MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES

Plan de implementación de la norma ISO/IEC 27001:2005

Jose Aurela Pereira
Director: Antonio Segovia Henares

Junio de 2013

Agradezco a todas las personas que hicieron posible este trabajo, a los compañeros del master por compartir sus ideas, a los profesores y tutores por su guía y confianza y finalmente a Silvia mi esposa, por su compañía y apoyo incondicional.

RESUMEN

Este documento presenta de manera práctica la construcción de un plan de implementación de la norma ISO/IEC 27001:2005, lo cual es considerado un aspecto clave para cualquier organización que desee alinear los objetivos del negocio y sus directrices de seguridad en relación a la normativa internacional.

Se plantean las bases para la implementación de un Sistema de Gestion de la Seguridad de la Información (SGSI) desarrollando las fases de documentación normativa, contextualización de la compañía y definición de la situación actual, análisis de riesgos, evaluación de nivel de cumplimiento de la norma, propuesta de proyectos que permitan alcanzar el nivel adecuado de seguridad y el esquema documental.

ABSTRACT

This paper presents a practical way to build a plan for implementation of ISO/IEC 27001:2005, which is considered a key aspect for any organization wishing to align their business objectives and security guidelines in relation to the international standard.

Proposing basics for the implementation of an Information Security Management System (ISMS) developing regulatory documentation phases, contextualization of the company and defining the current situation, risk assessment, evaluation of compliance level, projects definitions to achieve the appropriate level of security and the schema of documents for the ISMS.

CONTENIDO

1. INTRODUCCIÓN

Hoy en día el volumen y complejidad de la información así como la creciente dependencia de las organizaciones hacia procesos y sistemas informáticos han llevado a los profesionales de TI a enfrentar grandes retos y amenazas persistentes que no dan señales de desaceleración. Estos retos han obligado a las compañías a organizarse y crear estrategias y estándares que permitan proteger el activo intangible más valioso: "La información" [1].

Esta necesidad básica de proteger los activos ha colocado en una posición privilegiada a lo concerniente con seguridad de la información y gestión del riesgo, al punto de que estos elementos dejaron de ser conceptos cerrados resultantes de la aplicación de una serie de métodos o actividades puntuales y pasaron a ser organismos que evolucionan al ritmo de la organización gracias a los procesos de mejoramiento continuo donde regularmente se verifica el estado actual frente a las necesidades, requerimientos y amenazas del entorno para proveer la retroalimentación necesaria que permita ajustar y/o mejorar los procesos de la organización.

Por lo anterior y con el fin de resolver estas necesidades surgieron estándares aceptados internacionalmente para la gestión de la seguridad de la información, entre ellos encontramos la ISO/IEC 27001:2005 que será tratada en este trabajo, así como un método practico para su implementación.

2. OBJETIVOS

El presente trabajo tiene como objetivo general Ilustrar la forma en la que se puede implementar la norma ISO/IEC 27001:2005 a través del desarrollo de un plan de implementación. De igual forma, se busca cumplir con los siguientes objetivos específicos:

- Proporcionar documentación normativa acerca de las mejores prácticas en seguridad de la información.
- Utilizando una compañía de ejemplo, analizar su situación actual frente a los objetivos del SGSI.
- Proporcionar una guía para la realización de análisis de riesgos utilizando una compañía de ejemplo.
- Realizar una evaluación del nivel de cumplimiento de la norma ISO/IEC 27001:2005 en la compañía de ejemplo.
- Proponer e ilustrar una serie de proyectos de seguridad que permitan conseguir una adecuada gestión de la seguridad en la compañía de ejemplo.
- Proponer un esquema documental que de soporte al SGSI.

3. ALCANCE

El presente trabajo se desarrolla bajo un enfoque académico donde la compañía tomada de ejemplo es ficticia, es decir que no se encuentra constituida legalmente. De igual forma, las cuantificaciones monetarias no necesariamente relejan la realidad actual.

Para efectos prácticos se asume que la compañía seleccionada tiene algunos controles de seguridad implementados y que los proyectos y plan de implementación se encuentran limitados a los que han sido aprobados por la dirección de dicha compañía.

Los planes de proyectos no serán desarrollados, solo se presentaran como parte de las actividades necesarias para alcanzar un nivel de seguridad adecuado.

Finalmente, los activos relacionados en los análisis no representan la totalidad de los activos de la compañía pero sí los considerados críticos para el desarrollo de su actividad económica.

4. GENERALIDADES

4.1. Metodología

Este trabajo fue elaborado en fases que permitieran establecer objetivos específicos medibles y alcanzables en relación al diseño del plan de implementación de la norma ISO/IEC 27001:2005. Las fases abordadas fueron:

- **Fase 1: Situación actual**: Contextualización, objetivos y análisis diferencial en esta primera fase además de definir los objetivos del proyecto, se seleccionó la empresa que se utilizaría para aplicar los conceptos y técnicas utilizadas a lo largo del mismo. En esta misma fase se realizó un análisis diferencial de dicha empresa con respecto a ISO/IEC 27001+ISO/IEC 27002.

- **Fase 2: Sistema de Gestión Documental**. En esta fase se elaboró la política de seguridad de la empresa, declaración de aplicabilidad y la documentación mínima necesaria que requiere un SGSI.

- **Fase 3: Análisis de riesgos**. Se seleccionó una metodología de análisis de riesgos, se Identificaron y valoraron los activos, amenazas, vulnerabilidades, se calculó del riesgo, nivel de riesgo aceptable y riesgo residual.

- **Fase 4: Propuesta de Proyectos**. En este punto ya teniendo identificado los riesgos y puntos a mejorar, se proponen una serie de proyectos que permitan alcanzar un nivel de seguridad razonable.

- **Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2005**. En esta fase se evaluó hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad, utilizando como referencia la ISO/IEC 27002:2005.

- **Fase 6: Presentación de Resultados y entrega de Informes**. Esta fase es la consolidación de todas las anteriores y que se refleja en el presente documento.

4.2. Definiciones

- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización [2].

- **Análisis de riesgos:** Uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Controles de seguridad:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También utilizado como sinónimo de salvaguarda o contramedida.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

- **Disponibilidad:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Impacto:** El coste para la empresa de un incidente que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.

- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **No conformidad**: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **No repudio**: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

- **PDCA**: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

- **Política de seguridad**: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo residual:** Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- **SGSI:** Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4.3. Familia ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) [3].

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Estos documentos se encuentran en continuo desarrollo y algunos aún en fase de preparación. Esta familia o serie de normas esta compuerta por:

- ISO/IEC 27000: Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

- ISO/IEC 27001: "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Esta norma agrupa los requerimientos de implantación de un SGSI, esta norma es certificable por entidades externas a la organización. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799).

- ISO/IEC 27002: Este documente es una guía de buenas prácticas para la gestión de seguridad la cual describe los objetivos de control y controles recomendables, se encuentra organizado en 11 dominios, 39 objetivos de control y 133 controles.

- ISO/IEC 27003: Corresponde a una guía de implementación de un SGSI e información acerca del uso del ciclo Deming (PDCA). Su propósito principal es orientar hacia una implementación efectiva del modelo de seguridad que se encuentre acorde con ISO/IEC 27001.

- ISO/IEC 27004: Este estándar internacional ofrece una guía para el desarrollo y uso de métricas para medir la eficiencia del SGSI, objetivos de control y controles utilizados para implementar y administrar la seguridad de la información.

- ISO/IEC 27005: Este documento es una Guía para la gestión del riesgo de la seguridad de la información, soportado en los conceptos generales de la norma ISO/IEC 27001.

- ISO/IEC 27006: Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

- ISO/IEC 27007: Guía para auditar sistemas de gestión de la seguridad de la información.

- ISO/IEC 27008: Este reporte técnico provee una guía para la revisión de implementación y operación de controles, incluyendo la verificación de cumplimiento técnico de los controles de sistemas de información y cumplimiento con estándares establecidos por la compañía.

4.4. Ciclo de Deming (PDCA) y mejoramiento continúo

El ciclo de Deming, también conocido como círculo PDCA (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los Sistemas de Gestión de Calidad (SGC).

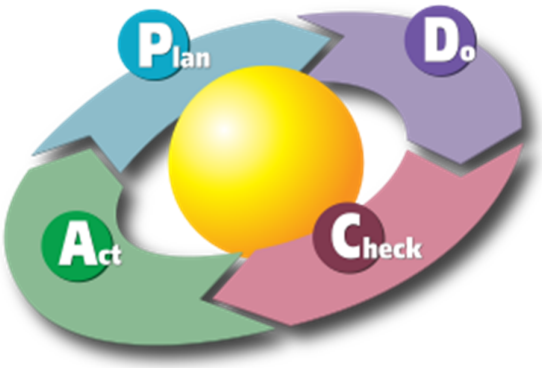


Imagen 1: ilustración modelo PDCA

Las siglas, PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), donde:

- Planear o Planificar: consiste en definir los objetivos y los medios para conseguirlos.
- Hacer: Se refiere al acto de implementar la visión preestablecida.
- Verificar: Implica comprobar que se alcanzan los objetivos previstos con los recursos previamente asignados.
- Actuar: Se refiere a analizar y corregir las posibles desviaciones detectadas, así como también se debe proponer mejoras a los procesos ya empleados.

5. SITUACIÓN ACTUAL

5.1. Contextualización: Compañía seleccionada

Para el desarrollo de las diferentes fases de este proyecto se utilizará la compañía descrita a continuación:

El Grupo **CoalCorp** es propiedad de la multinacional **MineX** International Plc. El grupo comprende las operaciones de **MineX** en Colombia para la exportación de carbón térmico y metalúrgico y su infraestructura asociada. Explora, produce, transporta y embarca carbón térmico y metalúrgico de alto grado con destino a los mercados en Europa, América y Asia.

El Grupo tiene grandes ventajas operativas pues es propietario de toda su infraestructura operacional esencial, incluyendo la infraestructura ferroviaria (mediante una participación en la propiedad de la infraestructura ferroviaria y la propiedad del equipo rodante) así como de la totalidad del equipo minero e instalaciones en las minas. Además, posee la totalidad de la participación accionaria en la Sociedad Portuaria S.A.

El grupo cuenta con aproximadamente 2.500 empleados repartidos en las diferentes seccionales de la operación (sedes administrativas, minas, ferrocarril y puertos) los cuales son soportados desde el punto de vista de tecnología y comunicaciones por un equipo de trabajo de 50 personas organizados en las Jefaturas de Servicios, Infraestructura, Seguridad Informática, Desarrollo de Software y Soporte SAP ERP (en todos sus módulos).

