapeo correspondiente. Los objetivos organizacionales que propone COBIT 5 y que la organización desea lograr son:

Tabla 13: Cascada de objetivos de negocio según COBIT 5.0

DIMENSIÓN BSC	N°	METAS DE LA ORGANIZACIÓN
Financiero	1	Valor para las partes interesadas de las inversiones del negocio.
Financiero	3	Riesgos de negocio gestionados (Salvaguarda de los activos).
Cliente	6	Cultura de servicios orientada al cliente.
Cliente	7	Continuidad y disponibilidad del servicio.
Cliente	8	Respuesta ágil a los cambios en el entorno empresarial.
Cliente	9	Información basada en toma de decisiones estratégicas.
Interno	11	Optimización de la funcionalidad de los procesos de negocio.
Interno	12	Optimización de los costos de los procesos de negocio.
Interno	14	Productividad de las operaciones y el personal.
Interno	15	Cumplimiento de las políticas internas.
Aprendizaje y Crecimiento	16	Personas preparadas y motivadas.
Aprendizaje y Crecimiento	17	Cultura de innovación de productos y del negocio.

Fuente: IT Governance Institute (2012).*COBIT 5.0*. USA: ISACA, p.49.

A continuación, en la tabla siguiente podemos apreciar la relación de los objetivos de TI requeridos para el logro de los objetivos organizacionales mencionados en la tabla anterior. La lista completa de los objetivos de TI propuestos por COBIT 5 se ubica en el ANEXO 31.

Tabla 14: Mapeo de los objetivos del negocio vs objetivos de TI

ID	OBJETIVOS DE LA EMPRESA	ID TI	OBJETIVOS DE TI
1	Valor para las partes interesadas de las inversiones del negocio.	3	Compromiso de la alta dirección para hacer decisiones relacionadas con TI.
		7	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
		11	Optimización de los activos, recursos y capacidades de TI.
3	Riesgos de negocio gestionados (Salvaguarda de los activos).	4	Gestión de riesgos del negocio relacionados con TI.
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.
		16	Personal del negocio y de las TI competente y motivado.
6	Cultura de servicios orientada al cliente.	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
7	Continuidad y disponibilidad del servicio.	4	Gestión de riesgos del negocio relacionados con TI.
		14	Disponibilidad de información fiable y útil para la toma de decisiones.
11	Optimización de la funcionalidad de los procesos de negocio.	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
		8	Uso adecuado de las aplicaciones, información y soluciones tecnológicas.
		9	Agilidad de TI.
		12	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en los mismos.
14	Productividad de las operaciones y el personal.	8	Uso adecuado de las aplicaciones, información y soluciones tecnológicas.
		16	Personal del negocio y de las TI competente y motivado.
15	Cumplimiento de las políticas internas.	2	Apoyo de TI para el cumplimiento de las leyes y reglamentos externos.
		15	Cumplimiento de TI con las políticas internas.
16	Personas preparadas y motivadas.	16	Personal del negocio y de las TI competente y motivado.
17	Cultura de innovación de productos y del negocio.	9	Agilidad de TI.

Fuente: Aliaga Flores, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima: Pontificia Universidad Católica del Perú, pp.66-68.

Siguiendo con el mapeo, en la siguiente tabla se procede a relacionar los objetivos de TI con los procesos habilitadores que COBIT 5 define. Cabe resaltar que estos procesos habilitadores dan soporte a la realización y logro de dichos objetivos.

Ahora elaboramos la declaración de aplicabilidad (SOA), que es el documento en donde se va a listar los controles a aplicar por cada dominio de la normativa, así como la justificación del porque implementar dichos controles y porque no. Ver el Anexo 17, para apreciar toda la tabla completa, aquí se está apreciando el formato de dicho documento, además nótese que en la tabla del anexo hay controles de la ISO que no están siendo considerados, ya que la empresa cumple con dichos controles, por lo tanto solo se considera las falencias que se tiene y los controles a aplicar para mitigar dichas falencias.

Tabla 15: Plantilla Declaración de Aplicabilidad (SOA)

DECLARACIÓN DE APLICABILIDAD(SOA)			
OBJETIVOS DE CONTROL	**CONTROL**	**APLICABLE**	**JUSTIFICACIÓN**
DOMINIO DE LA NORMATIVA			
CATEGORIA			
ID DEL CONTROL	Descripción de la implementación del control que debe aplicarse	Se puede o no aplicar el control?	Justificación del porqué implementarse el control y porque no de ser el caso.

Fuente: Merino Bada C, (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001*.Madrid: FC editorial, pp.137, 166.

2.3.3. Implantación y Operación

En esta parte ejecutamos los controles planteados, para ello ejecutamos el plan de riesgos planteado líneas más arriba, para efectos de explicar el proceso de Ejecución se tomara como ejemplos dos de los controles planteados en el documento Declaración de Aplicabilidad (SOA) los cuales son considerados de mayor relevancia, empezamos seleccionando los controles referentes a los objetivos de control 5.1.1. Documento de política de seguridad de la información (Ver ANEXO 15) y 7.2.2. Conocimiento, educación y capacitación en seguridad de la información.

Para ello, se debe establecer previamente un plan de capacitación como el que se observa a continuación en el siguiente formato. Ver en el ANEXO 17.

Tabla 16: Programa de formación y capacitación

Cargo o nombre	Conocimientos y habilidades necesarias	Qué capacitación es necesaria
Cargo o nombre de la persona que va a recibir la capacitación.	Fundamentos de seguridad de la información.	Uso adecuado de la información delicada.

Fuente: Elaboración del área de sistemas de SSS

Control 7.2.2. Conocimiento, educación y capacitación en seguridad de la información

Se optó por tomar como ejemplo este control, ya que el problema en sí es generado por el mismo personal, y si no se tiene un plan para capacitarlos y orientarlos, se seguirá teniendo la misma falencia y la situación empeoraría.

Objetivos

Tabla 17: Objetivos por acción para el control 7.2.2

ACCIONES	OBJETIVO	RESPONSABLE
Realizar una charla de seguridad de la información.	Crear conciencia en los colaboradores sobre los riesgos a los que está expuesta la información sensible.	Coordinador de calidad y seguridad.
Realizar la formación del personal.	Capacitar al personal en el uso correcto de la información.	Jefe de sistemas
Desarrollar un decálogo para difundir el correcto tratamiento de la información.	Promover en toda la empresa las buenas prácticas para que el personal haga uso correcto de la información que maneja.	Coordinador de calidad y seguridad y Jefe de sistemas
Evaluar al personal	Verificar que el personal haya entendido la importancia de proteger la información.	Coordinador de calidad y seguridad.

Fuente: Elaboración del área de sistemas de SSS

Planificación de acciones

Tabla 18: Planificación de acciones

OBJETIVOS	ACCIONES	RESPONBASILIDADES (QUIEN?)	RESULTADO ESPERADO
Crear conciencia en los colaboradores sobre los riesgos a los que está expuesta la información sensible.	Realizar una charla de seguridad de la información.	Coordinador de calidad y seguridad.	Que el personal tome conciencia de la importancia de proteger la información como un activo.
Capacitar al personal en el uso correcto de la información.	Realizar la formación del personal.	Jefe de sistemas.	Que el personal esté capacitado para hacer un tratamiento adecuando de la información.
Promover en toda la empresa las buenas prácticas para que el personal haga uso correcto de la información que maneja.	Desarrollar un decálogo para difundir el correcto tratamiento de la información.	Promover en toda la empresa las buenas prácticas para que el personal haga uso correcto de la información que maneja.	Que el personal ponga en práctica lo establecido en dicho decálogo.
Verificar que el personal haya entendido la importancia de proteger la información.	Evaluar al personal.	Coordinador de calidad y seguridad.	Que el personal haya comprendido las lecciones expuestas sobre la seguridad de datos.

Fuente: Elaboración del área de sistemas de SSS

2.3.4. Monitorización y Revisión

Durante esta fase la organización debe ejecutar los procedimientos de monitorización y revisión para:

La detección temprana de errores en los resultados generados en los procesos.

La identificación temprana de las vulnerabilidades y debilidades, así como posibles incidentes de seguridad.

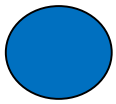
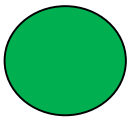
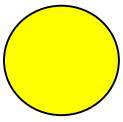
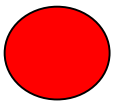
Permitir a la dirección determinar si las actividades desarrolladas por las personas en las que se han delegado las actividades de seguridad se desarrollaron en relación a lo previsto para garantizar la seguridad de la información.

Prevenir y detectar eventos e incidentes de seguridad mediante el uso de indicadores.

Determinar si las acciones realizadas para resolver brechas de seguridad han sido eficientes.

Al igual que en el análisis de brechas realizado al inicio en la etapa de planeación, se hizo un cuadro de estados para describir el nivel de madurez de la empresa, para este caso dicho cuadro de estados va a servir para medir la efectividad de los controles planteados en la etapa de planificación, para lo cual se usara los modelos de madurez de COBIT 5.0, pero estableciendo esta vez rangos, ya que a diferencia de la etapa inicial ahora si se cuenta con resultados obtenidos y no estimados.

Tabla 19: Cuadro de estados para la madurez de los controles

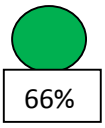
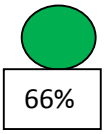
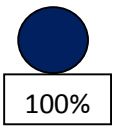
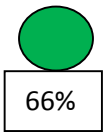
CUADRO DE ESTADOS			
CUADRO DE ESTADOS DE LOS NIVELES DE CAPACIDAD			
REPRESENTACION A COLORES	VALOR DE LA MEDICION	NIVEL	DESCRIPCION
	100%	5: Proceso Optimizado	El proceso predecible del nivel 4 es mejorado continuamente para alcanzar las metas de negocio actuales y futuras.
	[80%-99%>	4: Proceso Predecible	El proceso establecido en el nivel 3 es operado ahora dentro de los límites definidos para alcanzar sus resultados.
	[60%-79%>	3: Proceso Establecido	El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.
	[40%-59%>	2: Proceso Gestionado	El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.
	[20%-39%>	1: Proceso Ejecutado	El proceso implementado alcanza su objetivo.
	[0%-19%>	0: Proceso Incompleto	El proceso no está implantado o no alcanza sus objetivos.

Fuente: IT Governance Institute (2012).*COBIT 5.0*. USA: ISACA, p.42

Ahora se procederá a medir cada uno de los objetivos de cada una de las acciones planteadas para analizar qué tan efectivo fue dicho control.

Medición del control 7.2.2. Conocimiento, educación y capacitación en seguridad de la información

Tabla 20: Medición de la madurez del control 7.2.2.

ACCIONES	OBJETIVO(PRINCIPAL/OPERATIVO)	RESULTADO ESPERADO	NIVEL DE MADUREZ	EVIDENCIAS
Realizar una charla de seguridad de la información	Crear conciencia en los colaboradores sobre los riesgos a los que está expuesta la información sensible.	Que la mayoría del personal tome conciencia de la importancia de proteger la información como un activo.		Reportes estadísticos de la disminución de falencias e incidencias.
Realizar la formación del personal	Capacitar al personal en el uso correcto de la información.	Que el personal esté capacitado para hacer un tratamiento adecuando de la información.		Reportes estadísticos de la disminución de falencias e incidencias.
Desarrollar una decálogo para difundir el correcto tratamiento de la información	Promover en toda la empresa las buenas prácticas para que el personal haga uso correcto de la información que maneja.	Que el personal ponga en práctica lo establecido en dicho decálogo.		Documentación del decálogo/ Reportes estadísticos de la disminución de falencias e incidencias.
Evaluar al personal	Verificar que el personal haya entendido la importancia de proteger la información.	Que el personal haya comprendido las lecciones expuestas sobre la seguridad de datos.		Resultados de las evaluaciones/ Reportes estadísticos de la disminución de falencias e incidencias.

Fuente: Elaboración del área de sistemas de sss

Como se puede apreciar la acción “Evaluar al personal” fue la que resulto con la menor proporción de efectividad, para ello es necesario conocer las falencias de dicha acción, para ello será necesario realizar una auditoría en la oficina centras, en el almacén, así como en todos los puntos de atención.

En el documento informe de auditoría (Ver ANEXO 25) se establece puntos relevantes como criterio, sumilla, etc., esta estructura representa los hallazgos que voy a encontrar al momento de realizar la auditoria e identificar qué aspectos no se corrigieron.

A continuación se procede a realizar los hallazgos:

HALLAZGO 1

Sumilla

Los usuarios de la empresa Systems Support & Services S.A. ubicados en algunos puntos de atención no cumplen la política de seguridad de la información.

Situación

De la información proporcionada a la a comisión de la auditoria y de las visitas realizadas a los responsables de sistemas en otros puntos de atención se han podido identificar que se cuenta con la política de seguridad.

Sin embargo producto de la visita y de la encuesta realizada a las diferentes personas se ha podido identificar un incumplimiento de las políticas de seguridad, esto debido a que algunos miembros del personal de la empresa que labora en dichos puntos no han asistido a las charlas de capacitación.

Criterio

Para dicha debilidad se ha basado en el estándar COBIT 5.0 en el dominio Supervisar, Evaluar y Valorar", en el control "Supervisar, Evaluar y Valorar el Sistema de Control Interno".

Efecto

Información de la empresa y/o clientes expuesta a personas no autorizadas.

Causa

Dicha deficiencia es generada por los responsables de Sistemas por no asistir a las capacitaciones concienciación en la organización, por ende no se tiene conciencia de las consecuencias que se puede causar.

Recomendación

Asignar a un personal encargado de supervisar el manejo de la información delicada en cada punto de atención, so

meter a capacitación a los colaboradores que no hayan asistido y aplicarles las sanciones correspondientes en caso reincidan.

Además se deberá configurar la red de tal manera que se pueda evitar el acceso a sitios indebidos.

Conclusión

Para evitar una manipulación inadecuada de los datos es necesario tener un control diario del manejo de información en cada punto de atención.

HALLAZGO 2

Sumilla

Systems Support & Services S.A. no cuentan con controles adecuados para el acceso a áreas restringidas y la pérdida de objetos.

Situación

De la información proporcionada a la a comisión de la auditoria y de sucesos imprevistos ocurridos en la empresa se han podido identificar que los colaboradores, especialmente el personal nuevo, no cuenta con un carnet de identificación, así como un control para poder restringir su acceso a áreas a las que no pertenecen, así como la falta de cámaras de seguridad en puntos clave.

Criterio

Para dicha debilidad se ha basado en el estándar COBIT 5.0 en el dominio Supervisar, Evaluar y Valorar", en el control "Supervisar, Evaluar y Valorar el Sistema de Control Interno".

Efecto

Los activos tecnológicos están expuestos a caer en manos no autorizadas para un fin indebido.

Causa

Dicha deficiencia es generada por la materialización de este tipo de riesgos.

Recomendación

Asignar a todo el personal un carnet de identificación, así sean conocidos, así como asignar a cada entrada de un área un dispositivo con el cual el usuario del carnet pueda pasar la tarjeta para autentificarse y tener acceso al área a la que pertenece, en caso contrario que le sea negado el acceso.

Además se deberá instalar cámaras en puntos clave como en los pasillos.

Conclusión

Para evitar la pérdida de objetos y el acceso no autorizado a áreas restringidas se debe implementar controles más eficientes en el interior de la organización.

HALLAZGO 3

Sumilla

Systems Support & Services no cuentan con controles criptográficos para la protección de los datos que se transmiten.

Situación

De la información proporcionada a la a comisión de la auditoria se puedo identificar que no se cuenta con controles criptográficos para la protección de la data que se transmite.

Criterio

Para dicha debilidad se ha basado en el estándar COBIT 5.0 en el dominio Supervisar, Evaluar y Valorar", en el control "Supervisar, Evaluar y Valorar el Sistema de Control Interno" y la normativa ISO/IEC 27001: 2013 el dominio "Criptografía", en el control "Controles Criptográficos".

Efecto

La información confidencial está expuesta a ser interceptada por alguna persona externa al área de origen de dicha información y usarla para un fin indebido.

Causa

Dicha deficiencia se debe a que el área de sistemas no considera necesario el uso de los controles criptográficos.

Recomendación

Se debe evaluar el uso de los controles criptográficos al menos para las áreas de finanzas y administración que son las áreas que manejan información relacionada a facturas y reportes financieros.

Conclusión

Para evitar la pérdida de información delicada de sebe evaluar el uso de la criptografía como una alternativa de solución.

2.3.5. Mantenimiento y Mejora

Una vez identificada las disconformidades en la fase anterior, se procederá a aplicar las medidas preventivas y correctivas a fin de garantizar que dichas anomalías no se repitan. Ver ANEXO 26 Registro de Disconformidades y ANEXO 27 Procedimiento de Acciones Correctivas y Preventivas para tener mayor detalle sobre esta actividad realizada.

2.3.6. Culminación del Proyecto

En esta etapa se va a entregar y exponer el producto a fin de que el público objetivo se sienta convencido de la importancia y beneficios que traerá este proyecto.

Una vez que el proyecto haya sido evaluado y aprobado, recién se dará por concluido y se formalizará el acta de cierre del proyecto.

CAPÍTULO III
PRUEBAS Y RESULTADOS

3.1. Pruebas

Para ello se realizó un informe estadístico de las antes y después, en otras palabras, se pretende comparar por medio del análisis estadístico cual era la situación de la empresa antes de desarrollar este proyecto y después de haber implantado dicho proyecto. Para ello se va a realizar otro análisis de brecha para compararlo con el análisis de brecha inicial y a través de los niveles de madurez se podrá medir que tan eficientes fueron los controles implantados.

Previamente se podrá apreciar en la Tabla 21 las pruebas que sustentan los resultados obtenidos en este proyecto.

Tabla 21: Pruebas del análisis realizado

CONTROLES	NIVEL DE CUMPLIMIENTO 1	NIVEL DE CUMPLIMIENTO 2
POLITICAS DE SEGURIDAD	20%	72%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	20%	100%
GESTION DE ACTIVOS	0%	68%
CONTROL DE ACCESO	20%	75%
CRIPTOGRAFIA	0%	0%
SEGURIDAD AMBIENTAL	0%	0%
SEGURIDAD DE RRHH	0%	67%
OPERACIONES EN SEGURIDAD	0%	100%
RESULTADO FINAL	20%	80%

Fuente: Elaboración propia

3.2. Resultados

El siguiente cuadro se puede apreciar la comparación, un análisis de brecha inicial y uno final, para analizar cuáles fueron las mejoras, y como se observa, hubo una considerable mejora respecto a lo que se analizó al inicio, además se muestra el grado de cumplimiento sobre los objetivos.

Tabla 22: Objetivos vs Resultados

OBJETIVOS	INDICADORES (%)	FORMULA	META
Identificar amenazas y vulnerabilidades existentes en la empresa.	Amenazas y vulnerabilidades identificadas	Matriz de riesgos	100%
Realizar un análisis de riesgos de los activos de la empresa.	Riesgos identificados/Activo	Matriz de riesgos	100%
Mapear los riesgos de activos.	Riesgos mapeados	Mapa de riesgos	100%
Asignar controles asociados a los riesgos identificados.	Controles de riesgos	Declaración de Aplicabilidad(SOA)	100%
Validar que la efectividad de controles de la seguridad de la información funcionen a un 70%.	Efectividad Esperada	Sum(Efectividad de controles relacionados)/TotalControles	80%
Concientizar al 70% del personal de la empresa sobre los riesgos a los que están expuestos los activos.	Porcentaje del personal que cumple con la norma	Personal que cumplen normas/TotalPersonas	67%

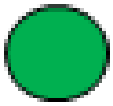
Fuente: Elaboración propia

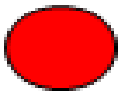
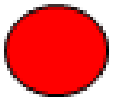
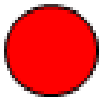
3.3. Desarrollo del GAP Analysis Post

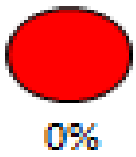
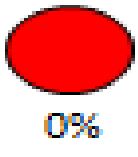
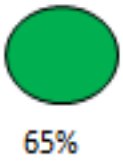
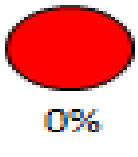
A continuación se aprecia el análisis de brecha pos, como se recordara al inicio del proyecto se hizo un análisis de brecha al cual denominamos análisis de brechas pre para saber cuál era la situación actual de la empresa en lo que respecta a seguridad de la información, una vez hecho el proceso descrito en los capítulos anteriores y realizada la auditoria se procede a realizar nuevamente un análisis de brecha pos con el cual se puede determinar la situación actual de la empresa una vez realizadas las acciones descritas al inicio, para tener una mejor comprensión se hace una comparación con entre el análisis pre y el post para ver el antes y el después y en base a ello apreciar

los resultados obtenidos, que en este caso representan una mejoría de lo que se encontró al inicio.

Tabla 23: GAP Análisis Post

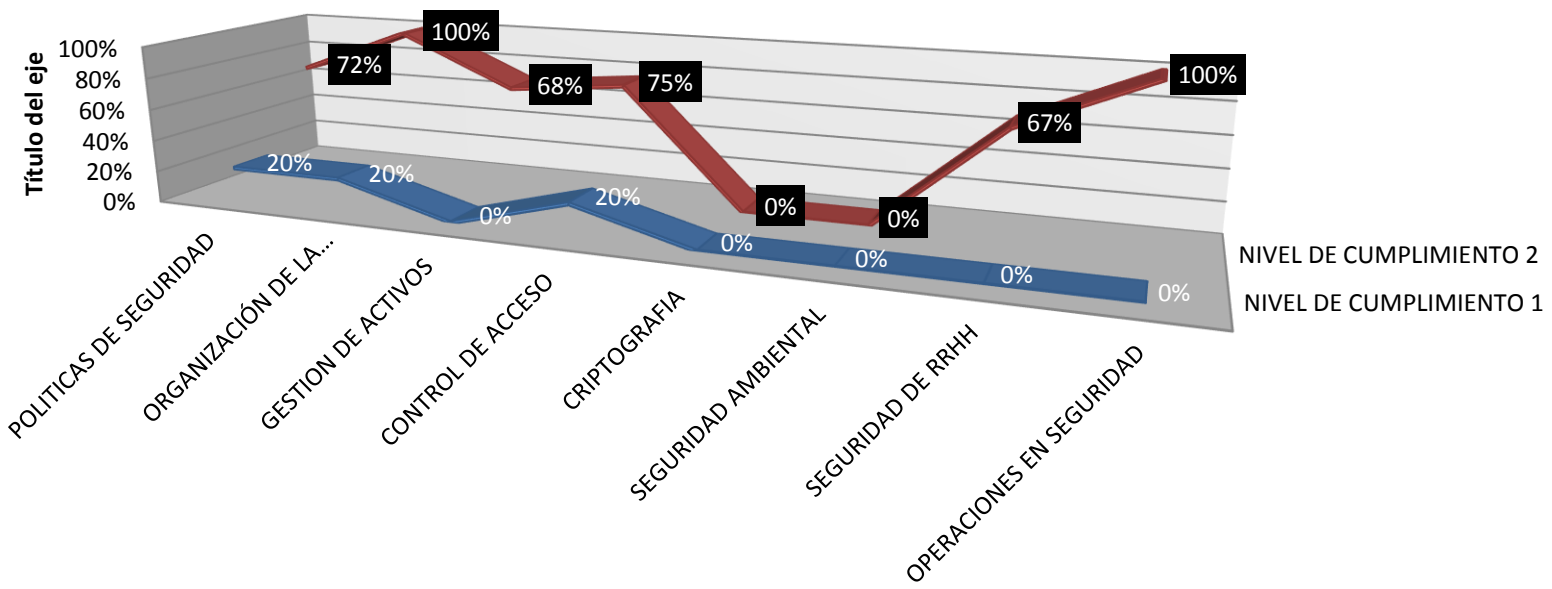
SITUACION ACTUAL	CONTROL	ANALISIS DE BRECHA PRE	NIVEL DE CUMPLIMIENTO 1	NIVEL DE CUMPLIMIENTO 2
5. POLITICAS DE SEGURIDAD				
La empresa SSS				
1. Tiene definidas sus políticas, pero no se encuentran documentadas ni formalizadas.		1. Debe crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad. Los documentos de política de seguridad de información debieran ser aprobados por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.		
2. No aplican las mismas políticas en todas las sedes.		2. Debe revisar las políticas de seguridad a fin de mantener todas las sedes o puntos de atención custodiados de igual manera como la central.	20%	72%
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION				
La empresa SSS				
1. Se tiene establecida, ni documentada ninguna política de divulgación y autorización de la información, mas no documentada.		1. Debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento.		
			20%	100%

7. GESTION DE ACTIVOS			
La empresa SSS			
1. No cuenta con un proceso para etiquetar sus activos.	1. Debe desarrollar en implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	 0%	 68%
8. CONTROL DE ACCESO			
La empresa SSS			
1. No se cuenta con una política de escritorio limpio.	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	 20%	 75%
10. CRIPROGRAFIA			
La empresa SSS			
1. No cuenta con una política para el uso de criptografía.	1. Debe desarrollar e implementar una política sobre el uso de controles criptográficos, para la protección de la información.	 0%	 0%

11. SEGURIDAD FISICA Y AMBIENTAL			
La empresa SSS			
1. No cuenta con alarmas para la detección de intrusos, ni con un PIN para controlar el acceso a personas no autorizadas a áreas restringidas.	1. Se debe proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.		
12.SEGURIDAD EN R.R.H.H.			
La empresa SSS			
1. No realiza una constante actualización y capacitación a los empleados en seguridad de la información de acuerdo a las políticas ya establecidas.	1. Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.		
13.OPERACIONES DE SEGURIDAD			
La empresa SSS			
1. No se usa alguna bitácora para el registro de fallas de tal manera que se identifiquen problemas con los sistemas de información.	1. Registro de fallas Las fallas se deben de registrar, analizar y se debe tomar una acción apropiada.		

Fuente: Elaboración propia

A continuación se aprecia el mismo análisis pero representado por un gráfico estadístico.



