Tabla de Contenido

Historial de Versiones:

Versión	Autor	Fecha	Descripción de la Modificación
1.0	Mauricio Lora Barbosa	04/03/2014	Creación del documento
1.1	Mauricio Lora Barbosa	09/03/2014	Correcciones al documento
1.2	Mauricio Lora Barbosa	01/04/2014	Correcciones al documento
1.3	Mauricio Lora Barbosa	04/05/2014	Correcciones al documento
1.4	Mauricio Lora Barbosa	25/05/2014	Correcciones al documento

Este documento ha sido revisado por Tutor TFM:

Versión	Revisor	Fecha	
1.0	Antonio José Segovia Henares	07/03/2014	

AGRADECIMIENTOS

Quiero dedicar la realización de este trabajo a mi novia Alexandra y mi familia por su valiosa colaboración y apoyo incondicional en el cumplimiento de mis logros académicos y profesionales.

También quiero agradecer Dios por darme la sabiduría, inteligencia, paciencia y el tiempo para lograr con satisfacción el logro de esta nueva meta cumplida para fortalecer mi perfil profesional y humano.

1 FASE 1: CONTEXTUALIZACIÓN Y ANÁLISIS DIFERENCIAL

1.1 DESCRIPCIÓN DE LA EMPRESA MLB

MLB es una empresa aseguradora, fundada en el año 2009 en la ciudad de Bogotá - Colombia, que en el transcurrir de estos cinco años(2009 – 2014) ha venido ofreciendo sus servicios asegurando bienes materiales y bienes comunes a sus clientes, contando con un manejo asertivo de la información, gracias a el nivel técnico y tecnológico con el que actualmente cuenta. La calidad en la prestación de sus servicios ha logrado un crecimiento y posicionamiento significativo; a la fecha la empresa cuenta con diez sucursales en toda la ciudad y el uso de la tecnología ha sido una herramienta indispensable para lograr este crecimiento como también para lograr una mejor relación de servicio con los clientes.

Debido al crecimiento de la información que maneja la empresa en su nivel de gestión de seguridad de la información ve necesario fortalecer el proceso de recolección, actualización y manejo de la información, para garantizar la confidencialidad, integridad y disponibilidad de la información de cada uno de los usuarios y/o clientes con los que cuenta la empresa.

1.2 OBJETIVO

Implementar y administrar eficientemente el Sistema de Gestión de Seguridad de la Información, identificando las responsabilidades de los funcionarios, custodios y responsables de la información y establecer los objetivos de seguridad para una protección apropiada y consistente de los activos de información que soportan los procesos del centro de información técnica y de tecnología de la empresa MLB, de acuerdo con la política general y el manual de Gestión Segura de la Información, y que a su vez la cultura en Seguridad de la información se irradie hacia toda la organización.

1.3 GLOSARIO

Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como

bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas:

- Impresa
- Almacenada electrónicamente
- Transmitida por medios electrónicos
- Mostrada en videos
- Suministrada en una conversación
- Conocimiento de las personas

Alcance de la auditoría: Extensión y límites de una auditoría.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

Análisis de Riesgos: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Audiovisuales: Colección conformada por videos, disquetes, casetes, usb, microfichas, CD-ROM, discos duros y cintas.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

Auditado: Organización o Dependencia a la cual se le vá a realizar una auditoría.

Auditor: Persona con la competencia para llevar a cabo una auditoría.

Auditor en seguridad de la información: Persona con la competencia para efectuar auditorías internas de seguridad de la información

CITT: Centro de Información Técnica y Tecnológica.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Comercio Electrónico: Según fuente de Laudon.K, E commerce Negocios, tecnología y sociedad, Prentice Hall, consiste en la compra y venta de productos o

de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo con el advenimiento de la Internet y la World Wide Web a mediados de los años 90 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

Competencia: Habilidad demostrada para aplicar conocimientos y aptitudes.

Composición del Grupo: Indica quienes son los miembros de cada uno de los grupos formados en todo el proceso del SGSI para que le sean asignadas sus responsabilidades y/o roles.

Conclusiones de auditoría: Resultado de una auditoría, proporcionada por el equipo auditor después de la consideración de los objetivos de la auditoría y de todos los hallazgos de auditoría.

Confidencialidad: La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información con confidencialidad alta o media implica un grave impacto en MLB, en términos económicos, de su imagen y ante sus clientes.

Conformidad: cumplimiento de un requisito.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Criterios de auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como una referencia frente a la cual se compara la evidencia de la auditoría.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.

