Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 PARA LA EMPRESA LIANCAR LTDA.

Nombre Estudiante: Emilio Barajas Largo

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: *Antonio José Segovia Henares*
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 30 de diciembre de 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 para la empresa LIANCAR LTDA.*
Nombre del autor:	*Emilio Barajas Largo*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*Gestión, ISO/IEC 27001:2013, Seguridad.*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El actual trabajo consiste en la elaboración de un plan de implementación de la norma ISO 27001:2013 en la empresa LIANCAR LTDA ubicada en Bogotá, Colombia y cuenta con las siguientes fases: recopilación de información del estado actual de los procesos de la empresa en materia de la seguridad de la información de acuerdo a los dominios, objetivos y controles, desarrollo del sistema de gestión documental básico, análisis de riesgos de los activos de la empresa, y propuestas de proyectos para disminuir los niveles de riesgo y la realización de una auditoría para verificar el nivel de cumplimiento de los controles de la norma.

No obstante, dentro de este proceso se elaboraron algunos documentos como el plan de capacitación, mitigación de riesgos, continuidad de la empresa y el plan de auditoría. Estos proyectos, se propusieron con el fin de mejorar algunos dominios de seguridad que se encontraban en estado desatendido. En consecuencia, los resultados serán visibles en el mediano plazo a través de la auditoría, evidenciando las no conformidades que permitirán la formulación de acciones para algunos procesos de la empresa y de esta manera dar cumplimiento en la mejora de las políticas de seguridad. Además, en el desarrollo del proyecto, se encontró, que LIANCAR, cuenta con un estado de madurez de la seguridad muy inicial, por lo tanto, es considerable canalizar esfuerzos con un mayor acompañamiento y compromiso de la alta dirección en lo concerniente a la aprobación de las políticas, organización y planificación de

la seguridad de la información.

Abstract (in English, 250 words or less):

The current work consists in the elaboration of a plan for the implementation of the ISO 27001: 2013 standard in the company LIANCAR LTDA located in Bogota, Colombia and has the following phases: information gathering on the current state of the company's processes in the field Security of information according to domains, objectives and controls, development of basic document management system, risk analysis of company assets, and project proposals to reduce risk levels and conduct an audit To verify the level of compliance of the controls of the standard.

However, some of the documents, such as the training plan, risk mitigation, company continuity and the audit plan were developed in this process. These projects were proposed in order to improve some security domains that were in an unattended state. Consequently, the results will be visible in the medium term through the audit, showing the nonconformities that will allow the formulation of actions for some processes of the company and thus comply with the improvement of security policies. In addition, in the development of the project, it was found, that LIANCAR, has a very initial state of safety maturity, therefore, it is considerable to channel efforts with greater accompaniment and commitment of the upper management regarding the approval Of the policies, organization and planning of the security of the information.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización para alinear los objetivos y principios de seguridad de la información. Este plan representa la ruta primordial que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de cualquier riesgo, sino también, en qué dirección se debe actuar para mejorarla contando con el modelo esencial de mejora continua como lo es el PDCA (Plan-Do-Check-Act).

Este plan, reúne la definición de las políticas y los objetivos de seguridad, el análisis diferencial con base en los estándares de seguridad ISO/IEC 27001:2013 e ISO/IEC 27002:2013, para tratar con la mejores prácticas de seguridad de la información, la identificación de los activos de valor de la empresa aplicando la metodología de análisis de riesgos, la elaboración de propuestas que lleven la entidad a la organización de la información y buen cumplimiento de los objetivos propuestos, así mismo, terminando con una evaluación de madurez y nivel existente dentro de la empresa de tipo corporativo muy específicamente en sus áreas u oficinas de la compañía, con el objetivo de establecer las bases de un Sistema de Gestión de la Seguridad de la Información (SGSI) teniendo en cuenta que lo que interesa son los Sistemas de Información que dan soporte a un eficiente funcionamiento de las actividades y servicios.

1.2 Objetivos del Trabajo

1.2.1. Objetivo general

El objetivo principal de este documento es integrar las estrategias de la seguridad de la información, presentar y activar en forma vigente las políticas de Seguridad, la documentación y actualización de los procedimientos de gestión del sistema y demás requerimientos del SGSI a todos los usuarios, contratistas y proveedores que utilicen los recursos y sistemas de información de LIANCAR basados en la norma ISO/IEC 27001:2013, para mejorar a corto mediano y largo plazo los aspectos de seguridad en esta empresa relacionados con el alcance definido.

1.2.2. Objetivos específicos

- Proteger la Información de LIANCAR, en las dimensiones de la seguridad de la información de acuerdo a la confidencialidad, integridad, disponibilidad,

trazabilidad y confiabilidad de la Información de la empresa y de cualquiera de sus clientes y proveedores.

- Identificar las amenazas y riesgos de alto impacto para el negocio como la fuga, el robo de datos, alteración o modificación, accesos no autorizados, el mal uso de la información que afecte en forma indebida su divulgación, y en consecuencia afecte la reputación de la empresa mitigándolos con salvaguardas y controles de seguridad.
- Realizar en forma clara y contundente al interior de LIANCAR, los roles y responsabilidades en términos de la seguridad de la información.
- Mejorar los procesos que se encuentran en estado de madurez de acuerdo con el análisis diferencial de la Empresa a corto plazo utilizando los dominios y cláusulas de la norma ISO 27001:2013.
- Desarrollar y mantener una cultura de buenas prácticas en seguridad de la información orientada a la revisión y el análisis de riesgos a través de una sensibilización de los funcionarios, clientes y proveedores de LIANCAR.
- Establecer planes de continuidad de negocio y reducir fallas, problemas, eventos e incidentes de seguridad reportándolos y registrándolos con el fin de generar experiencias aprendidas para que sean fuente de mejora continua en los procesos de seguridad.
- Promover el cumplimiento de las normas y leyes Colombianas relacionadas con los servicios que presta LIANCAR junto con la adopción del código de buenas prácticas y estándares de seguridad como los son ISO/IEC 17799 e ISO/IEC 27001:2013.

- Generar confianza sobre la seguridad de la información en los gerentes administrativos, gerentes regionales, financieros y responsables de los procesos en LIANCAR con respecto a las aplicaciones y sistemas de información que frecuentemente están utilizando.

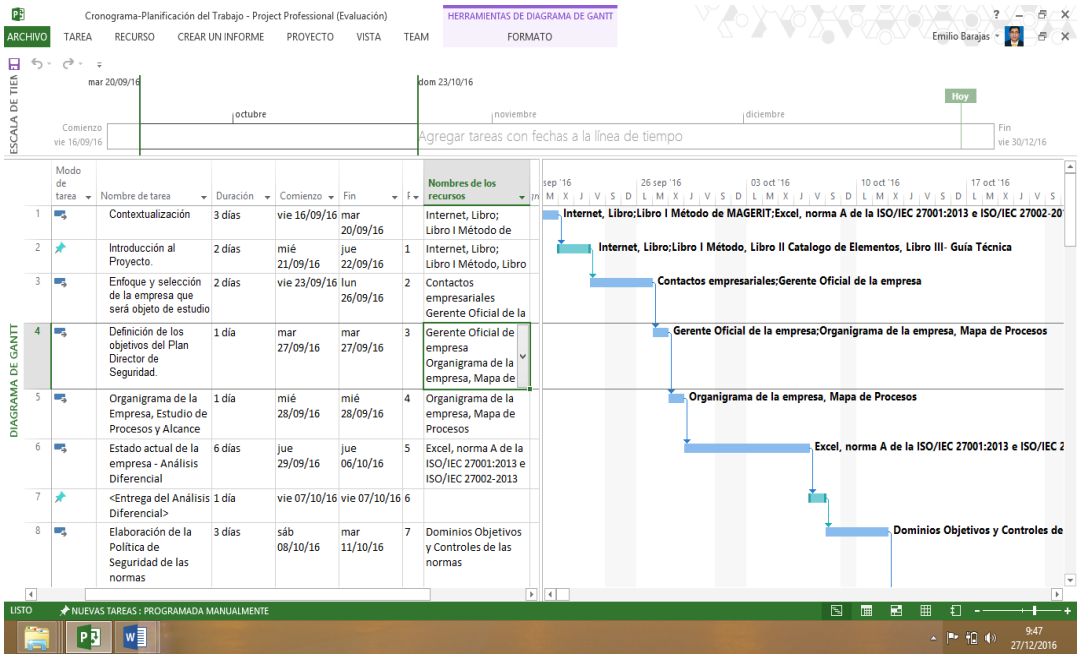
1.3 Enfoque y método seguido

En este proyecto se plantea el establecimiento de las bases para la implementación de un SGSI. Y para esta implementación, se han identificado posibles estrategias para lograr una adaptación del sistema de gestión de seguridad a la empresa LIANCAR. Dentro de las posibles estrategias para llevar a cabo el trabajo se encontraba un modelo de seguridad sin una metodologia válida que pudiera identificar las amenazas existentes en los procesos de las áreas, sin embargo es un modelo que contiene la información básica para la identificación de activos de información de la empresa. Se realizó una verificación de este modelo pero no se concreto la eleccción por motivos de una incompleta definición apta para controlar las amenazas y riesgos del sistema de la empresa. Ya después, de la revisión las directivas se inclinaron por la elección de un plan de seguridad de la información que les permitiera conocer paso a paso la identificación de sus debilitades y fortalezas.

Una vez, revisado el modelo de seguridad, se optó por elegir y desarrollar un plan maestro de seguridad de la información que permita realizar procedimientos claros y precisos con respecto a:
Una documentación normativa sobre las mejores prácticas en seguridad de la información, una definición clara de la situación actual y de los objetivos del SGSI, un Análisis de Riesgos, una Identificación y valoración de los activos corporativos como punto de partida al análisis de riesgos. También, una identificación de las amenazas para su respectiva evaluación y clasificación, una evaluación del nivel de cumplimiento tomándo como referencia el estándar ISO/IEC 27002:2013 adecuadamente. Después, precisar unas propuestas de proyectos con objetivos claros a conseguir una adecuada gestión de la seguridad de la información y posteriormente un Esquema Documental.

1.4 Planificación del Trabajo

En esta sección se describen los recursos necesarios para la realización del trabajo, todas las tareas elaboradas con su planificación temporal y referenciando con hitos las entregas parciales de cada una de las pruebas de evaluación continua. En la Figura siguiente se detalla en un diagrama de Gantt, solamente una parte. Se puede ver en totalidad en el Anexo de "Cronograma-Planificación del Trabajo".



1.5 Breve sumario de productos obtenidos

Los productos obtenidos del presente trabajo se describen a continuación, y la descripción detallada se realizará en los siguientes apartados.

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

1.6 Breve descripción de los otros capítulos de la memoria

Durante el desarrollo de este documento se abordará con precisión un conjunto de procedimientos referentes al análisis y gestión del riesgo, ya que es el principal objetivo de este trabajo, seguido de un desglose de información, propuestas y elaboración de documentos, que permitan la generación de un proyecto como plan director de seguridad de la información, teniendo en cuenta las fases primordiales para su formulación y desarrollo. En el (capítulo 1), se realiza un reconocimiento del plan director presentando sus objetivos y alcance. De igual forma los estándares de la seguridad reconocidos como ISO/IEC 27001:2013 e ISO/IEC 27002:2013, sus dominios, objetivos y controles que seran de especial necesidad para aplicarlos al estudio en cuestión. Además, un análisis del estado actual de la empresa LIANCAR LTDA, de acuerdo a la relación con la seguridad de la informática, mediante un análisis diferencial con respecto a las cláusulas de la norma ISO 27001:2013 y los dominios de control de la ISO 27002:2013. En el (Capítulo 2), abarca lo concerniente al esquema documental necesario para el cumplimiento normativo, de acuerdo a lo exigido por la propia norma ISO/IEC 27001:2013, se trata del cuerpo documental para el cumplimiento de esta normatividad y entre ellos se cuenta con la política de seguridad, el procedimiento de la Auditoría Interna, la gestión de indicadores, procedimientos de revisión por la dirección del gerente de la empresa, la gestión de Roles y Responsabilidades, la propia metodologia de Análisis de Riesgos y la declaración de Aplicabilidad. En el capítulo 3, respectivamente se aborda un análisis de los activos de la empresa vinculados a la información por medio de una encuesta al gerente de la empresa y seleccionándolos en grupos o categorias con su respectiva valoración económica. Ahora, el objetivo es tomar un conjunto de medidas que garanticen los activos para ello se realiza una valoración cuantitativa y cualitativa tomando como referencia las dimensiones de seguridad de la información (Confidencialidad, Disponibilidad, Integridad, Trazabilidad y Autenticidad), para, después, verificar su criticidad. Posteriormente se inicia el análisis de las amenazas clasificándolas en naturales, de origen industrial, en errores y fallos no intencionales y ataques intencionades. En general el análisis de riesgos está basado en la metodología MAGERIT, identificando activos, criticidad, impacto, amenazas, riesgos tanto aceptable como residual. Con este análisis se llega finalmente a la propuesta de proyectos que ayuden a mitigar los mayores riesgos encontrados en el corto y mediano plazo. Finalmente se realiza una auditoría de cumplimiento para evaluar el estado de madurez de los controles implantados para determinar el nivel de los controles de la norma. Esto, dará a la empresa LIANCAR LTDA, una pauta para

desarrollar sus planes a corto y mediano plazo en materia de seguridad de la información.

2. Descripción de los Capítulos

Los Capítulos de este trabajo se adecuan a un procedimiento por fases las cuales determinamos a continuación:

2.1 Fase 1 Orígenes de la norma ISO 27001

Sabemos bien, que la llegada de las Tecnologías de Información y de las Comunicaciones (TIC) y de nuevas formas de comercio, la información se ha convertido en un activo de vital importancia para las entidades corporativas y organizaciones hasta llegar a la necesidad de recurrir del aseguramiento de toda la información y los sistemas de información que ejecutan el procesamiento y almacenamiento.

No obstante, para gestionar en forma adecuada la seguridad de la información, es necesario de la creación de un sistema que garantice un procedimiento metodológico y a través de la documentación, cumpla con los objetivos de seguridad de la información planteados por la empresa y permita la evaluación de los riesgos a los que se ve comprometida.

Al ver en forma notória que el activo principal de una empresa es la información y como la primera fase de alguna auditoría es la revisión de la documentación que debe operar de acuerdo a las normas que se han implantado y a los controles establecidos con base a los riesgos que la empresa ha detectado y que estos controles estén alineados a lo que se indica en las normas ISO/IEC 17799:2005 y la ISO/IEC 27001. A continuación se realiza un estudio de estas normas para gestionar adecuadamente la seguridad de la información que cumpla con los objetivos de seguridad planteados por la organización y permita la evaluación de los riesgos a los que se encuentre comprometida. Este conjunto de estándares de la ISO/IEC 27000, los cuales proporcionan el marco para la gestión de la seguridad de la información de la organización pública o privada aparecen en el año de 1995. En este año, La organización británica de estandarización BSI (British Standard Institute) creó la Norma BS-7799, que contenia una primera versión del catálogo de buenas prácticas para la seguridad de la información. Esta misma organización creo posteriormente, en 1999, la Norma BS-7799-2, con los requerimientos para un sistema de gestión de la seguridad de la información que escogiera sus controles de la BS-7799. Ambas normas fueron la base para la creación de las Normas ISO/IEC 27002:2005 e ISO/IEC 27001:2005, respectivamente. La Norma ISO/IEC 27002:2005 fue inicialmente la ISO/IEC 17799:2000, que fue revisada en el 2005 y dió lugar a la ISO/IEC 17799:2005. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece

los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente [1].

Ya en el 2005, la ISO publicó el estándar 27001, a la vez que se revisó y actualizó la ISO17799, norma que el año 2007 fue declarada como ISO 27002:2005 [2]. Su estructura contiene 11 cláusulas de control de seguridad que abarca 39 categorías principales de seguridad y una cláusula introductoria que contiene temas de evaluación y tratamiento del riesgo [3].