	POLITICAS DE SEGURIDAD	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	GESTION DE ACTIVOS	CONTROL DE ACCESO	CRIPTOGRAFIA	SEGURIDAD AMBIENTAL	SEGURIDAD DE RRHH	OPERACIONES EN SEGURIDAD
NIVEL DE CUMPLIMIENTO 1	20%	20%	0%	20%	0%	0%	0%	0%
NIVEL DE CUMPLIMIENTO 2	72%	100%	68%	75%	0%	0%	67%	100%

Figura 6: Reporte Estadístico de niveles Fuente: elaboración propia

Esta figura nos muestra que en un mes de haber implantado ,los controles los controles, se alcanzó una mejora, la línea azul representa el antes , mientras que la celeste el después, los números del 1 al 8 representan los controles establecidos según el dominio de la ISO, por ejemplo obsérvese que en el dominio 1 antes se tenía un 20%, ahora se tiene un 72 %, esto indica que se mejoró, ya que ahora las políticas son revisadas y documentadas correctamente, en el 7 el 67% representa la efectividad del control de capacitación de empleados, el cual no se tenía al inicio de este proyecto.

Otra manera de representar las evidencias es por medio de la figura 7: Grafico de barras de los niveles alcanzados, el cual se aprecia en la siguiente página. Además, de las figuras 8, 9 y 10 de las siguientes paginas

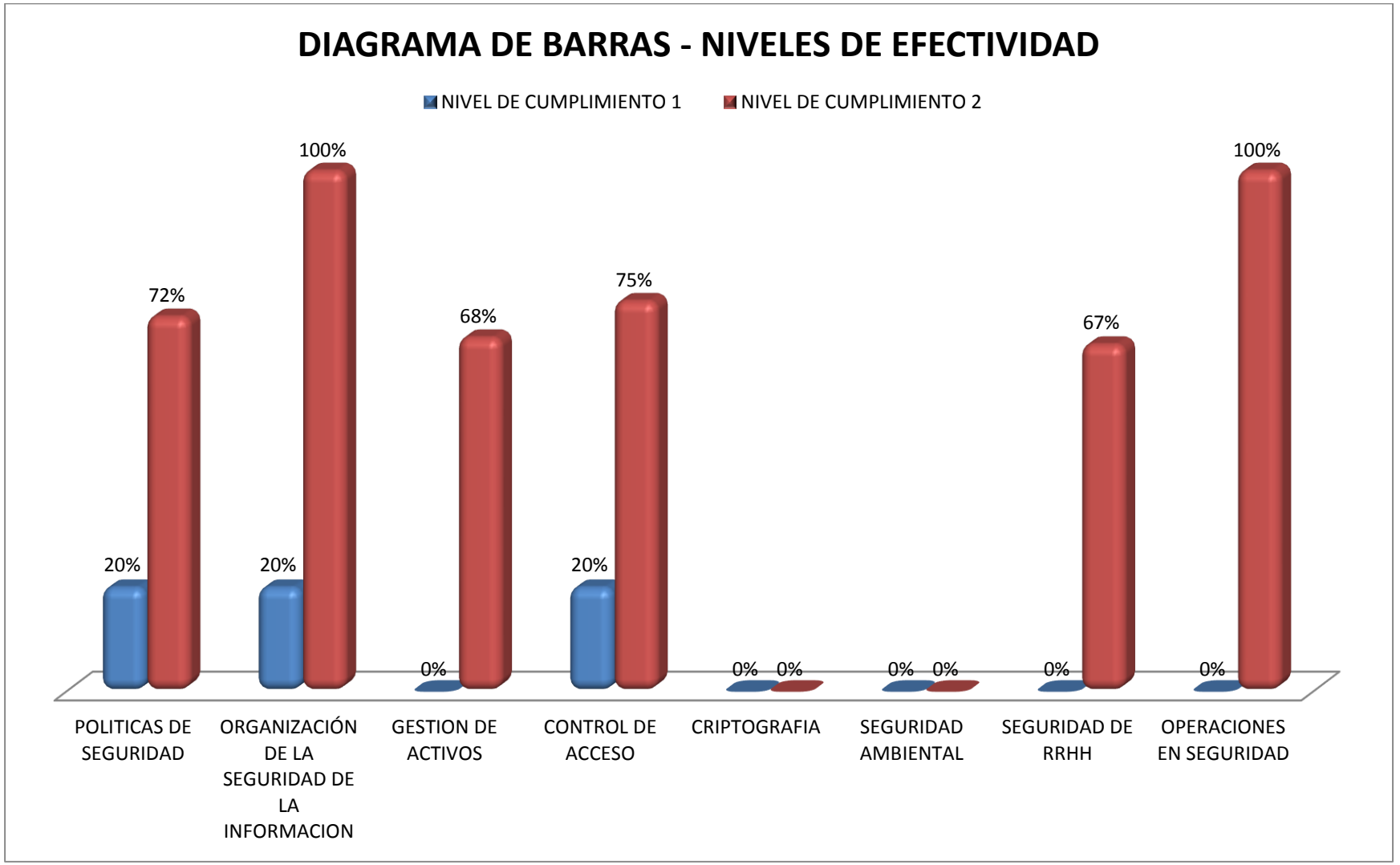


Figura 7: Gráfico de barras de los niveles efectividad de los controles **Fuente**: elaboración propia.

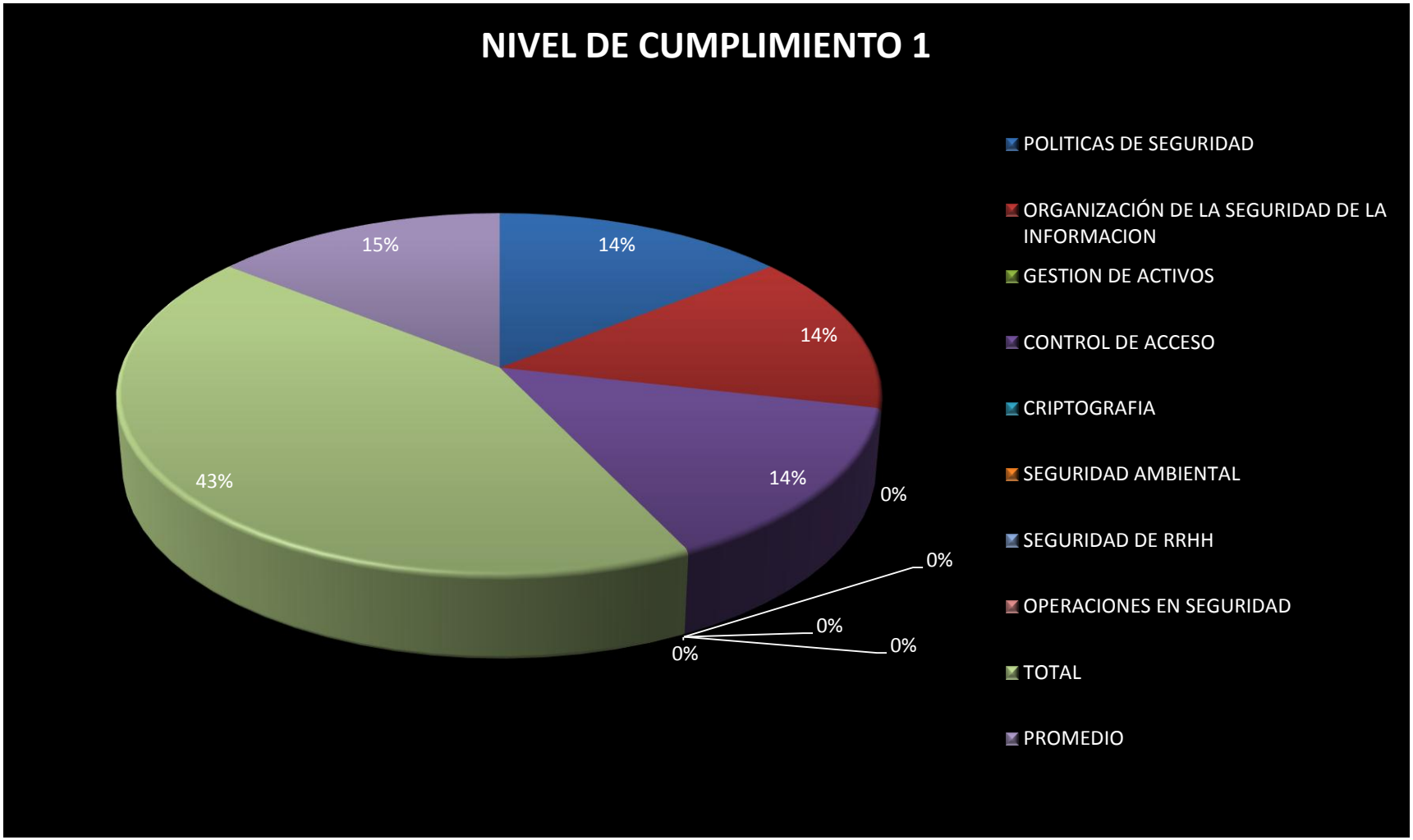


Figura 8: Gráfico de pastel de los niveles efectividad de los controles 1 **Fuente:** elaboración propia.

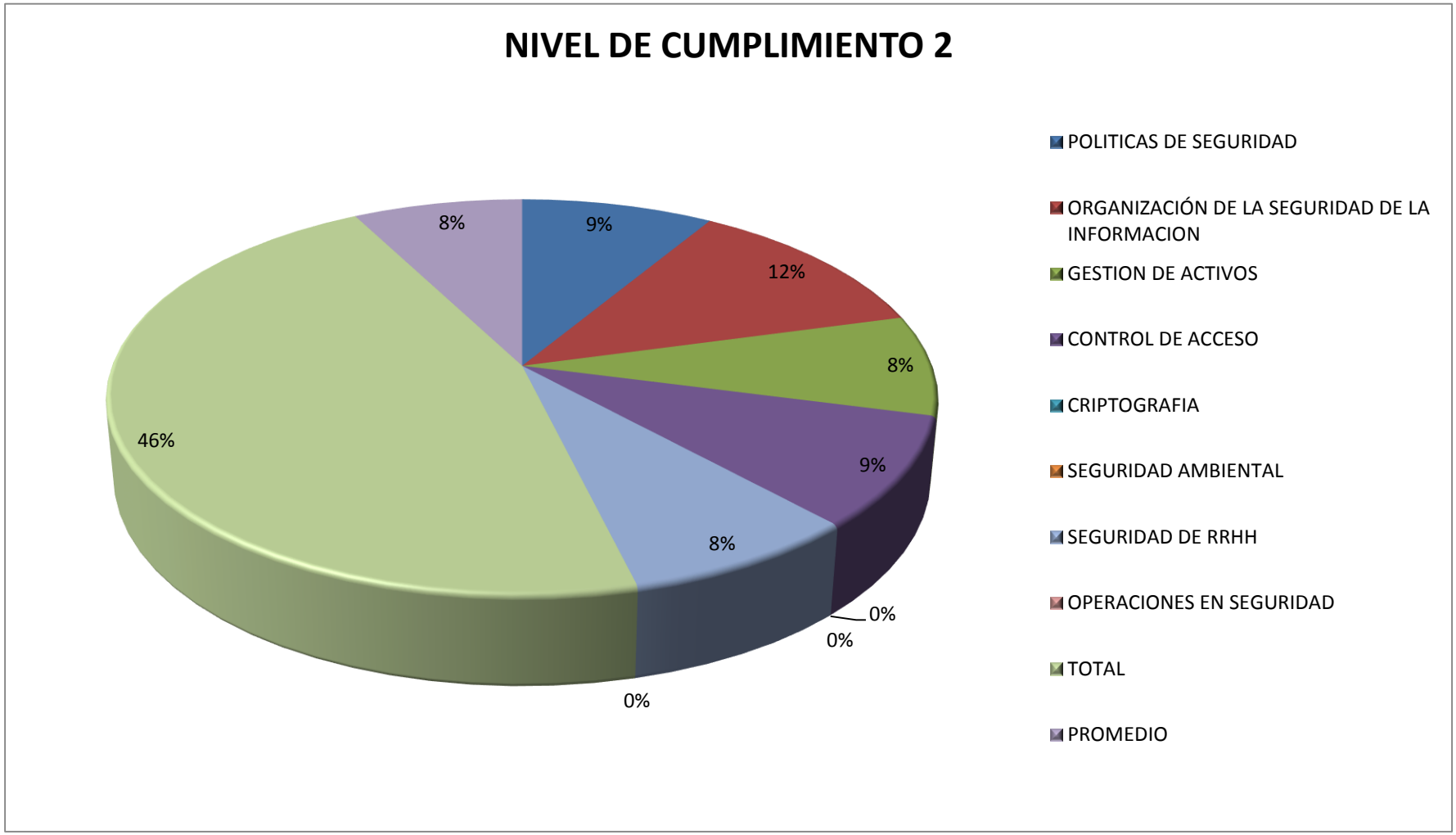


Figura 9: Gráfico de pastel de los niveles efectividad de los controles 2 **Fuente:** elaboración propia.

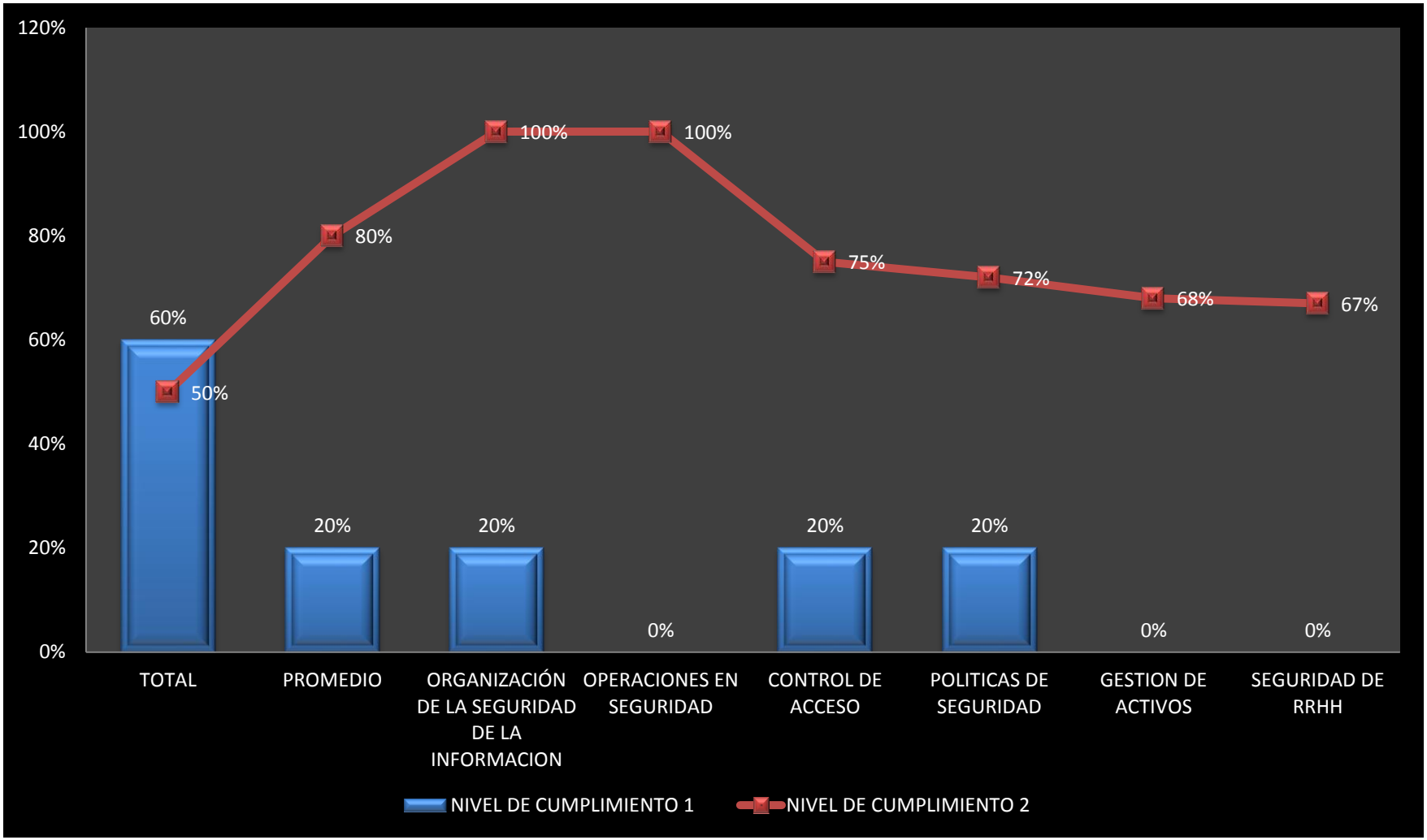


Figura 10: Diagrama de Pareto de los niveles de efectividad de los controles **Fuente**: elaboración propia.

CAPÍTULO IV
DISCUSIÓN Y APLICACIÓN

4.1. Discusiones

Del estudio realizado se pudo observar que la empresa, no contaba con controles adecuados para monitorear sus políticas, las cuales no estaban documentadas, así mismo su personal no tenía conciencia de la importancia de hacer un tratamiento adecuado de la información sensible.

Por medio de un reporte estadístico se puede analizar el antes y el después, con el cual se puede apreciar que actualmente la empresa ha mostrado una mejoría con respecto a los puntos tratados, por ejemplo, en lo que es entrenamiento de personal de la empresa ha mostrado una mejoría del 69.5% contra un 0%, de lo que se puede interpretar que un poco más de la mitad del personal de la empresa ha entendido la importancia de la seguridad de datos, así como el 100% de las políticas de seguridad documentadas contra el 20% inicial, que significa que ahora no solo las políticas están documentadas, sino que ahora incluso se monitorea para asegurar que se cumplan con dicha normativa.

Además, cabe resaltar que gracias a este trabajo, se pudo evitar que se pierdan datos relevantes, lo cual hubiera generado una tremenda pérdida para la empresa, tanto a nivel económico como a nivel institucional.

4.2. Aplicaciones

Conociendo los resultados obtenidos en esta primera instancia, se proyecta aplicar este proyecto a todos los puntos de atención, de tal manera que se pueda asegurar la integridad, disponibilidad y confiabilidad de la información que se maneja cada una de estas sedes en mención, así como los activos.

Además, se planea reforzar los controles que fueron efectivos pero que tuvieron un menor porcentaje de efectividad de tal manera que a futuro sean más eficientes.

CONCLUSIONES

1. Se pudo identificar los activos con los que cuenta la empresa, así como los niveles de riesgo a los que están expuestos aplicando las normativas de ISO 27001:2013.
2. Del análisis realizado se puede concluir que si bien es cierto la empresa no mostro un nivel crítico de riesgos y vulnerabilidades, pero si mostro falencias en torno a la seguridad de la información.
3. Se mapearon los riesgos, lo cual permitió determinar los niveles críticos de los activos antes de realizar la declaración de aplicabilidad (SOA).
4. Se identificó los controles asociados a los riesgos identificados previamente, estos controles son los que permitieron reducir los niveles de riesgo.
5. Con el cuadro de estados del nivel de madurez se validó que estos controles fueron efectivos, ya que al inicio no habían procesos implementados y si los habían no estaban documentados o no se realizaban con frecuencia.
6. Se pudo concientizar a la mayoría del personal y ellos comprendieron lo que la seguridad de la información es responsabilidad de todos los trabajadores de la empresa.

RECOMENDACIONES

1. Mantener una constante revisión y actualización de las políticas del SGSI y controlar constantemente el cumplimiento de estas.
2. Implementarlos controles faltantes de tal manera que se garantice un nivel superior de seguridad de la información.
3. Evaluar constantemente al personal de tal manera que se garantice el correcto uso de los recursos tecnológicos y de la información delicada.
4. Implementar los controles establecidos en todos los centros de atención a fin de garantizar que todos los colaboradores de la empresa sigan las políticas establecidas.
5. Designar a un personal que se encargue del monitoreo constante en los puntos de atención.

FUENTES DE INFORMACIÓN

Aliaga, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo*. Lima, Perú: Pontificia Universidad Católica del Perú.

Areito, J. (2008). *Seguridad de la Información. Redes, informática y sistemas de información*. Madrid, España: Paraninfo.

Godoy, C.(2011). *Historia de la seguridad de la información.* Recuperado de http://es.scribd.com/doc/59484913/Historia-de-La-Seguridad-a

Gutiérrez, C (2013). *ISO/IEC 27002 cambios-dominios-control*. Recuperado de http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control

Gutiérrez, C (2013). *Nueva estructura de la ISO 27001:2013, ESET*. Recuperado de http://www.welivesecurity.com/la-es/2013/10/18/renovados-anexos-iso-iec-27001-2013/

IT Governance Institute (2009).*RISK IT BASADO EN COBIT. USA: ISACA*.

IT – Governance, Risk & Compliance. (2010). *El blog de Franco sobre IT – GRC con visión de Negocio*. Recuperado de http://francoitgrc.wordpress.com/2012/01/23/pmbok-4-cobit-5-dos-potencias-se-saludan/

IT – Governance, Risk & Compliance. (2012). *El blog de Franco sobre IT – GRC con visión de Negocio*. Recuperado de

http://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/

IT – Governance, Risk & Compliance. (2012). *El blog de Franco sobre IT – GRC con visión de Negocio*. Recuperado de http://www.crisoltic.com/2012/04/cobit-5-que-hay-de-nuevo.html

Lahuara, E. (2007). *Metodología para desarrollar un plan de Seguridad de Información*. Lima, Perú: Universidad San Martin de Porres. Tesis para obtener el título de ingeniero de computación y sistemas.

Montenegro, L. (2014*). Seguridad de la Información: Más que una actitud*, un estilo de vida. Recuperado de http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

Muñoz, C. (1998). *Como Elaborar y Asesorar una Investigación de Tesis.* México: Prentice Hall.

Página web de la empresa *Systems Support & Servicies S.A.* (2008). *Systems Support & Services S.A.* Recuperado de http://www.sss.com.pe/historia

Ramírez, R. (2010). *Proyecto de investigación*. Lima-Perú: Universidad Mayor de San Marcos.

Sánchez, A. (2010). *Normativa e inducción en seguridad de información para el grupo telefónica.* Lima: Universidad San Martin de Porres. Tesis para obtener el título de ingeniero de computación y sistemas.

Tokeshi, A. (2008*). Planifique, desarrolle y apruebe su tesis: Guía para mejores resultados*. Lima-Perú: Universidad de Lima.

Web Site *GConsulting Compliance* (s.f). Recuperado de: http://www.gconsultingcompliance.com/producto

ANEXOS

ANEXO 1
PROJECT CHARTER

<table>
<tr><td colspan="5">Acta de constitución del proyecto</td></tr>
<tr><td colspan="5">A. Información General</td></tr>
<tr><td>Nombre del Proyecto:</td><td colspan="2">APLICACIÓN DE NORMATIVAS DE SEGURIDAD DE INFORMACION PARA SYSTEMS SUPPORT & SERVICES S.A.</td><td>Fecha de Preparación:</td><td>08/03/2014</td></tr>
<tr><td>Preparado por:</td><td>Mauro Luis Vento Meza</td><td>Autorizado por:</td><td colspan="2">Gerencia de Soluciones de Infraestructura</td></tr>
<tr><td colspan="5">B. Necesidad del Proyecto</td></tr>
<tr><td colspan="5">• Optimizar la gestión de seguridad de datos en toda la organización.</td></tr>
<tr><td colspan="5">C. Objetivos del Proyecto</td></tr>
<tr><td colspan="5">• Identificar amenazas y vulnerabilidades existentes en la empresa.
• Realizar un análisis de riesgos de los activos de la empresa.
• Mapear los riesgos de activos.
• Asignar controles asociados a los riesgos identificados.
• Validar la efectividad de controles de la seguridad de información.
• Concientizar al personal de la empresa sobre los riesgos a los que están expuestos los activos.</td></tr>
<tr><td colspan="5">D. Alcance del Proyecto</td></tr>
<tr><td colspan="5">• Definir el área de trabajo y realizar la planeación del proyecto.
•Realizar un levantamiento de información
• Identificar y analizar los riesgos y vulnerabilidades existentes.
• Aplicar controles de riesgos y validarlos.
• Realizar el entrenamiento y concientización del personal de la empresa.</td></tr>
</table>