La infraestructura tecnológica del grupo empresarial consta de una granja de 50 servidores virtuales ubicados en el datacenter principal y servidores físicos en cada una de las seccionales, con canales de comunicación en fibra y radio frecuencia (al interior de las minas). La totalidad de la infraestructura que soporta los servicios de ERP se encuentra tercerizada (Servidores y canales de comunicación).

A nivel se seguridad y continuidad de negocio la compañía se encuentra en un estado “Inicial” donde se tienen documentado e implementados algunos procedimientos, así como planes de contingencia para algunos servicios críticos (Como el ERP para el que se cuenta con un Hotsite de replicación en tiempo real y canales alternos de comunicación).

5.2. Análisis diferencial

Existen en el mercado infinidad de herramientas que nos facilitan realizar un análisis diferencias o de brecha (Gap Analysis) que permiten obtener el estado actual de una compañía frente a los controles de seguridad de normas como la ISO/IEC 27002, en ese caso utilizamos una herramienta desarrollada en Excel denominada "Data security maturity model" [5] (Ver Anexo 1).

DATA SECURITY MATURITY MODEL[SM]

Instructions: In each row where there is an 'x' in a yellow cell, delete that 'x' and type an 'x' in the cell in that same row that best approximates the status of the business unit or organization you are assessing.

	Security Maturity Levels >	0: Nonexistent	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized	
	Maturity Level Description >	There is no evidence of this standard or practice in the organization.	The organization has an ad hoc and inconsistent approach to this privacy standard or	The organization has a consistent overall approach, but it is mostly undocumented.	The organization has a documented, detailed approach, but no routine measurement or	The organization regularly measures its compliance and makes regular process	The organization has refined its compliance to the level of best practice.	
	process consistency	none	ad hoc	consistent	consistent	consistent	consistent	average maturity 1,35
	process documentation	none	none	minimal, high-level	detailed	detailed	detailed	scaled to 100 27,00
	business objectives	not met	not met	partially met	mostly met	fully met	value added	score out of 55 14,83
	process measurement	none	none	none	ad hoc	routine	systemic	
	policy enforcement	none	none	none	ad hoc	routine	systemic	
	process improvement	none	ad hoc	ad hoc	ad hoc	routine	systemic	
	process benchmarking	none	none	none	ad hoc	ad hoc	routine	
	Corresponding Level of Risk of a Data Breach or Regulatory Noncompliance	*Very high across the organization*	*High across the organization, and very high in key parts of the*	*Moderate across the organization, with some pockets of high risk*	*Moderate across the organization.*	*Low across the organization.*	*Remote across the organization.*	
ISO #	Domains							
5	Security Policy							1,3
6	Organization of Information Security							1,0
7	Asset Management							0,5
8	Human Resource Security							1,5
9	Physical and Environmental Security							1,0
10	Communications and Operations Management							2,3
11	Access Control							1,7
12	Information Systems Acquisition, Development and Maintenance							1,0
13	Information Security Incident Management							1,5
14	Business Continuity Management							2,0
15	Compliance							1,0

Imagen 2: Herramienta para calcular madurez del modelo de seguridad

La herramienta está basada en los 11 dominios de la ISO/IEC 27002 y se debe especificar un nivel de cumplimiento en aspectos claves que los componen, este nivel de cumplimiento está basado en la siguiente escala:

Valor	Nombre	Descripción
0	No existente	No existe evidencia del estándar o practica en la compañía.
1	Inicial	La organización tiene practicas hechas a la medida pero inconsistentes.
2	Repetible	La organización tiene un enfoque coherente pero no documentado.
3	Definido	Se tiene un enfoque coherente y documentado pero no medido.
4	Administrado	Los procesos son medidos frecuente mente y se realizan mejoras.
5	Optimizado	La organización ha refinado su cumplimiento con el nivel de las mejores prácticas.

Luego de completar los datos en la herramienta, se determinó que la compañía objeto de estudio tiene un nivel de madurez “Inicial” con una calificación promedio de 1.35/5.00.

De igual forma, se diligenciaron los datos que representan el estado deseado, lo que nos permite crear una representación gráfica del estado actual:

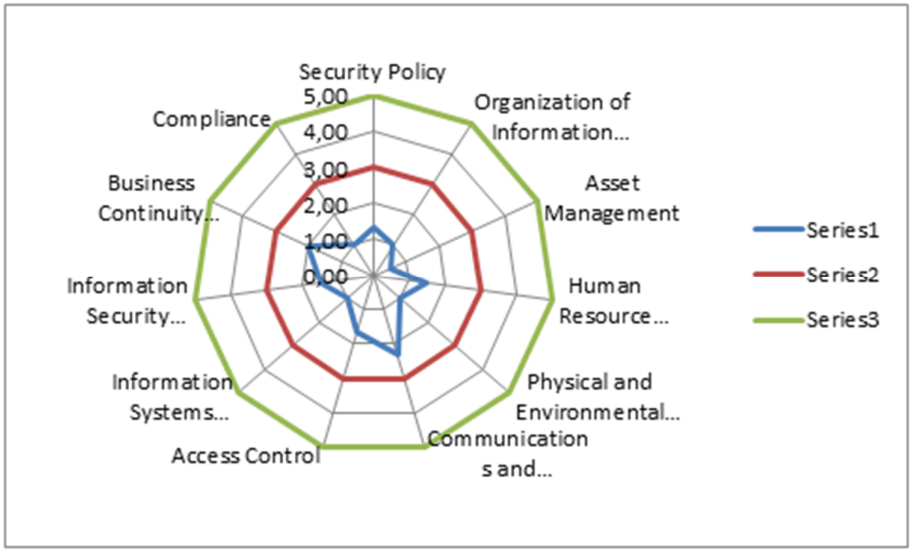


Imagen 3: Representación gráfica del estado actual de la compañía.

En azul se encuentra la ubicación actual de la compañía, en rojo en donde debería estar (y el objetivo inicial donde se llegará al realizar la implementación) y en verde donde se podría llegar gracias al proceso de mejora continua del SGSI.

6. SISTEMA DE GESTIÓN DOCUMENTAL

6.1. Esquema documental

Los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información debe contar con una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001.

6.2. Política de Seguridad

La política de seguridad hace parte de la normativa interna de la organización que todo el personal cubierto en el alcance del SGSI debe conocer y cumplir.

El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc. tal como se encuentra estructurada la política que se diseñó para la empresa seleccionada en este trabajo (Ver anexo 2):

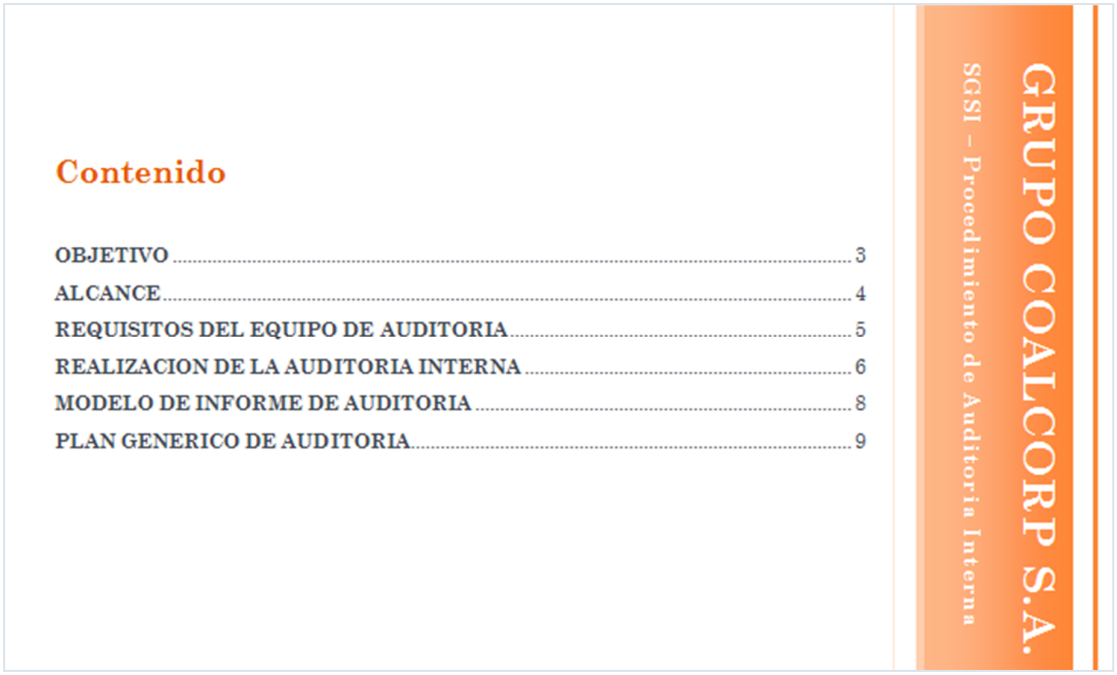
Contenido

Imagen 4: Tabla de contenido de la política de seguridad

6.3. Procedimiento de auditorías internas

Un SGSI debe ser auditable en todo momento, por esto es importante establecer las directrices de dichas auditorias, ese documento debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

Para la compañía que tomamos como ejemplo se desarrolló el procedimiento con el siguiente contenido (Ver Anexo 3):


Contenido

GRUPO COALCORP S.A.

SGSI – Procedimiento de Auditoria Interna

Imagen 5: Tabla de contenido del procedimiento de auditorías internas

6.4. Gestion de indicadores

El mejoramiento continuo de los SGSI se da gracias a la retroalimentación que este entrega lo cual solo es posible si tenemos métricas e indicadores para los controles implementados, por esto es importante no solo definir los indicadores en sí, sino también la sistemática utilizada para las mediciones. A continuación se muestra el contenido de dicho procedimiento el cual fue elaborado para la empresa de ejemplo (Ver anexo 4):


Contenido

GRUPO COALCORP S.A.

SGSI – Gestion de Indicadores

Imagen 6: Tabla de contenido del procedimiento de gestión de indicadores

6.5. Revisión por parte de la dirección

La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.

Como modelo se muestra la tabla de contenido del procedimiento de revisión diseñado para la compañía tomada como ejemplo (Ver anexo 5):

Imagen 7: Tabla de contenido del procedimiento de revisión por parte de la dirección

6.6. Gestion de roles y responsabilidades

El Sistema de Gestión de Seguridad de la Información debe estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

A partir de este contenido se pueden diseñar una serie de procedimientos que cumplan el objetivo o sencillamente hacerlo parte de la política de seguridad de la compañía, en nuestro caso la hemos incluido como parte de la política en los apartados de “Comité de seguridad” y “Responsabilidades” (ver Anexo 1).