Posteriormente, la norma ISO/IEC 27001:2005 fue revisada y reorganizada en septiembre de 2013. “Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información [4]. Esta es la norma que es certificable por auditores externos. En su ANEXO A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados [5]. En España esta norma se publicó como UNE-ISO/IEC 27001:2014, con modificaciones adicionales con respecto a la declaración de aplicabilidad en 2015 en el documento ISO/IEC 27001:2013/Cor.2:2015 [4].

Como se ha nombrado anteriormente en su estructura, la norma ISO/IEC 27002 es una guía de buenas prácticas en seguridad de la información, la cual no es certificable. Describe tanto los objetivos de control, como los controles recomendables para la organización. Consta de 11 dominios, 39 objetivos de control y 133 controles. En el año 2000 fue publicada por la ISO y por la comisión electrotécnica Internacional el estándar ISO/IEC 17799:2000 bajo el título de “Information Technology - Security tècniques - Code of practice for Information Security management”, después de haber sido publicada por primera vez por el British Standard Institucions bajo el nombre de BS-7799-1 [6]. Tras un período de revisión y actualización de los contenidos de este estándar se publicó en el año 2005 como ISO/IEC 17799:2005. Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007 [7]. En España fue publicada como “UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 [8]. Y en Colombia se consigue bajo el nombre de (NTC-ISO-IEC 27002) [9]. Esta norma, al igual que la 27001 fue recientemente actualizada en el 2013.

2. 2 Contextualización

A continuación se realizará una contextualización de la empresa LIANCAR LTDA, con la cual se trabajará, especificando su áreas de Gestión de Procesos y Servicios tecnológicos, en la cual se realizará el plan de implementación de la ISO 27001:2013, según las necesidades y requerimientos de la empresa.

2.3 La empresa

La intención primordial del proyecto es desarrollar la implementación del PDS con base en la Norma ISO 27001:2013 para la empresa LIANCAR, iniciando con una contextualización que permita ofrecer los detalles, modos de operación de sus procesos y formalización de su propósito. LIANCAR, se constituye como una empresa fuerte en el mercado especializada en el transporte terrestre en la modalidad de carga, hacia los diferentes puertos del país y desde los puertos hacia el interior, con amplia experiencia en el manejo de contenedores, carga masiva, semi-masiva, coordinación logística, paqueteo y distribución a nivel nacional. Cuenta con un excelente talento humano, un equipo profesional altamente calificado para cada una de las labores a realizar, adquiriendo un alto nivel de compromiso en el momento de prestar nuestros servicios, beneficiando a los clientes tanto externos como internos, mediante una sólida imagen corporativa basada en los lineamientos de seriedad, solidez y eficacia. Se desarrolla una gestión con valores y principios éticos, con un enfoque en el cliente, sentido económico y responsabilidad social y ambiental.

LIANCAR, dispone de seis (6) flotas de 4, 8, 17, 18, 28 y 35 toneladas respectivamente controladas por diferentes sucursales comenzado en Bogotá, Bucaramanga, Buenaventura, Cartagena, Medellín, Cúcuta, Barranquilla, Santa Rosa y Santa Marta para ofrecer sus servicios de carga terrestre, en cupos completos y contenedores a un sólo destinatario en todo el territorio nacional, desde los terminales portuarios hasta la planta del cliente. La carga viaja en tránsito, con suspensión de tributos aduaneros, desde el puerto de entrada, hacia una ciudad en el interior del país o un puerto de salida configurándose la operación. Para realizar estas operaciones en los depósitos temporales, deberá mediar autorización por parte de la aduana y presencia física del funcionario aduanero en dicho proceso. Se transporta en forma segura y efectiva esta clase de carga, contando con tecnología para este tipo de servicio. Ahora, Los alimentos perecederos y No perecederos se trasportan a la temperatura adecuada, con reglamentaciones sanitarias vigentes o la establecida por el remitente del producto. Es de vital importancia resaltar que LINCAR, es consciente que la seguridad de la información y física es una herramienta fundamental dentro del desarrollo de sus operaciones, por tal motivo en la seguridad física provee todos los recursos y esfuerzos para evitar actividades ilícitas en las que se declaran en contra del narcotráfico y el terrorismo. Además, está comprometida con sus empleados, clientes (generadores de carga), proveedores y visitantes; en minimizar los riesgos físicos que puedan presentarse en las operaciones propias de la empresa, para cumplir con los objetivos están en un proceso de mejoramiento continuo, ajustándose a la normatividad legal y a los parámetros de la norma de seguridad BASC (Business Alliance for Secure Commerce), que es una alianza empresarial internacional que promueve un comercio seguro en cooperación con gobiernos y organismos internacionales..

Todos los funcionarios de LIANCAR, están debidamente capacitados para colaborar con las autoridades nacionales e internacionales, a fin de lograr una exitosa operación de exportación de mercancías libres de contaminación de

drogas, sustancias y elementos ilícitos. Dentro de su estructura organizacional la empresa ha constituido como indispensable el contacto directo con los clientes, creando así una estrategia de interrelación y compromiso, inculcando las políticas del servicio ágil, oportuno y eficaz, siendo estos la clave para su desarrollo empresarial. En la figura Nro. 1, se detalla el organigrama cuya concepción básica orienta la gestión empresarial de la organización describiendo su filosofía, valores, propósitos empresariales y la forma de hacer el trabajo para mejorar la productividad y competitividad.

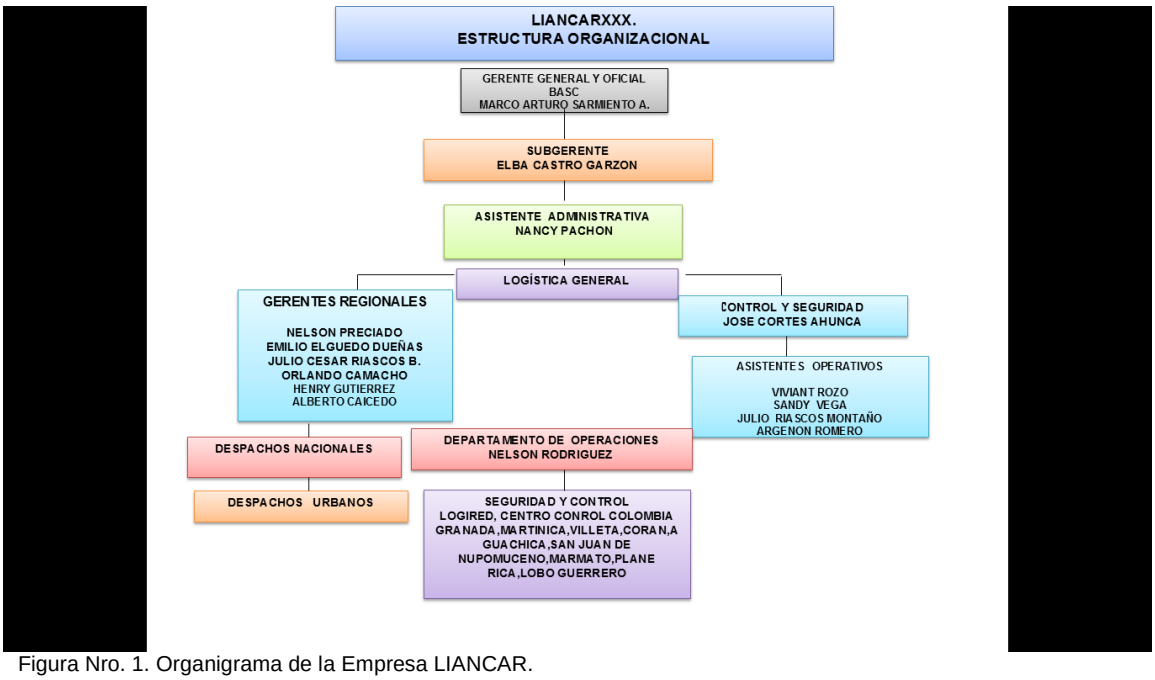
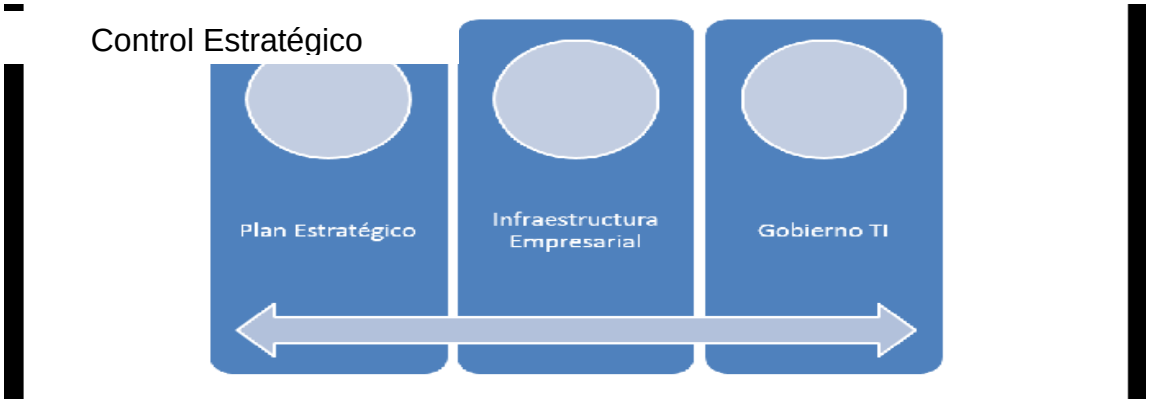


Figura Nro. 1. Organigrama de la Empresa LIANCAR.

Dentro de las áreas de apoyo se encuentra la unidad de Control y Seguridad (CyS) encargada del manejo de los proyectos de seguridad, controla y coordina los servicios TIC en cada una de las áreas de la empresa y el gobierno de TI. Además, la administración general de la infraestructura tecnológica existente como: servicios por Internet, control de correo interno y externo, servicios Web, infraestructura de red, etc. Esta unidad se encuentra ubicada físicamente en Bogotá Colombia, y en la figura Nro. 2, se visualiza el esquema de procesos de ésta área en su Control estratégico, su misión de ser y Control de soporte.



Su misión de ser

Control de soporte

Figura Nro. 2, Esquema de procesos del área de Control y Seguridad

La empresa cuenta con una aplicación web, servidores basados en sistemas operativos Windows y Linux, aplicaciones a la medida, un centro de datos, controles de acceso físicos, no existen barreras físicas que aíslen las áreas coyunturales de la entidad, no utilizan un circuito cerrado de televisión, tienen un sistema de cableado y canaletas, como muro de contención lógico configuran un firewall para la seguridad perimetral y toda una red de área local con concentradores, switches y Hubs, no utilizan métodos para actualización de servidores, nunca antes, han realizado pruebas de instrucción de cualquier tipo al sistema de la empresa, no hay manuales de políticas de la información, no se realizan en forma regular procesos de concienciación en lo referente a seguridad de la información entre otros casos.

Los datos anteriores, se han obtenido por medio de una encuesta clasificada mediante un estudio de los aspectos metodológicos existentes en la empresa como referencias a las políticas de seguridad, definiciones o contenido relacionado en la norma técnica NTC ISO/IEC 27001 y 27002 ver (ANEXO G). De igual manera, se adoptó un apartado para revisar la estructura lógica como actualizaciones de servidores, software y su Infraestructura física, acceso y medio ambiente.

2.4 Alcance del plan de seguridad

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información) para la empresa LIANCAR teniendo en cuenta que el alcance del SGSI es uno de los pasos más importantes de la seguridad de información, pues deben ser los más precisos, que englobe y que cubra toda la organización. Teniendo en cuenta lo dispuesto en reuniones sostenidas con el gerente y el director de Gestión Tecnológica de LIANCAR, se definió que los esfuerzos para la implementación

del SGSI deben estar centralizados en lo que respecta sobre los Sistemas de Información que dan soporte a actividades y servicios de la entidad, basados en los procesos generales, los cuales están relacionados con el proceso de Direccionamiento y Planeamiento Corporativo (DPC), el Departamento Operativo y Seguridad (OS), Recursos Humanos (RH), Departamento Administrativo Comercial y Financiero (ACF) y Departamento Sistema Integrado de Gestión (SIG), como lo demuestra el diagrama Nro. 1 del mapa de procesos.

Diagrama Nro.1 Mapa de procesos generales de LIANCAR

Además, se debe tener en cuenta los servicios que presta, su propia infraestructura tecnológica, el despliegue de soluciones, el espacio físico, protección contra incendios, Administración, Monitoreo, accesos lógicos, bases de datos, aplicativos de sistemas de información, almacenamiento de información, comunicaciones, seguridad lógica y redes de datos como se visualiza en el diagrama Nro. 2. Se pretende afianzar y generar la documentación y políticas que permitan a LIANCAR, madurar los procesos y procedimientos de modo que se obtenga una mejora continua tanto en el corto, mediano y largo plazo en todos los aspectos de la seguridad de la información.

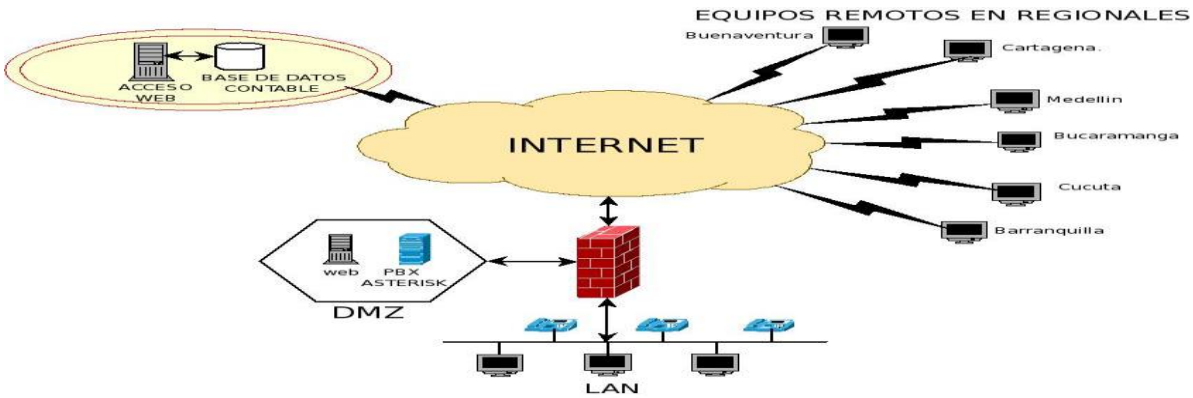


Diagrama Nro.2. Red de Datos de la Empresa LIANCAR

2.5 Análisis diferencial

En este espacio, tomamos como referencia las normas ISO/IEC 27002:2013 y la ISO/IEC 27001:2013, para realizar un análisis diferencial y destacar el estado actual de la empresa LIANCAR en relación a la seguridad de la información, permitiendo observar su modus operandi. Estas normas a diferencia de la norma ISO 27001:2005 incluye una cláusula independiente donde se específica la importancia de las partes interesadas y sus requerimientos deben estar debidamente identificados. Se combinan los conceptos de “documentos” y “registros” dentro del término información documentada eliminando el requisito del antiguo estándar que se refiere a tener procedimientos documentados para el control de documentos, auditorias y acciones correctivas. También, hay otro cambio que corresponde a la evaluación y tratamiento de los riesgos brindando una mayor libertad en el momento en que se identifican los riesgos.

Para dar inicio al análisis diferencial y entrar en detalle a la evaluación de diagnóstico de LIANCAR tomamos como referencia una valoración para las cláusulas de requisitos de la norma ISO 27002:2013 ver tabla No. 1, que con los dominios del ANEXO A de la norma ISO/IEC 27002:2013 se permite evaluar el estado actual de la empresa.

Valorización para los dominios establecidos en la ISO/IEC 27002:2013		
Códigos Status	Significado	% de valoración
D	El control se documentó e implementó	100
MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetivilidad del proceso y mitigar los riesgos.	90
RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	50
PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0
NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	

Tabla No. 1 Valorización para los dominios establecidos en la ISO/IEC 27002:2013.