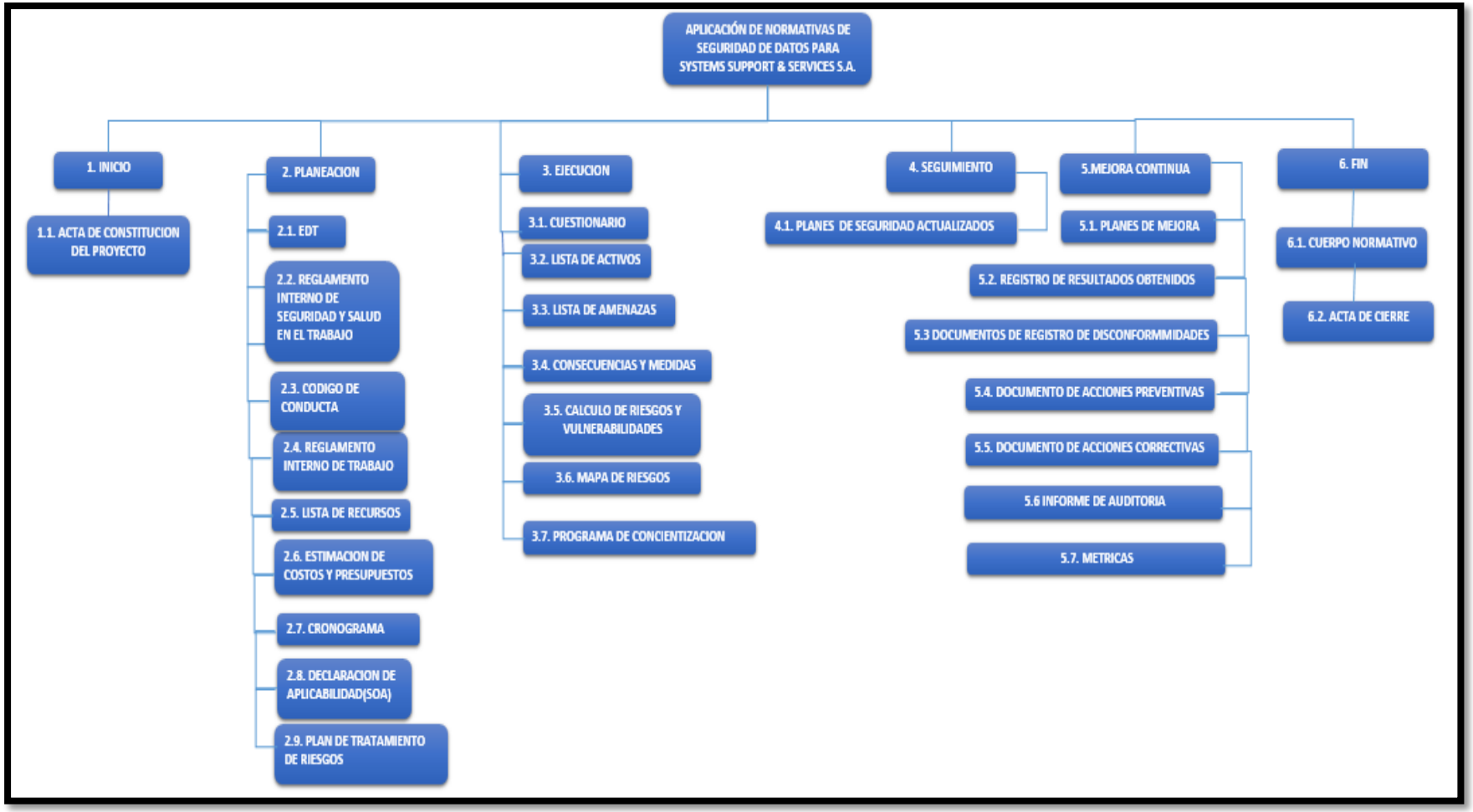
ANEXO 2
ALCANCE

LCANDE DEL PROYECTO

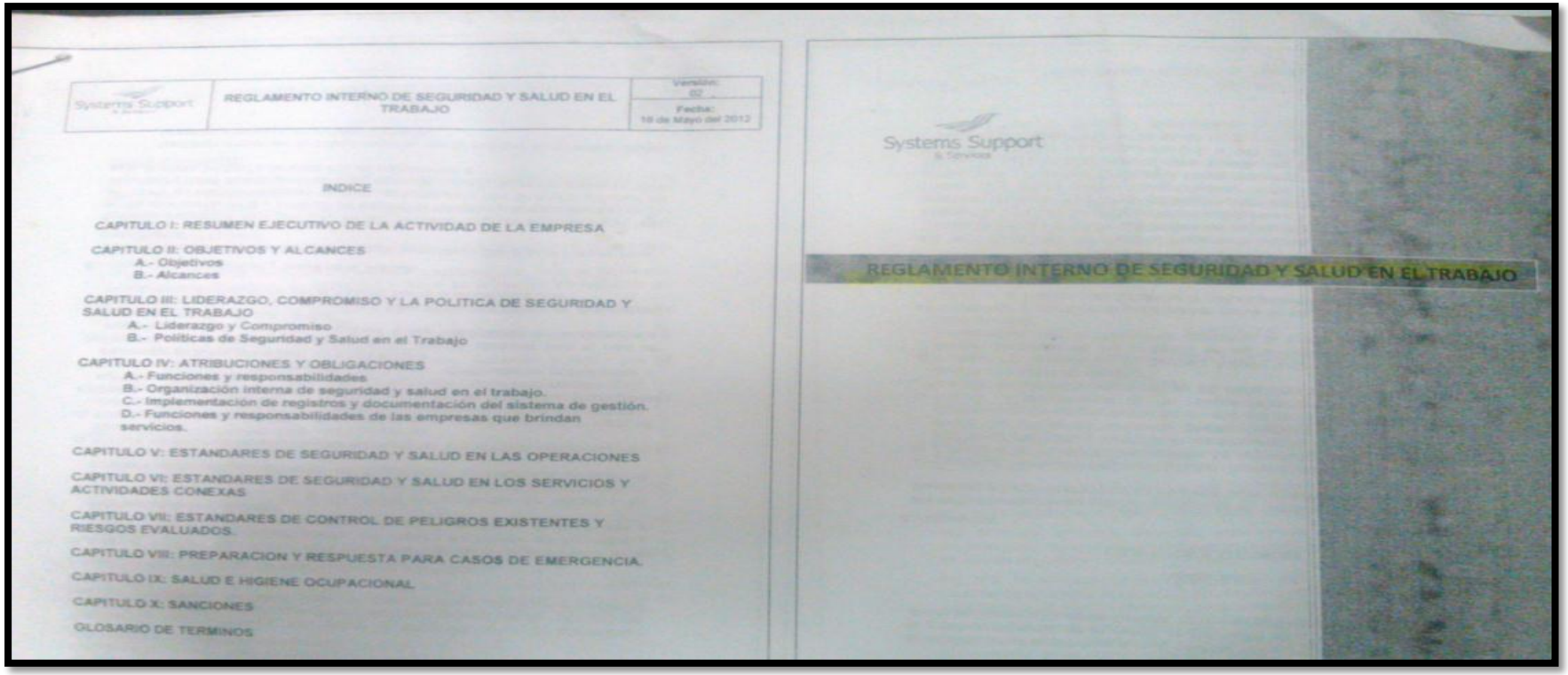
NOMBRE DEL PROYECTO
APLICACIÓN DE NORMATIVAS DE SEGURIDAD DE LA INFORMACION PARA SYSTEMS SUPPORT & SERVICES S.A.
JUSTIFICACION DEL PROYECTO
JUSTIFICACIÓN TEORICA Reforzar los conocimientos adquiridos en la parte teórica referido a lo que es seguridad de la información. **JUSTIFICACIÓN PRACTICA** Plasmar toda la teoría adquirida en una situación real. **JUSTIFICACIÓN TECNOLOGICA** Aplicar normativas a fin de proteger los recursos tecnológicos y asegurar el mantenimiento preventivo y correctivo a nivel de recursos de TI. **JUSTIFICACIÓN ECONOMICA** Evitar la suspensión del servicio pérdida de clientes e ingresos.
DESCRIPCIÓN DEL PRODUCTO
Implantación de un sistema de gestión de seguridad de la información , basado en la ISO 27001: 2013 y COBIT 5.0
ENTREGABLES DEL PROYECTO
Los entregables del proyecto son especificados en la estructura de Desglose (EDT), ver ANEXO 3.

ALCANCE
La investigación se ejecutara en la empresa Systems Support & Services S.A., siendo el área de sistemas la principal área de estudio en donde se tendrá la mayor parte del enfoque, además se realizara un breve análisis en otras áreas como por ejemplo el almacén de la empresa y los puntos de atención.
FUERA DEL ALCANCE El resto de las áreas como ventas, operaciones, proyectos, soluciones de software, administración y logística, contabilidad y finanzas y R.R.H.H.
El resto de las áreas como ventas, operaciones, proyectos, soluciones de software, administración y logística, contabilidad y finanzas y R.R.H.H. **ORGANIZACIÓN DEL PROYECTO**
• Gerente de soluciones de infraestructura. • Gerente de proyectos. • Jefe de proyectos. • Jefe de proyectos. • Coordinador de seguridad y calidad. • Analista.
• Gerente de soluciones de infraestructura. • Gerente de proyectos. • Jefe de proyectos. • Jefe de proyectos. • Coordinador de seguridad y calidad. • Analista. **OBJETIVO DEL CRONOGRAMA**
• Fecha Inicio: 10/03/2014 • Fecha de culminación: 04/07/2014 • Cumplir con las fechas establecidas. • Proporcionar una estructura de desarrollo del proyecto.

ANEXO 3
ESTRUCTURA DE DESGLOSE DE TRABAJO



ANEXO 4
REGLAMENTO INTERNO DE SEGURIDAD Y SALUD EN EL TRABAJO



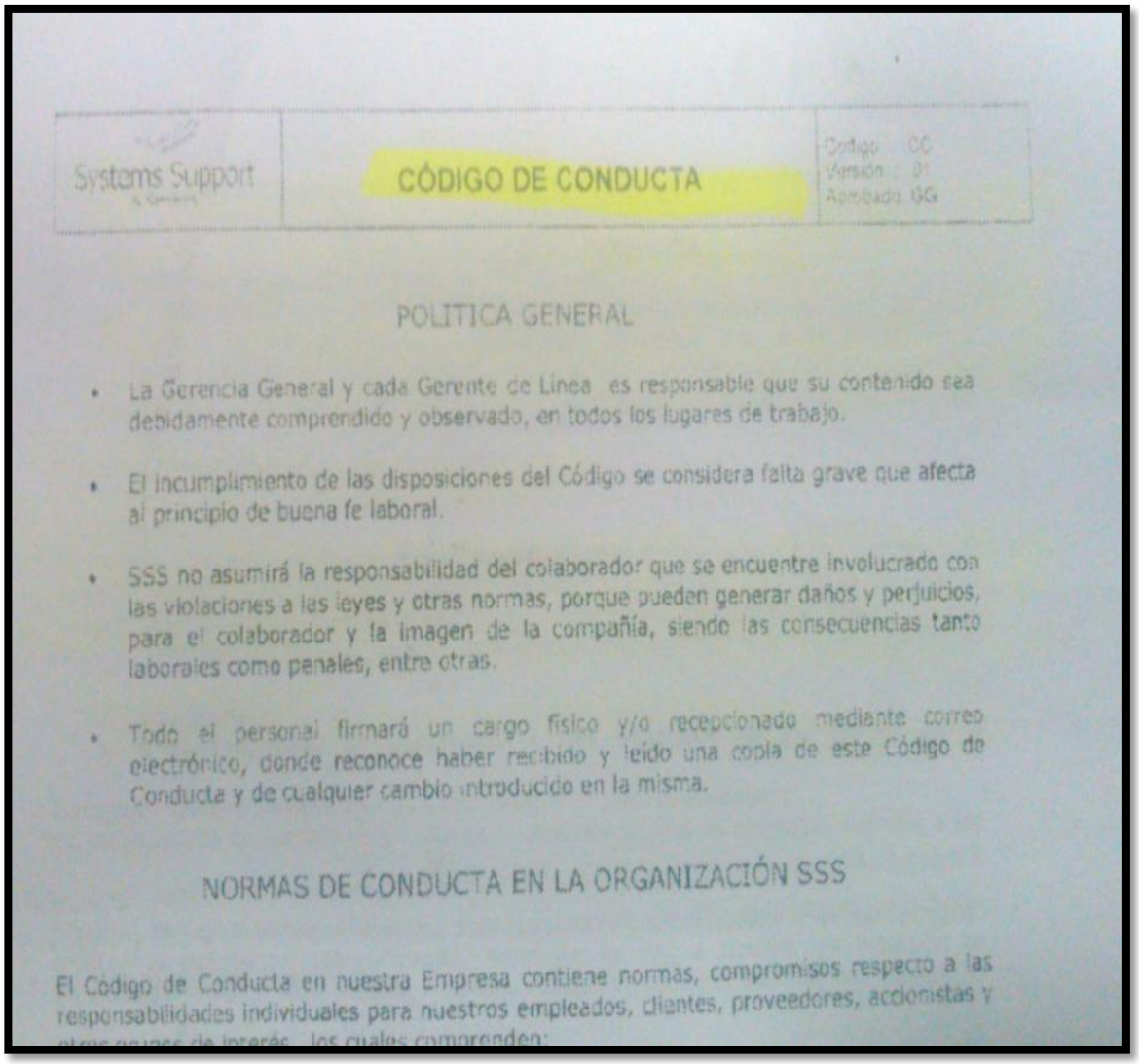
Systems Support | REGLAMENTO INTERNO DE SEGURIDAD Y SALUD EN EL TRABAJO | Versión: 02 | Fecha: 18 de Mayo del 2012

INDICE

Systems Support

REGLAMENTO INTERNO DE SEGURIDAD Y SALUD EN EL TRABAJO

ANEXO 5
CÓDIGO DE CONDUCTA



Systems Support

CÓDIGO DE CONDUCTA

Código CC
Versión 01
Aprobado GG

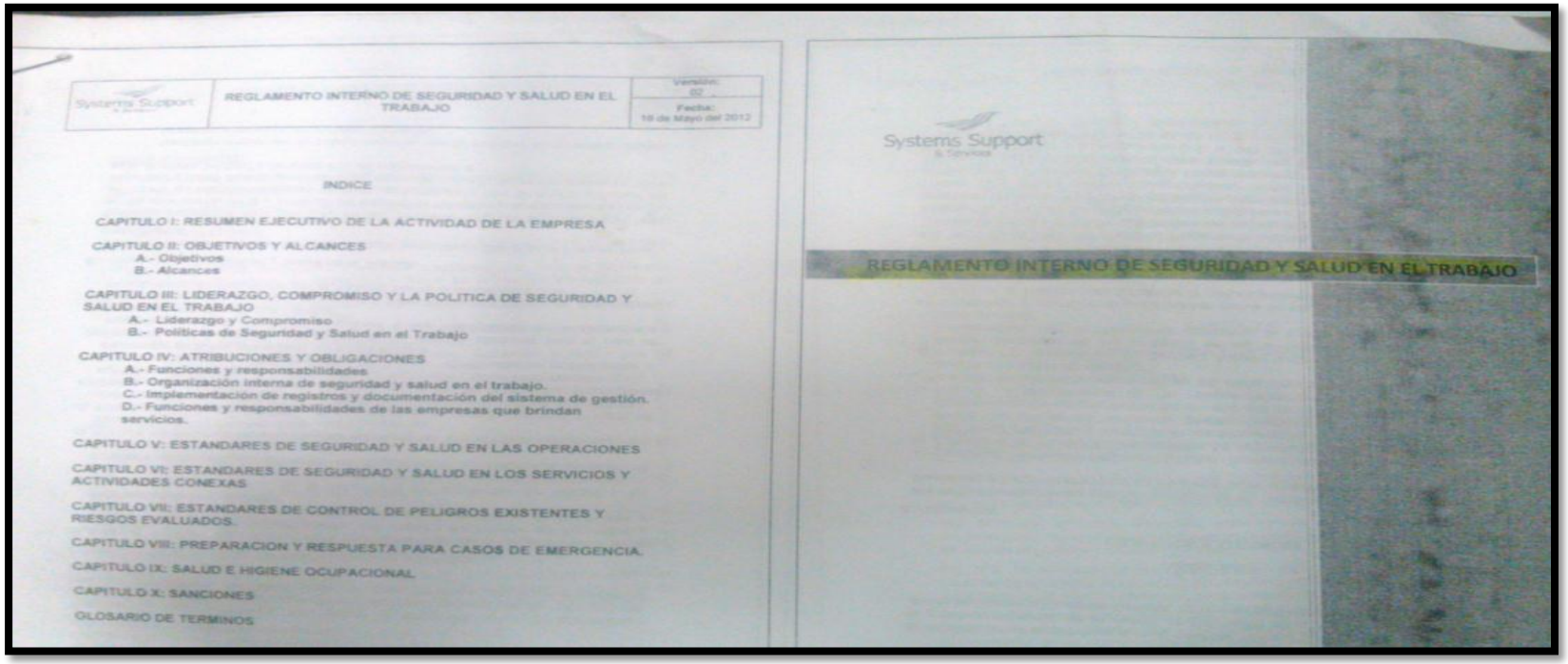
POLITICA GENERAL

- La Gerencia General y cada Gerente de Linea es responsable que su contenido sea debidamente comprendido y observado, en todos los lugares de trabajo.
- El incumplimiento de las disposiciones del Código se considera falta grave que afecta al principio de buena fe laboral.
- SSS no asumirá la responsabilidad del colaborador que se encuentre involucrado con las violaciones a las leyes y otras normas, porque pueden generar daños y perjuicios, para el colaborador y la imagen de la compañía, siendo las consecuencias tanto laborales como penales, entre otras.
- Todo el personal firmará un cargo físico y/o recepcionado mediante correo electrónico, donde reconoce haber recibido y leído una copia de este Código de Conducta y de cualquier cambio introducido en la misma.

NORMAS DE CONDUCTA EN LA ORGANIZACIÓN SSS

El Código de Conducta en nuestra Empresa contiene normas, compromisos respecto a las responsabilidades individuales para nuestros empleados, clientes, proveedores, accionistas y otros grupos de interés, los cuales comprenden:

ANEXO 6
REGLAMENTO INTERNO DE TRABAJO



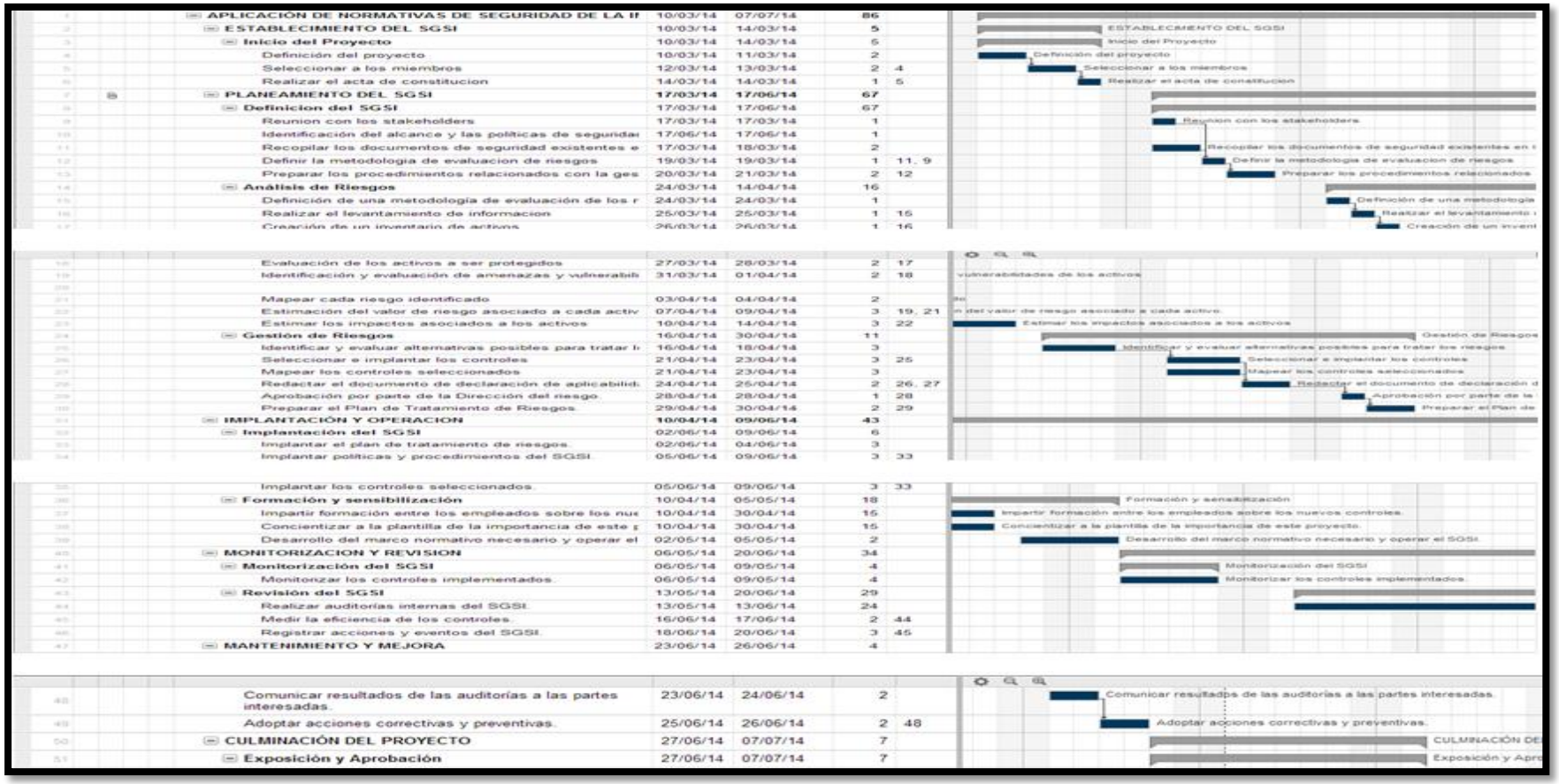
Systems Support | REGLAMENTO INTERNO DE SEGURIDAD Y SALUD EN EL TRABAJO | Versión: 02 | Fecha: 18 de Mayo del 2012

INDICE

Systems Support

REGLAMENTO INTERNO DE SEGURIDAD Y SALUD EN EL TRABAJO

ANEXO 7
CRONOGRAMA DEL PROYECTO



1		APLICACIÓN DE NORMATIVAS DE SEGURIDAD DE LA IF	10/03/14	07/07/14	86	
2		ESTABLECIMIENTO DEL SGSI	10/03/14	14/03/14	5	
3		Inicio del Proyecto	10/03/14	14/03/14	5	
4		Definición del proyecto	10/03/14	11/03/14	2	
5		Seleccionar a los miembros	12/03/14	13/03/14	2	4
6		Realizar el acta de constitucion	14/03/14	14/03/14	1	5
7		PLANEAMIENTO DEL SGSI	17/03/14	17/06/14	67	
8		Definicion del SGSI	17/03/14	17/06/14	67	
9		Reunion con los stakeholders	17/03/14	17/03/14	1	
10		Identificación del alcance y las políticas de seguridad	17/06/14	17/06/14	1	
11		Recopilar los documentos de seguridad existentes e	17/03/14	18/03/14	2	
12		Definir la metodologia de evaluacion de riesgos	19/03/14	19/03/14	1	11, 9
13		Preparar los procedimientos relacionados con la ges	20/03/14	21/03/14	2	12
14		Análisis de Riesgos	24/03/14	14/04/14	16	
15		Definición de una metodología de evaluación de los r	24/03/14	24/03/14	1	
16		Realizar el levantamiento de informacion	25/03/14	25/03/14	1	15
17		Creación de un inventario de activos	26/03/14	26/03/14	1	16
18		Evaluación de los activos a ser protegidos	27/03/14	28/03/14	2	17
19		Identificación y evaluación de amenazas y vulnerabili	31/03/14	01/04/14	2	18
20						
21		Mapear cada riesgo identificado	03/04/14	04/04/14	2	
22		Estimación del valor de riesgo asociado a cada activ	07/04/14	09/04/14	3	19, 21
23		Estimar los impactos asociados a los activos	10/04/14	14/04/14	3	22
24		Gestión de Riesgos	16/04/14	30/04/14	11	
25		Identificar y evaluar alternativas posibles para tratar l	16/04/14	18/04/14	3	
26		Seleccionar e implantar los controles	21/04/14	23/04/14	3	25
27		Mapear los controles seleccionados	21/04/14	23/04/14	3	
28		Redactar el documento de declaración de aplicabilid	24/04/14	25/04/14	2	26, 27
29		Aprobación por parte de la Dirección del riesgo	28/04/14	28/04/14	1	28
30		Preparar el Plan de Tratamiento de Riesgos	29/04/14	30/04/14	2	29
31		IMPLANTACIÓN Y OPERACION	10/04/14	09/06/14	43	
32		Implantación del SGSI	02/06/14	09/06/14	6	
33		Implantar el plan de tratamiento de riesgos	02/06/14	04/06/14	3	
34		Implantar políticas y procedimientos del SGSI	05/06/14	09/06/14	3	33
35		Implantar los controles seleccionados	05/06/14	09/06/14	3	33
36		Formación y sensibilización	10/04/14	05/05/14	18	
37		Impartir formación entre los empleados sobre los nue	10/04/14	30/04/14	15	
38		Concientizar a la plantilla de la importancia de este p	10/04/14	30/04/14	15	
39		Desarrollo del marco normativo necesario y operar el	02/05/14	05/05/14	2	
40		MONITORIZACION Y REVISION	06/05/14	20/06/14	34	
41		Monitorización del SGSI	06/05/14	09/05/14	4	
42		Monitorizar los controles implementados	06/05/14	09/05/14	4	
43		Revisión del SGSI	13/05/14	20/06/14	29	
44		Realizar auditorías internas del SGSI	13/05/14	13/06/14	24	
45		Medir la eficiencia de los controles	16/06/14	17/06/14	2	44
46		Registrar acciones y eventos del SGSI	18/06/14	20/06/14	3	45
47		MANTENIMIENTO Y MEJORA	23/06/14	26/06/14	4	
48		Comunicar resultados de las auditorías a las partes interesadas	23/06/14	24/06/14	2	
49		Adoptar acciones correctivas y preventivas	25/06/14	26/06/14	2	48
50		CULMINACIÓN DEL PROYECTO	27/06/14	07/07/14	7	
51		Exposición y Aprobación	27/06/14	07/07/14	7	

ANEXO 8
LISTA DE ACTIVIDADES DEL PROYECTO

Nombre de la tarea	Fecha de inicio	Fecha de finalización	Duración	Predecesoras
ESTABLECIMIENTO DEL SGSI	**10/03/14**	**12/03/14**	**3**	
Inicio del Proyecto	10/03/14	12/03/14	3	
Definición del proyecto	10/03/14	10/03/14	1	
Seleccionar a los miembros	11/03/14	11/03/14	1	3
Realizar el acta de constitución	12/03/14	12/03/14	1	4
PLANEAMIENTO DEL SGSI	**11/03/14**	**11/06/14**	**67**	
Definición del SGSI	11/03/14	11/06/14	67	
Reunión con los stakeholders	11/03/14	11/03/14	1	
Identificación del alcance y las políticas de seguridad	11/06/14	11/06/14	1	
Recopilar los documentos de seguridad existentes en la organización	11/03/14	11/03/14	1	
Definir la metodología de evaluación de riesgos	12/03/14	12/03/14	1	10, 8
Preparar los procedimientos relacionados con la gestión y la operación del SGSI.	13/03/14	13/03/14	1	11
Análisis de Riesgos	11/03/14	16/04/14	27	
Definición de una metodología de evaluación de los riesgos.	11/03/14	11/03/14	1	
Realizar el levantamiento de información	12/03/14	12/03/14	1	14
Creación de un inventario de activos	13/03/14	13/03/14	1	15
Evaluación de los activos a ser protegidos	14/03/14	21/03/14	6	16
Identificación y evaluación de amenazas y vulnerabilidades de los activos	24/03/14	31/03/14	6	17
Mapear cada riesgo identificado	24/03/14	31/03/14	6	
Estimación del valor de riesgo asociado a cada activo.	01/04/14	08/04/14	6	18, 19
Estimar los impactos asociados a los activos	09/04/14	16/04/14	6	20

Gestión de Riesgos	21/03/14	18/04/14	21	
Identificar y evaluar alternativas posibles para tratar los riesgos	21/03/14	28/03/14	6	
Seleccionar e implantar los controles	31/03/14	07/04/14	6	23
Mapear los controles seleccionados	31/03/14	07/04/14	6	
Redactar el documento de declaración de aplicabilidad (SOA).	08/04/14	10/04/14	3	24, 25
Aprobación por parte de la Dirección del riesgo.	11/04/14	15/04/14	3	26
Preparar el Plan de Tratamiento de Riesgos.	16/04/14	18/04/14	3	27
IMPLANTACIÓN Y OPERACION	**02/04/14**	**12/05/14**	**29**	
Implantación del SGSI	02/04/14	09/04/14	6	
Implantar el plan de tratamiento de riesgos.	02/04/14	04/04/14	3	
Implantar políticas y procedimientos del SGSI.	07/04/14	09/04/14	3	31
Implantar los controles seleccionados.	07/04/14	09/04/14	3	31
Formación y sensibilización	10/04/14	12/05/14	23	
Impartir formación entre los empleados sobre los nuevos controles.	10/04/14	30/04/14	15	
Concientizar a la plantilla de la importancia de este proyecto.	10/04/14	30/04/14	15	
Desarrollo del marco normativo necesario y operar el SGSI.	02/05/14	12/05/14	7	
MONITORIZACION Y REVISION	13/05/14	05/06/14	18	
Monitorización del SGSI	13/05/14	21/05/14	7	
Ejecutar procedimientos y controles de monitorización y revisión.	13/05/14	21/05/14	7	
Revisión del SGSI	13/05/14	05/06/14	18	
Medir la eficacia de los controles.	13/05/14	21/05/14	7	
Realizar auditorías internas y externas del SGSI.	22/05/14	30/05/14	7	42
Registrar acciones y eventos del SGSI.	02/06/14	05/06/14	4	43
MANTENIMIENTO Y MEJORA	14/06/14	23/06/14	7	
Mantenimiento del SGSI	14/06/14	18/06/14	4	
Comunicar resultados de las auditorías a las partes interesadas.	14/06/14	16/06/14	2	
Adoptar acciones correctivas y preventivas.	17/06/14	18/06/14	2	47
Mejora Continua	21/06/14	23/06/14	2	
Medir el rendimiento del SGSI.	21/06/14	21/06/14	1	
Implantar las mejoras identificadas en las revisiones del SGSI.	23/06/14	23/06/14	1	50
CULMINACIÓN DEL PROYECTO	27/06/14	16/07/14	14	

Exposición y Aprobación	27/06/14	16/07/14	14	
Exposición de la propuesta	27/06/14	07/07/14	7	
Aprobación	08/07/14	16/07/14	7	54

ANEXO 9
LISTA DE RECURSOS

Tipo de Recurso	Descripción	Cantidad
Hardware	Laptop	5
	Multifuncionales	5
	Impresoras laser	4
	Servidores	2
Software	Microsoft Office 2010	5
	Zotero	5
	Violet UML	1
R.R.H.H.	Gerente de soluciones de infraestructura	1
	Jefe de sistemas	1
	Gerente de Proyectos	1
	Coordinador de calidad y seguridad	1

ANEXO 10
CUESTIONARIOS

POLITICAS DE SEGURIDAD		
NÚMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se tienen definidas y documentadas políticas de seguridad de datos?	La empresa cuenta con distintas políticas de seguridad las cuales atienden los siguientes frentes: -Control del personal y de acceso a las distintas instalaciones -Registro de las actividades del personal dentro de las facilidades de la empresa -Control del acceso a la información y recursos informáticos de la empresa -Políticas de seguridad laboral Pero no se encuentran documentadas

2	¿Tienen las mismas restricciones las demás sucursales? (ej. Almacén (Asturias), o los operadores en los clientes donde laboran).	No.
3	¿Quién es el encargado de aplicar las sanciones correspondientes al uso indebido de los activos?	Las labores de asignación están distribuidas en 2 áreas: -Administración -Tecnología de la información La aplicación de sanciones es por parte de Recursos Humanos
4	¿Quién aprueba las políticas de seguridad, así como evaluarlas?	La Gerencia General y el comité de seguridad.
5	¿Cada cuánto tiempo se renuevan las políticas de seguridad?	Las políticas son revisadas semestralmente y ante la eventualidad de casos fortuitos o no contempladas, el comité de seguridad puede ser convocado si la incidencia lo demanda, considerando su impacto en las actividades de la empresa.