Equipo auditor: Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.

Estimación del riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad de la información.

Evidencia de auditoría: Registros, declaraciones de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoría puede ser cuantitativa o cualitativa.

Evitar el riesgo: Decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

Hallazgo de auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Integridad: La información de MLB debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

La Dirección: Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa.

No conformidad: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

No conformidad mayor: El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades.

No conformidad menor: El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento.

No conformidad potencial: Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia.

Observación: Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar.

Observador: Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo.

Plan de auditoría: Descripción de las actividades en el sitio y arreglos para una auditoría.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Proceso: conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

Programa de auditoría: Conjunto de una o más auditorías planificadas para un período de tiempo específico y dirigido hacia un propósito específico.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.

Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

Riesgo Inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

Riesgo Residual: Nivel restante de riesgo después de su tratamiento.

Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

Seguridad de la información: preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. *(Fuente: NTC-ISO/IEC 27001:2005).*

S.G.S.I: Sistema de Gestión de Seguridad de la Información.

Transferencia del riesgo: Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

Tratamiento de la Información: Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Vulnerabilidades: Debilidad de un activo de información frente a una amenaza.

1.4 NORMATIVIDAD ISO 27001 - 27002

1.4.1 ISO 27001

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. 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. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR (también en lengua gallega). En 2009, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2007/1M:2009). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Venezuela (Fondonorma ISO/IEC 27001), Argentina (IRAM-ISO IEC 27001), Chile (NCh-ISO27001), México (NMX-I-041/02-NYCE) o Uruguay (UNIT-ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013.[1]

1.4.2 ISO 27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en iso.org.[2]

[1] http://www.iso27000.es/iso27000.html
[2] http://www.iso27000.es/iso27000.html

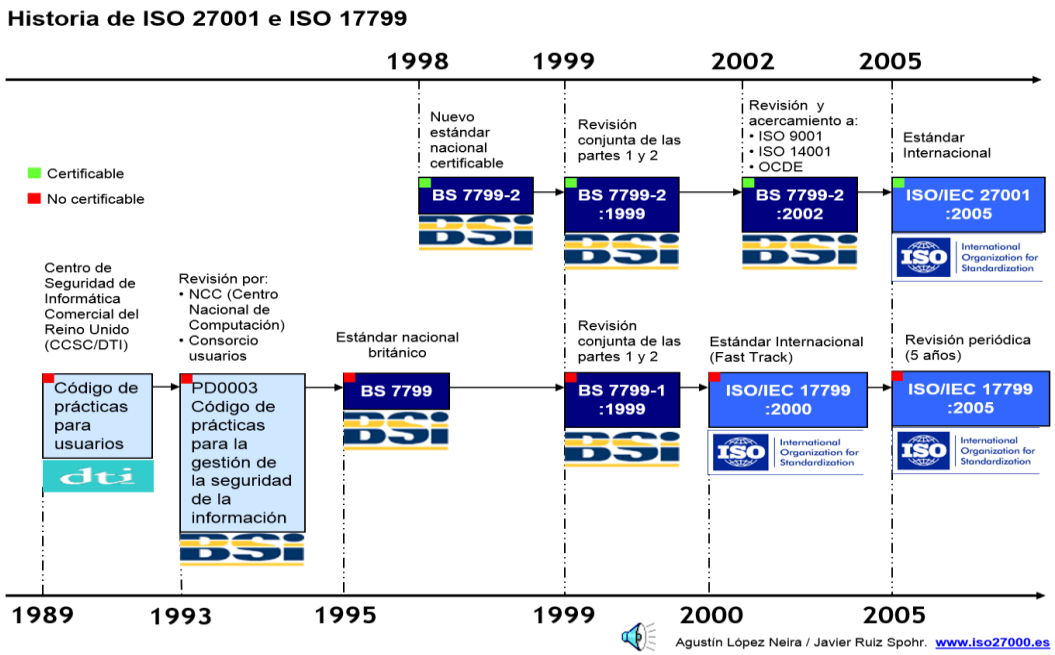

Figura 1. Evolucion de la ISO 27001

1.5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.5.1 GESTIÓN DE PROCESOS

El Mapa de Procesos que ha sido definido bajo el modelo de gestión planteado en el marco del proyecto MLBSGSI donde los requisitos para el Sistema de Gestión y Control Integral se expresan a través de elementos y subelementos, que indican debes lo que es obligatorio cumplir.