En la Figura Nro. 3 se denota el nivel de cumplimiento de los 114 controles del Anexo-A, donde se especifica la evaluación de los mismos, el status por código, su significado en porcentajes de valoración y cumplimiento, en donde la letra D se refiere a que el control es óptimo, MD (Gestionado), RD (Inicial) PNP (Inexistente), NA (No aplicable).

Nivel de cumplimiento en controles Anexo-A				
Controles evaluados	Códigos Status	Significado	% de valoración	% de cumplimiento
0	D	El control se documentó e implementó	100	0%
27	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos	90	24%
54	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	50	47%
31	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0	27%
2	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio		2%
114				

Figura No.3 Nivel de cumplimiento por control. Anexo-A norma ISO 27002:2013

En efecto, los controles evaluados se reflejan en la Figura Nro. 4.

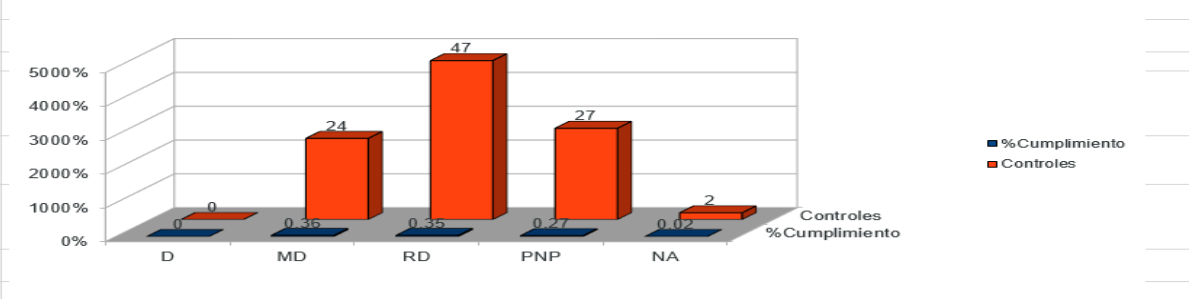


Figura Nro. 4. Porcentaje de cumplimento por control de la norma ISO/IEC 27002:2013

Seguidamente, determinamos por porcentajes y muestra de los dominios que pertenecen a la ISO/IEC 27002:2013 por medio de una tabla y una gráfica radial como lo deja ver la Figura Nro. 5.

DOMINIO	% DE CUMPLIMIENTO	
A.5-Políticas de seguridad de la información	25,00%	
A.6-Aspectos Organizativos de la Seguridad de la Información	22,00%	
A.7-Seguridad ligada a los recursos humanos	20,00%	
A.8-Gestión de activos	36,50%	
A.9-Control de accesos	28,00%	
A.10-Cifrados	0,00%	
A.11-Seguridad física y ambiental	45,00%	
A.12-Seguridad en la operativa	38,90%	
A.13-Seguridad en las telecomunicaciones	30,00%	
A.14-Adquisición, desarrollo y mantenimiento de sistemas	43,08%	
A.15-Relaciones con suministradores	30,00%	
A.16-Gestión de incidentes de Seguridad de la información	34,14%	
A.17-Aspectos de seguridad de la información dentro de la continuidad del negocio	37,50%	
A.18-Cumplimiento	22,00%	
	29,44%	412,12%
		0,117749371
		0,036151123

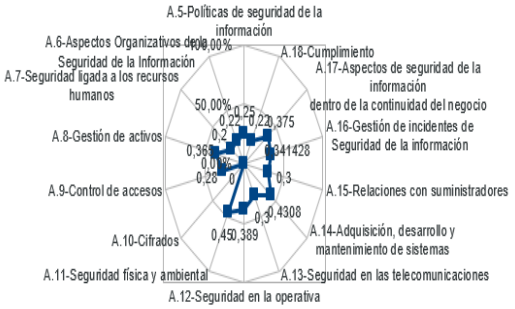


Figura Nro. 5. Gráfica radial representando la situación actual de LIANCAR

Ahora, para el análisis diferencial utilizando la norma ISO/IEC 27001:2013 se presenta una descripción de los criterios por su clasificación del estado actual de LIANCAR, como se describe en la figura Nro. 6, tomando como base la

valoración de los diferentes dominios establecidos en esta norma, de acuerdo con los datos entregados por la empresa.

Leyenda				
Cantidad	Codigos Status	Significado		Contribution %
0	D	El control se documentó e implementó. Está siendo monitoreado y mejorado		0%
2	MD	El Control se lleva a cabo y está completo; el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos. Recientemente comenzó a operar		3%
12	DEF	El control y Los procedimientos están mas o menos completos y/o aún no se han implementado; además el control no ha sido socializado por la alta dirección		20%
37	REP	El control no cumple con las normas/no hay capacitación o comunicación formal de procedimientos estándar		63%
8	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas		14%
0	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)		0%
0	NA (No Aplicable)	El control no es aplicable para la empresa ni para el negocio		0%
59				

Figura Nro. 6, Descripción de los Criterios y valores por requisitos y cláusulas de la ISO/IEC 27001:2013

No obstante, el cumplimiento en los dominios de esta norma la visualizamos en la Figura Nro. 7. En una representación radial y en barras, donde el estado actual de los requisitos presenta un 35% de cumplimiento en su contexto, un 40% en Liderazgo, un 35% en su planificación, un 47% en soporte, un 42% en las operaciones, un 0% en evaluación y un 10% en las mejoras.

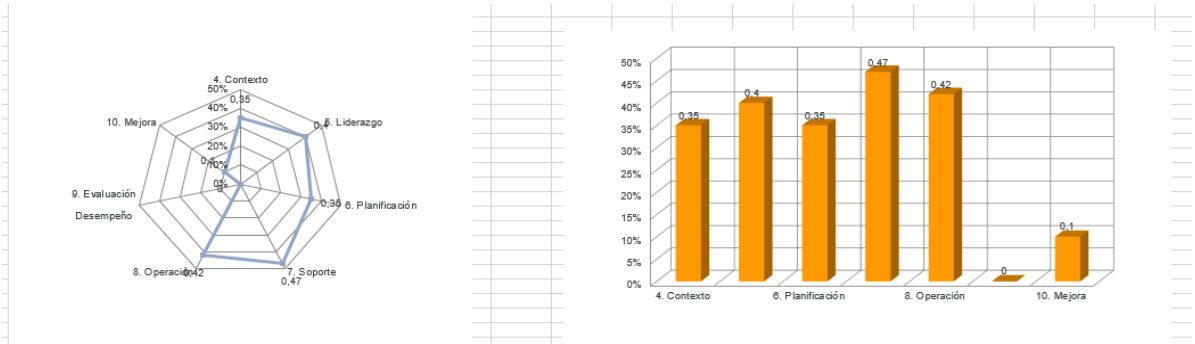


Figura Nro. 7 Cumplimiento de LIANCAR en los Dominios de la ISO/IEC 27001:2013

En el siguiente ítem, explicaremos detenidamente los resultados y representación del estado actual de la empresa de acuerdo a las gráficas obtenidas.

2.6 Resultados

En el apartado anterior, se deduce, que se espera un diseño de una política de seguridad de la información, procedimientos y una documentación al respecto. Se estima algunas evidencias de que la empresa LIANCAR ha reconocido que los problemas y riesgos de perder información valiosa existe. En cuanto a los procesos, se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea.

Por tal motivo el análisis diferencial de la norma ISO 27001:2013 deja entrever que no existe ningún procedimiento relacionado con la evaluación del desempeño. No se han establecido tiempos ni asignaciones de

responsabilidades en cuanto a los procesos, auditorías internas en relación con la seguridad de la información y controles para implementar un SGSI. Sin embargo, esto no quiere decir, que la empresa LIANCAR, no adecue y trabaje en estrategias para fortalecer la seguridad de la información pero si deben ser refinadas para lograr un estado de madurez mejor. En otra instancia, podemos decir, que el diagnóstico de seguridad de la información realizado por el análisis diferencial o GAP se basó en la norma ISO 27002:2013 y determina los resultados de cómo se encuentran actualmente los dominios describiendo las calificaciones en unos porcentajes muy inferiores a los requeridos por la norma. Vemos que la cláusula de mejora y evaluación se encuentra en un estado inexistente, mostrando la necesidad de generar procesos que ayuden en su formulación y postulación de un SGSI.

En cuanto al soporte, se encontró que en la unidad de control de TI de la empresa LIANCAR cuenta con personal a nivel técnico, pero falta adiestramiento y capacitación para resolver los problemas que se encuentran, y evaluar y gestionar los riesgos asociados. También, con relación a los controles del ANEXO A de la ISO 27002:2013, se evidencia claramente que la organización de la seguridad de la información, la criptografía, y la continuidad del negocio, por el momento no son prioridad para la empresa y que se realiza lo mínimo para su funcionalidad.

Esta empresa, urge de un SGSI por lo tanto trabajaremos por su implementación y certificación

3. Fase 2: Sistema de gestión documental

3.1. Introducción

En general, todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que el Sistema de Gestión de Seguridad de la Información que se plantea debe tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001. A continuación se describen estos documentos, los cuales pueden ser observados en los anexos correspondientes.

3.2 Esquema Documental

La propia ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema, pero para el desarrollo del trabajo fueron necesarios los siguientes documentos:

- **Política de Seguridad**: Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. 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. Uno de los principales objetivos que se tiene en cuenta desde la empresa LIANCAR es obtener todas las directrices que debe seguir el SGSI de acuerdo a sus necesidades por medio de una política de seguridad vigente. Esta política se encuentra en proceso de realización para que pueda entrar en fase de actualización y posteriormente a su aprobación por parte de la gerencia de forma tal que se indique un estado adecuado y detallado con el fin de ser socializada respectivamente a todos sus operarios o colaboradores de la empresa. Con respecto a esta política de la empresa LIANCAR LTDA aún, se encuentran en fase de actualización y aprobación por parte de la alta dirección, y en algunos aspectos todavía es genérica, por lo cual se recomienda a la empresa un ajuste antes de su aprobación para poder ser presentada a sus empleados. En el ANEXO B se observa la política de seguridad de la información actual.

- **Procedimiento de Auditorías Internas:** Documento que 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. En el caso especial y particular de LIANCAR, aún no se ha llevado a cabo ninguna acción relacionada con alguna auditoría interna de igual forma las auditorías técnicas faltan por realizar. Este motivo hace muy necesario iniciar un proceso exhaustivo por su gran importancia y en concordancia es factible construir y presentar un modelo o formato de guía como propuesta para el plan de auditorías internas en la empresa LIANCAR para ser entregado a las directivas del comité de Seguridad de la Información para su revisión, actualización, adaptación y aprobación. Se anexa el PLAN DE AUDITORÍAS INTERNAS, formato en el Anexo C.

- **Gestión de Indicadores**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medirlos. No obstante, es de gran importancia destacar un conjunto de procesos como la Seguridad Física y Ambiental, la Seguridad del Personal, la Seguridad de los controles de acceso, la misma seguridad en el desarrollo y Mantenimiento de los Sistemas, la Seguridad en las Operaciones y Comunicaciones y además, la Planificación de la Continuidad del Negocio, para que, teniendo en cuenta estos procesos en LIANCAR, se definan los indicadores que por supuesto estarán alineados a la política de seguridad de la empresa. Ver Anexo D.

- **Procedimiento Revisión por Dirección**: La Dirección de la empresa 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. Se desarrolla el

formato de procedimiento y revisión para la alta gerencia de la empresa LIANCAR, ANEXO E. Para dar una iniciativa al proceso de estas revisiones se presenta un modelo en la Figura Nro. 8. Donde se encuentra una estructura del proceso de Revisión conformada por su objetivo, alcance, definiciones y actividades a realizar en la revisión por el Gerencia General.

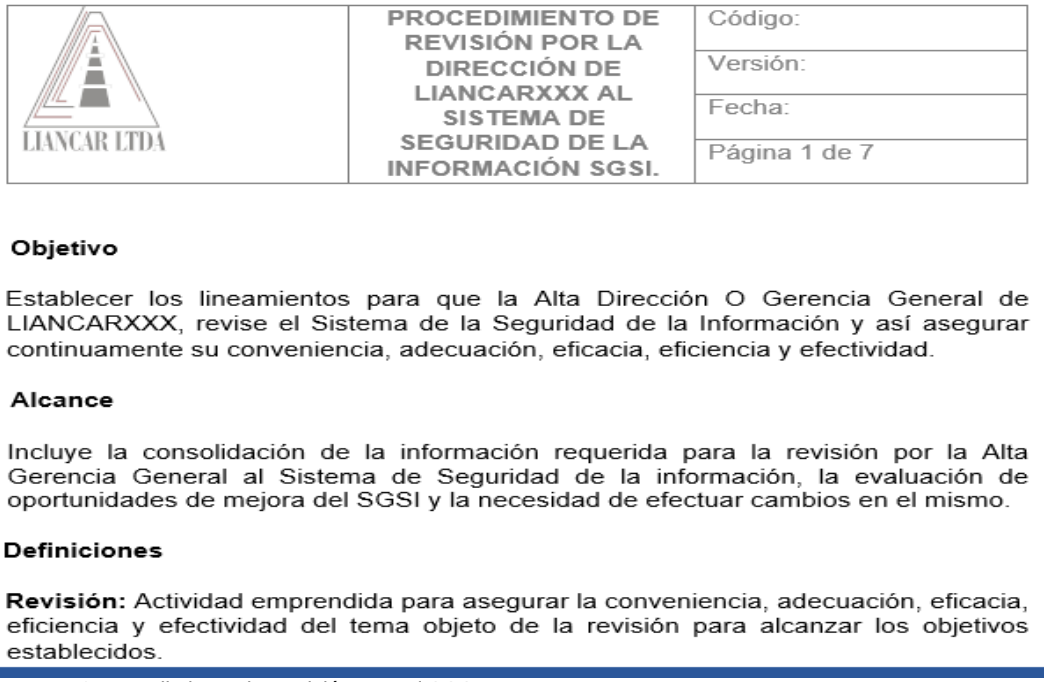


Figura Nro. 8 Procedimiento de Revisión para el SGSI

En estas revisiones se deben incluir por lo menos consideraciones al respecto como:

- El estado actual de las acciones en contraste con las revisiones anteriores.
- Existencia de cambios en el contexto de la empresa que sean pertinentes al SGSI.

A continuación se describe el procedimiento de revisión propuesto para el gerente oficial de la empresa LIANCAR LTDA:

La revisión del Sistema de Gestión por la Alta Dirección la realiza el Gerente General y Oficial, el Departamento Administrativo Comercial y Financiero, el Departamento Operativo y de Seguridad, el Departamento Sistema Integrado de Gestión como responsables del Direccionamiento y Planeamiento Corporativo verificando entre otros los siguientes puntos:

- El Departamento de Direccionamiento y Planeamiento Corporativo debe establecer metas a cumplir con relación a Las Políticas de Calidad, Seguridad y Salud Ocupacional, Seguridad de la información y Ambiental.
- El cumplimiento de los Objetivos de Calidad, seguridad de la información, objetivos ambientales y de seguridad y salud ocupacional teniendo en cuenta el presupuesto programado, ingreso, egresos y gastos.

- El desempeño en calidad, ambiental, seguridad de la información, y Salud Ocupacional.
- Los resultados de las auditorías internas y/o externas.
- Las acciones correctivas y/o preventivas necesarias para el mejoramiento del Sistema de Gestión, así como el estado de aquellas que se hayan identificado.
- Las acciones de seguimiento de las revisiones por la Dirección previas.
- El avance y cumplimiento de la implementación de los planes de tratamiento definidos para los riesgos identificados.
- Los cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.
- Además, las recomendaciones para la mejora.
- Los resultados de la gestión de riesgos corporativos, esto incluye vulnerabilidades o amenazas no tratadas en la valoración previa de riesgos.

Estos resultados quedarán registrados por la revisión en un formato establecido por la empresa LIANCAR LTDA, la cual se deberán ejecutarse por lo menos una vez al año.

- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que 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 algún Directivo encargado. No obstante, para la empresa LIANCAR, la definición de roles y responsabilidades está siendo elaboradas dentro de la nueva política de seguridad de la información ANEXO B. Estas responsabilidades y Roles se detallan a continuación:

  1. El Comité de Seguridad Informática, compuesto por los representantes de los distintos departamentos de la empresa, así como por el Gerente General de LIANCAR, el Director de Infraestructura Tecnológica, el Gestor o Administrador de Seguridad de la Información, el encargado de Redes y Telecomunicaciones, el Administrador de Servidores y el Abogado o representante legal de la Empresa. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la información. Además, es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Es preciso que durante las reuniones trimestrales o según cronograma, el Comité efectuará la evaluación y revisión de la situación de la empresa LIANCAR en cuanto a su Seguridad de la Información e Informática, incluyendo el análisis de incidentes ocurridos que afecten el sistema de la seguridad. Por ende, da soporte, dota de recursos de seguridad y establece las directrices de trabajo. Además, aprueba las políticas, normas y responsabilidades del SI, analiza

los posibles riesgos y aprueba los planes de seguridad y hace el seguimiento.

2. Los funcionarios de la empresa, contratistas o colaboradores de la empresa por lo general son los usuarios y serán responsables por la información de los procesos a su cargo.

3. En cuanto al subgerente o jefe de Recursos Humanos, tendrá la responsabilidad de poner al tanto o avisar al personal que se vincula a LINCAR, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

4. El Responsable de Seguridad (RSI) debe coordinar y controlar las medidas de seguridad de la información en cualquiera de sus formas y en todo el ciclo de vida de la Información. Debe implantar las directrices de seguridad de la Información, elaborar y mantener la política de Seguridad de la Información y proponer objetivos en materia de seguridad.

5. El responsable del Área de Tecnología, que junto con el RSI define las políticas, normas, procedimientos y se encarga de hacerlas cumplir. Implanta los controles de seguridad, las acciones de correción y gestiona las vulnerabilidades que se detectan.

6. La estructura organizativa de la seguridad de la información implica a toda la empresa LIANCAR junto con todo su personal y los responsables de las distintas áreas presentes en la organización deben trabajar en estrecha relación con el RSI para poner en práctica la seguridad en cada ámbito de actuación. En coordinación con la Gerencia General y Subgerente de los Servicios Tecnológicos son responsables de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. De esta forma, y de manera general se pone a consideración el siguiente listado para que la empresa LIANCAR analice de acuerdo a su composición orgánica cuales deben ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo a los siguientes perfiles:
6.1. Personal de seguridad de la información.
6.2. Un representante del área de Tecnología.
6.3. Un representante del área de Control Interno.
6.4. Un representante del área de Planeación.
6.5. Un representante de sistemas de Gestión de Calidad.
6.6 Un representante del área Jurídica.
6.7. Funcionarios, proveedores, y ciudadanos

- **Metodología de Análisis de Riesgos**: En esta sección, se establece un proceso sistemático que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades. En el ANEXO F, se encuentra la matriz de riesgos y el catálogo de probabilidad de amenazas definidas por la organización. Iniciando

con el levantamiento de información por medio de un cuestionario de preguntas, ver ANEXO G. Como la intención, es obtener un análisis de riesgos, cuyo resultado es una lista de los riesgos correspondientes a los posibles impactos en caso de que se materialicen las amenazas a las que están expuestos los activos, presentamos en la figura Nro. 9, el tratamiento correspondiente a los riesgos, donde se asuma, elimine, mitigue o se transfiera el riesgo.

Figura Nro. 9. Tratamiento del riesgo, metodología Magerit.

En la figura Nro. 9, vemos una categorización de los riesgos se identifica cuáles deberían ser tratados primero o después, respectivamente. Se debe escoger, a la vista de los resultados, cual es el nivel de riesgo que la empresa LIANCAR está dispuesta a tolerar, de manera que por debajo de ese nivel el riesgo es aceptable y por encima no será permitido y se tomará alguna decisión al respecto.

- **Declaración de Aplicabilidad**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada. Se ha comprobado la inexistencia de la declaración de aplicabilidad, por lo cual se está desarrollando una propuesta para ser entregada a la alta gerencia general de LIANCAR, para su revisión y aprobación. Se anexa la Declaración de aplicabilidad propuesta (ANEXO H).

3.3 Resultados

Una vez, realizada la revisión correspondiente al esquema documental básico, encontramos que la empresa LIANCAR carece de toda la documentación requerida, por lo cual se hizo necesario la realización de propuestas para la implementación de la política de seguridad, de Auditorías Internas, de un Procedimiento para la Revisión por la Alta Gerencia, de unos Indicadores de Gestión, la Gestión de Roles y Responsabilidades y la de Declaración de aplicabilidad, los cuales requieren la revisión y aprobación por parte del de Gerencia General, el Oficial de seguridad de la información en conjunto con el Comité de Seguridad de la información de la empresa. Estas aprobaciones son fundamentales para poder llevar a cabo las diferentes actividades de implantación del SGSI, como son la realización del análisis de riesgos, la implantación de controles necesarios, implantación de proyectos, la realización de auditoría interna, entre otros.

4. Fase 3: Análisis de riesgos.

4.1. Introducción

Es dificil, proteger aquello que no conocemos. Es por ello, que la primera etapa hacia la consecución del Plan de Implementación de un SGSI consistirá en la evaluación de los activos ubicados en la empresa LIANCAR, considerando sus oficinas, dependencias existentes entre ellos y realizando una valoración de los mismos. Los motivos por el cual debemos realizar este análisis se denota a continuación:

- Nos permite identificar los diferentes riesgos a los que se encuentra expuesta la empresa desde el punto de vista de la seguridad de la información y que podrían afectar al desarrollo de las diferentes actividades de negocio de la entidad.
- Le permite a la empresa realizar una selección de medidas de seguridad que se deben implantar en ella, mucho más ajustada a sus necesidades.

Para esta acción, determinamos los activos propios de la empresa LIANCAR como el software, personal, hardware y que se encuentran relacionados con los procesos de la empresa. Por lo tanto, se procederá a realizar el análisis de riesgos con la metodología MAGERIT permitiendo trabajar con los elementos en cuanto a los activos que se deben proteger, la valoración de las amenazas, determinación del impacto potencial, riesgo potencial, impacto residual, riesgo residual, con ello, identificaremos los riesgos y situaciones de las que deben protegerse los activos y los aspectos o vulnerabilidades que facilitan que se materialicen estas amenazas.

4.2 Inventario de Activos

No obstante, el objetivo principal de la ISO 27001 es proteger los activos de información, las cuales pueden ser desde archivos, bases de datos, acuerdos, contratos, información del sistema, aplicaciones del sistema, manuales de usuario, hasta sus mismos empleados[13]. Luego todo esto para la empresa LIANCAR es un activo. Algo muy importante que establece AENOR de acuerdo a UNE-ISO/IEC 27001:2014, es "contribuir y fomentar las actividades de protección de la información en las operaciones, mejorando la imagen de la empresa y generando confianza entre terceros"[14], y de igual forma según el Libro 1 – Método de Magerit V3 página 22 sección 3.1.1., un activo es un "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" por [UNE 71504:2008] . Por tanto, el inventario de activos son todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI [15].

Nuestro primer punto de partida para el análisis es analizar los activos vinculados a la información agrupándolos por categorías acorde con la metodología MAGERIT de la forma siguiente: Instalaciones, Hardware, Aplicación, Datos, Red, Servicios, Equipamiento auxiliar y Personal

Los resultados del inventario se recogen en la tabla Nro. 2, para su posterior estudio (La tabla no se encuentra completa por seguridad). Esta tabla tiene una estructura tan simple como el grupo al que pertenece el activo y el activo en sí y una valoración económica resultado del levantamiento de activos representada en pesos Colombianos aportados por LIANCAR.

Ámbito	**Activo**	**Valor ($ PESOS COP)**
Hardware		
	Computadores	$ 45.000.000,00
	Impresoras	$ 8.000.000,00
	memorias USB	$ 4.000.000,00
	Pbx	$ 6.000.000,00
	Portátiles	$ 32.000.000,00
Red		
	Switch core	$ 8.771.000,00
	Equipos de la red cableada (router)	$ 6.454.000,00
	Equipos de la red inalámbrica (router)	$ 8.200.000,00
	Equipos de la red inalámbrica (punto de acceso)	$ 8.200.000,00

	Cortafuego (Firewall)	$ 3.050.000,00
	Routers de borde	$ 12.000.000,00
Instalaciones		
	Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.) y cableado estructurado.	$ 750.000.000,00
Información		
	Informática (Planes, Documentación, etc.)	$ 18.000.000,00
	Infraestructura (Planes, Documentación, etc.)	$ 13.000.000,00
	Datos e información no empresarial	$ 60.000.000,00
Datos		
	Finanzas (SI & SI, Sap, Level Money, Spendee, PayPal, etc.,)	$ 16.000.000,00
	Directorio de Contactos	$ 4.000.000,00
	Bases de datos internas	$ 40.000.000,00
	RR.HH (SI & SI)	$ 30.000.000,00
	Respaldos -Copias de seguridad	$ 15.000.000,00
Aplicaciones-Software		
	Programas de administración (contabilidad, manejo de personal, etc.)	$ 6.000.000,00
	herramientas de desarrollo, aplicativos	$ 0,00
	Sistemas operativos	$ 12.000.000,00
	Aplicaciones de Servidores Locales	$ 18.000.000,00
Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.	$ 45.000.000,00
Servicios		
	Correo electrónico	$ 1.500.000,00
	Chat	$ 2.500.000,00
	llamadas telefónicas	$ 2.500.000,00
	Herramientas para empresas en la nube	$ 4.000.000,00
	Página Web Intranet incluso WIFI (Colaboradores)	$ 1.200.000,00

Tabla Nro. 2: Análisis de los activos de la empresa LIANCAR

4.3 Valoración de los activos

Para el presente estudio, se realizó un análisis de todos los activos que se encuentran a cargo de la empresa LIANCAR utilizando la tradicional metodología MAGERIT. Esta metodología es realmente un método para el desarrollo de un análisis y gestión de riesgos, diseñada inicialmente para la administración Española por el Consejo Superior de Administración Electrónica, pero que debido a su buena definición y aceptación, puede ser aplicada en otros contextos. (De MAGERIT se tomará en cuenta el libro 2: catálogo de elementos para realizar la definición de amenazas[18], y el libro I: método)[19].

La propuesta anterior realiza una clasificación según la siguiente valoración de los activos de la empresa presentados en la tabla Nro. 3, que serán aplicados al inventario de activos, teniendo en cuenta el valor en pesos y la criticidad que se tiene en las cinco dimensiones de seguridad para la organización de cada uno de ellos, de la siguiente forma:

Valor Cualitativo	Valor Cuantitativo en Pesos Col (COP)
Muy Alto (MA)	**> $50.000.000,00**
Alto (A)	**$40.000.000,00 - $50.000.000,00**
Medio (M)	**$20.000.000.00 - $39.999.000.00**
Bajo (B)	**$10.000.000.00 - $19.999.000**
Muy bajo (MB)	**< $10.000.000.00**

Tabla Nro. 3. Valoración de los activos de la empresa LIANCAR

4.4 Dimensiones de seguridad

Una vez identificados los activos, se estableció una valoración DICTA (Disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad), de acuerdo con el libro 1: método de MAGERIT, ver tabla No. 4. Esta valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada para el proceso de negocio. Esta valoración nos permitió a posteriori valorar el impacto que tendría la materialización de una amenaza sobre la parte del activo expuesto (no cubierto por las salvaguardas en cada una de las dimensiones).

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla Nro. 4, Valoración Dimensiones de Seguridad

4.5 Tabla resumen de valoración

Lo visto hasta ahora, nos debe permitir generar la tabla Nro. 5, donde reflejaremos tanto la valoración de activos como los aspectos críticos del mismo. A la tabla resultante la llamaremos "Valoración de los activos y aspectos críticos". En esta tabla vemos por ejemplo que el valor del activo "Computadores" es de $45.000.000.00 por lo tanto la valoración es Alta (A) y los aspectos críticos están valorados en 10, 7, 8, 7 y 6 para la disponibilidad, Integridad, Confiabilidad, Trazabilidad y Autenticidad respectivamente.

				Aspectos críticos				
Ámbito	**Activo**	**Valor**	**Valor ($ PESOS COP)**	**D**	**I**	**C**	**T**	**A**
Hardware								
	Computadores	A	$ 45.000.000,00	10	7	8	7	6
	Impresoras	MB	$ 8.000.000,00	4	2	3	1	1
	memorias USB	MB	$ 4.000.000,00	4	2	3	3	4
	Pbx	MB	$ 6.000.000,00	9	6	4	6	3
	Portátiles	M	$ 32.000.000,00	10	7	8	7	6
Red								
	Switch core	MB	$ 8.771.000,00	10	6	6	10	8
	Equipos de la red cableada (router)	MB	$ 6.454.000,00	10	6	6	10	8
	Equipos de la red inalámbrica (router)	MB	$ 8.200.000,00	10	6	4	10	8
	Cortafuego (Firewall)	MB	$ 3.050.000,00	10	4	4	4	3
	Routers de borde	MB	$ 1.000.000,00	10	10	10	10	10
Instalaciones								
	Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.) y cableado estructurado.	MA	$ 750.000.000,00	8	5	8	4	8
Información								
	Informática (Planes, Documentación, etc.)	M	$ 18.000.000,00	7	8	10	6	8
	Infraestructura (Planes, Documentación, etc.)	M	$ 13.000.000,00	7	8	10	6	8
	Datos e información no empresarial	MA	$ 60.000.000,00	7	7	10	4	2
Datos								
	Finanzas (SI & SI, Sap, Level Money, Spendee, PayPal, etc.,)	B	$ 16.000.000,00	10	8	8	4	2
	Directorio de Contactos	MB	$ 4.000.000,00	8	8	10	4	2
	Bases de datos internas	A	$ 40.000.000,00	10	10	8	4	2
	RR.HH (SI & SI)	M	$ 30.000.000,00	8	10	10	7	7
	Respaldos -Copias de	B	$ 15.000.000,00	8	10	8	7	7

	seguridad							
Aplicaciones-Software								
	Programas de administración (contabilidad, manejo de personal, etc.)	**MB**	$ 6.000.000,00	8	8	8	6	6
	herramientas de desarrollo, aplicativos		$ 0,00					
	Sistemas operativos	**B**	$ 12.000.000,00	10	6	4	6	8
	Aplicaciones de Servidores Locales	**B**	$ 18.000.000,00	10	8	8	6	8
Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.	**A**	$ 45.000.000,00	8	6	8	4	4
Servicios								
	Correo electrónico	MB	$ 1.500.000,00	8	8	8	6	10
	Chat	MB	$ 2.500.000,00	6	6	6	6	8
	llamadas telefónicas	MB	$ 2.500.000,00	6	6	6	6	4
	Herramientas para empresas en la nube	MB	$ 4.000.000,00	10	10	10	10	10
	Página Web Intranet incluso WIFI (Colaboradores)	MB	$ 1.200.000,00	8	6	6	10	10

Tabla Nro. 5, Valoración de los activos y aspectos críticos.

Es necesario aclarar que el valor que se observa en el inventario no es el valor comercial de los activos, sino un compendio de referencia entre el valor comercial y el valor que el activo posee para la empresa y poder cumplir con su misión y visión.

4.6 Análisis de amenazas

Una vez definidos los activos y su valor para la empresa se realizó el análisis para señalar cuales amenazas pueden llegar a afectar a los activos, para posteriormente estimar qué tan vulnerable es el activo a la materialización de dicha amenaza, así como también a la frecuencia estimada de la misma.

De acuerdo con lo anterior, se procedió a realizar la clasificación de las amenazas utilizando las tablas existentes en el libro 2: Catálogo de elementos de MAGERIT, el cual sugiere la agrupación de las amenazas en cuatro grandes grupos. Estos grupos se refieren a los Desastres naturales, accidentes Industriales, errores y fallos no intencionados, y Amenazas intencionales presenciales. De esta forma, analizamos para los grupos de amenazas, la dimensión de seguridad que puede afectar y por consiguiente el activo directamente afectado. En la tabla Nro.6, encontramos las amenazas de acuerdo al libro 2 “catálogo de elementos” Magerit, en donde reflejamos este análisis.