6	¿Qué planes de contingencia se tiene ante una eventual caída de los servidores?	Se cuenta con planes de contingencia dependiendo de la severidad de la caída: Severidad 1: En caso de impacto sobre algunos componentes de los servidores, tenemos redundancia en componentes con lo cual se asegura la continuidad en caso de una falla, registrando y alertando del incidente al administrador. Severidad 2: En caso de caída de 1 servidor, los servicios que se vean afectados son recuperados y atendidos en un servidor alterno. Siendo este proceso una tarea semiautomático. Severidad 3: En caso de una caída masiva se cuenta con respaldo de la información crítica, la misma que se actualiza cada 24 horas de manera incremental y de manera global cada 7 días. De manera preventiva se cuenta con respaldo en el suministro eléctrico permitiendo la operación continua por lapso de 1 hora.

ORGANIZACIÓN DE LA INFORMACION		
PREGUNTA		**RESPUESTA**
¿Quién establece y asigna los roles?		El comité de seguridad de la empresa.
2	¿De qué manera la gerencia contribuye a la seguridad?	La gerencia aprueba las políticas y audita periódicamente el cumplimiento de las mismas. Aprueba y respalda ante el directorio las inversiones en recursos necesarios para el sostenimiento, actualización y evolución continua de la seguridad empresarial y los elementos que la soportan.
3	Quienes intervienen en la coordinación y planeamiento de la seguridad de la organización?	Los gerentes y personal de las gerencias de administración, recursos humanos, operaciones y soluciones de infraestructura.
4	¿Quién realiza el monitoreo?	El área de Sistemas que reporta a la Gerencia de Administración.

5	¿Del monitoreo hecho, quien evalúa la información?	La información es revisada por los responsables encargados con el soporte de sus Gerencias respectivas, quienes a su vez reportan los casos pertinentes al comité de seguridad.
6	¿Quién aprueba y establece las metodologías y procesos para la seguridad de la información?	La Gerencia de Soluciones de Infraestructura con el soporte de fabricantes y consultores de soluciones de seguridad la información.
7	¿De qué manera se puede asegurar y medir la idoneidad, eficiencia y eficacia de las políticas de seguridad?	Con procesos de auditoria, pruebas y simulaciones periódicas de contingencia. Bajo un proceso de mejora continua.
8	¿Se cuenta con algún acuerdo de confidencialidad? Que es lo que se establece en dicho acuerdo?	Sí, dicho acuerdo establece que ninguna persona puede acceder a la información de un área que no sea la suya, así como la prohibición de descargas de cualquier aplicativo o herramienta sin la previa autorización de la gerencia inmediata, solo Service Desk son los que pueden hacer las instalaciones.
9	¿Cuáles son las políticas que se tienen para la divulgación y autorización de la información?	No se tiene establecida, ni documentada ninguna política de este tipo.
10	¿Existe perfiles de acceso de usuario? (ej. usuario, administrador)	Cada colaborador tiene definido su usuario y contraseña, la cual podrá cambiar esta última cada 3 meses.

11	¿Se tiene definido roles y responsabilidades en seguridad de información?	No al interno, pero si con algunas entidades con las cuales se tiene alianzas y acuerdos de distribución. Estos acuerdos regulan el uso y difusión de la información que es compartida por nosotros y terceros.
12	Existe coordinación de seguridad entre representantes de diferentes áreas	Sí
13	¿Se les comparte información nuestra a los clientes? De ser así, ¿existe algún control para darles acceso?	Sí, y el procedimiento es solicitar sus datos para poder otorgarles un pin y así puedan tener acceso a la red de la empresa, pero esto solo se da cuando se está dentro de las instalaciones de la empresa.
14	¿Se tienen identificados los riesgos y los medios de procesamiento de la información de la empresa a raíz de procesos comerciales que involucran a grupos externos y se implementan controles para otorgarles acceso?	Sí

GESTION DE ACTIVOS	
PREGUNTA	**RESPUESTA**
¿Se tiene identificados e inventariados los activos?	Sí
¿Cada activo tiene asignado un propietario responsable?	Sí

3	¿Se tiene definidas las restricciones de acceso?	Sí, solo en la central.
4	¿Se tienen establecidos reglas para el uso eficiente de la información y de los activos asociados? Ejemplo uso de correo o de celulares	Sí se cuenta con reglas de uso, en ellas se establece que el correo solo se puede usar para revisión de mensajes, mas no para chat, de igual manera los celulares, no se puede ingresar a redes sociales o páginas de entretenimiento.
5	¿Se tiene clasificada la información de las áreas de la empresa?	Si, se cuenta con dicha clasificación.
6	¿Se cuenta con un plan de contingencia en caso de pérdida de información?	Sí
7	¿Se tiene documentada la importancia de los activos?	Sí
8	¿Se tiene definido un procedimiento para etiquetar los activos?	No
9	¿Cuál es el nivel de protección de los activos de mayor importancia?	Seguros.
CRIPTOGRAFIA		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se establecen controles criptográficos para proteger la información?	No
2	¿En caso de ser no la respuesta, de qué manera se puede asegurar la protección de los datos?	Por medio del uso de certificados digitales y VPNS.

SEGURIDAD FISICA Y AMBIENTAL		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se tienen definidos perímetros de seguridad?	Sí, algunos.
2	¿Se cuenta con alarmas para detección de intrusos?	No
3	¿Los colaboradores o visitantes cuentan con algún carnet de identificación?	No, porque en el caso de los colaboradores, ellos marcan su ingreso y salida por medio de un aparato biométrico, y en el caso de las visitas es por medio de una notificación enviada con anticipación, en la cual se detallas sus datos personales y el de su laptop, en caso posea en ese momento.
4	¿Se notifica la visita de alguna persona externa?	Sí, por medio de un correo, se detallan los datos de las personas, el motivo de la visita y el contacto al que busca.
5	¿Qué mecanismos se usan para monitorear la labor del personal?	Solo por medio de las cámaras de vigilancia.
6	¿El personal de servicio o apoyo tiene restricción para el ingreso a las áreas seguras?	Sí, ellos solo ingresan al comedor u oficinas para realizar sus labores diarias, mas no se les permite que permanezcan ahí por mucho tiempo. Los lugares a los que sí tienen totalmente restringido el acceso son al cuarto de servidores.
7	¿Se cuenta con algún PIN, para controlar el ingreso de personas no autorizadas a una determinada área de la empresa?	No

8	¿Se le pone al tanto al personal de la empresa sobre las actividades de las áreas aseguradoras?	Sí, cuando la ocasión lo requiere, por ejemplo, cuando va a haber una migración o configuración de los servidores y requieren que no haya laptop operativa se comunica con anticipación a fin de que ellos tomen las precauciones del caso.
9	¿Se cuenta con equipos contra incendios?	Sí, los cuales están ubicados en determinados puntos del edificio, además se cuenta de vez en cuando con charlas de uso de estos equipos.
10	¿Se tiene permitido el uso de videocámaras a la empresa?	No está permitido el uso de cámaras, a menos que haya una autorización.
11	las áreas seguras son aseguradas con llave	Sí, todo el tiempo, para evitar accesos indebidos.

12	¿Cuándo vienen proveedores a dejar pedidos o courrieres a recoger pedidos, se les permite el acceso al edificio?	No, todos los paquetes son dejados en vigilancia, por mucho se les permite el ingreso a la recepción, en caso de ser un paquete pequeño.
13	Se pueden retirar los equipos o programas fuera de la oficina?	Si, con autorización previa, en el caso de los equipos son usados para reuniones con un cliente.
14	¿Se realiza algún chequeo del equipo en su devolución para saber en qué condiciones se encuentra?	Sí
SEGURIDAD EN RECURSOS HUMANOS		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se tiene definido y documentado los roles y responsabilidades de empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización?	Sí
2	¿Se tiene un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad?	Sí
3	¿Se verifican los antecedentes de los candidatos al empleo?	Sí
4	¿Se realiza una constante actualización y capacitación a los empleados en seguridad de la información de acuerdo a las políticas ya establecidas?	No

5	¿Los colaboradores firman una cuerdo de confidencialidad al firmar su contrato?	Sí
6	¿Se tiene definido un código de buenas conductas en las que se abarquen el uso adecuado de los activos de la empresa?	Sí
7	¿Se tiene establecidas las sanciones respectivas para una violación de los términos y condiciones firmados en el contrato?	Sí
8	¿Se tiene establecido algún proceso para denegar los accesos de información y solicitar la devolución de los equipos al personal que culmina su vínculo con la empresa?	Sí
9	¿Qué sanción se le pondría a aquellos ex colaboradores que no cumplan con estas normas?	Dependiendo de la falta.
OPERACIONES DE SEGURIDAD		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Hay segregación entre áreas en el manejo de información?	Sí
2	¿Se tienen establecidas las responsabilidades y procedimientos formales para asegurar un control satisfactorio en los cambios en el equipo, software o procedimiento?	Sí
3	¿Se usa alguna bitácora para el registro de fallas de tal manera que se identifiquen problemas con los sistemas de información?	Sí
4	¿Se cuenta con registros de auditorías de eventos de seguridad?	Sí
5	¿Se tienen establecidos procesos y para el monitoreo y se revisan los resultados?	Sí
6	¿Se tienen protegidos los medios de registros de información?	Sí

CONTROL DE ACCESO		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Cuáles son las políticas que se tienen para la divulgación y autorización de la información? Dichas políticas se encuentran documentadas?	Queda prohibida la divulgación de la información con la que se trabaje en la organización, así como difundirla por medios escritos, o electrónicos, mas no están documentadas.
2	¿Existe perfiles de acceso de usuario? (ej. usuario, administrador)	Sí, cada colaborador tiene definido su usuario y contraseña.
3	¿Cada vez que se le da acceso a un usuario se le entrega un escrito?	Sí, se aprueba y registra por vía electrónica y auditable, en el caso de los colaboradores, cada ingresante recibe un documento sobre el equipo y el usuario corporativo asignado.
4	¿Quiénes son las personas encargadas de crear y documentar las políticas de control de acceso?	El comité de seguridad.
5	¿Quiénes aprueban dichas políticas? ¿Qué cargo tienen dentro de la organización?	La Gerencia General y los Gerentes de área.
6	¿Cómo se maneja y se informa las fallas y/o violaciones del sistema?	Se cuenta con sistemas de control y auditoria que registran todos los accesos y reportan alertas al administrador, permitiendo total trazabilidad de los sucesos. Los informes y reportes se efectúan por vía electrónica a los Gerente de área y los círculos de interés impactados.
7	¿Bajo qué estándares de seguridad se permiten las claves secretas? (ej. 6 caracteres o más? ¿Deben ser solo letras o también solo números o ambos, deben contener mayúsculas?)	Solo de 6 caracteres o más y con cambios en periodos de 2 meses.

8	¿Se tiene una política de acceso a los servidores de la red?	Sí
9	¿Se controla el uso de los programas de utilidad del sistema?	Sí, según los roles y funciones
10	Se cuenta con alguna restricción de acceso a la web	Sí, solo correo o google, no se permite redes sociales ni chat.
11	Esto es en la central o en otros puntos.	No, solo en la central.
12	¿Se tiene establecidos procedimientos para otorgar privilegios así como para revocarlos?	Sí
13	¿Cada cuánto se realizan los Back-up de la información crítica?	A diario de forma incremental y totalmente cada semana.
14	¿Se comunica al personal relevante los detalles de los cambios?	Sí
15	¿Cuentan con la política del escritorio limpio?	No

ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Cuenta con personal que monitorea y revisa los servicios, reportes y registros de entregan los terceros?	No
2	¿Cuentan con procedimientos formales de aprobación de cambios propuestos?	Sí
3	¿Se comunica al personal relevante los detalles de los cambios?	No
4	¿Cuentan con procedimientos para que los usuarios de los sistemas tengan conocimientos de los posibles ataques?	No
5	¿Se realiza una gestión de versiones de las aplicaciones?	No
GESTION DE LA CONTINUIDAD DEL NEGOCIO		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se ha desarrollado algún proceso gerencia para garantizar la seguridad del negocio, de ser así cuál?	Se tiene el proceso gerencial en cual consiste de una serie de actividades pero no se llega a cumplir al 100 %
2	¿Se tiene identificados los activos involucrados en los procesos comerciales críticos? De ser posible, mencionar algunos.	Sí, se tiene identificados los activos involucrados como activo de información(proyectos, servicios y compras) , físicos (servidores , estaciones de trabajo)

3	¿Se tiene comprensión sobre los riesgos que enfrenta la organización? ejemplos de riesgos de ser posible?	Sí, se tiene la comprensión de ciertos riesgos como riesgo de robo de información, riesgo de problemas en la red pero contamos con un servicio externo el cual nos brinda reportes mensuales o nos alerta cada vez que existan problemas en la red.
4	¿Han elaborado y/o actualizado su plan de continuidad comercial (en caso de tenerlo) que asegure que ese sea efectivo?	Sí, contamos con un plan de continuidad
5	¿Han identificado cuales serían sus recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requerimientos de seguridad de información identificados?	Sí, tenemos identificados los recursos mencionados
6	¿Se ha desarrollado o implementado algún plan para mantener y restaurar las operaciones y asegurar e esta manera la disponibilidad de la información en el nivel y momento requerido, después de la interrupción o falla?	Sí, contamos con un plan para restaurar la información en el momento requerido después de una falla mediante backup.
7	¿Se ha designado responsabilidades para las revisiones regulares de cada plan e continuidad del negocio?	Sí, se tiene asignado las responsabilidades pero no la realizan por motivo de falta de tiempo.

8	¿Se cuenta con algún marco referencia para la continuidad del negocio?	Sí, se tiene conocimiento de lo que se realizó antes en la empresa y la situación actual de la empresa es por eso que se tiene establecido el plan de continuidad pero no dio resultado en el momento que se aplicó anteriormente es por eso que la empresa realización de modificar dicho plan
9	¿Se tienen establecidas actividades de conciencia, duración y capacitación para crear entendimiento de los procesos de continuidad del negocio?	No se realiza

CUMPLIMIENTO		
NUMERO	**PREGUNTA**	**RESPUESTA**
1	¿Se tiene definida alguna política de cumplimientos de derechos de propiedad intelectual y publicaciones que definan el uso legal de software e información?	Sí, cuenta con dicha política pero no se cumple
2	¿Se lleva a cabo chequeos para que no se instalen software no autorizado y productos sin licencia?	Sí
	¿Tienen establecido alguna política de protección y privacidad de la data?	Sí se cuenta con política de protección y privacidad de la información pero algunos usuarios no la cumplen
4	¿Se cuenta con algún inventario de fuentes de información clave?	Sí se tiene dicho inventario

5	¿Suelen realizar alguna disuasión para evitar que usuarios que usa medios de procesamiento de información para propósitos no autorizados? O ¿no hay ninguno que acceda a la información restringida?	Se tiene el plan para evitar el uso no autorizado de la información confidencial pero no se realiza ninguna campaña de disuasión
6	¿Se cuenta con alguna asesoría legal antes de implementar los procedimientos de monitoreo?	Sí
7	¿En el último incumplimiento que tuvieron, cuáles fueron las causas de dicho incidente?	Utilizo de forma incorrecta la información para beneficios propios , el usuario fue despedido
8	¿Cada cuánto tiempo se realiza el chequeo para ver el cumplimiento de los estándares de implementación de seguridad?	Cada 6 meses.

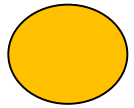
ANEXO 11
LISTA DE ACTIVOS Y NIVELES CRÍTICOS

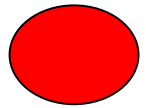
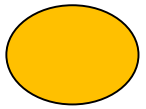
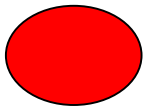
ID	DEFINICION DEL ACTIVO	CRITERIOS DE VALORIZACION			VALOR TOTAL	CRITICIDAD
		INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD		
1	ARCHIVOS DE DATA	3	3	3	9	ALTO
2	PROYECTOS	3	3	3	9	ALTO
3	PLANES DE TRABAJO	3	3	3	9	ALTO
4	CONTRATOS	3	3	3	9	ALTO
5	REGISTRO DE PERSONAL	3	3	3	9	ALTO
6	PLANILLA DEL PERSONAL	3	3	3	9	ALTO
7	PLANES DE RIESGO	3	3	3	9	ALTO
8	BASE DE DATOS	3	3	3	9	ALTO
9	TRANSACCIONES	3	3	3	9	ALTO
10	OPERACIONES	3	3	3	9	ALTO
11	REPORTES FINANCIEROS ESTADISTICOS	3	3	3	9	ALTO
12	CONTROL DE RETENCION DE FACTURAS	3	3	3	9	ALTO
13	SIGAF	3	2	3	8	ALTO
14	OFFICE 2010	3	3	1	7	ALTO
15	WINDOWS 7 SERVICE PACK 3	3	3	1	7	ALTO
16	SOLOMON	2	2	2	6	MEDIO

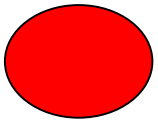
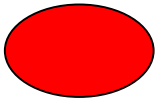
17	MARKVISION	3	3	2	8	ALTO
18	ELOY SYSTEM	2	2	2	6	MEDIO
19	ORACLE	3	3	3	9	ALTO
20	ANTIVIRUS MCCAFEE	0	3	1	4	MEDIO
21	ADOBE READER	0	1	0	1	BAJO
22	PDF CREATOR	0	1	0	1	BAJO
23	WIN RAR	0	1	0	1	BAJO
24	ACCES POINT	3	3	3	9	ALTO
25	SWITCH	3	3	3	9	ALTO
26	LAPTOS	3	3	3	9	ALTO
27	2 PROYECTORES	0	0	0	0	NO APLICA
28	PC'S	3	3	3	9	ALTO
29	TELEFONO IP	3	3	0	6	MEDIO
30	ROUTER	3	3	3	9	ALTO
31	AGUA POTABLE	0	3	0	3	BAJO
32	ENERGIA ELECTRICA	0	3	0	3	BAJO
33	AIRE ACONDICIONADO	0	3	0	3	BAJO
34	PERSONAL DEL AREA DE TI	3	2	0	5	MEDIO
35	PERSONAL DEL AREA DE R.R.H.H.	3	2	0	5	MEDIO
36	GERENTES	3	2	0	5	MEDIO
37	JEFE DE AREAS	3	2	0	5	MEDIO
38	SUPERVISORES DE CAMPO	3	2	0	5	MEDIO
39	COORDNADORES	3	2	0	5	MEDIO
40	OPERADORES	3	2	0	5	MEDIO

41	TECNICOS	3	2	0	5	MEDIO
42	PRESTIGIO	3	0	3	6	MEDIO
43	PATENTES	3	0	3	6	MEDIO
44	DERECHOS DE AUTOR	3	0	3	6	MEDIO
45	PROPIEDAD INTELECTUAL	3	0	3	6	MEDIO

ANEXO 12
ANALISIS DE BRECHA PRE

	SITUACION ACTUAL	CONTROL	ANALISIS DE BRECHA	
5. POLITICAS DE SEGURIDAD				
5	La empresa SSS			
	1. Tiene definidas sus políticas, pero no se encuentran documentadas ni formalizadas.		1. Debe crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad. Los documentos de política de seguridad de información debieran ser aprobados por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.	 20%
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION				
6	La empresa SSS			
	1. Se tiene establecida, ni documentada ninguna política de divulgación y autorización de la información, mas no documentada.		1. Debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento.	 20%

7. GESTION DE ACTIVOS		
La empresa SSS		
1. No cuenta con un proceso para etiquetar sus activos.	1. Debe desarrollar en implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	 0%
8. CONTROL DE ACCESO		
La empresa SSS		
Se tiene establecida y documentada las políticas de control de acceso, pero hace meses que no se ha revisado ni actualizado.	1. Debe establecer, documentar y revisar las políticas de control de acceso en base a los requerimientos de seguridad y comerciales.	 20%
9. CRIPROGRAFIA		
La empresa SSS		
1. No cuenta con una política para el uso de criptografía.	1. Debe desarrollar e implementar una política sobre el uso de controles criptográficos, para la protección de la información.	 0%

9. SEGURIDAD FISICA Y AMBIENTAL			
9	La empresa SSS		
	1. No cuenta con alarmas para la detección de intrusos, ni con un PIN para controlar el acceso a personas no autorizadas a áreas restringidas.	1. Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.	 0%
	2. No cuenta con carnet de identificación	2. Se debe controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar a las áreas restringidas.	
10.SEGURIDAD EN R.R.H.H.			
10	La empresa SSS		
	1. No realiza una constante actualización y capacitación a los empleados en seguridad de la información de acuerdo a las políticas ya establecidas.	1. Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.	 0%

ANEXO 13
LISTA DE RIESGOS

ID	DESCRIPCION
1	Carencia alarmas para detección de intrusos
2	Inadecuado control de acceso
3	Entrenamiento inadecuado de personal
4	Falta de manejo de versiones
5	Falta de control en el manejo de la energía eléctrica

ANEXO 14
MATRIZ DE RIESGOS

MATRIZ DE RIESGOS									
ID RIESGO	ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD QUE LA AMENAZA EXPLOTE LA VULNERABILIDAD		IMPACTO ESTIMADO EN LA EMPRESA		PRIORIDAD	NIVEL DE RIESGO
R1	Archivos de data	Entrenamiento inadecuado de usuarios	Infección de virus	POSIBLE	5	CATASTROFICO	5	25	ELEVADO
R2	Archivos de data	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales	POSIBLE	3	MAYOR	4	12	ELEVADO
R3	Archivos de data	Inadecuado control de acceso	Modificación no autorizada	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R4	Archivos de data	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	POSIBLE	3	MAYOR	4	12	ELEVADO
R5	Archivos de data	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R6	Archivos de data	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R7	Archivos de data	Deficiente control de acceso a zonas restringidas	Robo de información	IMPROBABLE	2	CATASTROFICO	5	10	ELEVADO
R8	Proyectos	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales.	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R9	Proyectos	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R10	Proyectos	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R11	Proyectos	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R12	Proyectos	Deficiente control de acceso a zonas restringidas	Robo de información	RARO	1	CATASTROFICO	5	5	ACEPTABLE
R13	Planes de trabajo	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales	POSIBLE	3	MAYOR	4	12	ELEVADO
R14	Planes de trabajo	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MAYOR	4	12	ELEVADO
R15	Planes de trabajo	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R16	Planes de trabajo	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	3	MODERADO	4	12	ELEVADO