6.7. Metodología de análisis de riesgos

Todo SGSI debe tener directrices claras a la hora de realizar el análisis de riesgos, estas directrices deben incluir el método seleccionado, la identificación y valoración de los activos, amenazas y vulnerabilidades.

A modo de ilustración, se desarrolló este procedimiento para la empresa tomada como ejemplo, siendo esta su tabla de contenido (Ver anexo 6):

Imagen 8: Tabla de contenido del procedimiento de metodología de análisis de riesgos

6.8. Declaración de aplicabilidad

Este documento incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

Puede ser un documento de texto que contenga dicha información o para facilidad y practicidad una plantilla o documento realizado en hojas de cálculo tipo Excel.

Para nuestro ejemplo práctico se optó por realizar el declaración de aplicabilidad en un documento Excel (Ver Anexo 7):

Declaración de Aplicabilidad

Leyenda (Razon de controles seleccionados)

LR: Requemimientos Legales, **CO**: Obligaciones Contractuales, **BR/BP**: Requerimientos del negocio/Mejores Practicas, **RRA**: Resultado de Analisis de Riesgos

Version: 1.0

Marzo de 2013

CONTROLES ISO 27001:2005			Control Actual	Comentarios (o Justificacion de exclusión)	Controles seleccionados y razones de selección				Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	Sec	Control/Objetivo de Control								
Politica de Seguridad	5,1	Política de seguridad de la información								
	5.1.1	Documento de política de seguridad de la información	■	Ya se encuentra documentado.						Se pueden incluir mejoras
	5.1.2	Revisión de la política de seguridad de la información					■		SI	Se revisará por lo menos una vez a año.
Aspectos Organizativos de la seguridad de la información	6,1	Organización interna								
	6.1.1	Compromiso de la Dirección con la seguridad de la información.	■	Politicas y presupuesto aprobado.		■	■			
	6.1.2	Coordinación de la seguridad de la información.	■	Ya existe un comité y coordinación.						
	6.1.3	Asignación de responsabilidades relativas a la seg. de la información.					■		SI	Diseño de matriz RACI.
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información.				■	■		SI	Por documentar y formalizar.
	6.1.5	Acuerdos de confidencialidad.	■	Control ya implementado.						
	6.1.6	Contacto con las autoridades.	■	Control ya implementado.						
	6.1.7	Contacto con grupos de especial interés.	■	Control ya implementado.						
	6.1.8	Revisión independiente de la seguridad de la información	■	Auditoria Externa Anual						
	6,2	Terceros								
	6.2.1	Identificación de los riesgos derivados del acceso de terceros.	■	Se evaluan los riesgos y firman acuerdos					SI	Se realizaran mejoras para establecer metricas
	6.2.2	Tratamiento de la seguridad en la relación con los clientes.		Solo son 5 grandes clientes ya regulados						
	6.2.3	Tratamiento de la seguridad en contratos con terceros.					■		SI	Diseñar procedimientos
Gestión de Activos	7,1	Responsabilidad sobre los activos.								
	7.1.1	Inventario de activos.	■	Control ya implementado.						
	7.1.2	Propiedad de los activos.	■	Control ya implementado.						
	7.1.3	Uso aceptable de los activos.	■	Control ya implementado.			■		SI	Reforzar (sanciones y registros)
	7,2	Clasificación de la información.								
	7.2.1	Directrices de clasificación.					■		SI	Diseñar e implementar controles
	7.2.2	Etiquetado y manipulado de la información.					■		SI	Diseñar e implementar controles

Imagen 9: Estructura de la declaración de aplicabilidad

7. ANÁLISIS DE RIESGOS

7.1. Metodología MAGERIT

Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas [6].

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. El método comprende las siguientes Fases:

Toma de datos y procesos de información
En esta Fase se debe definir el alcance del objeto de estudio o análisis.

Establecimiento de parámetros
Durante esta fase se deben definir los parámetros que serán utilizados durante todo el desarrollo. Los parámetros que deben identificarse son los siguientes:

- Valor de los activos
- Vulnerabilidad
- Impacto
- Efectividad del control de seguridad

Análisis de activos
Se deben identificar los activos que posee la organización y que necesita para llevar a cabo sus actividades.

Análisis de amenazas

Clasificar las amenazas que pueden afectar a una organización en cuatro grandes grupos:

- Accidentes
- Errores
- Amenazas intencionales presenciales
- Amenazas intencionales remotas

Establecimiento de las vulnerabilidades

Se identifican las vulnerabilidades que al materializarse puedan afectar los activos, esta fase sirve para determinar la frecuencia de ocurrencia de una determinada amenaza.

Valoración de impactos

Se determina el efecto de cada activo en caso de falla.

Análisis de riesgos intrínseco

Es el resultado del análisis de la situación en la que se encuentra la organización en el momento del estudio aunque ya posea medidas de seguridad implantadas.

Influencia de las salvaguardas

Consiste en tratar de escoger la mejor solución de seguridad que me permita reducir los riesgos identificados.

Análisis de riesgos efectivos

En esta fase se obtiene el resultado de estudiar cómo se reducirían los riesgos con cada una de las medidas de protección (controles o salvaguardas) que hemos identificado.

Gestión de riesgos

Esta es la fase final donde la organización toma las decisiones sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos.

7.2. Parámetros y convenciones

Para la valoración de activos se ha tenido en cuenta la siguiente escala:

Valoración de activos en USD		
Descripción	**Abreviatura**	**Valor**
Muy alto	MA	Valor > 200.000
Alto	A	100.000 < valor > 200.000
Medio	M	50.000 < valor > 100.000
Bajo	B	10.000 < valor > 50.000
Muy bajo	MB	1000 < valor > 10.000
Despreciable	D	valor < 1000

La frecuencia o probabilidad de ocurrencia de los eventos se encuentra definida así:

Frecuencia		
Descripción	**Abreviatura**	**Valor**
Extremadamente frecuente	EF	**1** (Una vez al día)
Muy frecuente	MF	**0.071233** (Quincenal)
Frecuente	F	**0,016438** (Bimestral)
Poco Frecuente	PF	**0,005479** (Semestral)
Muy poco frecuente	MPF	**0,002739** (Anual)
Despreciable	D	0

De igual forma, la relación del impacto está determinada así:

Impacto		
Descripción	**Abreviatura**	**Valor**
Critico	C	(80% – 100%]
Alto	A	(60% - 80%]
Medio	M	(30% - 60%]
Bajo	B	[5% - 30%]

Las dimensiones de seguridad utilizadas para identificación del impacto son:

A	Autenticidad
C	Confidencialidad
I	Integridad
D	Disponibilidad
T	Trazabilidad (Seguimiento)

Los tipos de activos que se incluyeron en este análisis son:

I	Instalaciones
H	Hardware
A	Aplicaciones / Software
D	Datos / Información
R	Redes / Comunicaciones
S	Servicios
P	Personal / Empleados

7.3. Inventario de activos

La clasificación del siguiente inventario de activos se realizó en base a lo sugerido por la metodología de Análisis de riesgos MAGERIT (Ver Anexo 8):

Ambito	Ref	Activo	Valor	$USD	Aspectos Críticos				
					A	C	I	D	T
Instalaciones	I01	CPD Principal	MA	$ 250.000,00	8	7	6	7	5
	I02	CPD Minas	A	$ 150.000,00	6	5	5	5	5
	I03	CPD Puerto Maritimo	A	$ 170.000,00	7	6	6	6	5
Hardware	H01	Controlador de dominio principal	A	$ 100.000,00	8	5	5	6	5
	H02	Controlador de dominio secundario	M	$ 60.000,00	5	4	4	5	4
	H03	Servidor de Base de Datos	M	$ 90.000,00	6	5	6	5	5
	H04	Servidor de correo	M	$ 90.000,00	7	6	6	5	6
	H05	Correo perimetral BackBerry	M	$ 60.000,00	6	4	4	4	5
	H06	Granja de Servidores Vmware	A	$ 150.000,00	7	6	6	5	4
	H07	SAP/BW Servers	M	$ 60.000,00	7	7	6	4	6
	H08	Administración Vmware	M	$ 60.000,00	5	5	5	4	4
	H09	Servidor Web	B	$ 30.000,00	4	3	4	4	4
	H10	File Server	M	$ 50.000,00	4	6	6	5	5
	H11	FTP, VPN, Terminal Server	B	$ 30.000,00	4	4	4	4	5
	H12	Antivirus, Ariadna	M	$ 50.000,00	4	3	4	4	3
	H13	SharePoint y Docuware Servers	B	$ 30.000,00	4	3	4	4	5
Aplicaciones	A01	SAP ERP	A	$ 150.000,00	8	6	6	6	6
	A02	Sistema de ferrocarril	M	$ 80.000,00	5	4	4	5	5
	A03	Basculas	M	$ 80.000,00	5	4	4	5	5
	A04	Bandas transportadoras	A	$ 10.000,00	5	4	4	5	5
	A05	Sistema de cargue (puerto Maritimo)	M	$ 80.000,00	5	5	5	5	5
	A06	Sistema de Laboratorio / Calidad	M	$ 80.000,00	4	4	4	4	5
Datos	D01	ERP Database	A	$ 140.000,00	7	7	6	6	6
	D02	BD Sistemas de control	M	$ 80.000,00	5	4	5	5	6
	D03	BD Gestion Documental	M	$ 60.000,00	6	6	5	5	6
Red	R01	Firewall x2	M	$ 80.000,00	7	4	4	4	5
	R02	Antispam	M	$ 80.000,00	5	3	4	4	5
	R03	Switch core x3	M	$ 60.000,00	5	3	3	4	5
	R04	Switch MPLS	M	$ 50.000,00	5	3	3	4	5
	R05	Tranceiver fibra principal	M	$ 60.000,00	5	3	3	4	5
Servicios	S01	Internet	M	$ 60.000,00	5	3	3	4	5
	S02	Correo Electrónico	A	$ 90.000,00	7	5	5	5	4
	S03	FTP	B	$ 30.000,00	4	3	4	4	4
	S04	VPN	B	$ 30.000,00	4	3	3	4	4
	S05	Red LAN	M	$ 60.000,00	4	4	4	4	4
	S06	Red WAN	M	$ 70.000,00	4	4	4	5	4
Personal	P01	Staff Desarrollo de Software	M	$ 80.000,00	4	5	4	4	4
	P02	Staff Soporte ERP	M	$ 80.000,00	4	5	4	4	4

Ambito	Ref	Activo	Valor	$USD	Aspectos Críticos				
					A	C	I	D	T
	P03	Staf Soporte tecnico	M	$ 80.000,00	4	4	4	4	4
	P04	Staff Servicios & Helpdesk	M	$ 80.000,00	4	4	4	4	4
	P05	Staff Seguridad Informatica	M	$ 80.000,00	6	6	5	4	4
	P06	Staff Infraestructrura y Comunicaciones	M	$ 90.000,00	4	5	4	5	5
	P07	Personal Directivo	M	$ 100.000,00	4	4	4	5	5

Los valores en $USD no corresponden al valores comercial de los activos, hace referencia al valor de los mismos para la organización (Estos valores son aproximados).