		Dimensión afectada					Activos afectados								
	Amenaza	**A**	**C**	**I**	**D**	**T**	**Hardware**	**Red**	**Instalaciones**	**Software Aplicaciones**	**Información**	**Datos**	**Servicios**	**Personal**	**logs**
Naturales Desastres	[]N.1Fuego				X		X	X	X		X				
	[N.2] daños por agua				X		X	X	X		X				
	[N.3] inundación				X		X	X	X		X				
	[N.4] Siniestro mayor				X		X	X	X		X				
	[N.5] Fenómeno sísmico				X		X	X	X		X				
	[N.6] Fenómeno meteorológico				X		X	X	X		X				
Accidentes de origen industrial	[I.1] Fuego				X		X	X	X		X		X		
	[I.2] daños por agua				X		X	X	X		X				
	[I.12] Sobrecarga eléctrica				X		X	X	X		X		X		
	[I.13] Fluctuación eléctrica			X	X		X	X		X	X				
	[I.3] Contaminación mecánica				X		X								
	[I.4] Contaminación electromagnética				X		X		X						
	[I.5] Avería de origen físico o lógico			X	X		X			X					
	[I.6] Corte del suministro eléctrico			X	X		X	X	X				X		
	[I.7]Condiciones inadecuadas de temperatura o humedad				X		X		X		X				
	[I.8]Fallos de servicios de comunicaciones				X			X							
	[I.9]Interrupción de otros servicios y suministros esenciales				X		X								
	[I.10]Degradación de los soportes de almacenamiento de la información				X						X				
	[I.11]Emanaciones electromagnéticas		X				X		X	X					
Errores y fallos no intencionados	[E.1]Errores de los usuarios		X	X	X					X	X	X	X		
	[E.2]Errores del administrador		X	X	X		X	X		X	X	X	X		
	[E.3]Errores de monitorización (log)			X		X					X				
	[E.4]Errores de configuración			X								X			
	[E.7]Deficiencias en la organización				X										
	[E.8]Difusión de software dañino		X	X	X					X					
	[E.9]Errores de re-encaminamiento		X					X		X			X		
	[E.10]Errores de secuencia			X				X		X			X		
	[E.14]Escapes de información		X												
	[E.18]Destrucción de información		X	X	X			X	X	X		X	X		
	[E.19]Fugas de información		X							X	X	X	X	X	
	[E.20]Vulnerabilidades de los programas (software)		X	X	X					X					
	[E.21]Errores de mantenimiento / actualización de programas (software)			X	X					X					

	[E.23]Errores de mantenimiento / actualización de equipos (hardware)				X		X	X							
	[E.24]Caída del sistema por agotamiento de recursos				X		X	X					X		
	[E.25]Pérdida de equipos		X		X		X								
	[E.28]Indisponibilidad del personal				X									X	
Amenazas intencionales presenciales	[A.3] Manipulación de los registros de actividad (log)			X		X									
	[A.4] Manipulación de la configuración	X	X	X	X					X		X			
	[A.5] Suplantación de la identidad del usuario	X	X	X				X		X		X	X		
	[A.6] Abuso de privilegios de acceso		X	X	X		X	X		X	X	X	X		
	[A.7] Uso no previsto		X	X	X		X	X	X	X		X	X		
	[A.8] Difusión de software dañino		X	X	X					X					
	[A.9] [Re-]encaminamiento de mensajes		X					X		X			X		
	[A.10] Alteración de secuencia			X				X		X			X		
	[A.11] Acceso no autorizado		X	X			X	X	X	X	X	X	X		
	[A.12] Análisis de tráfico		X					X							X
	[A.13] Repudio			X		X							X		X
	[A.14] Interceptación de información (escucha)		X					X							
	[A.15] Modificación deliberada de la información			X				X	X	X	X	X	X		
	[A.18] Destrucción de información				X				X	X		X	X		
	[A.19] Divulgación de información			X					X	X	X	X	X		
	[A.22] Manipulación de programas		X	X	X					X					
	[A.23] Manipulación de los equipos		X		X		X								
	[A.24] Denegación de servicio				X		X	X					X		
	[A.25] Robo		X		X		X								
	[A.26] Ataque destructivo				X		X		X		X				
	[A.28] Indisponibilidad del personal				X									X	
	A.29] Extorsión		X	X	X									X	
	[A.30] Ingeniería social (picaresca)		X	X	X			X						X	

Tabla Nro. 6, Amenazas de acuerdo al libro 2 “catálogo de elementos” Magerit.

En consecuencia, hacemos la definición de la probabilidad de ocurrencia de la materialización de cada amenaza con respecto a los activos que se tienen (frecuencia estimada/días del año), atendiendo las sugerencias por MAGERIT, y de acuerdo con las necesidades de la empresa LIANCAR. Ver Tabla Nro. 7.

Vulnerabilidad (frecuencia estimada/días del año)	Rango	Valor
Frecuencia Extrema	1 vez al día	1*100 = **100**
Frecuencia alta	1 vez al mes	12/365 = 0,03287*100 = **3,287**
Frecuencia media	1 vez cada 6 meses	2/365 = 0,005479*100 = **0,5479**
Frecuencia baja	1 vez al año	1/365 = 0,002739*100 = **0,2739**

Tabla Nro. 7. Escala de valores para la probabilidad y ocurrencia de una amenaza

Definidas las amenazas según MAGERIT y evaluados los puntos vulnerables tomando como referencia las dimensiones de seguridad para determinar los activos afectados, tomamos la información recopilada y debe dar lugar a una tabla resumen como la información que se muestra en la Tabla Nro. 8, donde para cada tipo de activo se analiza la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo. A continuación se muestran los datos obtenidos para el activo "computadores". En la tabla No. 8, solo se señala este activo por la extensión de la tabla. Para verla en forma completa, podemos acceder al archivo "ACTIVOS-AMENAZAS-RIESGOS E IMPACTO-LIANCAR", pestaña "Análisis de Amenazas".

Activo	Amenaza	Frecuencia estimada	A	C	I	D	T
Computadores	[N.1] Fuego	0,2739				100%	
	[N.2] daños por agua	0,2739				100%	
	[N.3] inundación	0,2739				100%	
	[N.4] Siniestro mayor	0,2739				100%	
	[I.1] Fuego	0,2739				75%	
	[I.12] Sobrecarga eléctrica	0,2739				50%	
	[I.13] Fluctuación eléctrica	0,5479			20%	40%	
	[I.5] Avería de origen físico o lógico	0,5479				50%	
	[E.2] Errores del administrador	0,5479			75%	50%	
	[E.8] Difusión de software dañino	3,287		55%	90%	80%	

	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,5479				50%	
	[E.25] Pérdida de equipos	0,2739		80%		80%	
	[A.6] Abuso de privilegios de acceso	0,2739		60%	50%	40%	
	[A.25] Robo	0,2739		80%		80%	
	[A.26] Ataque destructivo	0,2739				90%	

Tabla Nro.8. Activos y dimensiones de la seguridad para el análisis de amenazas

Podemos revisar como en la fila identificadora del activo, anotamos el impacto máximo de todos los impactos que pueden provocar las diferentes amenazas.

4.7 Impacto potencial

Dado que conocemos los valores de los diferentes activos, podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas. Así mismo, en el Libro I Método de MAGERIT se denomina impacto potencial "a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema", (página 28 de 127).

Para ello, es conveniente determinar la escala de valores que nos permitirán evaluar el nivel de impacto potencial. Por tanto, decimos que sí resulta ser una probabilidad de amenaza muy alta (MA), la explotación de la vulnerabilidad puede resultar en altas pérdidas financieras por daños de activos o recursos tangibles impidiendo el logro de los objetivos de la empresa. Si es alta (A), consistiria en la pérdida financiera significativa o amenaza con pérdida de imagen de la empresa LIANCAR, si es media (M), consistiria en una pérdida financiera moderada, no amenaza la imagen de la empresa, si es baja (B), sería una pérdida menor financiera y muy baja (MB), la empresa estaria sin prejuicios o costos bajos. No obstante, el impacto potencial estará representado en los siguientes niveles, valores cualitativos y cuantitativos visualizados en la tabla Nro. 9, de la siguiente forma:

Impacto	Valor
Muy Alto (MA)	[91%- 100%]
Alto (A)	[50% - 90%]

Medio (M)	[20% - 49%]
Bajo (B)	[10% -19%]
Insignificante (I)	[0%-09%]

Tabla Nro. 9. Valores del Impacto.

Para realizar el cálculo del impacto potencial, se toma el valor del activo se multiplica por la frecuencia de ocurrencia estimada y por el mayor de los impactos calculados en las cinco dimensiones de seguridad de cada una de las amenazas, es decir, (impacto potencial = valor del activo * frecuencia de ocurrencia * impacto mayor de las dimensiones). En la tabla Nro. 10, se puede observar los resultados del impacto potencial hallado para el activo "Computadores" solamente, por la dimensión de la tabla.

Ahora, de acuerdo al libro "método 1" de Magerit página 29, se denomina riesgo potencial a "la medida del daño probable sobre el sistema", entonces, conociendo el impacto de las amenazas sobre los activos, es directo derivar el **riesgo potencial** sin más que tener en cuenta la probabilidad de ocurrencia, por lo tanto, teniendo en cuenta el valor de los activos y la valoración de las amenazas, sin salvaguardas actualmente desplegadas podemos obtener el riesgo sumando todos los impactos potenciales generados por cada amenaza. En la tabla No. 10, en la fila de "Riesgo potencial" vemos la determinación de este riesgo. En el ANEXO-AMENAZAS-RIESGOS-EIMPACTO-LIANCARXXX, hoja de Excel pestaña "Impacto Potencial", también, se puede ver con más detalle todos los activos con su impacto potencial.

Activo	Amenaza	Frecuencia estimada	A	C	I	D	T	Valor activo	Impacto potencial
Computadores	[N.1] Fuego	0,2739				100%		$45.000.000,00	$12.325.500,00
	[N.2] daños por agua	0,2739				100%		$45.000.000,00	$12.325.500,00
	[N.3] inundación	0,2739				100%		$45.000.000,00	$12.325.500,00
	[N.4] Siniestro mayor	0,2739				100%		$45.000.000,00	$12.325.500,00
	[I.1] Fuego	0,2739				75%		$45.000.000,00	$9.244.125,00
	[I.12] Sobrecarga eléctrica	0,2739				50%		$45.000.000,00	$6.162.750,00
	[I.13] Fluctuación eléctrica	0,5479			20%	40%		$45.000.000,00	$9.862.200,00
	[I.5] Avería de origen físico o lógico	0,5479				50%		$45.000.000,00	$12.327.750,00
	[E.2] Errores del administrador	0,5479			75%	50%		$45.000.000,00	$18.491.625,00
	[E.8] Difusión de software	3,287		55%	90%	80%		$45.000.000,00	$133.123.500,00

	dañino								
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,5479				50%		$45.000.000,00	$12.327.750,00
	[E.25] Pérdida de equipos	0,2739		80%		80%		$45.000.000,00	$9.860.400,00
	[A.6] Abuso de privilegios de acceso	0,2739		60%	50%	40%		$45.000.000,00	$7.395.300,00
	[A.25] Robo	0,2739		80%		80%		$45.000.000,00	$9.860.400,00
	[A.26] Ataque destructivo	0,2739				90%		$45.000.000,00	$11.092.950,00
						Riesgo Potencial:		$675.000.000,00	$289.050.750,00

Tabla Nro. 10. Impacto Potencial y Riesgo Potencial.

4.8 Nivel de Riesgo Aceptable y riesgo Residual

Es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles. No obstante, la empresa LIANCAR, en consenso con la alta gerencia, el director del centro de tecnologia y el encargado de las finanzas establecieron un nivel de riesgo aceptable de $1.822.763,00 pesos teniendo en consideración criterios como la totalidad del valor de los activos, la pérdida de la imagen, su productividad, las multas y penas legales que se pueden dar, la seguridad y salud. Por tanto, se decidió aceptar este riesgo, porque fue necesario realizar un extenso monitoreo y una correcta elección de las medidas a adoptar basándose en la valoración de los costos del tratamiento del riesgo frente al beneficio representado por el riesgo. Por lo tanto, todas aquellas amenazas cuya materialización represente un monto igual o superior a este valor se seleccionan para la aplicación e implementación de un control o salvaguardas.

En consecuencia, se genera una gran cantidad de datos en este análisis que podemos ver a continuación para la decisión del control o salvaguarda en la tabla No. 11, solo para el Activo “Computadores”. El resto de datos se pueden ver en el anexo ANEXO-AMENAZAS-RIESGOS-EIMPACTO-LIANCARXXX, hoja de Excel pestaña “Aplicación del Control”.

En esta tabla, exactamente, en la columna “Control (SI o NO)”, se plantea con un “SI”, a las amenazas que hay que aplicarle el control respectivo o de lo contrario un “NO”. Ahora, Los valores resaltados en cada activo representan el mayor valor de riesgo cuantificado para el mismo.

Activo	Amenaza	Control (SI o NO)	Frecuencia estimada	Valor activo	Impacto potencial
Computadores	[N.1] Fuego	SI	0,2739	$45.000.000,00	$12.325.500,00
	[N.2] daños por agua	SI	0,2739	$45.000.000,00	$12.325.500,00
	[N.3] inundación	SI	0,2739	$45.000.000,00	$12.325.500,00
	[N.4] Siniestro mayor	SI	0,2739	$45.000.000,00	$12.325.500,00
	[I.1] Fuego	SI	0,2739	$45.000.000,00	$9.244.125,00
	[I.12] Sobrecarga eléctrica	SI	0,2739	$45.000.000,00	$6.162.750,00
	[I.13] Fluctuación eléctrica	SI	0,5479	$45.000.000,00	$9.862.200,00
	[I.5] Avería de origen físico o lógico	SI	0,5479	$45.000.000,00	$12.327.750,00
	[E.2] Errores del administrador	SI	0,5479	$45.000.000,00	$18.491.625,00
	[E.8] Difusión de software dañino	SI	3,287	$45.000.000,00	$133.123.500,00
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	SI	0,5479	$45.000.000,00	$12.327.750,00
	[E.25] Pérdida de equipos	SI	0,2739	$45.000.000,00	$9.860.400,00
	[A.6] Abuso de privilegios de acceso	SI	0,2739	$45.000.000,00	$7.395.300,00
	[A.25] Robo	SI	0,2739	$45.000.000,00	$9.860.400,00
	[A.26] Ataque destructivo	SI	0,2739	$45.000.000,00	$11.092.950,00

Tabla Nro. 11. Decisión del Control o salvaguarda para el activo Computadores.

No obstante, para cada una de las amenazas que fueron identificadas y cuyo impacto potencial de riesgo supera el riesgo aceptable establecido por la empresa LIANCARXXX, se les aplica 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. Así mismo, se vuelve a cuantificar el riesgo y en este caso todos han quedado por debajo del umbral establecido, lo que indica que en cierta forma los controles son adecuados. En la tabla No. 12, vemos las salvaguardas que se aplicaron a las amenazas para el activo “Computadores” de la empresa. Podemos ver el análisis completo en el Anexo ANEXO-AMENAZAS-RIESGOS-EIMPACTO-LIANCARXXX, hoja de Excel pestaña “Impacto Residual”.

Una vez establecido el control, se reducirá el riesgo, pero este seguirá existiendo, lo deseable es conseguir su reducción para que esté por debajo del nivel aceptable, a este riesgo que seguirá existiendo después de aplicar los controles de seguridad, se denomina riesgo residual.