R17	Planes de trabajo	Deficiente control de acceso a zonas restringidas	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO
R18	Contratos	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales.	POSIBLE	3	MENOR	2	6	ACEPTABLE
R19	Contratos	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R20	Contratos	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R21	Contratos	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	RARO	1	INSIGNIFICANTE	1	1	BAJO
R22	Contratos	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R23	Contratos	Deficiente control de acceso a zonas restringidas	Robo de información	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R24	Registro de personal	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales	POSIBLE	3	MAYOR	4	12	ELEVADO
R25	Registro de personal	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R26	Registro de personal	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R27	Registro de personal	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R28	Registro de personal	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R29	Registro de personal	Deficiente control de acceso a zonas restringidas	Robo de información	RARO	1	CATASTRÓFICO	5	5	ACEPTABLE
R30	Planilla del personal	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales.	POSIBLE	3	MAYOR	4	12	ELEVADO
R31	Planilla del personal	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R32	Planilla del personal	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R33	Planilla del personal	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R34	Planilla del personal	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R35	Planilla del personal	Deficiente control de acceso a zonas restringidas	Robo de información	RARO	1	CATASTRÓFICO	1	1	ACEPTABLE
R36	Planes de riesgo	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales	POSIBLE	3	MAYOR	4	12	ELEVADO
R37	Planes de riesgo	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MAYOR	4	12	ELEVADO
R38	Planes de riesgo	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R39	Planes de riesgo	Deficiente control de acceso a zonas restringidas	Riesgo por el personal de limpieza o personal externo	RARO	1	CATASTRÓFICO	1	1	ACEPTABLE
R40	Planes de riesgo	Entrenamiento inadecuado de usuarios	Falta de cuidado en el manejo de información	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R41	Planes de riesgo	Deficiente control de acceso a zonas restringidas	Robo de información	RARO	1	INSIGNIFICANTE	1	1	BAJO
R42	Base de datos	Inadecuado control de acceso	Modificación no autorizada	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R43	Base de datos	Inadecuado control de acceso	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO

R44	Base de datos	Inadecuado control de acceso	Robo de claves	POSIBLE	3	MAYOR	4	12	ELEVADO
R45	Base de datos	Inadecuado control de acceso	Accesos no autorizados a datos confidenciales	POSIBLE	3	MAYOR	4	12	ELEVADO
R46	Transacciones	Inadecuado control de acceso	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO
R47	Operaciones	Inadecuado control de acceso	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO
R48	Reportes Financieros Estadísticos	Inadecuado control de acceso	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO
R49	Control De Facturas	Inadecuado control de acceso	Robo de información	POSIBLE	3	MAYOR	4	12	ELEVADO
R50	SIGAF	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R51	Windows 7 Service Pack 3	Mal funcionamiento/ conducta anómala	Violación del sistema	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R52	Windows 7 Service Pack3	Mal funcionamiento/ conducta anómala	Ataque de seguridad	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R53	SOLOMON	Entrenamiento inadecuado de usuarios	Destrucción negligente de los datos	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R54	SQLSERVER 2008	Inadecuado control de acceso	Modificación no autorizada	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R55	ACCES POINT	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO
R56	SWITCH	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO
R57	Laptops	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO
R58	Laptops	Deficiente control de acceso a zonas restringidas	Pérdida de Laptops	RARO	1	INSIGNIFICANTE	1	1	BAJO
R59	Laptops	Mal funcionamiento/ conducta anómala	Violación del sistema	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R60	Laptops	Mal funcionamiento/ conducta anómala	Ataque de seguridad	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE

R61	Laptops	Mal funcionamiento/ conducta anómala	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R62	Laptops	Prueba de debilidades	Mal uso potencial	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R63	Laptops	Prueba de debilidades	Daños de información	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R64	Laptops	Prueba de debilidades	Errores de configuración	RARO	1	MODERADO	3	3	BAJO
R65	Laptops	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía.	RARO	1	MODERADO	3	3	BAJO
R66	Laptops	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de Telecomunicaciones	RARO	1	MODERADO	3	3	BAJO
R67	Servidor Correo	Deficiente control de acceso a zonas restringidas.	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO

R68	Servidor Correo	Mal funcionamiento / conducta anómala	Violación del sistema	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R69	Servidor Correo	Mal funcionamiento / conducta anómala	Ataque de seguridad	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R70	Servidor Correo	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R71	Servidor Correo	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de Telecomunicaciones	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R72	Servidor FTP	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO
R73	Servidor FTP	Mal funcionamiento / conducta anómala	Violación del sistema	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R74	Servidor FTP	Mal funcionamiento / conducta anómala	Ataque de seguridad	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE

R75	Servidor FTP	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R76	Servidor FTP	Mal funcionamiento / conducta anómala	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R77	Servidor FTP	Prueba de debilidades	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R78	Servidor FTP	Prueba de debilidades	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R79	Servidor FTP	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R80	Servidor FTP	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de Telecomunicaciones	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R81	Servidor Web	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO

R82	Servidor Web	Mal funcionamiento / conducta anómala	Violación del sistema	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R83	Servidor Web	Mal funcionamiento / conducta anómala	Ataque de seguridad	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R84	Servidor Web	Mal funcionamiento / conducta anómala	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R85	Servidor Web	Prueba de debilidades	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R86	Servidor Web	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía.	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R87	Servidor Web	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de Telecomunicaciones	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE

R88	PC'S	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	INSIGNIFICANTE	1	1	BAJO
R89	PC'S	Deficiente control de acceso a zonas restringidas	Pérdida (extravío)	RARO	1	INSIGNIFICANTE	1	1	BAJO
R90	PC'S	Prueba de debilidades	Errores de configuración	IMPROBABLE	2	MODERADO	3	6	ACEPTABLE
R91	PC'S	Prueba de debilidades	Mal uso potencial	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R92	PC'S	Prueba de debilidades	Fallas físicas de los equipos (averías)	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R93	PC'S	Mal funcionamiento / conducta anómala	Violación del sistema	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R94	PC'S	Mal funcionamiento / conducta anómala	Ataque de seguridad	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R95	PC'S	Prueba de debilidades	Fallas físicas de los equipos (averías)	POSIBLE	3	MODERADO	3	9	ACEPTABLE
R96	PC'S	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de energía.	RARO	2	MODERADO	3	6	BAJO

R97	PC'S	Falta de control en el manejo de la energía eléctrica	Interrupción del servicio de Telecomunicaciones	RARO	2	MODERADO	3	6	BAJO
R98	Teléfono IP	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	MAYOR	1	1	BAJO
R99	Router	Deficiente control de acceso a zonas restringidas	Robo de equipos	RARO	1	MAYOR	1	1	BAJO
R100	Personal del área de TI	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R101	Personal del área de R.R.H.H.	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R102	Gerentes	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R103	Gerentes	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MODERADO	3	12	ELEVADO
R104	Jefes de área	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R105	Jefes de área	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R106	Supervisores de campo	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R103	Gerentes	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MODERADO	3	12	ELEVADO
R104	Jefes de área	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R105	Jefes de área	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R106	Supervisores de campo	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO

R107	Supervisores de campo	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R108	Coordinadores	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R109	Coordinadores	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R110	Operadores	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R111	Operadores	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R112	Técnicos	Entrenamiento inadecuado de usuarios	Fraude	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R113	Técnicos	Entrenamiento inadecuado de usuarios	Deshonestidad y sabotaje	MUY PROBABLE	4	MAYOR	4	16	ELEVADO
R114	Prestigio	Administración inadecuada de la información delicada	Pérdida de imagen institucional	IMPROBABLE	2	CATASTRO FICO	5	10	ELEVADO
R115	Patentes	Inadecuado control de acceso	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R116	Patentes	Deficiente control de acceso a zonas restringidas	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE

R117	Derechos de autor	Inadecuado control de acceso	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R118	Derechos de autor	Deficiente control de acceso a zonas restringidas	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R119	Propiedad intelectual	Inadecuado control de acceso	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE
R120	Propiedad intelectual	Deficiente control de acceso a zonas restringidas	Plagio	IMPROBABLE	2	MAYOR	4	8	ACEPTABLE

ANEXO 15
PLAN DE TRATAMIENTO DE RIESGOS

Control 5.1.1. Documento de política de seguridad de la información

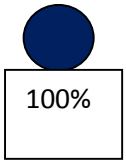
Objetivos

ACCIONES	OBJETIVO	RESPONSABLE	PLAZO DE EJECUCION
Definir e implementar la documentación de las políticas de seguridad de datos en la empresa.	Establecer las restricciones del uso de la información.	Coordinador de calidad y seguridad, Jefe de sistemas y Gerente de Infraestructura.	2 días

Planificación de acciones

OBJETIVOS	ACCIONES	RESPONBASILIDADES (QUIEN?)	RESULTADO ESPERADO
Establecer las restricciones del uso de la información.	Definir e implementar la documentación de las políticas de seguridad de datos en la empresa.	Coordinador de calidad y seguridad, Jefe de sistemas y Gerente de Infraestructura.	Que la mayoría del personal se rija a las restricciones establecidas en cuanto a seguridad de información se trata.

Control 5.1.1. Documento de política de seguridad de la información

ACCIONES	OBJETIVO(PRINCIPAL/OPERATIVO)	RESULTADO ESPERADO	NIVEL DE MADUREZ	EVIDENCIAS
Desarrollo del cuerpo normativo	Establecer normativas que rijan el uso correcto de la información y los recursos con los que cuenta la empresa.	Que la mayoría del personal tome conciencia de la importancia de proteger la información como un activo.		Políticas documentadas y Reportes de incidencias.

Esto representa que la empresa estableció sus políticas y las revisan continuamente para mejorarlas.

ANEXO 16
CONTROLES

NOMBRE DEL CONTROL	DESCRIPCIÓN	RIESGOS A CONTROLAR	ADAPTACION A LA EMPRESA
Documentar las políticas de seguridad de información.	Debe crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad.	TODOS	Se deberá crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad.
Revisión de las políticas de seguridad de información.	Los documentos de política de seguridad de información debieran ser aprobados por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.	TODOS	La gerencia deberá aprobar por la gerencia, publicar y comunicar a todos los empleados y las partes externas relevantes los documentos de las políticas de seguridad de información.
Procesos de autorización de recursos para el tratamiento de la información.	Debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento.	R4, R6,R11,R14, R20, R26, R28, R32, R34, R38, R40, R50, R53, R54	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento.
Acuerdos de confidencialidad.	Debe identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la empresa para la protección de la información.	R2, R13, R24, R30, R36, R34	Se debe identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la empresa para la protección de la información.
Uso adecuado de los activos.	Las reglas de uso aceptable de la información, deberían ser identificadas, documentadas e implantadas.	R4, R6, R11, R16, R20, R22, R26, R28, R32, R34, R38, R40, R50, R53	Las reglas de uso aceptable de la información, deben ser identificadas, documentadas e implantadas.

Política de pantalla y escritorio limpio.	Se debería adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	R2,R5,R7,R8,R9, R12, R29,R30, R33, R35, R39, R41, R43, R46, R47, R48, R49	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
Política sobre el uso de servicios en red.	Los usuarios solo deberían de tener acceso para los servicios para los cuales han sido específicamente autorizados.	R1, R2, R3,R8,R9, R13, R14, R17, R18, R19, R24, R25, R30, R31, R36, R37, R93, R94	Los usuarios solo deben de tener acceso para los servicios para los cuales han sido específicamente autorizados.
Control de 'routing' de redes.	Se deberían implementar controles de 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan las políticas de control de acceso de las aplicaciones comerciales.	R1, R2, R3,R8,R9, R13, R14, R17, R18, R19, R24, R25, R30, R31, R36, R37, R93, R94	Se deben implementar controles de 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan las políticas de control de acceso de las aplicaciones comerciales.
Desarrollar e implementar una política de controles criptográficos.	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos, para la protección de la información.	R1, R2, R4, R6, R11, R13, R14, R16, R17, R20, R22, R24, R26, R28, R30,R32, R34, R36, R38, R40, R46, R47, R48, R49	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos, para la protección de la información.
Áreas seguras.	Se deberían proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.	R17	Se debe proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.

Concientización y formación sobre la seguridad de la información.	Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.	R1, R4, R6, R11, R16, R20, R22, R26, R28, R32, R34,R38, R40, R50, R53, R100, R101, R102, R103, R104, R105,R106,R107,R108, R109, R110, R111, R112, R113	Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.
Registro de auditoria.	Se debe de contar con un registro de auditoria.	TODOS	Se deben producir registros de las actividades de auditoria, excepciones y eventos de seguridad de la información y se debe de mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
Registro de fallas.	Se debe contar con una bitácora para el registro de fallas de tal manera que se identifiquen problemas con los sistemas de información.	R51, R52, R59,R60, R61, R62,R63, R68, R69,R70, R71, R76,R77, R78,R79,R80, R82,R83,R84,R85,R86,R87, R90,R91,R92,R93,R94,R95	Las fallas se deben de registrar, analizar y se debe tomar una acción apropiada.

ANEXO 17
DECLARACION DE APLICABILIDAD (SOA)

DECLARACION DE APLICABILIDAD(SOA)			
OBJETIVOS DE CONTROL	**CONTROL**	**APLICABLE**	**JUSTIFICACION**
5. POLITICA DE SEGURIDAD			
5.1. POLITICA DE SEGURIDAD DE LA INFORMACION			
5.1.1. Documento de política de seguridad de la información.	Se debe crear documentos donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad. Los documentos de política de seguridad de información debieran ser aprobados por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.	Sí	Que la empresa se rija a lo establecido y evitar acciones indebidas.
5.1.2. Revisión de la politica de seguridad y la información.	Se debe revisar las políticas de seguridad a fin de mantener todas las sedes o puntos de atención custodiados de igual manera como la central.	Sí	Que todos los centros de atención cuenten con el mismo nivel de seguridad, a fin de garantizar protección en la información.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
6.1. ORGANIZACIÓN DE LA INFORMACION			
6.1.4. Proceso de autorización para los medios de procesamiento de información.	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento.	Sí	Que exista un proceso formal para establecer cuáles son los medios por los que se van a procesar una determinada información.
6.1.5. Acuerdos de confidencialidad.	Se debe identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la empresa para la protección de la información.	Sí	Mantener actualizados dichos requerimientos.

7. SEGURIDAD DE R.R.H.H.			
7.2.. DURANTE EL EMPLEO			
7.2.2. Conocimiento, educación y capacitación en seguridad de la información.	Todos los empleados contratistas deben recibir apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.	Sí	Crear conciencia en los usuarios sobre la importancia de proteger la información y darle el uso correcto.
8. GESTION DE ACTIVOS			
8.2. CLASIFICACION DE LA INFORMACION			
8.2.2. Etiquetado y manejo de la información	Se debe desarrollar en implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	Sí	Llevar un control adecuado de los activos.
9. CONTROL DE ACCESO			
9.3. RESPONSABILIDADES DEL USUARIO			
9.3.3.Política de pantalla y escritorio limpio.	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	Sí	Establecer un orden a fin de evitar la pérdida de información delicada

9.4.1. Política sobre el uso de servicios en red	Los usuarios solo deben de tener acceso para los servicios para los cuales han sido específicamente autorizados.	Sí	Controlar que los usuarios solo hagan uso de la red según las funciones que desempeñen.
9.4.7. Control de 'routing' de redes.	Se deben implementar controles de 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan las políticas de control de acceso de las aplicaciones comerciales.	Sí	Evitar que se infrinjan las políticas con accesos no autorizados.
10. CRIPTOGRAFIA			
10.1. CONTROLES CRIPTOGRAFICOS			
10.1.1. Políticas sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.	No	No se considera necesaria dicha implementación
11. SEGURIDAD FISICA Y AMBIENTAL			
11.1. AREAS SEGURAS			
11.1.2. Controles de ingreso físico	Se debe proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.	Sí	Evitar que personas no autorizadas obtengan acceso a información sensible.

12. OPERACIONES DE SEGURIDAD			
12.4. MONITOREO			
12.4.1. Registro de auditoria	Se deben producir registros de las actividades de auditoria, excepciones y eventos de seguridad de la información y se debe de mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso.	Sí	Contar un registro de las falencias encontradas.
12.4.7. Registro de fallas	Las fallas se deben de registrar, analizar y se debe tomar una acción apropiada.	Sí	Llevar un control de las fallas ocurridas a fin de saber cómo corregirlas en caso se vuelva a repetir.

ANEXO 18
PROGRAMA DE CONCIENTIZACIÓN

Con el objetivo de preparar al personal para que pueda cumplir una función en la seguridad de la información, se debe llevar a cabo la siguiente capacitación:

Cargo o nombre	Conocimientos y habilidades necesarias	Qué capacitación es necesaria
Cargo o nombre de la persona que va a recibir la capacitación.	Fundamentos de seguridad de la información.	Uso adecuado de la información delicada.

Para que el personal comprenda la importancia de la gestión de la seguridad de la información y de su propio aporte al SGSI, y para que acepte las políticas y planes y comprenda las consecuencias de violar las normas de seguridad de la información, se deben aplicar los siguientes métodos de concienciación:

- Establecer normativas de uso de la información.
- Elaboración de un decálogo de uso de la información.
- Desarrollar jornadas de capacitación y concientización.
- Monitorear con frecuencia y asegurar el cumplimiento de las normativas establecidas.
- Aplicar las sanciones correspondientes para aquellos colaboradores que incumplan con las políticas establecidas.

ANEXO 19
DECÁLOGO DE SEGURIDAD

DECÁLOGO DE SEGURIDAD PARA ADMINISTRADORES

1. **Permisos y autentificación.** Es necesario asignar permisos y tener una buena política de contraseñas. De esta manera se asegura que solo las personas autorizadas tengan acceso a la información.
   Estas no deberán estar formadas por palabras o números fácilmente atribuibles al usuario ni a la empresa, como números de teléfono, fechas de nacimiento, nombres y/o apellidos, nombre de la empresa, etc., puesto que darían lugar a contraseñas muy vulnerables. Asimismo, una vez generadas, han de protegerse de modo que solo sean conocidas y accesibles por el propio usuario, cambiándolas siempre que lo considere necesario o cuando se lo exija el sistema.
2. **Soluciones contra código malicioso.** No disponer de un sistema antivirus o contra código malicioso de actualización automática, es sinónimo de problemas para los sistemas y la continuación de la organización.
3. **Comunicaciones seguras**. Por la red de la organización, circulan datos muy importantes y confidenciales, por eso es necesario que las comunicaciones sean lo más seguras posibles.
4. **Actualizaciones y Mantenimiento.** Actualizar frecuentemente los sistemas de información utilizadas en la organización con los parches del proveedor, ayudan a cubrir posibles vulnerabilidades que posean estos sistemas, así como corregir incidencias o potenciales amenazas.
5. **Adecuación a la legislación vigente.**
   Software Legal: Asegúrese que todo el software instalado proviene de una fuente conocida y segura. No instale copias de software ilegal, aplicable con los de su ordenador, lo cual provocara inestabilidad en su equipo.
   Adecuación a la LOPD. En el caso de que trate datos de carácter personal, asegúrese de que estos datos se tratan según marca la legislación aplicable en protección de datos LOPD (Ley Orgánica de Protección de Datos), si no se realiza de esta manera, se pueden incurrir en multas.
6. **Monitorización/Auditoria.** Una vez se tiene implementada una solución de seguridad, no se puede abandonar. Hay que estar pendiente de actualizar todos los dispositivos y asegurarse de que todo funciona correctamente.

7. **Continuidad de las actividades.**
   Alta disponibilidad. La parada de un servidor, un router, una línea de comunicaciones, aunque solo sea durante unas horas, puede suponer costos importantes. Por ello es recomendable redundarlos, eliminando así los puntos únicos y garantizando que todo funcione sin interrupciones.
   Backup. Tener un backup es fundamental, ¿Qué pasaría si mañana, por un robo o por un error, desaparecieran mis datos? ¿Estamos cubiertos?
   Plan de contingencia. Tener un plan de contingencia es tener los procedimientos claros y accesibles, para recuperar la normalidad de las funciones de la organización en caso de un fallo de los sistemas.
8. **Manténgase Informado.** Manténgase periódicamente informado de las novedades de la seguridad informática a través de boletines de las compañías fabricantes de software así como de los servicios de información y boletines.

DECÁLOGO DE SEGURIDAD PARA USUARIOS

1. Utilizar contraseñas que sean difíciles de adivinar, pero fáciles de recordar, combinando letras, números y signos.
2. No utilice la funcionalidad “Recordar Contraseña”, implica no teclear las claves de acceso cada vez que se conecte pero facilita en gran medida acceso a personal no autorizado.
3. Apagar el ordenador cuando no se vaya a utilizar durante un periodo de tiempo largo y bloquearlo cuando no estemos delante del mismo.
4. Utilizar programas legales y no instalar programas sin la autorización del responsable de informática.
5. Borrar sin leer aquellos mensajes de correo electrónico con remitentes desconocidos o que resulten sospechosos.
6. No enviar o recibir mensajería electrónica que contengan material de carácter explícitamente sexual, discriminatorio racial, ni que pueda llegar a ser ofensivo, difamatorio, amenazante o insultante para cualquier persona basándose en su raza, religión, sexo, nacionalidad, origen, estado civil, edad, discapacidad o aspecto.
7. Internet tiene carácter de privilegio y no de derecho ya que su uso está directamente relacionado con las actividades propias de la organización.
8. Si se guarda información restringida en una PC portátil, es obligatorio cifrarla. En un equipo de sobremesa, es muy recomendable.
9. Alertar al responsable de informática sobre cualquier comportamiento extraño del ordenador.
10. Ante cualquier eventualidad utilizar el sentido común y ser cauteloso ante cualquier programa o mensaje extraño.

ANEXO 20
PLAN DE AUDITORíA

1. OBJETIVOS

1.1. OBJETIVO GENERAL

- ✓ Evaluar si los controles de seguridad de la información implantados son los más adecuados para el cumplimiento de los objetivos del proyecto, así mismo, establecer si se está administrando adecuadamente los riesgos tecnológicos relacionados al área de sistemas y los Data Center en cada uno de los centros de atención.

1.2. OBJETIVOS ESPECÍFICOS

- ✓ Evaluar si los niveles de riesgo identificados inicialmente han disminuido.
- ✓ Determinar si la protección de los activos de información son los idóneos.

2. ALCANCE

El presente documento tiene como alcance la central de la empresa Systems Support & Services S.A , el almacén de la empresa, así como cada uno de los puntos de atención, esta evaluación tendrá un periodo de estudio de dos meses comprendido entre los meses del 22 de mayo al 13 de junio del 2014.

3. **METODOLOGÍA**

Durante la ejecución del proyecto se utilizará la metodología COBIT 5.0, la metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

4. **DESCRIPCIÓN DE LAS ACTIVIDADES**

Las actividades del área de sistemas de Systems Support & Services S.A. son los que a continuación se detallan:

- Mantenimiento de las Bases de Datos de la empresa.
- Administración de contenidos Web para otras Empresas.
- Virtualización de sistemas.
- Administración de la red interna.
- Administración de cuentas de usuarios internos.
- Mejorar la seguridad para ayudar a proteger los datos y abordar los mandatos corporativos y gubernamentales.

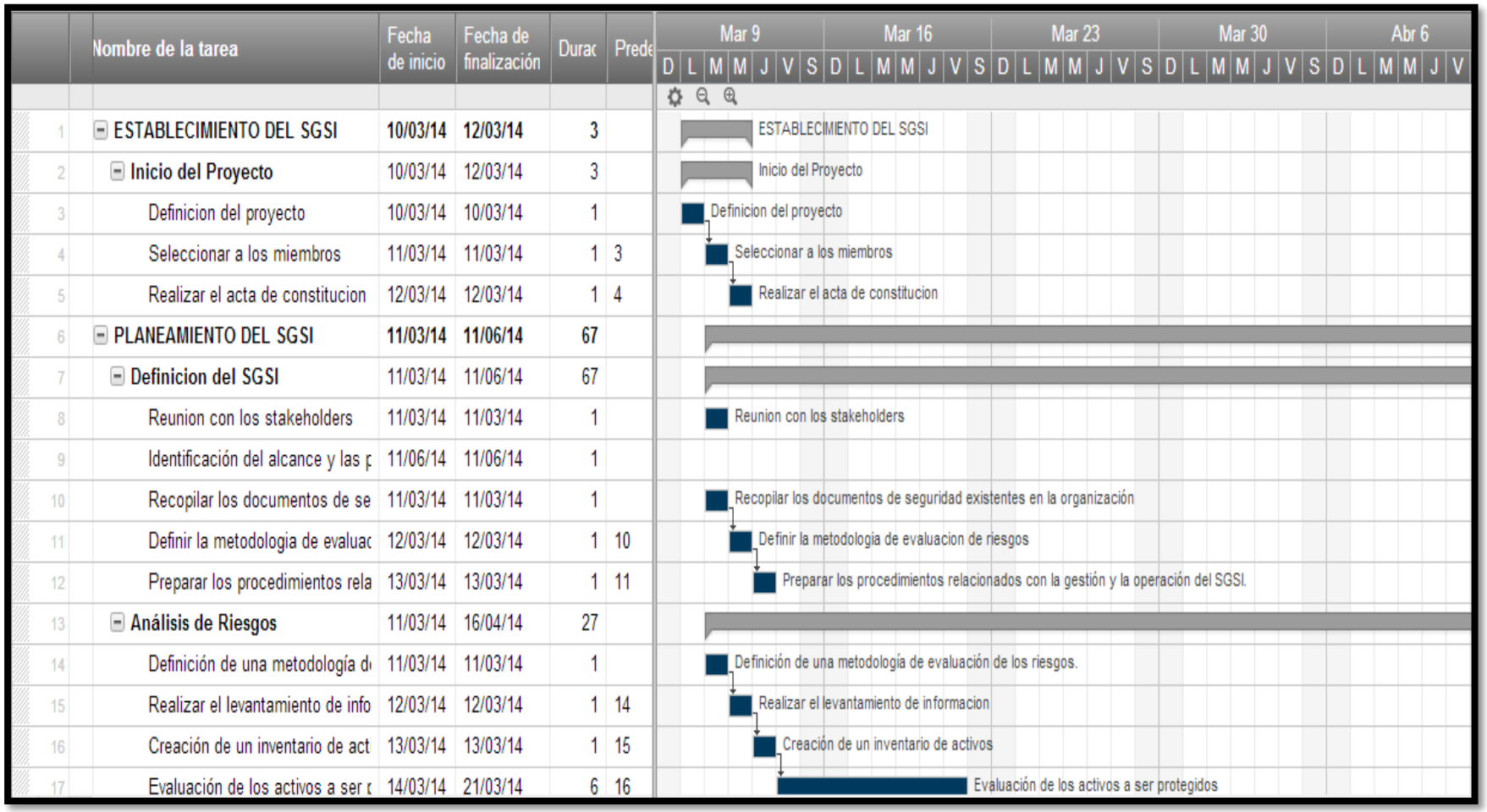
5. PROCEDIMIENTOS A UTILIZAR

Para el desarrollo del trabajo se tiene previsto el uso de cuestionarios y entrevistas para tener un conocimiento global de la empresa, y enfocarnos en la central y los puntos de atención para realizar el análisis de sus procesos. La empresa ha solicitado un cuidado especial de la documentación sobre todo aquella que implica los procedimientos para la realización del servicio.