Las columnas A,C,I,D y T representan la importancia del activo en relación a las dimensión de Seguridad.

7.4. Amenazas

Para la clasificación de las amenazas se ha utilizado el enfoque metodológico de MAGERIT el cual el su libro 2 (Catalogo de elementos) sugiere la agrupación de amenazas en cuatro grandes grupos. Adicional a la agrupación, se ha incluido información referente a las dimensiones de seguridad que afecta dicha amenaza y los posibles tipos de activos que son objeto de estas amenazas (Ver Anexo 8):

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
Desastres naturales	N1	Fuego				x		x	x					
	N2	Daños por agua				x		x	x					
	N3	Otros desastres Naturales				x		x	x					
De Origen Industrial	I1	Fuego				x		x	x					
	I2	Daños por agua				x		x	x					
	I3	Contaminación Mecánica				x			x					
	I4	Contaminación electromagnética				x			x					
	I5	Avería de origen físico o lógico				x			x	x				

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
	I6	Corte del suministro eléctrico				x			x					
	I7	Condiciones inadecuadas de temperatura o humedad				x			x					
	I8	Fallo de servicios de comunicaciones				x						x		
	I9	Interrupción de otros servicios y suministros esenciales				x					x			
	I10	Degradación de los soportes de almacenamiento de la información				x					x			
	I11	Emanaciones electromagnéticas				x		x	x					
Errores y fallos no intencionados	E1	Errores de los usuarios		x	x	x				x	x		x	
	E2	Errores del administrador		x	x	x			x	x	x	x	x	
	E3	Errores de monitorización (log)			x		x				x			
	E4	Errores de configuración			x						x			
	E7	Deficiencias en la organización				x								x
	E8	Difusión de software dañino		x	x	x				x				
	E9	Errores de [re-]encaminamiento		x						x		x	x	
	E10	Errores de secuencia			x					x		x	x	
	E14	Escapes de información		x							x			
	E15	Alteración accidental de la información			x					x	x	x	x	
	E18	Destrucción de información				x				x	x	x	x	
	E19	Fugas de información		x						x	x		x	x
	E20	Vulnerabilidades de los programas (software)		x	x	x				x				
	E21	Errores de mantenimiento / actualización de programas (software)			x	x				x				
	E23	Errores de mantenimiento / actualización de equipos (hardware)				x			x					

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
	E24	Caída del sistema por agotamiento de recursos				x			x	x		x		
	E25	Pérdida de equipos		x		x			x					
	E28	Indisponibilidad del personal				x								x
Ataques intencionados	A3	Manipulación de los registros de actividad (log)			x		x				x			
	A4	Manipulación de la configuración	x	x	x						x			
	A5	Suplantación de la identidad del usuario	x	x	x					x	x	x	x	
	A6	Abuso de privilegios de acceso		x	x	x			x	x	x	x	x	
	A7	Uso no previsto		x	x	x			x	x	x	x	x	
	A8	Difusión de software dañino		x	x	x				x				
	A9	[Re-]encaminamiento de mensajes		x						x		x	x	
	A10	Alteración de secuencia			x					x		x	x	
	A11	Acceso no autorizado		x	x			x	x	x	x	x	x	
	A12	Análisis de tráfico		x								x		
	A13	Repudio			x		x				x		x	
	A14	Interceptación de información (escucha)		x								x		
	A15	Modificación deliberada de la información			x				x	x	x	x	x	
	A18	Destrucción de información				x				x	x	x	x	
	A19	Divulgación de información		x						x	x	x	x	
	A22	Manipulación de programas		x	x	x				x				
	A23	Manipulación de los equipos		x		x			x					
	A24	Denegación de servicio				x			x	x	x	x	x	
	A25	Robo		x		x			x		x			

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
	A26	Ataque destructivo				x		x	x					
	A27	Ocupación enemiga		x		x		x						
	A28	Indisponibilidad del personal				x								x
	A29	Extorsión		x	x	x								x
	A30	Ingeniería social		x	x	x								x

7.5. Análisis de amenazas

Para este análisis se tomó cada uno de los activos del inventario frente a las posibles amenazas que lo puedan llegar a afectar y se determinó la frecuencia de que dicha amenaza se pueda materializar en el activo, así mismo, se determinó el impacto que podría tener dicha materialización frente a las cinco (5) dimensiones de seguridad.

El mayor de los impactos de las dimensiones en una amenaza se tomará para calcular el valor de la materialización de la misma. Dada la cantidad de datos que genera este análisis a continuación solo se muestra datos para activos del grupo “Instalaciones” (Puede ver el análisis completo en el Anexo 8):

ACTIVO		AMENAZA		FRECUENCIA	A	C	I	D	T
I01	CPD Principal	N01	Fuego	0,002739				90%	
		N02	Daños por agua	0,002739				80%	
		N03	Otros desastres Naturales	0,002739				80%	
		I01	Fuego	0,002739				90%	
		I02	Daños por agua	0,002739				80%	
		I11	Emanaciones electromagnéticas	0,002739				50%	
		A11	Acceso no autorizado	0,002739		70%	60%		

ACTIVO		AMENAZA		FRECUENCIA	A	C	I	D	T
		A26	Ataque destructivo	0,002739				80%	
		A27	Ocupación enemiga	0,002739		80%		80%	
I02	CPD Minas	N01	Fuego	0,002739				90%	
		N02	Daños por agua	0,002739				80%	
		N03	Otros desastres Naturales	0,002739				80%	
		I01	Fuego	0,002739				90%	
		I02	Daños por agua	0,002739				80%	
		I11	Emanaciones electromagnéticas	0,002739				50%	
		A11	Acceso no autorizado	0,002739		70%	60%		
		A26	Ataque destructivo	0,002739				80%	
		A27	Ocupación enemiga	0,002739		80%		80%	
I03	CPD Puerto Maritimo	N01	Fuego	0,002739				90%	
		N02	Daños por agua	0,002739				80%	
		N03	Otros desastres Naturales	0,002739				80%	
		I01	Fuego	0,002739				90%	
		I02	Daños por agua	0,002739				80%	
		I11	Emanaciones electromagnéticas	0,002739				50%	
		A11	Acceso no autorizado	0,002739		70%	60%		
		A26	Ataque destructivo	0,002739				80%	
		A27	Ocupación enemiga	0,002739		80%		80%	

7.6. Impacto potencial

Para calcular el impacto potencial de la materialización de las amenazas se ha tomado el valor que se le asignó inicialmente a los activos y se realizó el producto de la frecuencia que establecimos anteriormente y el mayor de los impactos que se estableció en las cinco dimensiones de seguridad para cada una de las amenazas.

Asimismo, y teniendo en cuenta los resultados obtenidos la dirección de la compañía estableció que el nivel de riesgo aceptable será aquel que esté por debajo de los USD$360, por lo tanto todas aquellas amenazas cuya materialización represente un monto igual o superior a este han sido seleccionadas para diseño e implementación de salvaguardas como se muestra a continuación.

Dada la cantidad de datos que genera este análisis a continuación solo se muestra datos para activos del grupo "Instalaciones" (Puede ver el análisis completo en el Anexo 8):

(Los valores resaltados en cada activo representan el mayor valor de riesgo cuantificado para el mismo).

ACTIVO		AMENAZA		FRECUENCIA	FRECUENCIA * IMPACTO * VALOR	¿SALVAGUARDAR?
I01	CPD Principal	N01	Fuego	0,002739	$ 616,28	SI
		N02	Daños por agua	0,002739	$ 547,80	SI
		N03	Otros desastres Naturales	0,002739	$ 547,80	SI
		I01	Fuego	0,002739	$ 616,28	SI
		I02	Daños por agua	0,002739	$ 547,80	SI
		I11	Emanaciones electromagnéticas	0,002739	$ 342,38	NO
		A11	Acceso no autorizado	0,002739	$ 479,33	SI
		A26	Ataque destructivo	0,002739	$ 547,80	SI
		A27	Ocupación enemiga	0,002739	$ 547,80	SI
I02	CPD Minas	N01	Fuego	0,002739	$ 369,77	SI

ACTIVO		AMENAZA		FRECUENCIA	FRECUENCIA * IMPACTO * VALOR	¿SALVAGUARDAR?
		N02	Daños por agua	0,002739	$ 328,68	NO
		N03	Otros desastres Naturales	0,002739	$ 328,68	NO
		I01	Fuego	0,002739	$ 369,77	SI
		I02	Daños por agua	0,002739	$ 328,68	NO
		I11	Emanaciones electromagnéticas	0,002739	$ 205,43	NO
		A11	Acceso no autorizado	0,002739	$ 287,60	NO
		A26	Ataque destructivo	0,002739	$ 328,68	NO
		A27	Ocupación enemiga	0,002739	$ 328,68	NO
I03	CPD Puerto Maritimo	N01	Fuego	0,002739	$ 419,07	SI
		N02	Daños por agua	0,002739	$ 372,50	SI
		N03	Otros desastres Naturales	0,002739	$ 372,50	SI
		I01	Fuego	0,002739	$ 419,07	SI
		I02	Daños por agua	0,002739	$ 372,50	SI
		I11	Emanaciones electromagnéticas	0,002739	$ 232,82	NO
		A11	Acceso no autorizado	0,002739	$ 325,94	NO
		A26	Ataque destructivo	0,002739	$ 372,50	SI
		A27	Ocupación enemiga	0,002739	$ 372,50	SI

7.7. Riesgo residual

Para cada una de las amenazas que fueron identificadas y cuya cuantificación de riesgo supera el establecido por la compañía, se diseña una serie de controles o salvaguardas que ayudan a mitigar el riesgo (ya sea por su probabilidad de ocurrencia o por su impacto), basado en la reducción del riesgo se vuelve a cuantificar el riesgo y en este caso todos quedaron por debajo del umbral establecido, lo que indica que en cierta forma los controles son adecuados.