Activo	Amenaza	Salvaguarda	Frecuencia estimada	A	C	I	D	T	Valor activo	Impacto Residual
Computadores	[N.1] Fuego	Sistema de supresión y protección contra incendios	0,002739				70%		$45.000.000,00	$86.278,50
	[N.2] daños por agua	Detectores de humedad	0,002739				60%		$45.000.000,00	$73.953,00
	[N.3] inundación	Pólizas de seguro	0,002739				70%		$45.000.000,00	$86.278,50
	[N.4] Siniestro mayor	Pólizas de seguro	0,002739				70%		$45.000.000,00	$86.278,50
	[I.1] Fuego	Sistema de supresión y protección contra incendios	0,002739				60%		$45.000.000,00	$73.953,00
	[I.12] Sobrecarga eléctrica	Ups	0,002739				50%		$45.000.000,00	$61.627,50
	[I.13] Fluctuación eléctrica	Ups	0,005479			20%	60%		$45.000.000,00	$147.933,00
	[I.5] Avería de origen físico o lógico	Mantenimiento periódico del hardware, Sistemas de alimentación ininterrumpida	0,005479				50%		$45.000.000,00	$123.277,50
	[E.2] Errores del administrador	Capacitación y actualización personal	0,005479			55%	50%		$45.000.000,00	$135.605,25
	[E.8] Difusión de software dañino	Antivirus y actualización de bases datos	0,03287		45 %	50%	50%		$45.000.000,00	$739.575,00
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Capacitación y actualización personal	0,005479				60%		$45.000.000,00	$147.933,00
	[E.25] Pérdida de equipos	Seguro	0,002739		80 %		60%		$45.000.000,00	$73.953,00
	[A.6] Abuso de privilegios de acceso	Cuentas y privilegios de usuario	0,002739		60 %	50%	40%		$45.000.000,00	$73.953,00
	[A.25] Robo	Seguro	0,002739		80 %		80%		$45.000.000,00	$98.604,00
	[A.26] Ataque destructivo	Pólizas de seguro	0,002739				90%		$45.000.000,00	$110.929,50

Tabla No. 12. Impacto y riesgo residual para el activo “Computadores”

Es decir, dado este conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual, se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

Ahora, para el **cálculo del riesgo residual**, podemos decir que, como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia por lo que la

magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

4.9 Resultados del Análisis de riegos

En este apartado dejaremos ver por medio de la tabla Nro. 13 (La tabla no se encuentra completa por seguridad), los riesgos obtenidos del análisis, de acuerdo a sus amenazas por cada activo de la empresa destacando aquellos que están por encima del nivel aceptable. Estos riesgos se trataron por medio de un control o salvaguarda para su respectiva mitigación. A continuación presentamos una lista de riesgos encontrados en la empresa LIANCAR LTDA.

Id	Riesgo Identificado
1	La empresa está ubicada cerca al río Bogotá, por lo que puede presentarse inundaciones.
2	No existen barreras físicas que aíslen las áreas coyunturales de la empresa
3	No hay Controles de acceso físico, lo que pueden incluir el uso de sistemas biométricos y vigilantes para acceso en áreas específicas
4	No hay Controles a nivel de equipos, tales como ubicación y protección, seguridad en cableado o mantenimiento periódico de equipos
5	No utilizan un circuito cerrado de televisión

Tabla No. 13, Riesgos obtenidos del análisis

4.10 Resultados

En este análisis, se ha encontrado los diferentes riesgos que son generados por las diferentes amenazas, más relevantes para la empresa LIANCAR, que repercuten en la información almacenada en el sistema contable (SI&SI) y en su infraestructura iniciando por su centro de datos. Así mismo, los datos de SI&SI del Departamento Administrativo Comercial y Financiero, Departamento Sistema Integrado de Gestión, Recursos Humanos y los respaldos como las copias de seguridad, constituyen en los activos un valor agregado a la entidad por encontrarsen ubicadas en la oficina del gerente oficial.

Después de hacer el análisis de las posibles amenazas se ubicaron las siguientes como las posibles sobre los sistemas de información: Todas las relacionadas con desastres naturales sobre las instalaciones, encontrándose que el impacto en caso de materializarse, dejaría inoperativa a la empresa.

Las amenazas de difusión de software dañino y destrucción de información, se constituyen en las que más activos impactan, teniendo un valor muy alto en caso de materializarse. Esto, es debido a una sistematización de procesos dentro de las oficinas y son manejados en un 85% desde sistemas informáticos, en consecuencia, si no se protege el canal de datos, los equipos y las aplicaciones de manera apropiada, se puede presentar una caída del sistema de la entidad,

dejándola inoperativa durante un intervalo de tiempo muy amplio, creando traumatismos en todos los procesos de la empresa en sus diferentes departamentos y áreas.

5. Fase 4: Propuestas de proyectos

5.1. Introducción

Con el proceso sobre el análisis de los riesgos, ya se conoce el estado actual de la empresa LIANCAR LTDA en lo relativo a los riesgos residuales a los que está expuesta, por lo cual deben plantearsen proyectos que ayuden a alcanzar los niveles de seguridad que se necesitan con extrema urgencia.

No obstante, los proyectos que se mencionan y tratan a continuación son el resultado del análisis de riesgos elaborado para la empresa LIANCAR, y en conformidad con el directivo de alta gerencia de la empresa, por lo tanto estos resultados presentan datos de alta fidelidad y de acuerdo a las solicitudes planteadas a la gerencia se ha controlado información en la que los riesgos son más cercanos a la realidad de la empresa. Por ende, en este espacio proponemos tres proyectos que consisten en el plan de capacitación, plan de mitigación de los riesgos y el plan de continuidad del negocio respectivamente.

5.2 Propuestas

Estos proyectos, deben derivarse de los resultados obtenidos del análisis de riesgos y recomendaciones asociadas a las amenazas identificadas y tienen un nivel de objetividad y forma para su desarrollo, entre los proyectos mencionados a realizar presentamos sus objetivos:

En el plan de Sensibilización y Capacitación tendrá el objetivo general de diseñar la campaña, estrategia de sensibilización, divulgación, concienciación y capacitación sobre el nuevo plan de seguridad de la información para la empresa LIANCAR, creando un compromiso y un impacto positivo en los funcionarios, proveedores y terceros, además de los clientes, comunidad y los ciudadanos en general.

De conformidad, en el plan de continuidad del Negocio se tendrá el objetivo de proteger los procesos críticos y operativos de la empresa contra desastres naturales o fallas mayores por la interrupción de las operaciones de una empresa, disminuyendo el impacto en las pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad, debido a que los recursos de la organización no están disponibles.

No obstante, el objetivo del plan de mitigación de riesgos será el de establecer acciones para mitigar los riesgos por difusión de software dañino, interceptación de información, y destrucción de información con el fin de alcanzar los objetivos

de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

Estos proyectos planteados son el resultado del análisis de riesgos, ya que se detectó un nivel bajo en capacitación y concienciación del personal, junto con problemas de recuperación en caso de desastres. Adicionalmente se pudo establecer con este análisis la necesidad de acciones adicionales para la red de datos, los sistemas de aplicaciones, la falta de personal y el equipo de cómputo que ayuden a mitigar la difusión de software dañino.

Como propuestas importantes según el análisis de riesgos de la empresa LIANCAR, tenemos un plan de sensibilización (ANEXO I) y capacitación, un plan de continuidad del negocio (ANEXO J) y un plan de mitigación de los riesgos (ANEXO K) de la empresa desde la parte inicial o básica, precisamente porque el personal o empleados no tienen una cultura sobre la seguridad de la información, en ello determinamos las amenazas, riesgos obtenidos, la dimensión de seguridad afectada según la integridad, disponibilidad y confiabilidad detallados en los aspectos críticos de la información, las acciones a implementar, el impacto y la prioridad de desarrollo como se muestra en la tabla Nro.14. (La tabla no se presenta en su totalidad por seguridad)

Nombre del Proyecto	Amenazas identificadas	Riesgos Identificados	Dimensión afectada	Acciones	impacto	Prioridad desarrollo
Plan de Sensibilización Formación	[E.1] Errores de los usuarios.	La Educación y capacitación continua en aspectos de seguridad de la información es nula.	Integridad	Campaña publicitaria Concienciación Ejercicios de buenas prácticas Cursos de capacitación	Alto Medio Alto Medio	Medio
	[E.2] Errores del administrador.	La falta de capacitación tanto para los usuarios y administrador del sistema informático es nula	Integridad			
	[E.7] Deficiencias en la organización.	Los Procedimientos e instructivos para el manejo de información y segregación de funciones carecen de existencia.	disponibilidad			
	[E.18] Destrucción de información.	No existe un monitoreo y trazabilidad de la información y del software utilizado en la empresa	integridad			
	[E.19] Fugas de información.	No se cuenta con un Monitoreo de los sistemas, sincronización de relojes y protección sobre registros	confidencialidad			

Tabla 14. Relación de proyectos con riesgos identificados por encima del valor aceptable, con las diferentes acciones a realizar.

Estos proyectos tienen un nivel de objetividad y forma para su desarrollo, entre los proyectos mencionados se tratan en las secciones siguientes.

5.2.1 Plan de Sensibilización y Capacitación

En el alcance de este Plan se involucra al personal empleados de la empresa. En etapas posteriores también se involucrará a proveedores y usuarios o terceros anexos a la empresa de forma que se adquiera educación en aspectos básicos de seguridad de la información. Así mismo, para las personas que son en cierto modo avanzadas en los procesos de seguridad, se tienen contempladas capacitaciones de nivel técnico y jurídico, de modo que se mejore el proceso de educación y concienciación en manejo de la seguridad de la información. En el plan de Sensibilización y Capacitación tendrá el objetivo general de diseñar las campañas, estrategias de sensibilización, divulgación, concienciación y capacitación sobre el nuevo plan de seguridad de la información para la empresa LIANCAR, creando un compromiso y un impacto positivo en los funcionarios, proveedores y terceros, además de los clientes, comunidad y los ciudadanos en general.

Con respecto a sus Fases sobre todo en el Diseño del plan de sensibilización se diseñan las estrategias para sensibilizar a todos los actores de la entidad. Para ello se utilizarán diferentes estrategias, las cuales serán seleccionadas y planteadas en este proyecto. Se calcula un tiempo de 15 días para esta fase.

En el Diseño del plan de capacitación, se revisará y diseñará los cursos relacionados con seguridad de la información para personal clave, así como talleres prácticos para las mismas personas. Se calcula un tiempo de 24 días para el desarrollo de esta fase.

En la parte de la Consecución de los recursos, se realizará la gestión de los recursos financieros y de personal que se necesitan para poner en funcionamiento el plan de sensibilización y capacitación. Debido a los tiempos administrativos y financieros, se calcula que esta fase puede tardar hasta 6 meses.

Para la Ejecución del plan, de acuerdo con lo planeado, tendrá una duración de 8 meses y se entregaran memorias y documentos de soportes del plan de capacitación. En el Anexo I se encuentra el cronograma del plan de sensibilización y capacitación.

5.2.2 Plan de Continuidad del Negocio

En lo referente al plan de la continuidad de la empresa, notamos, que, para iniciar el plan, la dirección general o alta gerencia, los directores de operaciones, sistemas, administración, finanzas y recursos humanos son los directos responsables de iniciar este Plan [16]. De conformidad, con el plan de continuidad del Negocio se tendrá el objetivo de proteger los procesos críticos y operativos de la empresa contra desastres naturales o fallas mayores por la interrupción de las operaciones de una empresa, disminuyendo el impacto en las

pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad, debido a que los recursos de la organización no están disponibles.

Este Plan, en su esencia debe ser preventivo y no correctivo para continuar con las actividades críticas de la empresa LIANCAR en el caso de que una falla o desastre inesperado que pudiera seriamente interrumpir los procesos de la empresa. En el ANEXO J encontramos la descripción de este Plan y su cronograma con respecto a la capacitación. Sin embargo, se realiza una descripción del mismo.

El alcance del plan de continuidad del negocio está adherido a la empresa, y busca generar las pautas que permitan restituir en el menor tiempo posible la operatividad del negocio, en caso de que en la sede ubicada en Bogotá, quede inoperativa a causa de un incidente que impida su funcionamiento de manera parcial o total.

En esto, se supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, Software y Equipos Activos involucrados en los procesos críticos definidos en este Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del Centro de Cómputo para ser implementados en la sede de Medellín Antioquia.

El plan busca reducir el nivel de riesgo de las amenazas de [I13] fluctuación eléctrica, [I5] avería de origen físico o lógico, [N.1] Fuego, [N.2] daños por agua, [N.3] inundación, [N.4] Siniestro mayor, [N.5] Fenómeno sísmico, [I.1] Fuego, [I.12] Sobrecarga eléctrica, [I.6] Corte del suministro eléctrico, [A.18] Destrucción de información, y [A.26] Ataque destructivo, con respecto a la disponibilidad en el centro de datos, el cual posee alojado el servidor principal, con las aplicaciones críticas para el negocio.

En cuanto a las Fases tenemos:

En la Evaluación del estado actual, el equipo realizará un análisis de riesgos para identificar los activos con que cuenta, activos críticos a ser protegidos, el estado de los controles actuales y la definición de los equipos que deben ser adquiridos y los procesos y procedimientos que deben ser desarrollados. Esto se ha desarrollado a lo largo del proyecto.

En la Estrategia de respaldos, la empresa LIANCAR después de discutir diferentes alternativas decidió contar con un centro de réplica ubicado en la ciudad de Medellín Antioquia, la cual permitirá trasladar en el menor tiempo posible la operación para continuar con sus actividades. Esta decisión fue tomada desde la Alta Gerencia y sus colaboradores. Este sitio es una sede de LIANCAR en donde, los recursos técnicos y humanos para su adecuación vienen siendo contemplados en su momento y se encuentran en fase de compra, contratación e instalación.

Para el Desarrollo del plan, se definirán los equipos necesarios para un desarrollo adecuado del plan, con sus responsabilidades y funciones. También se hará una descripción de los procedimientos de alerta y actuación ante los eventos que pueden llegar a activar el plan. Y finalmente el procedimiento de vuelta a la normalidad.

Con respecto a las Pruebas, éstas se realizarán para verificar que el plan funcione de manera correcta, teniendo en cuenta el modelo de pruebas. Se realizará una Capacitación y entrenamiento respectivo al personal a cargo del plan de contingencias, y se realizará un plan de concientización entre todo el personal de la empresa.

Ahora, en la Puesta en marcha del plan, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del Centro de Cómputo principal para ser implementados en el Centro de Datos alterno en la Ciudad de Medellín.

5.2.3. Plan de mitigación de riesgos

En su alcance, el plan de mitigación de riesgos busca establecer acciones y recursos que restrinjan de la mejor forma posible la propagación de software autoejecutable o dañino, que destruya o intercambie información tanto en los equipos de cómputo, como en las aplicaciones y las redes utilizadas por LIANCAR. Así mismo, se busca con este plan restringir el acceso a la información contenida en los discos duros de los equipos de cómputo, de acuerdo con los niveles de acceso. No obstante, el objetivo del plan de mitigación de riesgos será el de establecer acciones para mitigar los riesgos por difusión de software dañino, interceptación de información, y destrucción de información con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

En el proyecto sobre la mitigación de riesgos se especifica una serie de pasos que se deben realizar para el tratamiento de los riesgos encontrados en la empresa. El ANEXO K detalla el Plan de Mitigación de Riesgos que tendrá un alcance y sus respectivas fases.

Igualmente, para mayor compendio en resumen se detalla los cronogramas de los proyectos propuestos en esta sección como se demuestra a continuación en las figuras No. 10, 11 y 12.