6. ENTREGABLES

- Plan de Trabajo de Auditoria.
- Cuestionario COBIT 5.0.
- Informe Final de Auditoria.

ANEXO 21
CRONOGRAMA GENERAL DE AUDITORíA



	Nombre de la tarea	Fecha de inicio	Fecha de finalización	Durac	Prede
1	**ESTABLECIMIENTO DEL SGSI**	**10/03/14**	**12/03/14**	**3**	
2	**Inicio del Proyecto**	10/03/14	12/03/14	3	
3	Definicion del proyecto	10/03/14	10/03/14	1	
4	Seleccionar a los miembros	11/03/14	11/03/14	1	3
5	Realizar el acta de constitucion	12/03/14	12/03/14	1	4
6	**PLANEAMIENTO DEL SGSI**	**11/03/14**	**11/06/14**	**67**	
7	**Definicion del SGSI**	11/03/14	11/06/14	67	
8	Reunion con los stakeholders	11/03/14	11/03/14	1	
9	Identificación del alcance y las p	11/06/14	11/06/14	1	
10	Recopilar los documentos de se	11/03/14	11/03/14	1	
11	Definir la metodologia de evaluac	12/03/14	12/03/14	1	10
12	Preparar los procedimientos rela	13/03/14	13/03/14	1	11
13	**Análisis de Riesgos**	11/03/14	16/04/14	27	
14	Definición de una metodología d	11/03/14	11/03/14	1	
15	Realizar el levantamiento de info	12/03/14	12/03/14	1	14
16	Creación de un inventario de act	13/03/14	13/03/14	1	15
17	Evaluación de los activos a ser p	14/03/14	21/03/14	6	16

ANEXO 22
CRONOGRAMA DE SEDES DE AUDITORíA

CRONOGRAMA DE AUDITORIA SSS DEL 13 DE MAYO AL 13 DE JUNIO DEL 2014						
ITEM	LOCAL	DIRECCION	DISTRITO	AREA/DPTO	RESPONSABLE	FECHA
1	SUNAT	AV. NICOLAS AYLLON 017	SAN LUIS	SISTEMAS	MAURO VENTO	13/05/2014
2	SUNAT	Avenida Nicolás de Piérola 589	CERCADO	INFORMATICA	LIDIA ACEVEDO	13/05/2014
3	SCOTIABANK	RICARDO ANGULO 791	SAN ISIDRO	SISTEMAS	MAURO VENTO	13/05/2014
4	SCI	Jr. Puno 181	CERCADO	INFORMATICA	LIDIA ACEVEDO	13/05/2014
5	AFP INTEGRA	AV. CANAVAL Y MOREYRA 522	SAN ISIDRO	SISTEMAS	ANTONIO SOLIS	14/05/2014
6	CREDISCOTIA	AV. JAVIER PRADO ESTE 4200 CC JOCKEY PLAZA - TDA. 146-A	SURCO	SISTEMAS	ANTONIO SOLIS	14/05/2014
7	SUNAT	CARRETERA CENTRAL KM 4.2	SANTA ANITA	INFORMATICA	LIDIA ACEVEDO	14/05/2014
8	SUNAT	AV. BENAVIDES 222	MIRAFLORES	DATA CENTER	MAURO VENTO	15/05/2014
9	SUNAT	RICARDO ANGULO 791	SAN ISIDRO	DATA CENTER	LIDIA ACEVEDO	15/05/2014
10	ALBIS	Calle Los Negocios 185	SURQUILLO	SISTEMAS	MAURO VENTO	15/05/2014

11	DIMERC	Ricardo Angulo 873	SAN ISIDRO	DATA CENTER	LIDIA ACEVEDO	16/05/2014
12	PRODUCE	Calle Uno 060 Corpac	SAN ISIDRO	SISTEMAS	MAURO VENTO	16/05/2014
13	MINISTERIO DE DEFENSA	AV. AVENIDA DE LA PERUANIDAD #S/N	JESUS MARIA	INFORMATICA	LIDIA ACEVEDO	19/05/2014
14	MINISTERIO DE EDUCACION	AV. AVENIDA LA POESIA #155	SAN BORJA	INFORMATICA	LIDIA ACEVEDO	20/05/2014
15	SUNAT	AV. GAMARRA Nro. 680-CHUCUITO	CALLAO	SISTEMAS	MAURO VENTO	22/05/2014
16	AUSA	Av. Elmer Faucet S/N - Centro Aéreo Comercial Of. 301-C Sector B	CALLAO	INFORMATICA	ANTONIO SOLIS	12/06/2014
17	AUSA	AV. Oquendo Mza. H.R. Lote. 1 CALLAO	VENTANILLA	INFORMATICA	ANTONIO SOLIS	12/06/2014
18	PODER JUDICIAL	Av. Abancay Cdra. 8	CERCADO	SISTEMAS	LIDIA ACEVEDO	13/06/2014
19	PODER JUDICIAL	Av. Lima Cuadra 24 Urb. San Martín de Porres	SMP	SISTEMAS	ANTONIO SOLIS	13/06/2014
20	PODER JUDICIAL	Av. Carlos Izaguirre Nº 176 5º. Piso Edificio Nuevo	INDEPENDENCIA	SISTEMAS	MAURO VENTO	13/06/2014
21	PODER JUDICIAL	Paradero 13 de la Av. Wiesse	SJL	SISTEMAS	ANTONIO SOLIS	13/06/2014

ANEXO 23
CUESTIONARIO DE AUDITORíA

PREGUNTA	CUMPLE?	
	SI	NO
1. ¿Se tiene definidas y documentadas las políticas de seguridad?	X	
2. ¿Se está aplicando en todos los puntos de atención?	X	
3. ¿Se están revisando los requerimientos de confidencialidad?	X	
4. ¿Se está definiendo procesos de autorización de nuevos medios de transmisión de datos?	X	
5. ¿Se cuenta con un proceso para clasificar y etiquetar activos?	X	
6. ¿ Se tiene establecida, documentada y actualizadas las políticas de acceso a los medios?	X	
7. ¿No se cuenta con controles criptográficos?		X
8. ¿Se cuenta con alarmas para detectar intrusos o PIN para el acceso a áreas restringidas?		X
9. ¿Los empleados cuentan con carnet de identificación?		X
10. ¿Se realiza capacitación constante?	X	
11. ¿Se usa algún registro o bitácora para el registro de incidentes?	X	
12. ¿Se cuenta con un registro de auditorías?	X	

ANEXO 24
EJEMPLO DE MÉTRICAS

Algunas de las métricas elaboradas en este proyecto.

MEDIDA	MT_SATISFACCIÓN DEL USUARIO
PROPÓSITO	MEDIR EL NIVEL DE SATISFACCION DE LOS USUARIOS.
CLIENTE	BARREDA MOLLER
MÉTODO DE MEDIDA	RESULTADOS FAVORABLES/TOTAL ENCUESTADOS
ESCALA	A: 1.0 (PERFECTO) B: [0.8, 1> (MUY BUENO) C: [0.6, 0.8> (BUENO) D: [0.4, 0.6> (ACEPTABLE) E: [0.2, 0.4> (REGULAR) F: [0.0, 0.2> (MALO) G: 0.0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO A ENCUESTAR A LOS USUARIOS Y SEGÚN LAS REPUESTAS OBTENIDAS ESTIMO EL PORCENTAJE FINAL.
COBIT 5	MEA03. SUPERVISAR, EVALUAR Y VALORAR LA CONFIRMIDAD CON LOS REQUERIMIENTOS EXTERNOS
FUENTE DE MEDICION	USUARIOS DE BARREDA MOLLER
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

MEDIDA	MT_SATISFACCIÓN DE LA ALTA GERENCIA
PROPÓSITO	MEDIR EL INDICE DE SATISFACCION DE LOS GERENTES
CLIENTE	SSS
MÉTODO DE MEDIDA	RESULTADOS FAVORABLES/TOTAL ENCUESTADOS
ESCALA	A: 1.0 (PERFECTO) B: [0.8, 1> (MUY BUENO) C: [0.6, 0.8> (BUENO) D: [0.4, 0.6> (ACEPTABLE) E: [0.2, 0.4> (REGULAR) F: [0.0, 0.2> (MALO) G: 0.0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO A ENCUESTAR A LOS GERENTES Y SEGÚN LAS REPUESTAS OBTENIDAS ESTIMO EL INDICE FINAL.
COBIT 5	MEA02. SUPERVISAR, EVALUAR Y VALORAR ELSISTEMA DE CONTROL INTERNO.
FUENTE DE MEDICION	GERENTES DE SSS
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

MEDIDA	MT_EMPLEADOS CERTIFICADOS
PROPÓSITO	MEDIR EL INDICE DE EMPLEADOS CERTIFICADOS EN LA CAPACITACION
CLIENTE	SSS
MÉTODO DE MEDIDA	#APROBADOS/#TOTAL.EVALUADOS
ESCALA	A: 20 (PERFECTO) B: [17, 19> (MUY BUENO) C: [15, 17> (BUENO) D: [13, 15> (ACEPTABLE) E: [11, 13> (REGULAR) F: [00, 11> (MALO) G: 0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO A DETERMINIAR EL TOTAL DE COLABORADORES APROBADOS Y SEGÚN EL TOTAL DE EMPELADOS DE LAEMRPESA SE DETERMINO ELPORCENTAJE DE APROBADOS Y CERTIFICADOS.
COBIT 5	MEA02. SUPERVISAR, EVALUAR Y VALORAR ELSISTEMA DE CONTROL INTERNO.
FUENTE DE MEDICIÓN	PERSONAL DE SSS
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

MEDIDA	MT_TIEMPO DE RESPUESTA
PROPÓSITO	MEDIR TIEMPO DE RESPUESTA EN LAS ATENCIONES
CLIENTE	SSS
MÉTODO DE MEDIDA	T.RPTA=T.ACTUAL-T.INCIAL
ESCALA	A: 20 (PERFECTO) B: [17, 19> (MUY BUENO) C: [15, 17> (BUENO) D: [13, 15> (ACEPTABLE) E: [11, 13> (REGULAR) F: [00, 11> (MALO) G: 0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO A COMPARAR EL TIEMPO QUE EN PROMEDIO DE DEMORABA EN ATENDER UN PEDIDO CONTRA EL TIEMPO ACTUAL.
COBIT 5	MEA02. SUPERVISAR, EVALUAR Y VALORAR ELSISTEMA DE CONTROL INTERNO.
FUENTE DE MEDICIÓN	PERSONAL DE SSS
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

MEDIDA	MT_FRECUENCIA_REUNIONES_GENRENTES
PROPÓSITO	MEDIR LA FRECUENCIA DE REUNIONES DE LOS GERENTES
CLIENTE	SSS
MÉTODO DE MEDIDA	PROM.REUS=TOTAL.REUS.MENSUAL/22
ESCALA	A: 20 (PERFECTO) B: [17, 19> (MUY BUENO) C: [15, 17> (BUENO) D: [13, 15> (ACEPTABLE) E: [11, 13> (REGULAR) F: [00, 11> (MALO) G: 0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO A REGISTRAR LAS REUNIONES REALIZADAS POR PARTE DE LAS CABEZAS DE LA ORGANIZACIÓN Y PROMEDIARLAS PARA DETERMINAR ELPROMEDIO MENSUAL.
COBIT 5	
FUENTE DE MEDICIÓN	PERSONAL DE SSS
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

MEDIDA	MT_SALVAGUARDAS_APROBADOS
PROPÓSITO	MEDIR EL PORCENTAJE DE MEDIDAS SALVAGUARDAS APROBADAS POR PARTE DE LA GERENCIA.
CLIENTE	SSS Y TODOS LOS CLIENTES
MÉTODO DE MEDIDA	%ACEPTACION=SALVAG.APROB/TOTAL.SALVAG.
ESCALA	A: 20 (PERFECTO) B: [17, 19> (MUY BUENO) C: [15, 17> (BUENO) D: [13, 15> (ACEPTABLE) E: [11, 13> (REGULAR) F: [00, 11> (MALO) G: 0 (MUY MALO)
PROCEDIMIENTO	SE PROCEDIO TOTALIZAR LAS MEDIDAS ESTABLECIDAS, Y PROMEDIARLAS EN BASE A LAS MEDIDAS APROBABAS.
COBIT 5	MEA02. SUPERVISAR, EVALUAR Y VALORAR ELSISTEMA DE CONTROL INTERNO.
FUENTE DE MEDICIÓN	PERSONAL DE SSS Y CLIENTES
ALCANCE O DOMINIO	PERSONAL QUE LABORA EN LA EMPRESA.

ANEXO 25
INFORME DE AUDITORíA

INTRODUCCIÓN

1. ORIGEN DEL EXAMEN

El grupo de trabajo ha elaborado un informe de Auditoria para el periodo comprendido entre del 13 de mayo al 13 de junio del 2014, en cumplimiento a las políticas y estándares de calidad.

El Área de Sistemas de Systems Support & Services requiere saber si los controles implantados en la fase de ejecución están cumpliendo con reducir los niveles de riesgo a los que se encontraron expuestos los activos de TI y la información sensible de la empresa.

2. NATURALEZA Y OBJETIVOS DE LA EVALUCIÓN

Se llevó a cabo, la evaluación al área de Sistemas perteneciente a la gerencia Soluciones de Infraestructura de Systems Support & Services S.A., y sus centros de atención de carácter programada y cuyos objetivos fueron los siguientes:

3. OBJETIVO GENERAL

Evaluar si los controles de seguridad de la información implantados son los más adecuados para el cumplimiento de los objetivos del proyecto, así mismo, establecer si se está administrando adecuadamente los riesgos tecnológicos relacionados al área de sistemas y los Data Center en cada uno de los centros de atención.

4. OBJETIVOS ESPECÍFICOS

- ✓ Evaluar si los niveles de riesgo identificados inicialmente han disminuido.
- ✓ Determinar si la protección de os activos de información son los idóneos.

5. ALCANCE DE LA EVALUACIÓN

El presente documento tiene como alcance la central de la empresa Systems Support & Services S.A , el almacén de la empresa, así como cada uno de los puntos de atención, esta evaluación tendrá un periodo de estudio de dos meses comprendido entre los meses del 22 de MAYO al 13 de JUNIO del 2014.

6. PROCEDIMIENTOS Y TÉCNICAS DE AUDITORIA

Para la realización del presente informe se han tenido en cuenta procedimientos para cada objetivo específico propuesto, los cuales se encuentran disponibles en el Plan de Trabajo.

7. ASPECTOS DE CONTROL

El desarrollo de la auditoria, así como, la evaluación del Informe resultante, se debe efectuar de acuerdo a la normativa vigente de control.

Normas a ser aplicadas en la auditoria:

1. ISO 27001.
2. Normas del COBIT v 5.0.

8. ANTECEDENTES Y BASE LEGAL DE LA ENTIDAD

8.1. ANTECEDENTES

Systems Support & Services S.A, empresa integradora de tecnología fue fundada el 18 de Agosto de 1989 por el ingeniero Luis Reátegui Sánchez.

Luego de seleccionar cuidadosamente a su personal con base de conocimiento y vocación de servicio, a la empresa empezó a brindar servicios en mantenimiento de equipos a clientes como el Banco de Crédito, Banco del Comercio, entre otros.

En 1994, Systems Support & Services S.A se inicia en las ventas y provisión de infraestructura de TI, alcanzando alianzas con empresas de prestigio como Microsoft, Epson, 3Com y recién en el año 1995 se da la relación comercial con la IBM.

En la actualidad, Systems Support & Services S.A, cuenta con más de 400 clientes para los cuales tiene destinados a aun equipo de profesionales que en su mayor parte se dedican a la atención y servicio 80% de los cuales están dedicados al área de soporte, servicios y comercial y un 20% a las áreas de soporte administrativo, ambas dispuestas a ofrecer un servicio de alta calidad.

8.2. BASE LEGAL

1. Plan de continuidad de negocios.
2. Plan de contingencia de tecnología de la información.
3. Reglamento interno de seguridad y salud en el trabajo.
4. Código de conducta.
5. Reglamento interno de trabajo.

9. OTROS ASPECTOS DE IMPORTANCIA

Para el desarrollo de la auditoria se desarrollaron hallazgos, documentos que serán de utilidad para describir las falencias encontradas, así como su impacto, entre otros, dicha documento posee la siguiente estructura:

a) SUMILLA

Es el título o encabezamiento que resume la observación.

b) SITUACIÓN

También conocida como condición, la cual se refiere al hecho irregular o deficiencia determinada, cuyo grado de desviación debe ser sustentada y demostrada con evidencias.

c) CRITERIO

Es la norma o estándar técnico-profesional que permiten al auditor tener la convicción de que es necesario superar una determinada acción u omisión. Los más comunes criterios a ser empelados en la auditoria son: Las normas judiciales vigentes, las normas técnicas o estándares profesionales, las opiniones de expertos, indicadores de gestión, índices de desempeño, entre otros.

a) EFECTO

Es la consecuencia que ocasiona la observación.

b) SITUACIÓN

También conocida como condición, la cual se refiere al hecho irregular o deficiencia determinada, cuyo grado de desviación debe ser sustentada y demostrada con evidencias.

c) CRITERIO

Es la norma o estándar técnico-profesional que permiten al auditor tener la convicción de que es necesario superar una determinada acción u omisión. Los más comunes criterios a ser empelados en la auditoria son: Las normas judiciales vigentes, las normas técnicas o estándares profesionales, las opiniones de expertos, indicadores de gestión, índices de desempeño, entre otros.

d) EFECTO

Es la consecuencia que ocasiona la observación.

d) CAUSA

La razón fundamental por la que ocurrió la condición o el motivo por el cual no se cumplió un criterio o norma.

e) RECOMENDACIÓN

Las medidas que se deben adoptar para mitigar las falencias.

f) CONCLUSIÓN

La conclusión final obtenida del hallazgo realizado.

10. EVALUACIÓN DE LA SITUACIÓN DE LA ACTIVIDAD

En base a la evaluación realizada dentro de la empresa Systems Support & Services S.A., se ha podido encontrar algunas deficiencias de control interno, las cuales se mostrarán en el desarrollo del proyecto, en base a ello se formuló una serie de recomendaciones de acuerdo a las buenas prácticas establecidas en la metodología de evaluación empleada, ISO 27002:2013 y COBIT 5.0. Estas recomendaciones que se detallaran más adelante en este informe.

11. PERSONAL ENCARGADO DEL EXAMEN

El equipo de auditoria estará integrado por el siguiente personal:

Nro.	Nombres y Apellidos	Cargos
01	Acevedo Clemente, Lidia.	Coordinadora de seguridad y calidad.
02	Solis Gayoso, Antonio.	Jefe de sistemas.
03	Pineda Ramirez, Jose.	Gerente de Infraestructura (Supervisor).
04	Vento Meza, Mauro	Auditor Junior

12. FECHA DE INICIO Y TÉRMINO

El presente trabajo se ha realizado, de acuerdo al Plan de Trabajo establecido, desde el 13 de mayo al 13 de junio del presente año y que son detallados en el Plan de Trabajo.

ANEXO 26

REGISTRO DE DISCONFORMIDADES

<table>
<tr><td colspan="3">Medida correctiva Nro.1</td></tr>
<tr><td colspan="3">Descripción de la no-conformidad:

Algunos usuarios no siguen las políticas establecidas, ni siguen lo explicado en las jornadas de capacitación, teniendo acceso a redes sociales, como a páginas de dudosa procedencia.</td></tr>
<tr><td>No-conformidad identificada en: SUNAT-Miraflores</td><td>Nombre de la persona que identificó la no-conformidad
LIDIA ACEVEDO CLEMENTE</td><td>Firma</td></tr>
<tr><td colspan="3">Causa de la no-conformidad:
Dicha deficiencia es generada por los responsables de Sistemas por no asistir a las capacitaciones concienciación en la organización, por ende no se tiene conciencia de las consecuencias que se puede causar.</td></tr>
<tr><td colspan="3">Es necesario tomar medidas correctivas: SÍ - NO (marcar con un círculo)</td></tr>
<tr><td colspan="3">Medida correctiva a implementar:
Las medidas establecidas para poder mitigar la disconformidad detectada es someter a los usuarios a la capacitación a al cual no asistieron, así como designar a un supervisor que monitoree el tratamiento de la información sensible y que configure la red de tal manera que no se tenga acceso a sitios indebidos.</td></tr>
</table>

ANEXO 27

PROCEDIMIENTO DE ACCIONES CORRECTIVAS Y PREVENTIVAS

1. Objetivo, alcance y usuarios

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de registros de correcciones, como también de medidas correctivas.

Este procedimiento se aplica a todas las actividades implementadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son todos los empleados de Systems Support & Services S.A.

2. Documentos de referencia

- Normas ISO/IEC 27001:2013 e ISO/IEC 27002: 2013.
- Estándar Internacional COBIT 5.0.
- Reglamento interno de seguridad y salud en el trabajo.
- Código de conducta.
- Reglamento interno de trabajo.

3. Correcciones y medidas correctivas

3.1. No conformidades y correcciones

De la visita realizada al cliente SUNAT, ubicado en la Avenida Benavides 222, se detectó que los operarios del dentro de computo no siguen las políticas establecidas, ni siguen lo explicado en las jornadas de capacitación, teniendo acceso a redes sociales, como a páginas de dudosa procedencia.

3.2. Medidas correctivas

Las medidas establecidas para poder mitigar la disconformidad detectada es someter a los usuarios a la capacitación a al cual no asistieron, así como designar a un supervisor que monitoree el tratamiento de la información sensible y que configure la red de tal manera que no se tenga acceso a sitios indebidos.

ANEXO 28

ACTA DE CIERRE DEL PROYECTO

<table>
<tr><td colspan="4">ACTA DE CIERRE</td></tr>
<tr><td colspan="4">Información General</td></tr>
<tr><td>Nombre del Proyecto:</td><td colspan="2">APLICACIÓN DE NORMATIVAS DE SEGURIDAD LA DE INFORMACION PARA SYSTEMS SUPPORT & SERVICES S.A.</td><td>Fecha de Preparación:</td><td>04/07/2014</td></tr>
<tr><td>Preparado por:</td><td>Mauro Luis Vento Meza</td><td>Aceptado por:</td><td colspan="2">Gerencia de Soluciones de Infraestructura</td></tr>
<tr><td colspan="4">Hoy 04 de Julio del 2014, siendo las 5: 00 PM, se procede al cierre del proyecto " APLICACIÓN DE NORMATIVAS DE SEGURIDAD LA DE INFORMACION PARA SYSTEMS SUPPORT & SERVICES S.A." en el área de sistemas de la empresa Systems Support & Services S.A.</td></tr>
<tr><td colspan="4">Declaración formal de aceptación del proyecto</td></tr>
<tr><td colspan="4">Por parte de la presente se deja constancia que el proyecto a cargo de " MAURO LUIS VENTO MEZA", ha sido aceptado y aprobado por la Gerencia de Soluciones de Infraestructura, dando constancia por la presente que el proyecto ha culminado exitosamente.</td></tr>
</table>

ANEXO 29
METAS DE TI SEGUN COBIT 5

DIMENSION DE TI	ID	METAS DE INFORMACION Y TECNOLOGIA RELACIONADA
FINANCIERA	1	Alineamiento de TI y estrategia de negocio.
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
	4	Riesgos de negocio relacionados con las TI gestionados.
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.
	6	Transparencia de los costes, beneficios y riesgos de las TI.
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas.
INTERNA	9	Agilidad de las TI.
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.
	11	Optimización de activos, recursos y capacidades de las TI.
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones.
	15	Cumplimiento de las políticas internas por parte de las TI.
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado.
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio.

ANEXO 30
CUERPO NORMATIVO

1. Objetivo

La organización, sustenta su actividad principal de servicios en el soporte y mantenimiento tecnológico mediante los sistemas de información, siendo este un soporte básico de la operativa interna, tanto a funciones comerciales como a las funciones de gestión. Los sistemas, programas, infraestructuras de comunicación, ficheros, bases de datos, etc., que tratan información de sus clientes constituyen el activo principal de la organización, de tal manera que el daño o perdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la información.

La política de seguridad de la información, proporciona las bases para definir y delimitar los objetivos y responsabilidades para diversas actuaciones técnicas y organizativas que se requieran para garantizar, la seguridad de la información, cumpliendo el marco legal de aplicación y las directivas, políticas específicas y procedimientos definidos.

Estas actuaciones son seleccionadas e implantadas en base al análisis de riesgos y el equilibrio entre el riesgo aceptable y costo de las medidas.

El comité de seguridad de la información, en adelante CSI, junto con los responsables de los activos de información son quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de distintos elementos de la actividad realizada, de modo que los procesos más importantes y/o sensibles reciban mayor protección.

Es responsabilidad de la Dirección de la organización y del CSI, promover y apoyar la implantación de las medidas y técnicas organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio.

El objeto de esta política es alcanzar una protección adecuada de la información de la organización, dentro de un alcance definido para el Sis

tema de Gestión de Seguridad de la Información, preservando los siguientes principios de seguridad:

Confidencialidad: Garantizar que la información sea accesible solo para quien este autorizado a tener acceso a la misma.

Integridad: Garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.

Disponibilidad: Garantizar que los usuarios autorizados tienen acceso cuando lo requieren a la información y sus activos asociados.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de la organización o fuera de ellas.

Así mismo, estos principios deberán contemplar en las siguientes áreas de seguridad:

Física: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.

Lógica: Incluyendo los aspectos de protección de las aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos.

Político-corporativa: Formada por los aspectos de seguridad relativos a la propia compañía, a las normas internas, regulaciones y normativa legal.

2. Alcance

La presente política es aplicable a todos los procesos de negocio definidos dentro del alcance del SGSI, así como a todas las personas que tengan acceso a la información objeto de alcance, y/o presten servicios para la organización. El alcance del Sistema de Gestión de Seguridad de la Información se acota a:

Gestión de la seguridad de la información en el soporte y mantenimiento de aplicaciones informáticas.