Dada la cantidad de datos que genera este análisis a continuación solo se muestra datos para activos del grupo "Instalaciones" (Puede ver el análisis completo en el Anexo 8):

ACTIVO		AMENAZA		SALVAGUARDA	REDUCCION DEL RIESGO (POR FECUENCIA O IMPACTO)	NUEVA CUENTIFICACION
I01	CPD Principal	N01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 184,88
		N02	Daños por agua	Detectores de humedad	60%	$ 219,12
		N03	Otros desastres Naturales	Pólizas de seguro	40%	$ 328,68
		I01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 184,88
		I02	Daños por agua	Detectores de humedad	60%	$ 219,12
		I11	Emanaciones electromagnéticas	N/A	0%	$ 342,38
		A11	Acceso no autorizado	Video vigilancia y tarjetas de proximidad	70%	$ 143,80
		A26	Ataque destructivo	Pólizas de seguro	40%	$ 328,68
		A27	Ocupación enemiga	Pólizas de seguro	40%	$ 328,68
I02	CPD Minas	N01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 110,93
		N02	Daños por agua	N/A	0%	$ 328,68

ACTIVO		AMENAZA		SALVAGUARDA	REDUCCION DEL RIESGO (POR FECUENCIA O IMPACTO)	NUEVA CUENTIFICACION
		N03	Otros desastres Naturales	N/A	0%	$ 328,68
		I01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 110,93
		I02	Daños por agua	N/A	0%	$ 328,68
		I11	Emanaciones electromagnéticas	N/A	0%	$ 205,43
		A11	Acceso no autorizado	N/A	0%	$ 287,60
		A26	Ataque destructivo	N/A	0%	$ 328,68
		A27	Ocupación enemiga	N/A	0%	$ 328,68
I03	CPD Puerto Maritimo	N01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 125,72
		N02	Daños por agua	Detectores de humedad	60%	$ 149,00
		N03	Otros desastres Naturales	Pólizas de seguro	40%	$ 223,50
		I01	Fuego	Sistema de supresión y protección contra incendios	70%	$ 125,72
		I02	Daños por agua	Detectores de humedad	60%	$ 149,00
		I11	Emanaciones electromagnéticas	N/A	0%	$ 232,82
		A11	Acceso no autorizado	N/A	0%	$ 325,94
		A26	Ataque destructivo	Pólizas de seguro	40%	$ 223,50
		A27	Ocupación enemiga	Pólizas de seguro	40%	$ 223,50

8. PROPUESTA DE PROYECTOS

8.1. Aspectos generales

En este punto ya se conocen los riesgos residuales de la organización, por lo tanto se deben plantear proyectos que ayuden a alcanzar el nivel de seguridad deseado.

Los proyectos planteados son el resultado de agrupar las recomendaciones identificadas en la fase de análisis de riesgos para facilitar. Se incidirá no sólo en la mejora en relación con la gestión de la seguridad, sino también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada. El documento de presentación de proyectos puede ser consultado en el Anexo 9.

8.2. Objetivo de los proyectos

Para el ejemplo desarrollado el compendio de proyectos presentados tienen como objetivos:

- Minimizar los riesgos identificados a un nivel aceptable.
- Contribuir en el desarrollo corporativo mediante la adopción de mejores prácticas.
- Asegurar la continuidad del negocio frente posibles eventualidades.
- Brindar herramientas que permitan conocer el estado de salud de la compañía en cuanto a seguridad de la información se refiere.

8.3. Alcance general de los proyectos presentados

Los proyectos son resultado de la cuantificación del riesgo realizado por la compañía y se enfocan en resolver las debilidades de control o vulnerabilidades identificadas. Dichos proyectos están asociados directamente a los activos que en caso de materialización del riesgo signifiquen una pérdida considerable para la compañía; por esto, no solo se han considerado componentes tecnológicos sino que en la implementación de los mismos también incluyen procesos, personas, cultura organizacional, etc.

8.4. Agrupación de proyectos

Dada la afinidad de los proyectos a realizar estos se han dividido en tres grandes grupos:

- Mitigación de riesgos asociados a desastres de origen natural o Industrial.

- Mitigación del riesgo asociado a ataques intencionados.
- Mitigación del riesgo asociado a errores no intencionados.

8.5. Mitigación de riesgos asociados a desastres de origen natural o industrial

Descripción: Este proyecto busca fortalecer los controles actuales de seguridad física y ambiental, de igual forma se pretende causar un impacto positivo a la cultura organizacional en cuanto a conciencia de riesgos y adopción de mejores prácticas.

Objetivos: al finalizar este proyecto la compañía será capaz de:

- Manejar incidentes de forma centralizada y tener alertas tempranas de incendio, inundación (o alto índice de humedad), corto circuito u otros problemas electicos.
- Gestionar mantenimientos preventivos a dispositivos de control físico y ambiental.
- Contar con una cobertura de seguros frente a desastres naturales no predecibles como terremotos, maremotos, huracanes, etc.
- Contar con personal capacitado para enfrentar emergencias de origen natural o industrial.
- Crear conciencia en los empleados de la compañía frente a la importancia de protección y prevención de incidentes.

Beneficios: Se fortalecerá la seguridad física y controles ambientales, se establecerán procedimientos claros y buenas prácticas frente a amenazas del tipo natural o industrial, se implementaran mecanismos de medición que contribuyan al mejoramiento continuo y posibilidad de generar indicadores y se brinda apoyo a otros estándares certificables como el de calidad y continuidad.

Alcance: Este proyecto cobija instalaciones y hardware, más específicamente:

- CPD Principal
- CPD Minas
- CPD Puerto Marítimo
- Granja de servidores VMware

Fases: Este proyecto comprende las siguientes fases:

- **Evaluación del estado actual**: El equipo de trabajo analizará los controles actuales con los que cuenta la compañía y realizará un análisis de brecha para identificar los equipos que deben ser adquiridos y los procedimientos que deben ser desarrollados.

- **Establecer acuerdos con terceros**: Una vez obtenido los resultados del análisis de brecha y sean aprobados los equipos que serán adquiridos (estos serán pocos dado que ya existen controles implementados), se establecerán acuerdos con terceros en lo relacionado con: acuerdos de niveles de servicio, periodicidad de mantenimiento de equipos, adquisición de pólizas de seguro para la protección frente a desastres naturales y de origen industrial, personal de contacto, conexión de equipos de monitoreo y alarmas con las centrales locales (bomberos, policía, etc.).

- **Estructuración de procedimientos**: Conociendo las capacidades del equipo y habiendo establecido los acuerdos con terceros, en esta fase se diseñaran los procedimientos de: reporte y atención de incidentes, gestión de cambios y mantenimientos, registro de eventos, entrenamiento, configuración de equipos, métricas, prueba de equipos/escenarios y evaluación de proveedores.

- **Ejecución de trabajos:** En esta etapa se realizaran los trabajos de instalación y configuración de equipos.

- **Pruebas**: Se diseñaran escenarios de pruebas que se ejecutaran para verificar que se hayan alcanzado los objetivos propuestos.

- **Entrenamiento**: Se realizará el entrenamiento respectivo a los responsables e administración y monitoreo de equipos y se entregaran pautas al equipo de seguridad industrial de la compañía para realizar una campaña de concientización.

- **Puesta en marcha**: Ya habiendo probado los equipos y con personal de la compañía entrenado, se formaliza la puesta en marcha de los nuevos equipos y sistemas.

- **Reporte**: La gerencia del proyecto presenta los resultados de implementación a la dirección de la compañía.

Cronograma: El cronograma propuesto para este proyecto es de tres (3) meses:

Fase	Mes 1	Mes 2	Mes 3
Evaluación del estado actual			
Establecer acuerdos con terceros			
Estructuración de procedimientos			
Ejecución de trabajos			
Pruebas			
Entrenamiento			
Puesta en marcha			
Reporte			

Cabe aclarar que aunque el proyecto tiene la duración mostrada en el cronograma, existen actividades de mantenimiento y pruebas que se deben ejecutar con una periodicidad establecida la cual fomenta el continuo desarrollo de los sistemas de gestión de seguridad de la compañía.

Costos: a continuación se muestran los costos del proyecto:

Integrante	% Participación	Honorarios
Gerente de proyecto	10	€ 1.000,00
Coordinador de proyecto	20	€ 1.200,00
Consultores	70	€ 3.000,00

El valor de compra de equipos, pólizas y mantenimientos se estimó en € 2.000,00

Costo total del proyecto: **€ 7.200,00**

8.6. Mitigación del riesgo asociado a ataques intencionados

Descripción: Este proyecto busca fortalecer los controles actuales de seguridad lógica y física que puedan afectar activos críticos de la compañía frente a ataques intencionados de personal externo o interno de la compañía, los controles propuestos siguen el siguiente esquema de protección: evitar el riesgo, identificar el riesgo, mitigar el riesgo.

Objetivos: al finalizar este proyecto la compañía será capaz de:

- Restringir y monitorear el acceso de áreas protegidas.
- Contar con alertas tempranas frente a posibles ataques y accesos no autorizados.
- Tener cobertura de seguros frente a robos, ocupación enemiga y ataques destructivos.
- Monitorear la integridad de la información y configuración de equipos y aplicaciones.

Beneficios: Se fortalecerá la seguridad física y lógica de la compañía, se incrementará la confianza tanto para los clientes externos como internos y se contribuirá a la cultura de la prevención.

Alcance: Este proyecto cobija instalaciones, hardware, Aplicativos, datos y servicios, más específicamente:

- CPD Principal
- CPD Minas
- CPD Puerto Marítimo
- Granja de servidores VMware
- Controlador de dominio principal
- Servidor de bases de datos
- Servidor de correo electrónico
- SAP ERP
- Base de datos ERP
- Servicio de mensajería

Fases: Este proyecto comprende las siguientes fases:

- **Evaluación del estado actual**: El equipo de trabajo analizará los controles actuales con los que cuenta la compañía y realizará un análisis de brecha para identificar los elementos que deben ser adquiridos y los procedimientos que deben ser desarrollados.

- **Establecer acuerdos con terceros**: Una vez obtenido los resultados del análisis de brecha y sean aprobados los elementos que serán adquiridos, se establecerán acuerdos con terceros en lo relacionado con: acuerdos de niveles de servicio, periodicidad de mantenimiento de equipos, adquisición de pólizas de seguro para la protección frente a robo, Ataques destructivos y ocupación enemiga, personal de contacto.