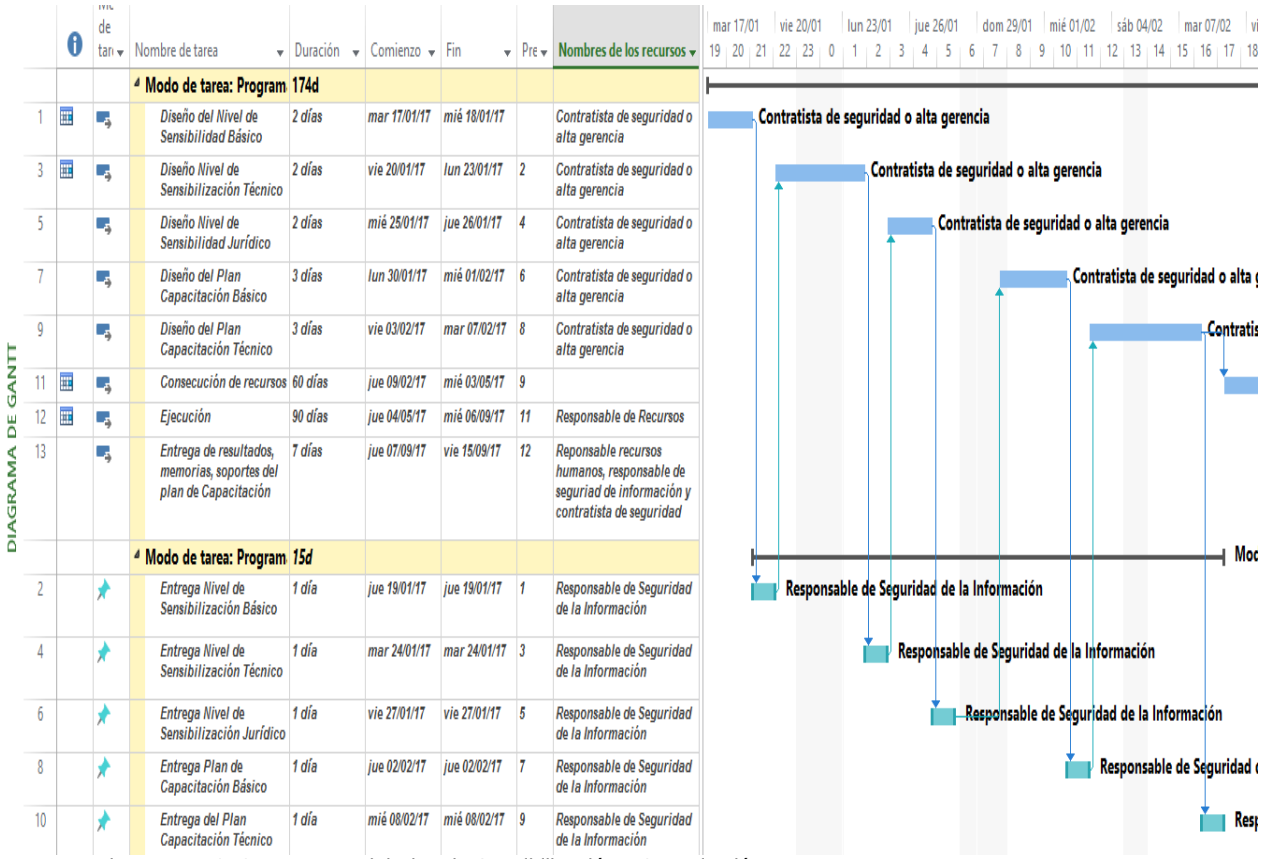


Figura No. 10, Cronograma del Plan de Sensibilización y Capacitación

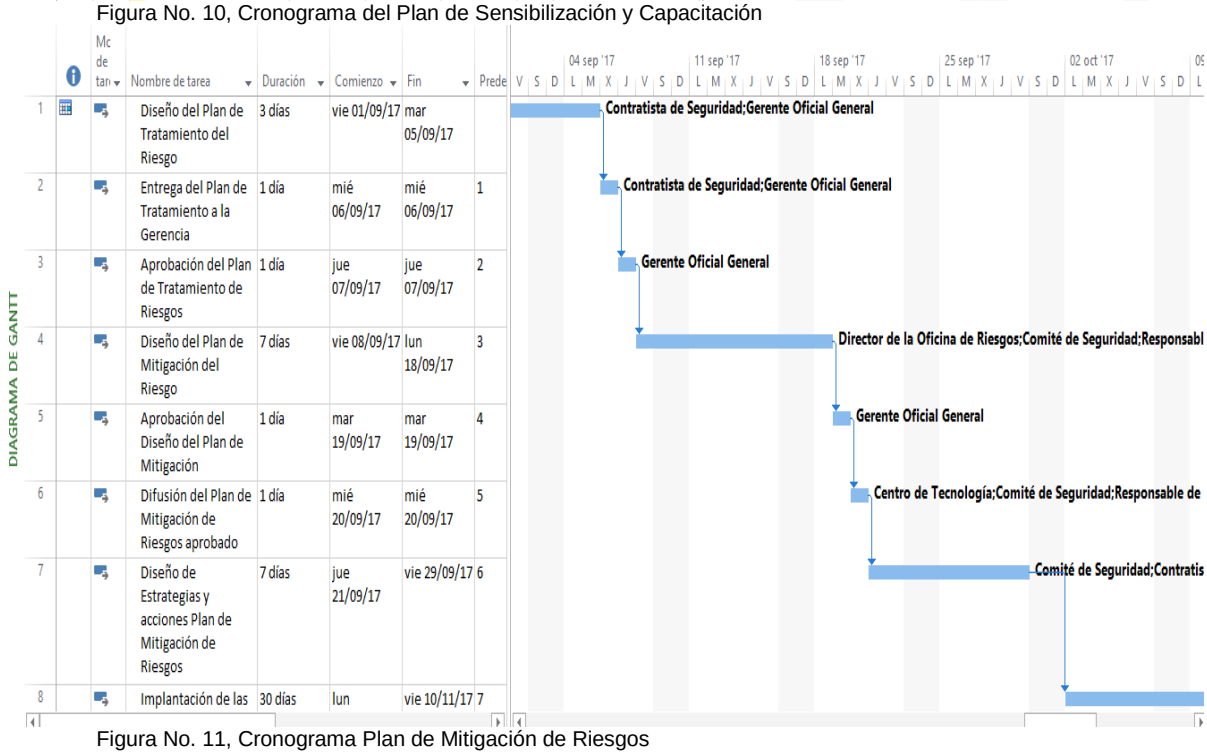


Figura No. 11, Cronograma Plan de Mitigación de Riesgos

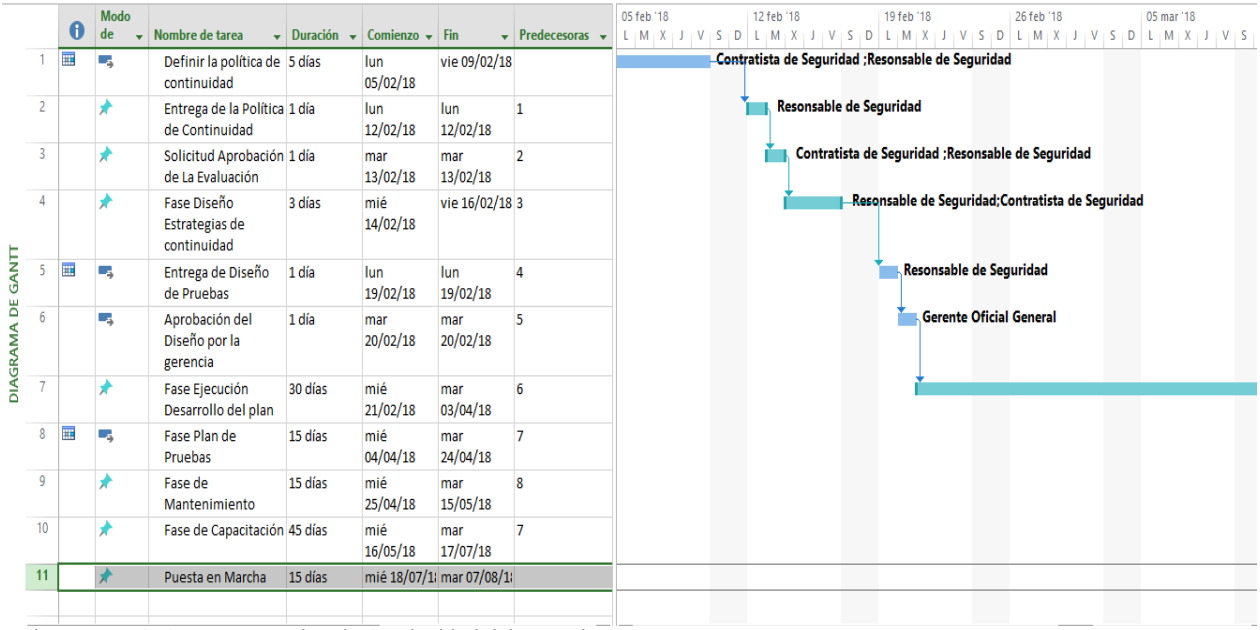


Figura No. 12, Cronograma Plan de Continuidad del Negocio

5.3 Resultados

La propuesta de proyectos debe alinearse con un análisis del impacto sobre la seguridad. El plan de continuidad del negocio está relacionado con los posibles escenarios de desastre, condiciones que se deben obtener para cumplir que se active el plan y planes de recuperación. Esto comporta, que su ejecución nos debe indicar cómo evoluciona el riesgo y el impacto de materialización, así como el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002. En cuanto al plan de sensibilización y capacitación es muy necesaria su implantación por razones con respecto a las dificultades que tienen los empleados de la empresa con respecto a la seguridad de la información. Ahora, en el plan de mitigación de riesgos, se incluye en detalle las acciones que se van a implementar para el tratamiento de los riesgos identificados, agregando los recursos para implementar las acciones los responsables de dichas acciones, los plazos que se deben establecer para asegurarnos de su cumplimiento y los controles del anexo A de la ISO 27001 relacionados.

6. Fase 5: Auditoría de cumplimiento

6.1 Introducción

Llegados a esta fase, se conoce los activos de la empresa y se ha realizado una evaluación de las amenazas. Es el momento de hacer una evaluación para saber hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 sirve como marco de control del estado de la seguridad. La realización de esta evaluación servirá como punto de partida para la formulación de los planes y proyectos de mejora en materia de seguridad

de la información a corto, mediano y largo plazo, marcando las pautas de desarrollo de los mismos.

6.2 Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

No obstante, para efectos de interés sobre el nivel de cumplimiento iniciamos a la realización de la auditoría interna al SGSI de la empresa LIANCAR. Para llevar a cabo este objetivo, se tienen en cuenta los dominios de control y los controles planteados por ISO/IEC 27002:2013. En consecuencia, se ha definido el plan de auditoría interna FORMATO FAI-01, que contempla las exclusiones de acuerdo a la declaración de aplicabilidad, además, una lista de verificación de conformidades y no conformidades encontradas en el Anexo M “REALIZACION DE LA AUDITORIA INTERNA” y dentro del documento se reflejan los apartados de “ANEXO FICHAS DE NO CONFORMIDADES Y OBSERVACIONES” con varios formatos para el control de “OPORTUNIDADES DE MEJORA Y OBSERVACIONES”, de todas las acciones con los que deben contar para la obtención de un nivel de calidad en la seguridad de la información dentro de la empresa.

Como la metodología a seguir, para llevar a términos precisos los procesos de la auditoría de cumplimento ha sido planteada a partir de los dominios y objetivos de la norma ISO/IEC 27001:2013, se tienen los siguientes pasos:

1. Determinar el grado de madurez inicial de los controles y medidas de seguridad de la información de la empresa LIANCAR.
2. Verificación de la existencia de medidas y controles de seguridad de la información mediante documentos escritos y/o aprobados, como la política del personal, solicitudes técnicas y la seguridad física.
3. La valorización de los grados de madurez de los salvaguardas y medidas de seguridad implementados en la empresa a través de instrumentos de verificación definidos en los puntos de control de la norma ISO/IEC 27002:2013.
4. La valoración del grado de madurez de la empresa con respecto a la norma ISO/IEC 27001:2013 antes y después de haber implementado el SGSI.

Los tres primeros pasos se han venido desarrollando a través del plan de SGSI con el análisis diferencial ISO/IEC 27001:2013 - 27002:2013, con un esquema documental utilizando instrumentos de evaluación elaborados para las propuestas del plan de acción para el tratamiento de riegos, diseñados en la fase anterior. También, con el documento de verificación teniendo en cuenta la información aportada por la declaración de aplicabilidad coincidiendo con el análisis diferencial.

Ahora, para el cuarto paso, se toma como base el análisis diferencial inicial y para la valoración del grado de madurez se utiliza una escala que está basada en el modelo CMM, que se detalla en el siguiente apartado.

6.3 Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

De forma resumida, los dominios que se analizaron son:

- 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

En este estudio se realizó una revisión de los controles planteados por la norma para cumplir con los diferentes objetivos de control. Esta estimación se desarrollo basado en el Modelo de Madurez de la Capacidad (CMM), ver la tabla Nro. 15.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	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.

50%	**L2**	Reproducible, pero intuitivo	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.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	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.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla Nro. 15, Modelo de Madurez de la Capacidad (CMM)

Los procesos para realizar esta valoración, se inició evaluando los diferentes controles, a partir de los cuales se realiza el cálculo del nivel de cumplimiento del control. Este nivel de cumplimiento del dominio será tomado del cálculo del promedio de cumplimiento de los objetivos de control que lo componen. En el Anexo N "AUDITORÍA DE CONTROLES", se encuentra la valoración de todos los controles y dominios. Para referencia en la Tabla No. 16, presentamos una ilustración sobre el control de la auditoría teniendo en cuenta la metodología establecida y con base en el análisis de implementación de los controles actuales de la empresa.

		NIVEL DE CUMPLIMIENTO		PORCENTAJE
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	L2		58%
5.1	*Directrices de la Dirección en seguridad de la información.*	L2		57,5%
5.1.1	Conjunto de políticas para la seguridad de la información	L3	Se ha establecido una Política General de Seguridad que ha sido revisada por el Gerente Oficial de la empresa LIANCARXXX, pero aún no la ha aprobado. Sin embargo, existen normativas específicas respecto al uso de los recursos de información así como procedimientos	90%
5.1.2	Revisión de las políticas para la seguridad de la información	L1	El gerente oficial de la empresa revisa y aprueba la política de seguridad y para ello, el Gerente Oficial de la empresa LIANCARXXX, debe reunirse con los encargados de los procesos y el comité encargado de la seguridad de la información en lapsos de cada dos semanas pero no han logrado realizar esta revisión, actualización y aprobación de todas las políticas.	25%
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMA**	L2		59%

Tabla No. 16, Control de Auditoría

6.4 Presentación de resultados

Como resultado de la evaluación de los riesgos se ha encontrado un cumplimiento en porcentajes de los controles de seguridad como lo señala la Figura No. 13.

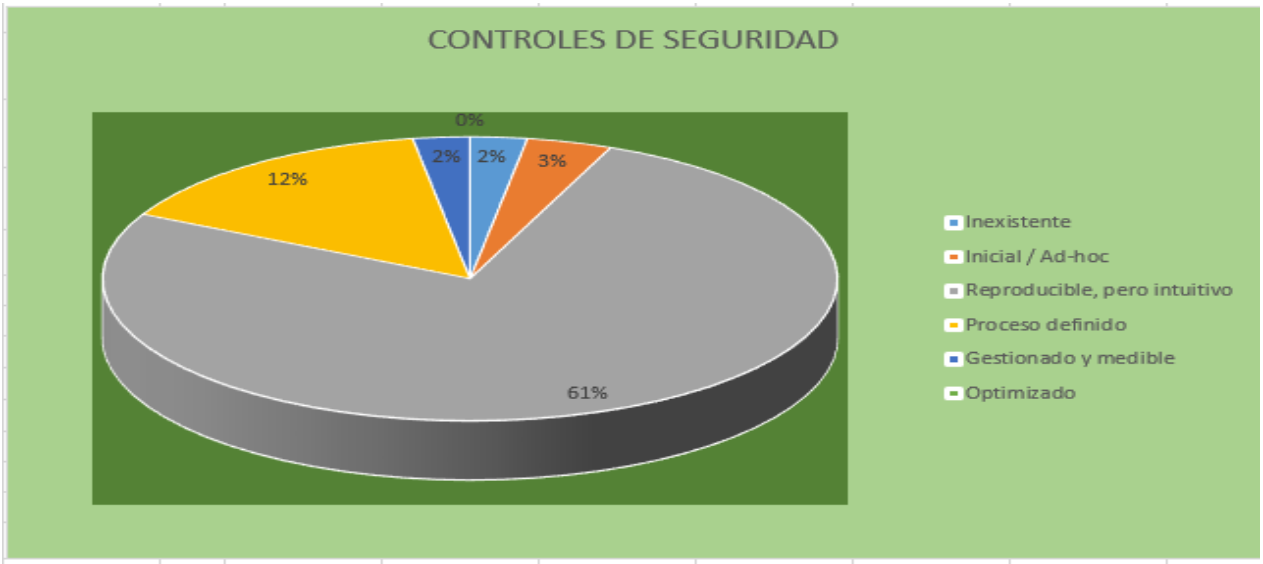


Figura No. 13, Porcentaje de Madurez de los Controles de Seguridad ISO

No obstante, de la auditoría encontramos que el 61% de los controles, de (9 dominios) se encuentran en estados reproducibles pero intuitivos, mientras que el 12% de solo 3 dominios están en estado “proceso definido” y se trata de los controles sobre seguridad en la operativa, seguridad física y ambiental, todo esto, es debido a que, las políticas y los procedimientos en su gran mayoría están redactados en un documento que se encuentra en poder del gerente oficial y son usados por algunos empleados de la empresa, pero carecen de la revisión y aprobación de todos los miembros de la empresa.