3. Declaración de intenciones por parte de la dirección

El gerente de la organización, es consciente de la importancia que tiene para la compañía la seguridad de la información de cara conseguir un grado óptimo de competitividad en el mercado actual.

Por ello, la organización ha desarrollado la presente política de seguridad y las correspondientes normas que garantizan la confidencialidad, integridad y disponibilidad de la información.

La dirección ha pretendido definir los procesos más adecuados para que la organización emprenda un proceso de mejora de sus Sistemas de seguridad de la Información con el convencimiento que redundara en una mayor eficacia de sus procesos de producción. Por ello cuando se detallen las aplicaciones o soluciones concretas a los puntos contenidos en el presente documento, se hará bajo dicha perspectiva, potenciando en lo posible aquellas soluciones que lleven seguridad a la información relevante de la organización.

La intención final de todo sistema definido y desarrollado, es la de ofrecer el mejor servicio a nuestros clientes, mejorando nuestros procesos y respetando escrupulosamente sus derechos legalmente establecidos.

Por todo ello, la dirección de la organización quiere dejar constancia y expresa de su conocimiento y aprobación tales políticas desarrolladas de este documento, de forma que todo el personal la debe de conocer y asumir como una parte de sus funciones laborales.

Para que todo esto sea posible se asignaran los recursos necesarios para el buen desarrollo de lo aquí establecido, tanto en el inicio del proyecto como en su mantenimiento futuro.

Lima, 27 de Junio del 2014

Gerente General | Gerente de Soluciones de Infraestructura

4. **Políticas de seguridad**

- **Crear documentos** donde estén detalladas las políticas, principios y estándares de seguridad de información en su totalidad.
- **Aprobar** por parte de la gerencia, publicar y comunicar a todos los empleados y las partes externas relevantes los documentos de las políticas de seguridad de información.
- **Definir e implementar** un proceso de autorización gerencial para los nuevos medios de procesamiento.
- **Identificar y revisar** regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la empresa para la protección de la información.
- **Documentar e implantar** las reglas de uso aceptable de la información.
- **Proteger** las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.
- **Proporcionar** un apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales conforme sean relevantes para su función laboral.

5. **Incumplimiento de la política**

El incumplimiento de estas obligaciones por parte del personal podrá dar lugar a las medidas disciplinarias correspondientes y al ejercicio de los procesos legales de la empresa.

6. Procedimientos de negocio

6.1. Mantenimiento Preventivo

Objetivo:	Establecer, documentar y mantener un procedimiento para la ejecución de las actividades requeridas para el Mantenimiento Preventivo de Impresoras y Multifuncionales, con la finalidad de asegurar un servicio de calidad.
Alcance:	Se aplica al mantenimiento preventivo de impresoras y multifuncionales, desde la recepción del requerimiento hasta la entrega del equipo verificado por el cliente.

Nº	Responsable	Descripción
ELABORAR CRONOGRAMA DE MANTENIMIENTOS PREVENTIVOS (TENTATIVOS)		
1	Gestor de Impresión	En base al F-Se-St-013 Cuadro Anual de Mantenimientos Preventivos Lima, creado a inicio de cada año, informar al STI con 2 semanas de anticipación el registro del formato: F-Se-St-014 Cronograma de Mantenimiento Preventivo para su evaluación.
COORDINAR CON EL GESTOR		
2	STI	¿Aprueba F-Se-St-014 Cronograma de Mantenimiento Preventivo? NO: Ir a la Actividad 1. SI: Ir a la Actividad 3.

3	Gestor de Impresión	¿El cliente aprueba F-Se-St-014 Cronograma de Mantenimiento Preventivo? NO: Ir a la Actividad 1. SI: Enviar un correo electrónico al STI, confirmando la programación del mantenimiento preventivo.
4	STI	Informar al Coordinador de Impresión el F-Se-St-14 Cronograma de Mantenimiento Preventivo, por correo electrónico, para realizar la asignación al RTN2. Ir a la Actividad 5.
VERIFICAR CONDICIONES		
5	Coordinador de Impresión	De acuerdo al Cronograma de Mantenimientos, enviar correo electrónico a Service Desk para la creación del ticket tipo requerimiento y la asignación del RTN2. Nota: El Gestor de Impresión y/o RT N1 debe de comunicar y/o confirmar al usuario final, la hora, fecha y nombre del técnico de mantenimiento.
6	RTN2	Debe contar con los implementos de limpieza necesarios para la labor del Mantenimiento Preventivo: - Spray limpiador de contactos: Para dispositivos eléctricos/electrónicos. - Líquido de limpieza de cubiertas, alcohol isopropílico, líquido siliconado. - Aspiradora de servicio (de ser necesario), trapos de algodón blancos, y herramientas descritas en Lista de Herramientas e Implementos para un Técnico. - Mascarillas y guantes de látex.
VERIFICAR OPERATIVIDAD DEL EQUIPO		

7	RTN2	Se realizara pruebas de operatividad del equipo (Copias, Impresión, Fax, Escaneo, etc.). ¿Paso las pruebas de operatividad? SI: Proceder a dar el servicio. Ir a la actividad 9. NO: Informar al cliente la falla encontrada en el equipo al momento que sea detectada y luego se ejecutara el mantenimiento preventivo una vez solucionada la falla. Ir a la Actividad 12 Nota: En el caso que no se pueda realizar la prueba de operatividad del equipo, no se realizara el mantenimiento preventivo.

EJECUTAR EL MANTENIMIENTO PREVENTIVO		
	RTN2	<u>Limpieza de Hardware</u> <u>Al inicio</u> - Asegurarse que el equipo se encuentre apagado y desconectado. - Según sea el caso, retirar el equipo al área destinada por el cliente para realizar el mantenimiento preventivo. <u>Limpieza interna</u>: a) Abrir las cubiertas y bandejas del equipo. b) Desarmar o retirar partes del equipo necesarias como: cubiertas, bandejas, cartucho de tóner, cilindro, módulo fusor, ensambles de transporte del papel y área xerográfica. c) Retirar el polvo y/o suciedad con la ayuda de una aspiradora de servicio, brocha, trapo. d) Aplicar limpia contactos a las áreas que lo requieran. e) Armar el equipo. f) Colocar las cubiertas del equipo. <u>Limpieza externa:</u> a) Realizar la limpieza de las cubiertas externas con CopyCleaner y si es necesario alcohol isopropílico. b) Para el acabado final, utilizar un material siliconado. <u>Al final:</u> - Concluido el Mantenimiento Preventivo del Equipo, instalarlo en su respectiva ubicación. - Dejar el área de trabajo limpia.

REALIZAR PRUEBAS DE VERIFICACIÓN		
9	RTN2	Verificar el funcionamiento de la impresora realizando pruebas por cada bandeja, impresión y copia en modo simple y dúplex, alimentador de documentos, accesorios y otras funciones. Llenar el F-Se-St-029 Check List de Mantenimiento Preventivo de Impresoras/Multifuncionales. ¿Pasó la prueba de verificación? SI: Ir a la actividad 10. NO: Ir a la actividad 11. Nota: Llenar 01 check list por cada equipo.
CONTROL DE CALIDAD		

10	RTN2	Llenar F-Se-St-001 Guía de Ingeniería, imprimir la hoja de configuración del equipo y contadores. ¿Conformidad del cliente? NO: Ir a la actividad 11. SI: Ir a la actividad 13.
REALIZAR LABOR CORRECTIVA SOBRE EL MANTENIMIENTO PREVENTIVO		
11	RTN2	Revisar el equipo y solucionar cualquier falla que presente. ¿La falla persiste, requiere servicio de mantenimiento correctivo? NO: - Si el caso se debió a que no haya pasado la prueba de verificación. Ir a la Actividad 10. - Si el caso se debió a que el cliente no haya brindado la conformidad. Ir a la Actividad 11. SI: Definir la falla. Informar al usuario la falla encontrada en el equipo, en el momento que es detectada. A su vez al Coordinador de Impresión. Ir a la Actividad 12.

12	RTN2	Solicitar a Service Desk la creación de un ticket tipo incidente (Padre-Hijo), ir al procedimiento: P-Se-001 Service Desk Gestión de Configuraciones y Diagnóstico. A su vez el registro del caso en el formato: F-SGC-009 Reporte de Servicio No Conforme. Nota: Al culminar la atención del ticket tipo incidente. Ir a la Actividad 8.
CONFORMIDAD DEL SERVICIO		
14	RTN2	Junto con el equipo revisado, entregar al cliente la F-Se-St-001 Guía de Ingeniería y F-Se-St-029 Check List de Mantenimiento Preventivo de Impresoras/Multifuncionales, para dar la conformidad del servicio. Ir al procedimiento: P-Se-001 Service Desk Gestión de Configuraciones y Diagnóstico - ACTUALIZAR BD DE INCIDENTES O PETICIÓN DEL SERVICIO.
ENTREGA DE INFORME		
15	Coordinador de Impresión	Elaborar el Informe del Mantenimiento Preventivo al culminar todos los Mantenimientos Preventivos programados por cliente, adjuntando los reportes del servicio y enviarlo al Supervisor de Técnicos de Impresión para su revisión.

16	Supervisor de Técnicos de Impresión	El Supervisor de Técnicos de Impresión lo revisa y lo envía al Gestor de Impresión.
17	Gestor de Impresión	Enviar el Informe del Mantenimiento Preventivo en forma digital y/o físico, adjuntando los reportes del servicio al Cliente. *Fin de proceso*.

Elaborado por:RED	**Revisado por:** JSI	**Aprobado por:** GO

6.2. Mantenimiento Correctivo

Objetivo:	Establecer, documentar y mantener un procedimiento para la ejecución del proceso de mantenimiento correctivo de impresoras y multifuncionales en la atención del requerimiento del cliente, con la finalidad de asegurar un servicio de calidad.
Alcance:	Comprende desde la revisión de la información requerida para iniciar el proceso de mantenimiento correctivo hasta la reparación del equipo.

Nº	**Responsable**	**Descripción**
REVISAR INFORMACIÓN		
1	RT N2	Recepcionar los datos y la descripción del requerimiento de servicio o incidente brindada por el cliente, los cuales son alcanzados vía teléfono y/o mail por el RT N1
BRINDA INFORMACIÓN A RTN1		
2	RT N2	Informar al RT N1 su desplazamiento. Estado del ticket: EN DESPLAZAMIENTO Al llegar al cliente, informa a RTN1 su estado de ticket si es EN PROCESO o PENDIENTE POR USUARIO si éste no se encontrase o está usando el equipo.
EJECUCIÓN DE MANTENIMIENTO CORRECTIVO		

3	RTN2	Analizar e investigar la causa del requerimiento o incidente ¿Se logró resolver el incidente reportado? SI: Ir a la actividad 14. NO: ¿La falla es originada por el cliente? SI: Informar al cliente que parte defectuosa será cotizada. Llenar el F-SE-ST-001 Guía de Ingeniería, elaborar el informe técnico F-Se-St-012 Informe de Cliente y luego enviarlo vía email al Supervisor de Técnicos de Impresión. Ir a la actividad 4 NO: Es Gestión de Garantías de Impresión. Ir al procedimiento de "P-Se-006 Gestión de Garantías – PROCESO DE GESTIÓN DE GARANTÍA DE IMPRESIÓN". Luego ir a la actividad 11. Para ambos casos se informa el cambio de estado del incidente al RT N1. Estado del ticket: DIAGNOSTICADO
ANALISIS DEL INFORME AL CLIENTE		
4	STI	Revisa y controla el informe técnico: F-Se-St-012 Informe al Cliente y lo envía al Gestor y/o JSI.
SOLICITAR COTIZACIÓN A PROVEEDORES		
5	Gestor de Impresión / JSI	Solicitar cotización a proveedores: vía e-mail y/o sistema de la marca. Ver documento: F-Ad-Lo-002 Lista de Proveedores Críticos.

6	Gestor de Impresión / JSI	Llenar el F-Ad-001 Cuadro de Costo, donde se registra los costos, mano de obra y utilidad del servicio.
COTIZAR AL CLIENTE		
7	Gestor de Impresión / JSI	Llenar F-Se-St-004 Cotización y adjuntar el F-Se-St-012 Informe al Cliente elaborado por el RT N2 a la cotización y luego enviar al cliente y comunica a RT N1 para la actualización del estado de Ticket: COTIZACIÓN ENVIADA
10	Gestor de Impresión / JSI	Cliente acepta: Recepciona documentos de Aprobación: Boucher de pago, u Orden de Compra formal. (Excepciones: Correo electrónico) y comunica a Jefe de Producto para la generación de ID y luego lo envía Logística para la compra respectiva. Procedimiento P-Ad-Lo-001 Logística - COMPRA DE PARTES O REPUESTOS A su vez comunica a RTN1, lo cual actualiza el Estado de ticket: COTIZACIÓN ACEPTADA o en su defecto; Cliente no acepta: RTN1 actualiza el Estado de ticket: COTIZACIÓN NO APROBADA *Fin de Proceso/Cierre de Ticket*
EJECUTAR MANTENIMIENTO CORRECTIVO EN CASO DE CAMBIO DE PARTE O REPUESTO		
11	RTN1	Informa al RT N2 la llegada de la parte y el número de ticket del incidente. Estado de Ticket: PARTES RECIBIDAS
12	RT N2	Revisar las partes que llegan por garantías o compras efectuadas por el área de logística para el reemplazo de las partes dañadas.
EJECUTAR MANTENIMIENTO		
13	RT N2	Reparar el equipo según la información brindada en el Manual de Servicio del modelo del equipo de Impresión, para el reemplazo de la(s) parte(s) solicitada(s) y solucionar la falla. Informar a RTN1 el cambio de estado de la llamada. Estado del ticket: INICIO DE REPARACION. Hacer uso de las herramientas e implementos descritos en el Anexo: Lista de Herramientas e Implementos para un Técnico.

REALIZAR PRUEBAS DE VERIFICACIÓN		
14	RT N2	*Realizar las pruebas de las funciones configuradas en el equipo con el cliente.
15	RT N2	¿Pasó la Prueba de Verificación? SI: Ir a la actividad 16. NO: Informar a RTN1 el nuevo diagnóstico, para que éste realice la actualización en el sistema de Service Desk. Ir a la actividad 3. En los casos que la parte recibida se encuentre defectuosa, se informa a RTN1 para que coordine con el CGA el cambio del mismo. Ir al procedimiento: P-Ad-Lo-001 Logística - COMPRA DE PARTES O REPUESTOS - COMUNICARSE CON PROVEEDOR. En ambos casos se informara al cliente el estado de las pruebas de verificación y se solicitara a RTN1 el registro del caso en el F-SGC-009 Reporte de Servicio No Conforme.
SERVICIO ONSITE		
16	RT N2	Presentar la F-Se-St-001 Guía de Ingeniería llenada al cliente, para obtener su firma de conformidad del servicio brindado. Ir a la actividad 17.
MANTENIMIENTO CORRECTIVO SOLUCIONADO		
17	RT N2	Informar a RTN1 el recojo del repuesto defectuoso y/o reingreso de la parte no usada, si lo hubiese. Estado del ticket SOLUCIONADO. Entregar al RT N1 la copia de la F-Se-St-001 Guía de Ingeniería firmada por el cliente, dentro de un plazo de 2 días hábiles después de realizado el servicio.

6.3. Service Desk y Configuraciones

Objetivo:	Establecer, documentar y mantener un procedimiento para atender y registrar los incidentes y/u requerimientos de servicio que solicitan los usuarios del servicio de Service Desk.
Alcance:	Se aplica a todo servicio solicitado al Service Desk

Nº	Responsable	Descripción
SOLICITAR ATENCIÓN AL SERVICE DESK (SD)		
1	Usuario	Comunicarse con el Service Desk (SD) mediante los distintos medios disponibles: teléfono, correo y/u otros.
RECIBIR SOLICITUD		
2	RT N1	Recibir el requerimiento. Saludar: “Service Desk buenos días/tardes/noches, lo saluda: Nombre RTN1 ¿En qué podemos ayudarlos?”. Nota: La información recepcionada vía telefónica y/o otros debe encontrarse completa. Si no se solicitara al cliente los datos necesarios (Ver: Procedimiento de Requerimientos de Servicio a SS&S) para definir el tipo de servicio.
VERIFICAR SOLICITUD CREADA		
3	RT N1	Verificar si la solicitud ha sido reportada anteriormente. ¿Es una solicitud nueva? SI: Ir a la actividad 4 NO: Verificar el estado del ticket que se encuentra en el sistema y brindar los detalles del mismo al usuario. *Fin de proceso.*
DEFINIR TIPO DE SERVICIO		

4	RT N1	Definir el tipo de servicio requerido (A, B, C, D). Ver: La Lista de Compromisos de Servicios, donde se detalla todos los acuerdos establecidos entre Systems Support & Services y el cliente asimismo la organización asigna a un responsable para cada cliente con la finalidad que verifique y realice seguimiento a todos los requisitos acordados. A (Contratos). Clientes que se encuentran dentro de la Lista de Compromisos. B (Gestión de Garantía): *Seguir el procedimiento P-Se-006 Gestión de Garantías. C (Sin Contrato): Servicio es por cotización * D (Comercial): Producto de una venta Nota: La lista de Compromisos de Servicios de Systems Support & Services S.A. es revisada y actualizada por el jefe de área responsable del servicio, quien lo comunica al RED.

5	RT N1	¿El cliente, usuario o equipo (CI – elemento de configuración) se encuentran registrados? SI: Ir a la actividad 6. NO: Se procederá a realizar el registro en el sistema de Service Desk. Ir a PROCESO DE REGISTRO DE CLIENTE, USUARIO Y CI – ELEMENTO DE CONFIGURACIÓN
REGISTRO DE REQUERIMIENTO DE SERVICIO O INCIDENTE		
6	RT N1	Definir el servicio: Incidente o Requerimiento: <u>Incidente</u>: Interrupción no planificada de un servicio de TI o reducción en la calidad de un servicio de TI. Por ejemplo, el fallo de uno de los discos. <u>Requerimiento:</u> Petición formal por parte de un usuario para que algo sea provisto. Por ejemplo, una solicitud de información o asesoría; restablecer una contraseña o instalar una estación de trabajo para un nuevo usuario. Registrar la información del requerimiento de servicio o incidente * y categorizar el servicio en el Sistema del Service Desk. Estado del ticket: ABIERTO. Para las atenciones del caso Tipo de Servicio: C, ir a la actividad 8, de lo contrario ir a la actividad 7.
SOPORTE INICIAL		

7	RT N1	Evaluar si se puede brindar soporte inicial vía teléfono al requerimiento del servicio o incidente de usuario, buscando la solución del servicio reportado. ¿Puede ser atendido vía teléfono? SI: Brindar Soporte a usuario vía teléfono. Estado de ticket: ASIGNADO Analizar e investigar la causa del requerimiento o incidente Estado de ticket: EN PROCESO Ir a la siguiente pregunta. NO: Ir a la actividad 8. ¿Se logró resolver el requerimiento de servicio o incidente reportado? SI: Ir a la actividad 11. NO: Actualizar estado del ticket en el sistema: REASIGNADO y escalar la atención a RTN2 – Estado de Ticket: CONTACTO CON USUARIO. * Ir a la actividad 9.
ESCALAR Y ASIGNAR		

8	RT N1	Escalar y asignar de acuerdo al tipo de servicio: Para los casos Tipo de Servicio A, D Escalar el requerimiento de servicio o incidente al RT N2 automáticamente vía teléfono y/o vía Mail. Estado del ticket: ASIGNADO Informar al cliente vía correo y/o teléfono, el número de ticket que será atendido. Estado de ticket: CONTACTO CON USUARIO Luego ir a la actividad 9. Para los casos Tipo de Servicio C Escalar el requerimiento al Jefe de Área correspondiente, quien elaborara la cotización al cliente. Estado del ticket: ASIGNADO Informar al cliente el número de ticket que será atendido. Estado de ticket: CONTACTO CON USUARIO. Ir a la actividad 10. Nota: En los casos de servicios fuera de horario de oficina se consulta al F-Se-St-009 Cuadro Mensual de Técnicos de Turno
SEGUIMIENTO A RT N2		

9	RT N1	RT N2 informa la hora de su desplazamiento. Estado del ticket: EN DESPLAZAMIENTO El RT N2 informa su llegada al Cliente e inicio del servicio requerido, y el cambio de estado del ticket si es EN PROCESO o PENDIENTE POR USUARIO si éste no se encontrase o está usando el equipo ¿RTN2 logró resolver el requerimiento de servicio o incidente reportado? SI: Ir a la actividad 11. NO: Actualizar los estados del servicio en el sistema de acuerdo a las indicaciones del RTN2 de acuerdo a los procedimientos: Para los casos de mantenimiento correctivo ir: P-Se-004 Mantenimiento Correctivo. Para los casos de mantenimiento correctivo de impresión ir: P-Se-007 Mantenimiento Correctivo Impresión. Para los casos de mantenimiento preventivo de impresión ir: P-Se-008 Mantenimiento Preventivo Impresión.
SEGUIMIENTO DE COTIZACIÓN		

10	Jefe de área	Informa que la cotización ha sido enviada al cliente. Estado de Ticket: COTIZACIÓN ENVIADA. Luego informa el estado de la cotización. La cotización aceptada? SI: RTN1 Actualizara el estado de ticket: COTIZACIÓN APROBADA. Y luego de acuerdo al tipo de requerimiento continuar con el procedimiento: P-Se-007 Mantenimiento Correctivo Impresión o P-Se-008 Mantenimiento Preventivo Impresión o P-Se-004 Mantenimiento Correctivo. NO: RTN1 Actualiza el estado de ticket: COTIZACIÓN NO APROBADA *Fin de Proceso/Cierre de Ticket* Nota: El estado del ticket: COTIZACIÓN ENVIADA solo estará abierto durante el periodo de 7 días hábiles, y luego se asumirá que el Cliente no acepta la cotización, actualizar el estado de ticket: COTIZACIÓN NO APROBADA *Fin de Proceso/Cierre de Ticket*
ACTUALIZAR BD DE INCIDENTES O REQUERIMIENTO DEL SERVICIO		
11	RT N1	Actualizar la base de datos de Incidentes o requerimiento de servicio. Estado del ticket: SOLUCIONADO. Ir al Proceso de Cierre de Ticket (Actividad 12).
CIERRE DE TICKET		

		Si fuese solucionado por el RTN1/RT GARANTIA: Cambiar estado: CERRADO. Si fuese solucionado por el RTN2: Recepciona el F-Se-St-001 Guía de Ingeniería firmado por el usuario y/o cliente como muestra de conformidad del servicio brindado, para el cierre del ticket.
12	RT N1	¿Usuario brinda conformidad del servicio? SI: Cerrar ticket. NO: Crear nuevo ticket relacionado al número de ticket anterior (Padre – Hijo). Relacionarlo en el Service Desk como Padre/Hijo. Regresar a la actividad 6. Reportar al Coordinador de Centro de Servicios, Gestor de Service Desk y/o STI para que registre el caso en el F-SGC-009 Reporte de Servicio No Conforme. Estado de ticket: CERRADO.

Nota 1: los estados reflejados en el presente procedimiento son aquellos que se usan frecuentemente, de ser necesario mayor detalle de la totalidad de estados

y su migración entre ellos consultar el Flujograma de Proceso: Estados.

6.4. Proceso de registro de cliente, usuario y ci – elemento de configuración

Nº	Responsable	Descripción
REGISTRAR CLIENTE		
1	RTN1	Viene de la Act. 4. *Ver procesos previos.* ¿Existe cliente en el Sistema del Service Desk? SI: ir a la actividad 2. NO: registrar cliente en el Sistema del Service Desk. Colocar el nombre de la empresa o institución.
REGISTRAR USUARIO		
2	RTN1	¿Existe usuario en el Sistema del Service Desk? Si: ir a la actividad 3. No: registrar usuario en el Sistema del Service Desk. Colocar el apellido y nombres de la persona y de preferencia los datos personales: teléfono, e-mail, cargo, dirección.
REGISTRAR CI (CONFIGURATION ITEMS)		
3	RTN1	¿Existe CI en el Sistema del Service Desk? Si: ir a la actividad 4. No: registrar el número de serie del equipo el tipo, el modelo y marca del equipo. NOTA: El RT N1 solo podrá ingresar el texto "*Compatible*" cuando el cliente no envía sus datos completos.
RELACIONAR CLIENTE, USUARIO Y CI		
4	RTN1	Una vez registrado y/o modificado: Cliente, Usuario y/o CI, se valida la información ligada a la relación cliente-usuario y CI que corresponda. Volver a la Act. 4. *Ver proceso previos*

6.5. Gestión de Suministros

Objetivo:	Establecer, documentar y mantener un procedimiento para atender y registrar la atención de las solicitudes de suministros de los equipos que están bajo contrato.
Alcance:	Se aplica a toda la gestión de solicitud de suministro hasta su entrega al cliente.

Nº	Responsable	Descripción
SOLICITAR REQUERIMIENTO AL SERVICE DESK		
1	Cliente/Gestor de Impresión	Enviar a Service Desk mediante correo la solicitud F-Se-St-28-Solicitud de Suministros. ¿La solicitud es por cambio de suministro? SI: Ir a la actividad 16 NO: Ir a la actividad 2
RECIBIR SOLICITUD DE SUMINISTRO		
2	RT GARANTÍA	Verifica el F-Se-St-28-Solicitud de Suministros, que todos los campos están llenados correctamente, para poder tramitar su envío con el área de logística. ¿Formato se encuentra llenado correctamente? SI: Ir a la actividad 3 NO: Se envía el F-Se-St-28-Solicitud de Suministros al Gestor de Impresión para completar el formato correctamente. Ir actividad 4.
VERIFICACIÓN DE STOCK DE SUMINISTRO		

3	RT GARANTÍA	¿Se cuenta con Stock del suministro? SI: El part number del suministro, se encuentra en el documento: F-Ad-Lo-011 Stock de Suministros. Ir a la siguiente pregunta. ¿El Stock del suministro pertenece al cliente? SI: Ir actividad 5. NO: Informar al Gestor de Impresión que cliente cuenta con stock para que realice las gestiones de préstamo interno. ¿Préstamo interno es aprobado? SI: Ir a la actividad 5 NO: Ir a la actividad 9 NO: Se genera ticket de tipo Requerimiento en el sistema de Service Desk, estado del ticket: ASIGNADO y se informa vía mail a Gestor de Impresión que la solicitud se encuentra en Pendiente. Ir a la actividad 9. Nota: En los casos que no se encontrase la totalidad de suministros; F-Se-St-28-Solicitud de Suministros, se procede a gestionar el envío de la cantidad encontrada; y se procede a crear nuevo ticket relacionado al número de ticket anterior (Padre – Hijo) para los Ítem pendientes. Se informa vía mail al Gestor de Impresión los Ítem que se encuentran en estado pendiente. Ir a la actividad 9.
VALIDAR SOLICITUD		
4	Gestor de Impresión	Revisa y actualiza el registro: F-Se-St-28-Solicitud de Suministros, correctamente y lo envía a RT Garantía para que proceda con el despacho. Ir actividad 2.