- **Estructuración de procedimientos**: Conociendo las capacidades del equipo y habiendo establecido los acuerdos con terceros, en esta fase se diseñaran los procedimientos de: Gestión de cambios y mantenimientos, registro de eventos, entrenamiento, configuración software y equipos, métricas, prueba de equipos/escenarios y evaluación de proveedores.

- **Ejecución de trabajos:** En esta etapa se realizaran los trabajos de instalación y configuración de equipos.

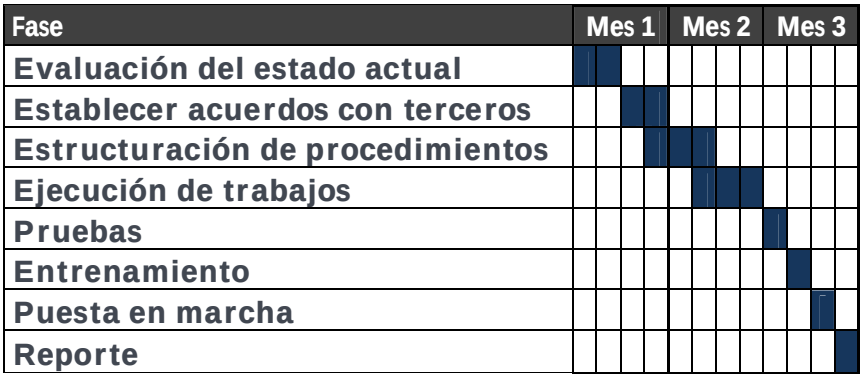
- **Pruebas**: Se diseñaran escenarios de pruebas que se ejecutaran para verificar que se hayan alcanzado los objetivos propuestos.

- **Entrenamiento**: Se realizará el entrenamiento respectivo a los responsables de administración y monitoreo de equipos y software, del mismo modo se entregaran pautas para elaborar una campaña de concientización a los usuarios finales.

- **Puesta en marcha**: Ya habiendo probado los equipos y con personal de la compañía entrenado, se formaliza la puesta en marcha de los nuevos equipos y sistemas.

- **Reporte**: La gerencia del proyecto presenta los resultados de implementación a la dirección de la compañía.

Cronograma: El cronograma propuesto para este proyecto es de tres (3) meses:



Cabe aclarar que aunque el proyecto tiene la duración mostrada en el cronograma, existen actividades de mantenimiento y pruebas que se deben ejecutar con una periodicidad establecida la cual fomenta el continuo desarrollo de los sistemas de gestión de seguridad de la compañía.

Costos: a continuación se muestran los costos del proyecto:

Integrante	% Participación	Honorarios
Gerente de proyecto	10	€ 1.000,00
Coordinador de proyecto	20	€ 1.200,00
Consultores	70	€ 3.000,00

El valor de compra de equipos, software, pólizas y mantenimientos se estimó en € 6.000,00

Costo total del proyecto: **€ 11.200,00**

8.7. Mitigación del riesgo asociado a errores no intencionados

Descripción: Este proyecto busca fortalecer los controles actuales de seguridad lógica y física que puedan afectar activos críticos de la compañía frente a errores no intencionados de personal externo o interno de la compañía, los controles propuestos siguen el siguiente esquema de protección: evitar el riesgo, identificar el riesgo, mitigar el riesgo.

Objetivos: al finalizar este proyecto la compañía será capaz de:

- Contar con administración centralizada de antivirus.
- Contar con alertas tempranas frente a posibles errores o fallas.
- Tener cobertura de seguros frente a perdida y daño de equipos.
- Monitorear la integridad de la información y configuración de equipos y aplicaciones.
- Contar con estándares y baselines de configuración.
- Contar con controles DLP para evitar la fuga de datos.

Beneficios: Se fortalecerá la seguridad física y lógica de la compañía, se incrementará la confianza tanto para los clientes externos como internos y se contribuirá a la cultura de la prevención.

Alcance: Este proyecto cobija instalaciones, hardware, Aplicativos, datos, servicios y personas, más específicamente:

- Controlador de dominio principal
- Controlador de dominio secundario
- Servidor de Base de Datos
- Servidor de correo
- Correo perimetral BackBerry
- Granja de Servidores Vmware
- SAP/BW Servers
- Administración Vmware
- File Server
- Antivirus, Ariadna
- SAP ERP
- Sistema de ferrocarril
- Sistema de Basculas
- Sistema de cargue (puerto Maritimo)
- Sistema de Laboratorio / Calidad
- ERP Database
- BD Sistemas de control
- BD Gestion Documental
- Internet
- Correo Electrónico
- Red LAN
- Red WAN
- Staff Infraestructrura y Comunicaciones
- Personal directivo

Fases: Este proyecto comprende las siguientes fases:

- **Evaluación del estado actual**: El equipo de trabajo analizará los controles actuales con los que cuenta la compañía y realizará un análisis de brecha para identificar los elementos que deben ser adquiridos y los procedimientos que deben ser desarrollados.

- **Establecer acuerdos con terceros**: Una vez obtenido los resultados del análisis de brecha y sean aprobados los elementos que serán adquiridos, se establecerán acuerdos con terceros en lo relacionado con: acuerdos de niveles de servicio, periodicidad de mantenimiento de equipos, adquisición de pólizas de seguro para la protección frente a robo, Ataques destructivos y ocupación enemiga, personal de contacto.

- **Estructuración de procedimientos**: Conociendo las capacidades del equipo y habiendo establecido los acuerdos con terceros, en esta fase se diseñaran los procedimientos de: Gestión de cambios y mantenimientos, registro de eventos,

entrenamiento, configuración software y equipos, métricas, prueba de equipos/escenarios y evaluación de proveedores.

- **Ejecución de trabajos:** En esta etapa se realizaran los trabajos de instalación y configuración de equipos.

- **Pruebas**: Se diseñaran escenarios de pruebas que se ejecutaran para verificar que se hayan alcanzado los objetivos propuestos.

- **Entrenamiento**: Se realizará el entrenamiento respectivo a los responsables de administración y monitoreo de equipos y software, del mismo modo se entregaran pautas para elaborar una campaña de concientización a los usuarios finales.

- **Puesta en marcha**: Ya habiendo probado los equipos y con personal de la compañía entrenado, se formaliza la puesta en marcha de los nuevos equipos y sistemas.

- **Reporte**: La gerencia del proyecto presenta los resultados de implementación a la dirección de la compañía.

Cronograma: El cronograma propuesto para este proyecto es de cuatro (4) meses:

Fase	Mes 1				Mes 2				Mes 3				Mes 4			
Evaluación del estado actual																
Establecer acuerdos con terceros																
Estructuración de procedimientos																
Ejecución de trabajos																
Pruebas																
Entrenamiento																
Puesta en marcha																
Reporte																

Cabe aclarar que aunque el proyecto tiene la duración mostrada en el cronograma, existen actividades de mantenimiento y pruebas que se deben ejecutar con una periodicidad establecida la cual fomenta el continuo desarrollo de los sistemas de gestión de seguridad de la compañía.

Costos: a continuación se muestran los costos del proyecto:

Integrante	% Participación	Honorarios
Gerente de proyecto	10	€ 1.500,00
Coordinador de proyecto	20	€ 1.900,00
Consultores	70	€ 6.000,00

El valor de compra de equipos, software, pólizas y mantenimientos se estimó en € 9.000,00

Costo total del proyecto: **€ 18.400,00**

9. AUDITORIA DE CUMPLIMIENTO

9.1. Metodología

Con el fin de establecer el nivel de cumplimiento que tiene la organización frente a la guía de mejores prácticas **ISO/IEC 27002:2005** se ha elaborado una plantilla donde se encuentran los 11 dominios o áreas de aplicación, los 39 objetivos de control y los 133 controles de seguridad (Ver Anexo 10).

Para cada control se evaluó su nivel o estado de cumplimiento con base a la siguiente convención:

Nivel	Porcentaje	Descripción
Inexistente	0%	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver. Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
Reproducible, pero intuitivo	50%	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
Proceso definido	90%	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.

Nivel	Porcentaje	Descripción
Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
Optimizado	100%	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
No Aplica	N/A	El control no es aplicable a la organización.

Teniendo en cuenta el nivel de cumplimiento para cada control, se calcula el promedio de los mismos, proporcionando así el nivel de cumplimiento con los objetivos de control y a más grandes rasgos el nivel de alineamiento con las 11 áreas que comprende la norma, es decir:

- Política de seguridad
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

Nota: Para el ejemplo desarrollado el nivel de cumplimiento que desea alcanzar la compañía es de un 80%.

9.2. Evaluación de la madurez

Teniendo en cuenta la metodología establecida y con base al análisis de implementación de los controles actuales de la compañía, se procedió con la siguiente clasificación:

CONTROLES ISO 27002:2005			Efectividad	% Efectividad
Clausula	**Sec**	**Control/Objetivo de Control**		
Politica de Seguridad	5,1	Política de seguridad de la información		30%
	5.1.1	Documento de política de seguridad de la información	Reproducible, pero intuitivo	50%
	5.1.2	Revisión de la política de seguridad de la información	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**30%**
Aspectos Organizativos de la seguridad de la información	6,1	Organización Interna		35%
	6.1.1	Compromiso de la Dirección con la seguridad de la información.	Reproducible, pero intuitivo	50%
	6.1.2	Coordinación de la seguridad de la información.	Reproducible, pero intuitivo	50%
	6.1.3	Asignación de responsabilidades relativas a la seg. de la información.	Inicial / Ad-hoc	10%
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información.	Reproducible, pero intuitivo	50%
	6.1.5	Acuerdos de confidencialidad.	Reproducible, pero intuitivo	50%
	6.1.6	Contacto con las autoridades.	Reproducible, pero intuitivo	50%
	6.1.7	Contacto con grupos de especial interés.	Inicial / Ad-hoc	10%
	6.1.8	Revisión independiente de la seguridad de la información	Inicial / Ad-hoc	10%
	6,2	Terceros		37%