Otra causa es que algunos procesos dependen de varias oficinas de la empresa, y por lo tanto se necesita de su aprobación, como la seguridad en los recursos humanos, seguridad en las telecomunicaciones, causando lentitud en la ejecución de proyectos y actividades, y por lo tanto causando retrasos en los procesos de mejora. De conformidad tenemos un nivel de cumplimiento del 46%.

Una visión más detallada es la que se presenta como ‘diagrama de radar’, ver figura No. 14, que mostraría el nivel de cumplimiento por capítulo ISO. En este diagrama mostramos un contraste entre el estado actual con el estado deseado.

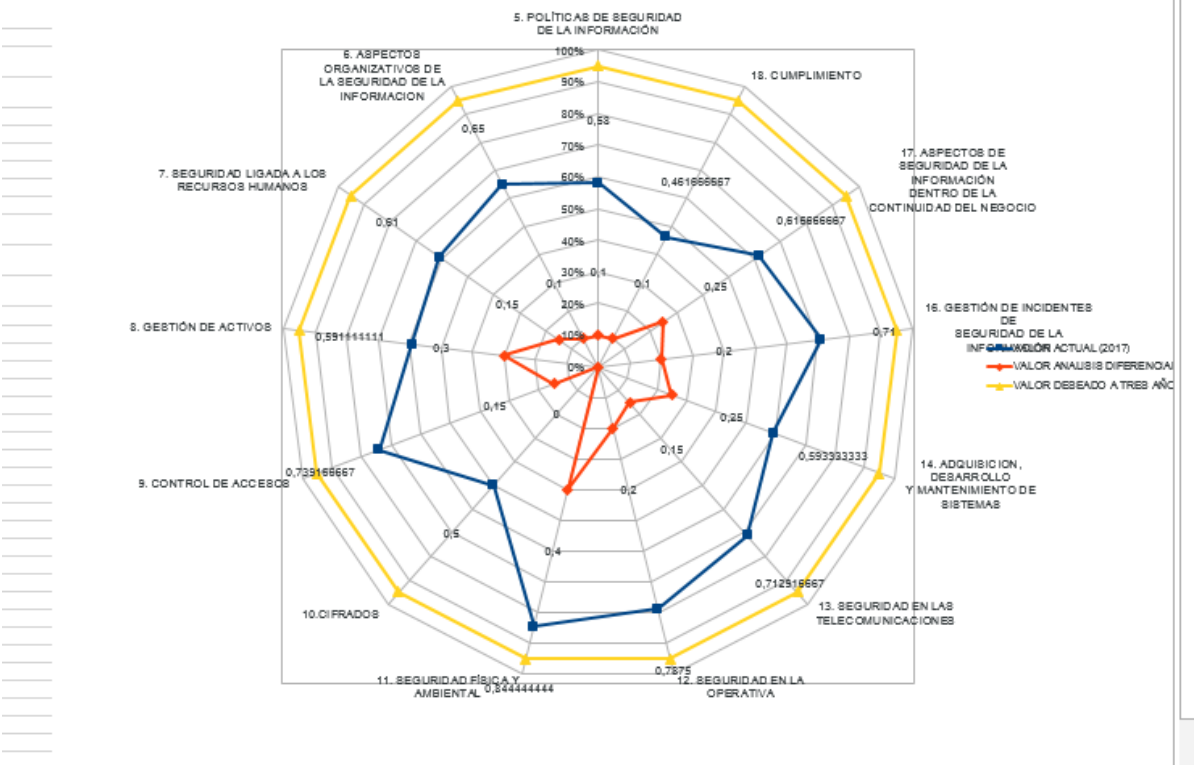


Figura No. 14 Diagrama radial estado madurez controles ANEXO A 27002:2013.

6.5 Resultados

Es de notar que la gráfica radial Figura No. 14, deja entrever que los dominios de seguridad en la operativa, seguridad física y ambiental, seguridad en las telecomunicaciones y los aspectos en la organización son los que se encuentran con un estado de madurez mayor, sin desconocer que existen otros dominios en los que la empresa LIANCAR, ha dado atributos y esfuerzos por llegar a un estado de madurez mejor. Por lo tanto, cabe destacar que durante este plan de trabajo se mejoraron los aspectos relacionados con la continuidad del negocio, pasando de un 25% de cumplimiento en el análisis diferencial, a un 62% en la auditoría realizada, lo cual es algo que denota esfuerzo por alcanzar la mejora continua desde la oficina de seguridad de la información.

Se debe, contar con el apoyo y esfuerzo desde la gerencia oficial de la empresa por implementar los planes de sensibilización y capacitación relacionada, implantar los controles de protección de los registros y la realización del plan de auditoría para mejorar los niveles de cumplimiento, ya que en este momento no llegan al 50%.

Es de notar, que también se encuentra un buen interés desde la gerencia general por la implementación y puesta en marcha del sistema de gestión de seguridad de la información y es claro que en algunos roles de la empresa todavía hay falta de compromiso para su cumplimiento, lo cual sugiere que debe reforzarse las acciones de toma de conciencia y apropiación de las acciones propias de la seguridad de la información.

7. Conclusiones

Con la elaboración de este trabajo se ha logrado el objetivo de crear de manera practica un plan maestro de seguridad de la información, el cual ayudó a mejorar distintas habilidades, muy necesarias sobre todo en el manejo de metodologías específicas como MAGERIT y la realización de informes finales de auditoría, las cuales permitieron desarrollar de forma más especializada trabajos concernientes a la gestión de la seguridad de la información relacionada con las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. 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 la empresa LIANCAR LTDA en lo que refiere a los objetivos del SGSI que se desea implementar.

Sin embargo, se encontró que uno de los mayores obstáculos a la hora de desarrollar trabajos de esta índole, fue el de contar con el apoyo y liderazgo de la alta dirección, lo cual es fundamental para el éxito de este trabajo.

No obstante, hacer lograr una concienciación de la gerencia en cuanto al manejo seguro de la información en todos sus ámbitos, permite que la empresa vea en mejora continua y de forma razonable sus procesos y procedimientos relacionados a corto, mediano y largo plazo.

Se proporcionó información relevante para realizar el análisis de riesgos en la empresa. Tanto en fundamentación teórica como su desarrollo. Y de acuerdo a los objetivos planteados inicialmente, se puede concluir que en el análisis de riesgos se pudo observar la necesidad de crear un plan de continuidad de negocio que permita a la empresa LIANCAR LTDA, estar a la Vanguardia, estar lista en caso de tener un incidente que comprometa el funcionamiento normal de sus procesos u operaciones críticas. Su propuesta y diseño permitió incluirlo dentro de los planes administrativos y financieros, quedando planteado ante la dirección administrativa y financiera.

Además, durante el trabajo se evidenció la necesidad de involucrar no solo al personal empleado de LIANCAR en el alineamiento de los procesos de sus oficinas para cumplir con la norma ISO 27001:2013, sino también, al gerente oficial y subgerentes de las distintas sedes, al Direccionamiento y Planeamiento Corporativo, al Departamento de Recursos Humanos, al Departamento Administrativo Comercial y Financiero y al Departamento de Integración y Gestión, ya que el trabajo en conjunto de estos departamentos permite generar los recursos humanos, técnicos y de capital que se necesitan para modificar los procesos. En consecuencia, todavía debe cumplirse con una serie de procesos largos y engorrosos que retrasan el cumplimiento de los objetivos propuestos, esto debido a lo inmensa que es la empresa por lo que cuenta son sus sedes a nivel nacional y a los tiempos asignados anualmente para generación de solicitudes, presupuestos, finanzas, etc.

De estos Departamentos que tiene la empresa, se identificó que los procesos sobre todo los estratégicos como la planeación estratégica, su arquitectura organizacional y su infraestructura tecnológica y la gerencia de proyectos, son

fundamentales dentro de la alineación con esta norma. Sin embargo, los procesos de soporte son los que proporcionan el sustento al sistema de gestión de seguridad de la información y su buen manejo es fundamental para el éxito y buen desarrollo de los procesos.

Con respecto al análisis diferencial y de la actualización y desarrollo de la gestión documental, se pudo evidenciar la baja y casi inexistente capacitación que tiene el personal de la empresa LIANCAR y de las dependencias o departamentos que manejan procesos críticos. Esto, conllevo a generar propuestas de proyectos que permitieran alcanzar el nivel de seguridad deseado, como el caso de un plan de capacitación y concienciación que involucre a funcionarios de distinto nivel de conocimiento, y que permita mejorar los ámbitos relacionados con normativa legalidad, política y tratamiento de riesgos, así como también, genere una cultura de seguridad que permita disminuir eventos como destrucción de información (accidental o por ataques) y errores de los usuarios por desconocimiento de los mismos, los cuales se constituyen en amenazas con alto impacto y frecuencia dentro de la empresa.

No obstante, para que las estrategias de seguridad de la información puedan ser implementadas y mantenidas en el tiempo, es vital el apoyo económico gerencial que permita contar con más personal y equipos hardware o software. Por ejemplo, se debe conseguir personal capacitado y certificado para realizar las auditorías internas. Adicionalmente, se debe desarrollar un análisis de carga para establecer el número de personas que deben ser adicionadas para el tratamiento y la respuestas a incidentes, ya que en este momento solo se cuenta con una persona de seguridad para resolverlas. También se debe destinar parte de los rubros conseguidos para la adquisición de software de análisis y gestión de riesgos, ya que el gran volúmen de activos que se maneja hace difícil su correcta gestión sin una ayuda de este tipo de paquetes.

Es necesario, proponer varias auditorías internas, la cual permita establecer el estado de los controles que fueron propuestos en esta primera parte del proyecto y que no han sido implantados en su totalidad en este momento. Luego, esta auditoría permitirá establecer los pasos a seguir, como nuevos proyectos a ejecutar, encontrar por ejemplo “cuáles controles deben ser reforzados o cambiados para mejorar el nivel de madurez en cuestiones de seguridad dentro de la empresa”. Adicionalmente, se podrá establecer formalmente el tiempo necesario para alcanzar la madurez y buscar una certificación de los procesos de la entidad, en lo relacionado con la ISO/IEC 27001:2013.

Es de notar y destacar dentro de este trabajo la mejora obtenida en el dominio 10 en lo referente a “Cifrados” porque no se contava con las técnicas de uso del cifrado, en la cual, en el análisis diferencial pasó del 0% al 50% en la auditoría de cumplimiento, también, en el dominio 13 con respecto a la “Seguridad en Telecomunicaciones” pasó de un 15% a un 71% y que decir del dominio 17 que trata los “Aspectos de Seguridad de la Información dentro de la Continuidad del Negocio”, que pasó de un 25% en el análisis diferencial a un 62% en la auditoría de cumplimiento. Esto, debido a la generación y búsqueda de amenazas comentadas a raíz del análisis de riesgos que evidenciaron la falta de acciones

en estas áreas. Si , vemos también, el dominio 8 “GESTION DE ACTIVOS”, el cual pasó del 30% al 59%, al identificar fallas en el procedimiento y la política de etiquetado y manipulado de la información, y en los inventarios de activos, los cuales fueron examinados y corregidos. Por lo tanto, se proporcionó teoría y ejemplos de la documentación mínima que debe dar soporte al SGSI para su correcto funcionamiento. Ahora, 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.

8. Glosario

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008].

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Análisis de impacto: Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización y permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. [UNE-ISO Guía 73:2010].

Ataque: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006] Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID: 1997].

Auditoría de seguridad : Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados [UNE 71504:2008].

Declaración de aplicabilidad: Documento formal en el que, para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Degradación: Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

Dimensión de seguridad: Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. (Minsiterio de hacienda y administraciones públicas).

Impacto residual: Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.

Incidente de seguridad: Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE 71504:2008] Evento con consecuencias en detrimento dela seguridad del sistema de información. [Magerit:2006].

Informe de insuficiencias: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir el riesgo sobre el sistema.

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008].

Plan de seguridad: Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

Probabilidad: Posibilidad de que un hecho se produzca. [UNE-ISO Guía 73:2010]

Riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (Minsiterio de hacienda y administraciones públicas).

Riesgo acumulado: Es el calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

Riesgo potencial: Los riesgos del sistema de información en la hipótesis de que no hubieran salvaguardas presentes. [UNE 71504:2008].

Riesgo residual: Riesgo remanente en el sistema después del tratamiento del riesgo. [UNE-ISO Guía 73:2010] Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006].

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo o Control y Medida que modifica un riesgo. [UNE-ISO Guía 73:2010].

Seguridad: La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o ma-lintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Seguridad de la información: Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE 71504:2008].

Sistema de información: Son los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados,procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008] Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997].

Tratamiento de riesgos: Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010] El proceso de selección e implantación de las medidas o salvaguardas para el tratamiento de los riesgos.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008]

Valor: De un activo. Es una estimación del coste inducido por la materialización de una amenaza. Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE].
Vulnerabilidad: Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.

9. Bibliografía

[1] Estevan de Quesada, Rafael. Auditoría técnica y de certificación. Barcelona: FUOC, 2009.
[2] https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
[3] http://www.17799.com/papers/iso17799scope.pdf , Documento genérico que describe la norma.
[4] http://www.iso27000.es/iso27000.html
[5] https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
[6]http://normaiso2700.blogspot.com.co/2015/12/norma-iso-27002-precedentes-y-evolucion.html
[7] http://iso27002jhan.blogspot.com.co/2015/06/iso-27002-historia.html
[8]http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0044393#.V_XRWPl97IU
[9]http://docplayer.es/9997936-Norma-tecnica-ntc-iso-iec-colombiana-27002.html
[10]http://www.iso27000.es/download/doc_iso27000_all.pdf
[11]http://seguridadinformacioncolombia.blogspot.com.co/2010/03/iso-27001-e-iso-27002-politica-de_02.html
[12]http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf
[13] https://www.isotools.org/2014/08/19/iso-27001-activos-informacion-empresa-3/
[14]
http://www.aenor.es/aenor/certificacion/seguridad/seguridad_27001.asp#.WCDqni197IU
[15] http://www.iso27000.es/download/doc_iso27000_all.pdf página 14/19
[16] http://www.dineroenimagen.com/2013-07-01/22403
[17] «ISO27000.es» - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. (s. f.). Recuperado 14 de septiembre de 2016, a partir de http://www.iso27000.es/iso27000.html
[18] Ministerio de Hacienda y administraciones públicas. (Octubre de 2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de riesgos de los sistemas de información: libro II Catálogo de elementos. Madrid, España
[19] Ministerio de Haciendas y administraciones públicas. (Octubre de 2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I. Método. Madrid, España.

10 Anexos