5	RT GARANTÍA	Revisar y validar si el requerimiento ha sido atendido anteriormente, haciendo uso de F-Ad-Lo-008 Control de Despachos. Verificar el tiempo de envío del suministro. En caso se haya enviado en corto tiempo, informar vía mail a Gestor de Impresión para su revisión. Ir a la Actividad 6. Caso contrario atender requerimiento. Ir a la Actividad 7.
6	Gestor de Impresión	Revisa solicitud de cliente, mediante el consumo del suministro (Contador). ¿Procede solicitud? SI: Informa a RT Garantía que procede solicitud. Ir actividad 7. NO: Informa al cliente y a SD que la solicitud no procede. *Fin del proceso.*
ATENDER REQUERIMIENTO - ASIGNADO		
7	RT GARANTÍA	Generar Ticket tipo Requerimiento en el sistema de Service Desk, estado de ticket: ASIGNADO a LOGISTICA.
8	RT GARANTÍA	Solicitar a almacén vía correo el suministro (F-Se-St-28 Solicitud de Suministros) para su despacho. Ir actividad 11. Estado de ticket: EN PROCESO.
ATENDER REQUERIMIENTO - PENDIENTE		
9	RT GARANTÍA	Generar Ticket tipo Requerimiento en el sistema de Service Desk, * quedando el estado de ticket: REASIGANDO a LOGISTICA.
10	RT GARANTÍA	Se procede a actualizar F-Se-St-030 Pendientes de Suministros enviándose vía correo a Logística, Gestor de Impresión para continuar con su proceso de compra. Ir a la actividad 15.
ATENDER DESPACHO DE SUMINISTRO		

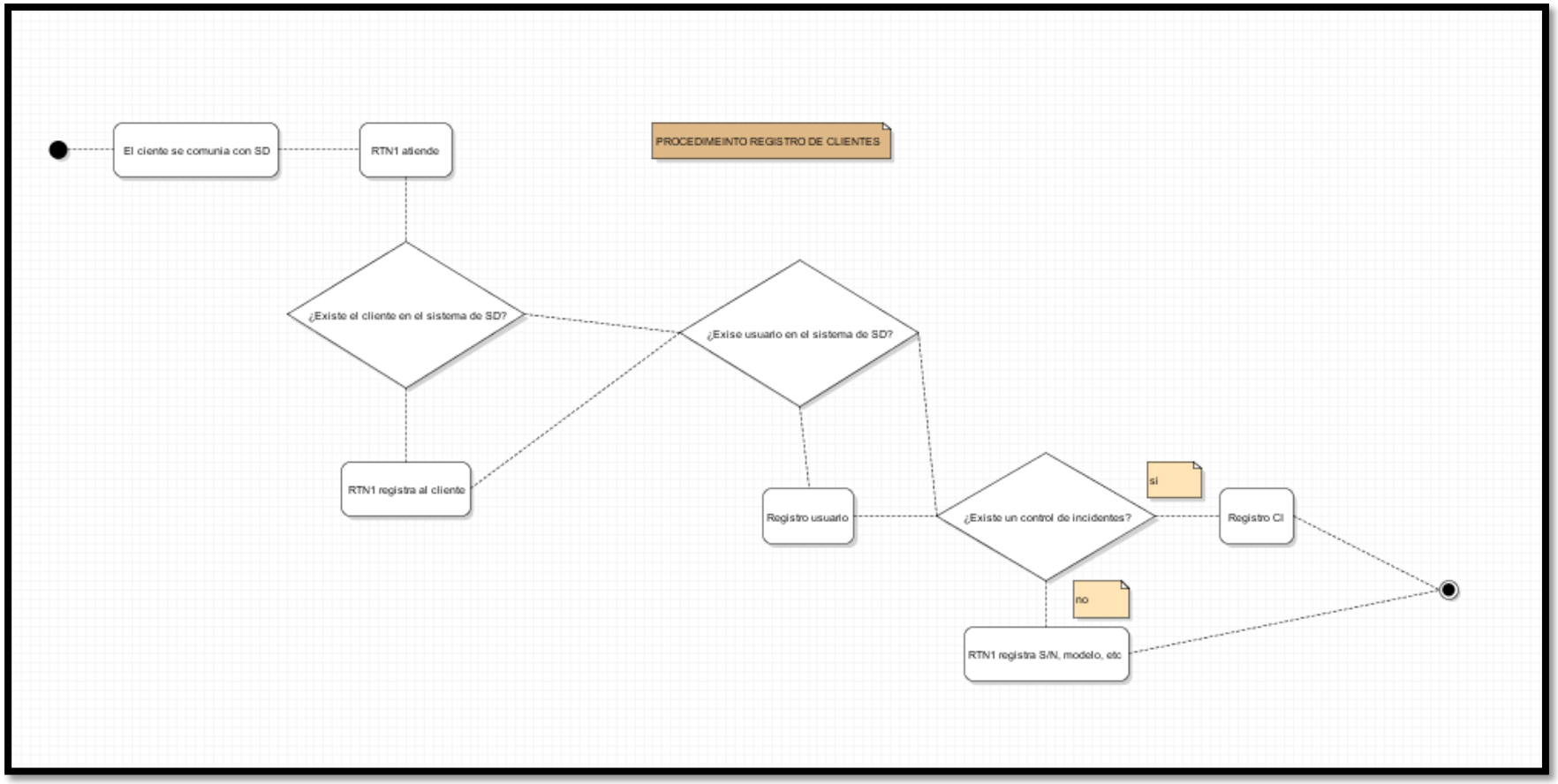
11	Almacén	Para el despacho de suministros, ir al procedimiento: P-Ad-Lo-001 Logística, COMPRA DE SUMINISTROS - DESPACHO DE SUMINISTROS. Luego ir a la actividad 12.
VALIDACION DE ENTREGA		
12	RT GARANTÍA	Enviar el F-Se-St-031 Consolidado de Despachos Diarios a logística al medio día y al finalizar el día, para su control.
13	RT GARANTÍA	Actualizar F-Ad-Lo-008 Control de Despachos con todos los despachos solicitados al área de logística.
14	RT GARANTÍA	Revisar el estado de la solicitud de suministro haciendo uso del formato: F-Ad-Lo-008 Control de Despachos. Dicho documento será actualizado por el área de logística dentro de un plazo de 2 días hábiles después de entregado el producto. Actualizar el estado de Ticket en el sistema de Service Desk. Estado de ticket: SOLUCIONADO y luego CERRADO. (Nota) *Fin de Proceso.* Nota: En el caso de presentarse una falla de suministro registrar como servicio no conforme en el formato: F-SGC-009 Reporte de Servicio No Conforme. Ir a la actividad 16.
MONITOREO DE PENDIENTES		
15	Gestor de Impresión	Informa a JSI para la actualización del archivo Forecast Mensual. Para el proceso de compras, revisar el procedimiento: P-Ad-Lo-001 Logística - COMPRA DE SUMINISTROS. Luego logística informara al RT Garantía, Gestor de Impresión; la llegada del suministro pendiente. Estado del Ticket: EN PROCESO. Ir a la actividad 8.
GARANTIA DE SUMINISTROS		

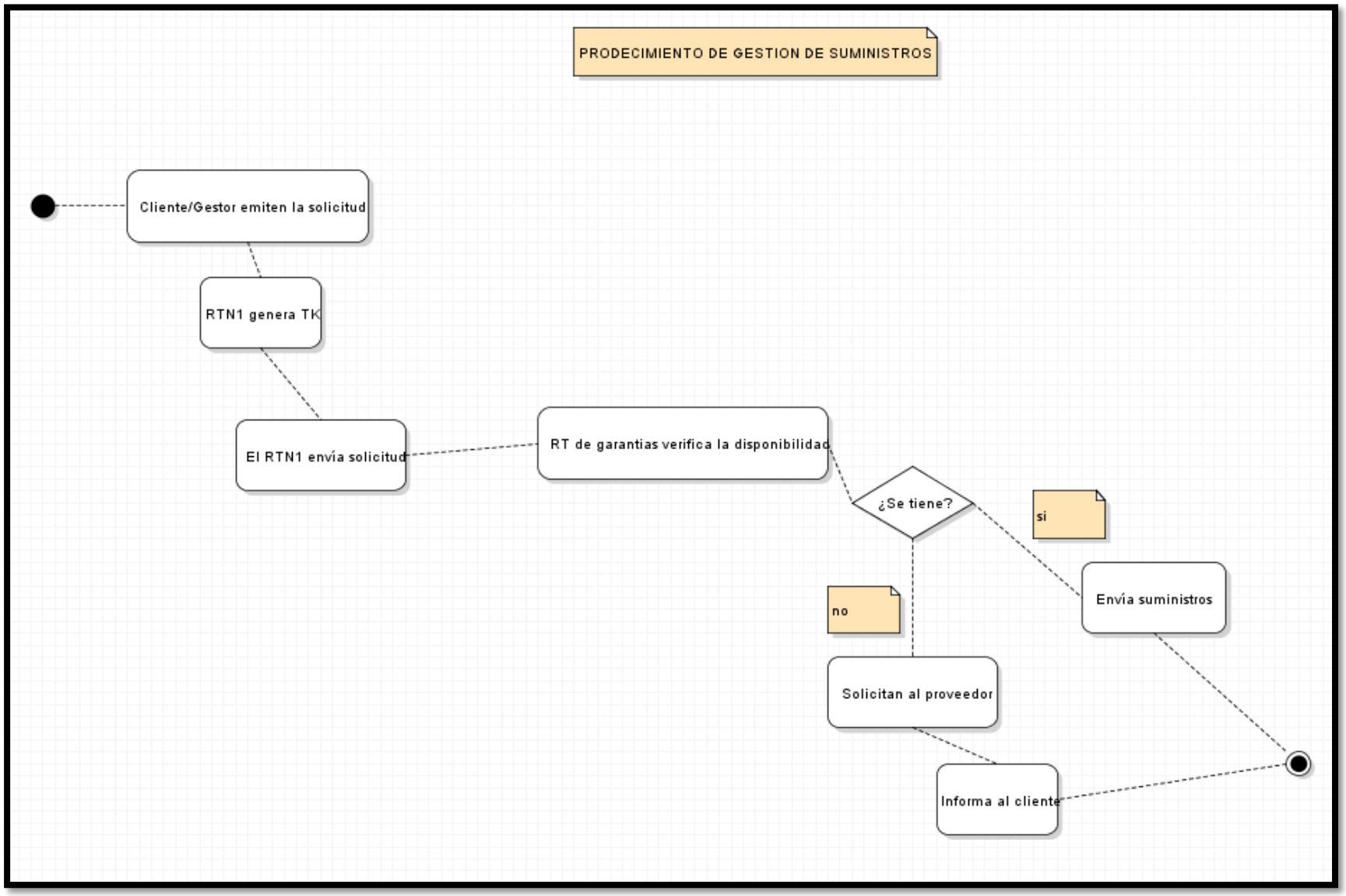
16	RT GARANTÍA	Proceder a crear nuevo ticket relacionado al número de ticket anterior (Padre – Hijo), y se solicita vía correo almacén el envío del nuevo suministro, haciendo uso del formato F-Se-St-28 Solicitud de Suministros y adjuntando el F-Se-St-001 Guía de Ingeniería. Ir a la actividad 3. Nota: Sólo se atenderá la solicitud cuando el Gestor de Impresión lo haya validado.

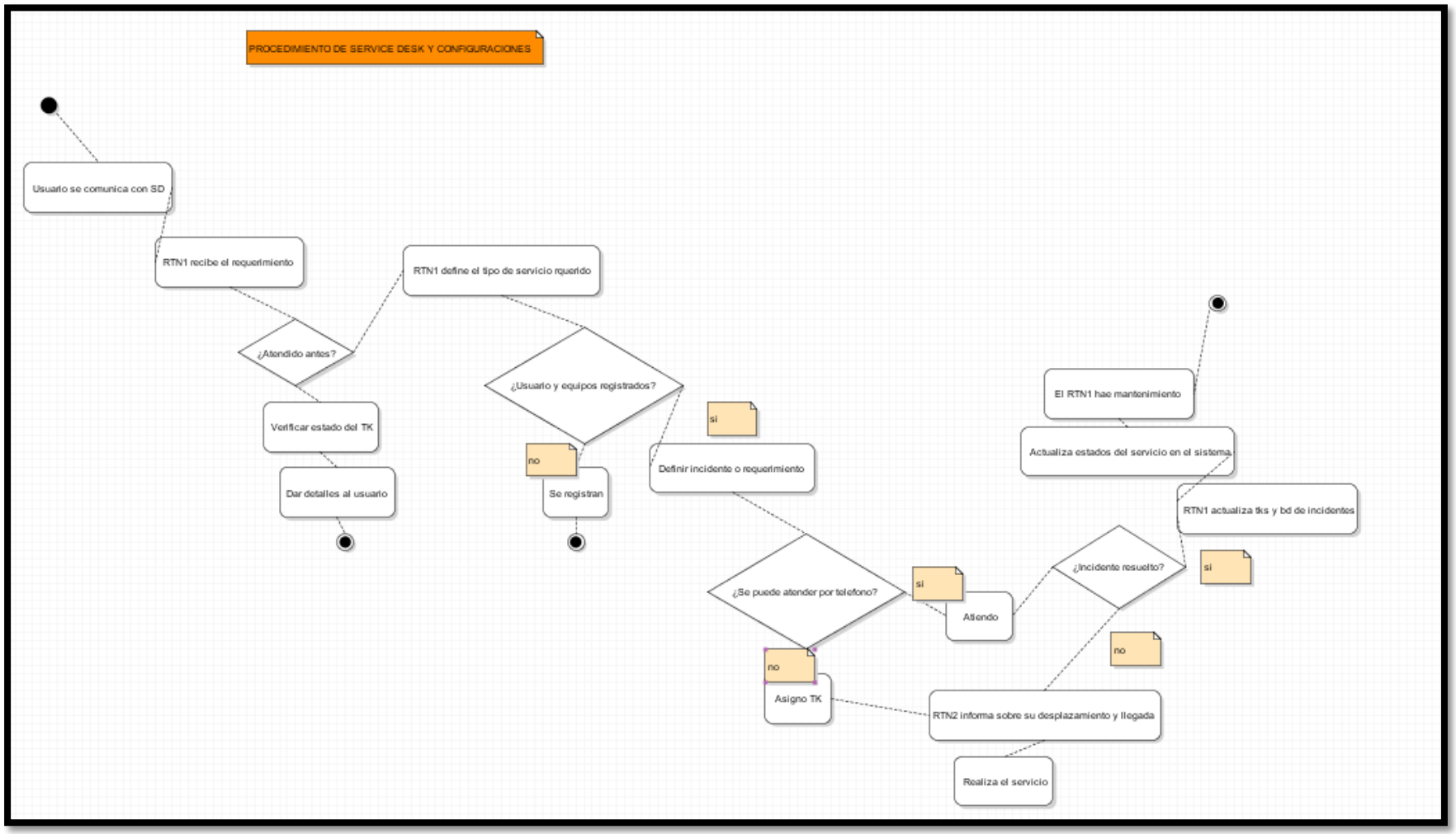
ANEXO 31
CASCADA DE OBJETIVOS DE COBIT 5

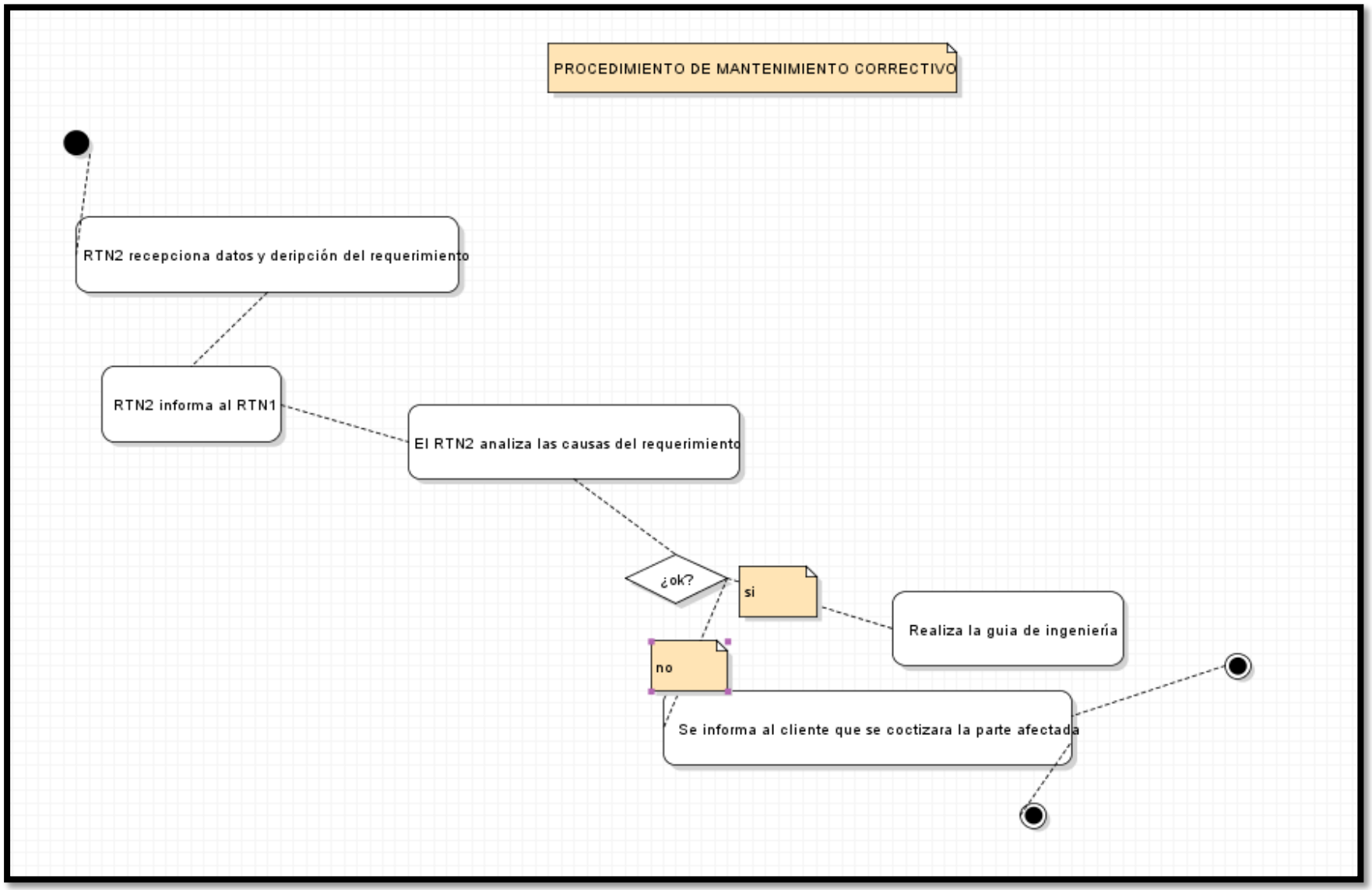
DIMENSIÓN BSC	N°	METAS DE LA ORGANIZACIÓN
Financiero	1	Valor para las partes interesadas de las inversiones del negocio.
Financiero	2	Portafolio competitivo de los productos y servicios.
Financiero	3	Riesgos de negocio gestionados (Salvaguarda de los activos).
Financiero	4	Cumplimiento de las leyes y reglamentos externos.
Financiero	5	Transparencia financiera.
Cliente	6	Cultura de servicios orientada al cliente.
Cliente	7	Continuidad y disponibilidad del servicio.
Cliente	8	Respuesta ágil a los cambios en el entorno empresarial.
Cliente	9	Información basada en toma de decisiones estratégicas.
Cliente	10	Optimización de costos de entrega del servicio.
Interno	11	Optimización de la funcionalidad de los procesos de negocio.
Interno	12	Optimización de los costos de los procesos de negocio.
Interno	13	Programas gestionados del cambio de negocio.
Interno	14	Productividad de las operaciones y el personal.
Interno	15	Cumplimiento de las políticas internas.
Aprendizaje y Crecimiento	16	Personas preparadas y motivadas.
Aprendizaje y Crecimiento	17	Cultura de innovación de productos y del negocio.

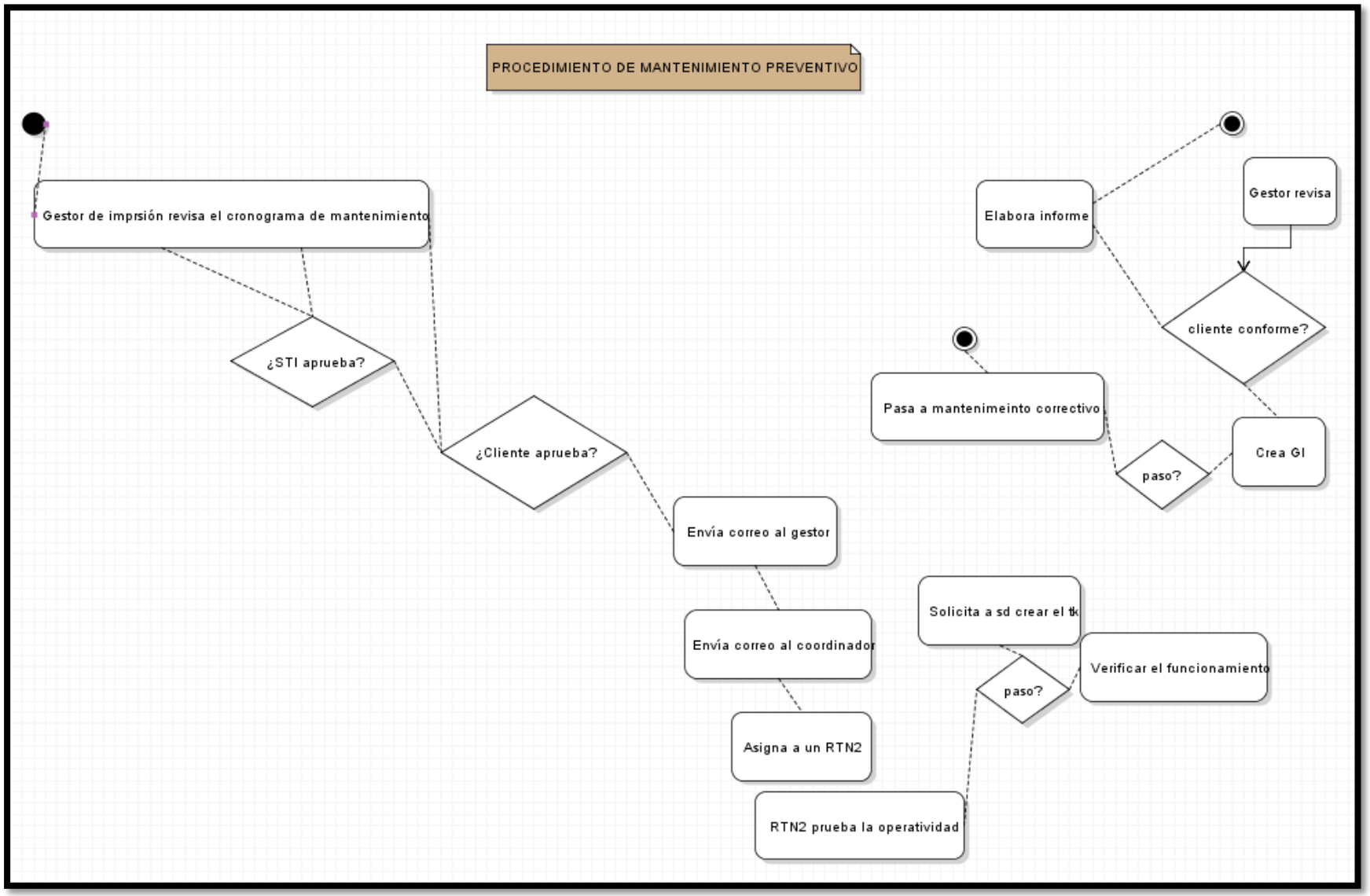
ANEXO 32
MODELO DE LOS PROCESOS DE NEGOCIO




PRODECIMIENTO DE GESTION DE SUMINISTROS
Cliente/Gestor emiten la solicitud
RTN1 genera TK
El RTN1 envía solicitud
RT de garantias verifica la disponibilidad
¿Se tiene?
si
no
Envía suministros
Solicitan al proveedor
Informa al cliente


PROCEDIMIENTO DE SERVICE DESK Y CONFIGURACIONES
Usuario se comunica con SD
RTN1 recibe el requerimiento
¿Atendido antes?
Verificar estado del TK
Dar detalles al usuario
RTN1 define el tipo de servicio querido
¿Usuario y equipos registrados?
no
Se registran
si
Definir incidente o requerimiento
¿Se puede atender por telefono?
si
Atiendo
no
Asigno TK
RTN2 informa sobre su desplazamiento y llegada
Realiza el servicio
¿Incidente resuelto?
si
no
El RTN1 hae mantenimiento
Actualiza estados del servicio en el sistema
RTN1 actualiza tks y bd de incidentes


PROCEDIMIENTO DE MANTENIMIENTO CORRECTIVO
RTN2 recepciona datos y deripción del requerimiento
RTN2 informa al RTN1
El RTN2 analiza las causas del requerimiento
¿ok?
si
Realiza la guia de ingeniería
no
Se informa al cliente que se coctizara la parte afectada


PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO
Gestor de imprsión revisa el cronograma de mantenimiento
¿STI aprueba?
¿Cliente aprueba?
Envía correo al gestor
Envía correo al coordinador
Asigna a un RTN2
RTN2 prueba la operatividad
Solicita a sd crear el tk
Verificar el funcionamiento
paso?
Pasa a mantenimeinto correctivo
paso?
Crea GI
Elabora informe
Gestor revisa
cliente conforme?