	6.2.1	Identificación de los riesgos derivados del acceso de terceros.	Reproducible, pero intuitivo	50%
	6.2.2	Tratamiento de la seguridad en la relación con los clientes.	Inicial / Ad-hoc	10%
	6.2.3	Tratamiento de la seguridad en contratos con terceros.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**36%**
Gestión de Activos	7,1	Responsabilidad sobre los activos.		50%
	7.1.1	Inventario de activos.	Reproducible, pero intuitivo	50%
	7.1.2	Propiedad de los activos.	Reproducible, pero intuitivo	50%
	7.1.3	Uso aceptable de los activos.	Reproducible, pero intuitivo	50%
	7,2	Clasificación de la información.		50%
	7.2.1	Directrices de clasificación.	Reproducible, pero intuitivo	50%
	7.2.2	Etiquetado y manipulado de la información.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**50%**
Seguridad asociada a Recursos Humanos	8,1	Antes del empleo.		92%
	8.1.1	Funciones y responsabilidades.	Proceso definido	90%
	8.1.2	Investigación de antecedentes.	Gestionado y medible	95%
	8.1.3	Términos y condiciones de contratación.	Proceso definido	90%
	8,2	Durante el empleo.		37%
	8.2.1	Responsabilidades de la Dirección.	Inicial / Ad-hoc	10%
	8.2.2	Concienciación, formación y capacitación en seguridad de la información.	Inicial / Ad-hoc	10%
	8.2.3	Proceso disciplinario.	Proceso definido	90%
	8,3	Cese del empleo o cambio de puesto de trabajo.		50%

	8.3.1	Responsabilidad del cese o cambio.	Reproducible, pero intuitivo	50%
	8.3.2	Devolución de activos.	Reproducible, pero intuitivo	50%
	8.3.3	Retirada de los derechos de acceso.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**59%**
Seguridad Fisica y del Entorno	9,1	Áreas seguras.		43%
	9.1.1	Perímetro de seguridad física.	Inicial / Ad-hoc	10%
	9.1.2	Controles físicos de entrada.	Reproducible, pero intuitivo	50%
	9.1.3	Seguridad de oficinas, despachos e instalaciones.	Reproducible, pero intuitivo	50%
	9.1.4	Protección contra las amenazas externas y de origen ambiental.	Reproducible, pero intuitivo	50%
	9.1.5	Trabajo en áreas seguras.	Reproducible, pero intuitivo	50%
	9.1.6	Áreas de acceso público y de carga y descarga.	Reproducible, pero intuitivo	50%
	9,2	Seguridad de los equipos.		44%
	9.2.1	Emplazamiento y protección de equipos.	Reproducible, pero intuitivo	50%
	9.2.2	Instalaciones de suministro.	Reproducible, pero intuitivo	50%
	9.2.3	Seguridad del cableado.	Reproducible, pero intuitivo	50%
	9.2.4	Mantenimiento de los equipos.	Reproducible, pero intuitivo	50%
	9.2.5	Seguridad de los equipos fuera de las instalaciones.	Reproducible, pero intuitivo	50%
	9.2.6	Reutilización o retirada segura de equipos.	Inicial / Ad-hoc	10%
	9.2.7	Retirada de materiales propiedad de la empresa.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**44%**

Gestión de Comunicaciones y operaciones	10,1	Responsabilidades y procedimientos de operación.		30%
	10.1.1	Documentación de los procedimientos de operación.	Inicial / Ad-hoc	10%
	10.1.2	Gestión de cambios.	Inicial / Ad-hoc	10%
	10.1.3	Segregación de tareas.	Inicial / Ad-hoc	10%
	10.1.4	Separación de los recursos de desarrollo, prueba y operación.	Proceso definido	90%
	10,2	Gestión de la provisión de servicios.		37%
	10.2.1	Provisión de servicios.	Reproducible, pero intuitivo	50%
	10.2.2	Supervisión y revisión de los servicios prestados por terceros.	Reproducible, pero intuitivo	50%
	10.2.3	Gestión del cambio en los servicios prestados por terceros.	Inicial / Ad-hoc	10%
	10,3	Planificación y aceptación del sistema.		30%
	10.3.1	Gestión de capacidades.	Reproducible, pero intuitivo	50%
	10.3.2	Aceptación del sistema.	Inicial / Ad-hoc	10%
	10,4	Protección contra el código malicioso y descargable.		50%
	10.4.1	Controles contra el código malicioso.	Reproducible, pero intuitivo	50%
	10.4.2	Controles contra el código descargado en el cliente.	Reproducible, pero intuitivo	50%
	10,5	Copias de seguridad.		90%
	10.5.1	Copias de seguridad de la información.	Proceso definido	90%
	10,6	Gestión de la seguridad de las redes.		50%
	10.6.1	Controles de red.	Reproducible, pero intuitivo	50%
	10.6.2	Seguridad de los servicios de red.	Reproducible, pero intuitivo	50%
	10,7	Manipulación de los soportes.		18%

10.7.1	Gestión de soportes extraíbles.	Inexistente	0%
10.7.2	Retirada de soportes.	Reproducible, pero intuitivo	50%
10.7.3	Procedimientos de manipulación de la información.	Inicial / Ad-hoc	10%
10.7.4	Seguridad de la documentación del sistema.	Inicial / Ad-hoc	10%
10,8	Intercambio de información.		34%
10.8.1	Políticas y procedimientos de intercambio de información.	Inicial / Ad-hoc	10%
10.8.2	Acuerdos de intercambio.	Inicial / Ad-hoc	10%
10.8.3	Soportes físicos en tránsito.	Reproducible, pero intuitivo	50%
10.8.4	Mensajería electrónica.	Reproducible, pero intuitivo	50%
10.8.5	Sistemas de información empresariales.	Reproducible, pero intuitivo	50%
10,9	Servicios de comercio electrónico.		50%
10.9.1	Comercio electrónico.	No Aplica	N/A
10.9.2	Transacciones en línea.	No Aplica	N/A
10.9.3	Información públicamente disponible.	Reproducible, pero intuitivo	50%
10,10	Supervisión.		50%
10.10.1	Registros de auditoría.	Proceso definido	90%
10.10.2	Supervisión del uso del sistema.	Reproducible, pero intuitivo	50%
10.10.3	Protección de la información de los registros.	Inicial / Ad-hoc	10%
10.10.4	Registros de administración y operación.	Inicial / Ad-hoc	10%
10.10.5	Registro de fallos.	Reproducible, pero intuitivo	50%
10.10.6	Sincronización del reloj.	Proceso definido	90%
		Efectividad conjunta:	**40%**

Control de Acceso	11,1	Requisitos de negocio para el control de acceso.		50%
	11.1.1	Política de control de acceso.	Reproducible, pero intuitivo	50%
	11,2	Gestión de acceso de usuario.		60%
	11.2.1	Registro de usuario.	Reproducible, pero intuitivo	50%
	11.2.2	Gestión de privilegios.	Reproducible, pero intuitivo	50%
	11.2.3	Gestión de contraseñas de usuario.	Reproducible, pero intuitivo	50%
	11.2.4	Revisión de los derechos de acceso de usuario.	Proceso definido	90%
	11,3	Responsabilidades de usuario.		50%
	11.3.1	Uso de contraseñas.	Reproducible, pero intuitivo	50%
	11.3.2	Equipo de usuario desatendido.	Reproducible, pero intuitivo	50%
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	Reproducible, pero intuitivo	50%
	11,4	Control de acceso a la red.		44%
	11.4.1	Política de uso de los servicios en red.	Reproducible, pero intuitivo	50%
	11.4.2	Autenticación de usuario para conexiones externas.	Proceso definido	90%
	11.4.3	Identificación de los equipos en las redes.	Reproducible, pero intuitivo	50%
	11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Reproducible, pero intuitivo	50%
	11.4.5	Segregación de las redes.	Inicial / Ad-hoc	10%
	11.4.6	Control de la conexión a la red.	Reproducible, pero intuitivo	50%
	11.4.7	Control de encaminamiento (routing) de red.	Inicial / Ad-hoc	10%

	11,5	Control de acceso al sistema operativo.		57%
	11.5.1	Procedimientos seguros de inicio de sesión.	Reproducible, pero intuitivo	50%
	11.5.2	Identificación y autenticación de usuario.	Reproducible, pero intuitivo	50%
	11.5.3	Sistema de gestión de contraseñas.	Reproducible, pero intuitivo	50%
	11.5.4	Uso de los recursos del sistema.	Inicial / Ad-hoc	10%
	11.5.5	Desconexión automática de sesión.	Proceso definido	90%
	11.5.6	Limitación del tiempo de conexión.	Proceso definido	90%
	11,6	Control de acceso a las aplicaciones y a la información.		90%
	11.6.1	Restricción del acceso a la información.	Proceso definido	90%
	11.6.2	Aislamiento de sistemas sensibles.	Proceso definido	90%
	11,7	Ordenadores portátiles y teletrabajo.		70%
	11.7.1	Ordenadores portátiles y comunicaciones móviles.	Reproducible, pero intuitivo	50%
	11.7.2	Teletrabajo.	Proceso definido	90%
		Efectividad conjunta:		**57%**
Adquisición, desarrollo y mantenimiento de Sistemas de Información	12,1	Requisitos de seguridad de los sistemas de información.		50%
	12.1.1	Análisis y especificación de los requisitos de seguridad.	Reproducible, pero intuitivo	50%
	12,2	Tratamiento correcto de las aplicaciones.		40%
	12.2.1	Validación de los datos de entrada.	Reproducible, pero intuitivo	50%
	12.2.2	Control del procesamiento interno.	Reproducible, pero intuitivo	50%
	12.2.3	Integridad de los mensajes.	Inicial / Ad-hoc	10%
	12.2.4	Validación de los datos de salida.	Reproducible, pero intuitivo	50%
	12,3	Controles criptográficos.		5%

	12.3.1	Política de uso de los controles criptográficos.	Inexistente	0%
	12.3.2	Gestión de claves.	Inicial / Ad-hoc	10%
	12,4	Seguridad de los archivos de sistema.		7%
	12.4.1	Control del software en explotación.	Inicial / Ad-hoc	10%
	12.4.2	Protección de los datos de prueba del sistema.	Inexistente	0%
	12.4.3	Control de acceso al código fuente de los programas.	Inicial / Ad-hoc	10%
	12,5	Seguridad en los procesos de desarrollo y soporte.		24%
	12.5.1	Procedimientos de control de cambios.	Reproducible, pero intuitivo	50%
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Inexistente	0%
	12.5.3	Restricciones a los cambios en los paquetes de software.	Inicial / Ad-hoc	10%
	12.5.4	Fugas de información.	Inicial / Ad-hoc	10%
	12.5.5	Externalización del desarrollo de software.	Reproducible, pero intuitivo	50%
	12,6	Gestión de la vulnerabilidad técnica.		
	12.6.1	Control de las vulnerabilidades técnicas	No Aplica	N/A
		Efectividad conjunta:		**24%**
Gestión de incidentes de la seguridad de la Información	13,1	Notificación de eventos y puntos débiles de seguridad de la información.		73%
	13.1.1	Notificación de los eventos de seguridad de la información.	Gestionado y medible	95%
	13.1.2	Notificación de puntos débiles de seguridad.	Reproducible, pero intuitivo	50%
	13,2	Gestión de incidentes y mejoras de seguridad de la información.		37%
	13.2.1	Responsabilidades y procedimientos.	Reproducible, pero intuitivo	50%

	13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Inicial / Ad-hoc	10%
	13.2.3	Recopilación de evidencias.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**52%**
Gestión de la continuidad del negocio	14,1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.		26%
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Inicial / Ad-hoc	10%
	14.1.2	Continuidad del negocio y evaluación de riesgos.	Inicial / Ad-hoc	10%
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Reproducible, pero intuitivo	50%
	14.1.4	Marco de referencia para la planificación de la cont. del negocio.	Reproducible, pero intuitivo	50%
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Inicial / Ad-hoc	10%
			Efectividad conjunta:	**26%**
Cumplimiento	15,1	Cumplimiento de los requisitos legales.		30%
	15.1.1	Identificación de la legislación aplicable.	No Aplica	N/A
	15.1.2	Derechos de propiedad intelectual (DPI).	No Aplica	N/A
	15.1.3	Protección de los documentos de la organización.	Reproducible, pero intuitivo	50%
	15.1.4	Protección de datos y privacidad de la información de carácter personal.	Inicial / Ad-hoc	10%
	15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.	No Aplica	N/A
	15.1.6	Regulación de los controles criptográficos.	No Aplica	N/A
	15,2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		30%
	15.2.1	Cumplimiento de las políticas y normas de seguridad.	Reproducible, pero intuitivo	50%

	15.2.2	Comprobación del cumplimiento técnico.	Inicial / Ad-hoc	10%
	15,3	Consideraciones sobre las auditorías de los sistem. de información.		50%
	15.3.1	Controles de auditoría de los sistemas de información.	Reproducible, pero intuitivo	50%
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Reproducible, pero intuitivo	50%
			Efectividad conjunta:	**37%**

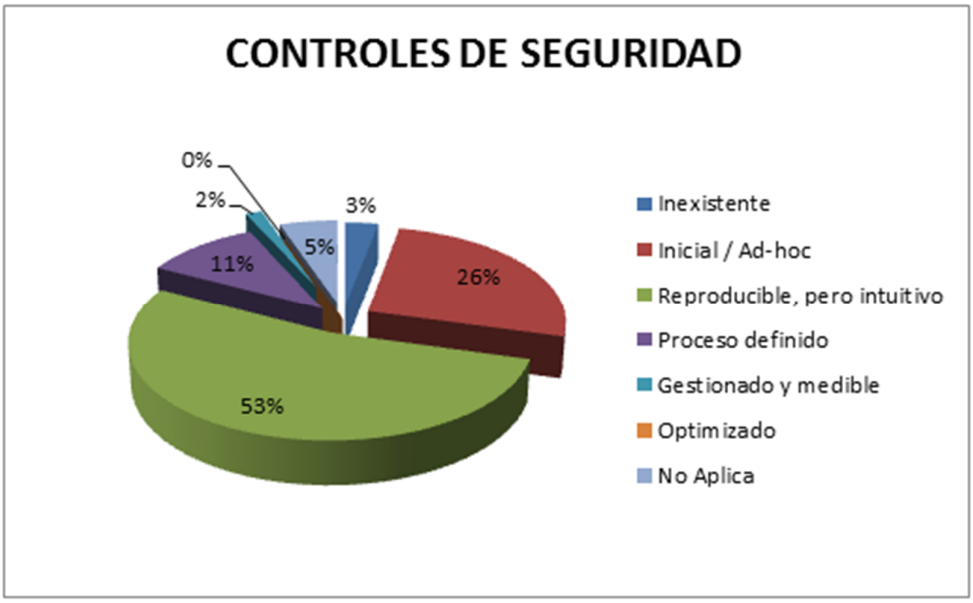
9.3. Resultados

Teniendo en cuenta que el nivel de cumplimiento deseado por la compañía es de un 80%, se puede concluir que la compañía se encuentra a mitad del camino con un nivel de cumplimiento general del 41%.

La efectividad de los controles se encuentra distribuida así:

Nivel	Controles
Inexistente	4
Inicial / Ad-hoc	35
Reproducible, pero intuitivo	71
Proceso definido	14
Gestionado y medible	2
Optimizado	0
No Aplica	7

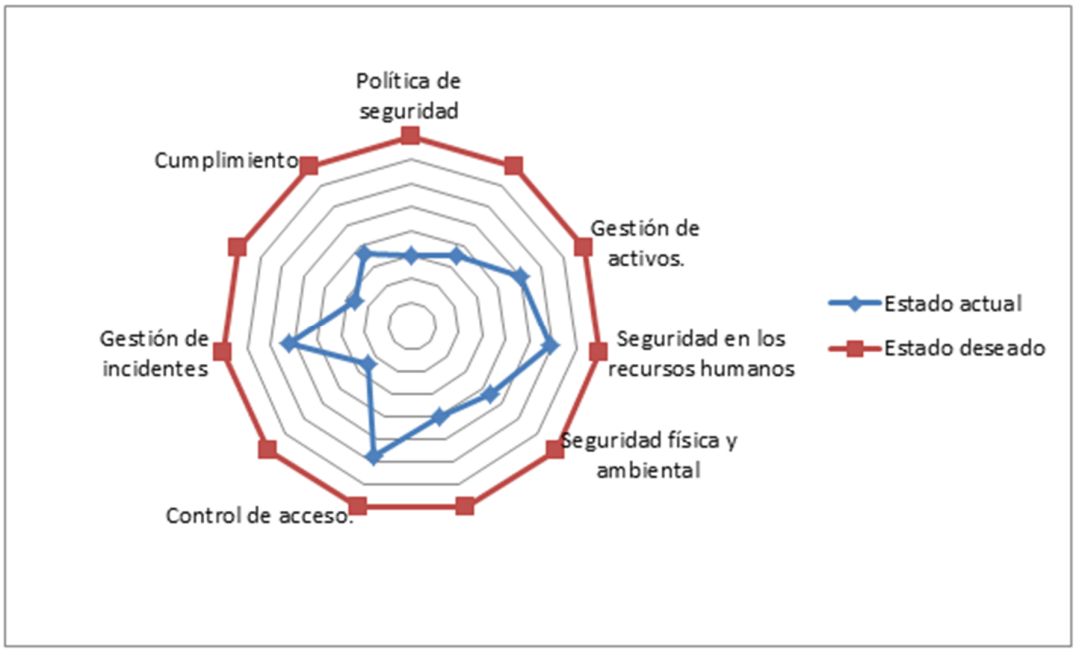
Representado gráficamente de la siguiente forma:



De igual forma, se identificó que obtuvo que el nivel de cumplimiento de las 11 áreas (dominios) evaluados es:

Dominio	Estado actual
Política de seguridad	30%
Organización de la seguridad de la información.	36%
Gestión de activos.	50%
Seguridad en los recursos humanos	59%
Seguridad física y ambiental	44%
Gestión de comunicaciones y operaciones.	40%
Control de acceso.	57%
Adquisición, desarrollo y mantenimiento de Sistemas de Información	24%
Gestión de incidentes	52%
Gestión de continuidad de negocio	26%
Cumplimiento	37%

El cual se evidencia mediante el siguiente grafico de radar:



10. CONCLUSIONES

Con la realización de este trabajo se han logrado el objetivo de crear de manera practica un plan de trabajo que permita implementar la ISO/IEC 27001:2005. Así mismo, se desarrolló la información normativa y conceptos generales que deben conocerse antes de iniciar un proceso de implementación.

Fue posible establecer de manera práctica el estado actual de una compañía en lo que refiere a los objetivos del SGSI que se desea implementar.

Se proporcionó información relevante para realizar el análisis de riesgos de una compañía. Tanto en fundamentación teórica como su desarrollo.

A manera de ejemplo, se presentaron propuestas de proyectos que permitirían alcanzar el nivel de seguridad deseado.

Asimismo, se proporcionó teoría y ejemplos de la documentación mínima que debe dar soporte a un SGSI para su correcto funcionamiento.

Como posible ampliación a este trabajo se propone: el “Diseño de indicadores y métricas para la construcción de un cuadro de mando de seguridad” lo cual será el complemento perfecto a la implantación de un SGSI permitiendo una mayor fluidez en el proceso de mejoramiento continuo.

11. ANEXOS

Anexo 1: Anexo externo a este documento en formato Excel con el nombre "1- Data security maturity model.xls".

Anexo 2: Anexo externo a este documento en formato Word con el nombre "2- Política de Seguridad.docx".

Anexo 3: Anexo externo a este documento en formato Word con el nombre "3- Procedimiento de Auditorias Internas.docx".

Anexo 4: Anexo externo a este documento en formato Word con el nombre "4- Gestion de Indicadores.docx".

Anexo 5: Anexo externo a este documento en formato Word con el nombre "5- Procedimiento de revisión por parte de la Direccion.docx".

Anexo 6: Anexo externo a este documento en formato Word con el nombre "6- Metodología de Análisis de Riesgos.docx".

Anexo 7: Anexo externo a este documento en formato Excel con el nombre "7- Declaración de Aplicabilidad.xlsx".

Anexo 8: Anexo externo a este documento en formato Excel con el nombre "8- Análisis de Riesgos.xlsx".

Anexo 9: Anexo externo a este documento en formato Word con el nombre "9- Propuesta de proyectos SGSI.docx".

Anexo 10: Anexo externo a este documento en formato Excel con el nombre "10- Modelo de Madurez de la Capacidad (CMM).xlsx".

12. REFERENCIAS

[1] Alexander Marcombo. Diseño De Un Sistema De Seguridad Informática.

Alfaomega. México, 2007.

[2] Alan Calder. Iso27000 and Information Security: A Combined Glossary

[3] ISO/IEC 27001:2005, www.iso.org

[4] Mary Walton. The Deming Management Method.

[5] ISO27000 Toolkit. http://www.iso27001security.com/html/iso27k_toolkit.html

[6] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Ministerio de Administraciones Públicas, http://administracionelectronica.gob.es