Sin embargo, no establecen la manera de hacerlo. Cada proceso, en sus diferentes niveles, dará cumplimiento a los requisitos (“debes”) según su objetivo y alcance dentro de la organización, en conjunto con las disposiciones legales que le sean aplicables. Cabe anotar que cuando alguno de los requisitos establecidos en este marco no apliquen por la naturaleza de la organización, de sus procesos o por decisión de la Alta Dirección, la justificación de la no aplicabilidad del o los requisito(s) se debe documentar y comunicar.

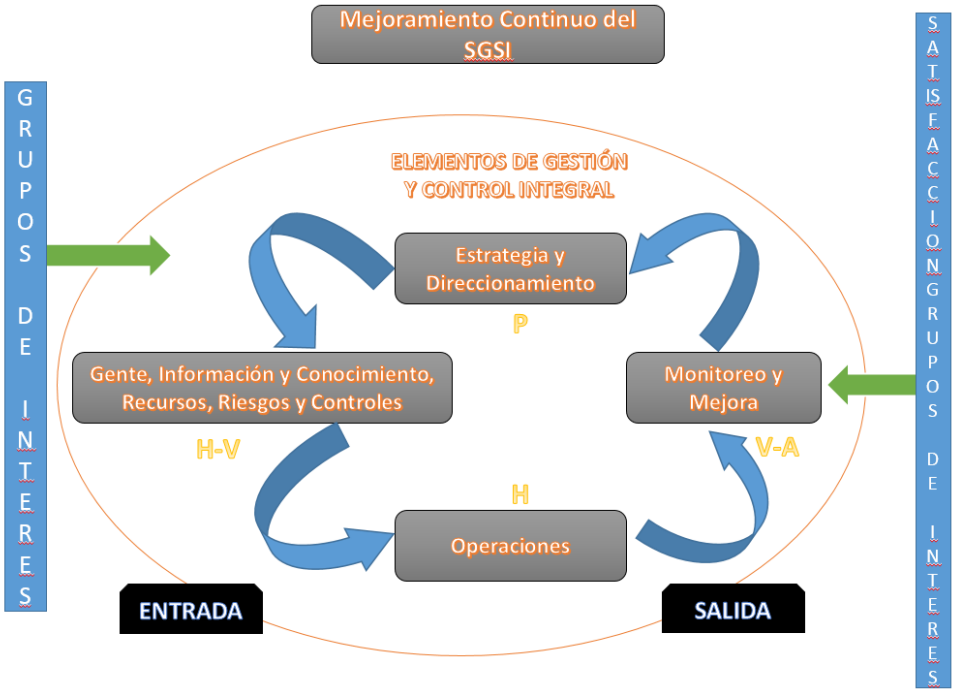

Figura 2. Visión esquemática del Marco de requisitos del SGSI

La orientación de este marco de requisitos promueve la adopción de un enfoque integral basado en procesos. Consiste en determinar, gestionar y controlar de manera eficaz una serie de actividades relacionadas entre sí. Una ventaja que proporciona este enfoque es el control continuo sobre los vínculos entre los procesos individuales que forman parte de un sistema conformado por procesos, así como sobre su combinación e interacción.

En ese sentido, se ha tomado la decisión de gestionar, bajo el marco del elemento de información y conocimiento, la aplicación de los requisitos establecidos en la Norma NTC-ISO/IEC 27001:2005 asociada a los Sistema de Gestión de Seguridad de la Información como parte del Sistema de Gestión integral de MLB, buscando la determinación de los activos críticos, sus riesgos y las medidas adecuadas para la mitigación de los mismos.

INFORMACIÓN Y CONOCIMIENTO

El elemento Información y Conocimiento, agrupan, integran y correlacionan las normativas locales y Estándares internacionales y los definidos por MLB, mediante las cuales se genera, estructura y mantiene la información. Se incorpora y asegura el conocimiento, transformándolos en activos estratégicos que estén a disposición

de una comunidad de usuarios, garantice su seguridad, para orientarlos a la toma de decisiones con el propósito de apalancar el cumplimiento del marco estratégico corporativo.

SEGURIDAD DE LA INFORMACIÓN

El subelemento Seguridad de la Información agrupa e integra las normativas locales y estándares internacionales y los definidos en MLB, con el fin de establecer las responsabilidades, principios, criterios, directrices y conductas para asegurar el adecuado tratamiento de la información dentro de los lineamientos de ética y buen gobierno de la organización.

1.5.1.1 ALCANCE

El alcance físico del Sistema de Gestión de la Seguridad de la Información se encuentra delimitado hacia el Centro de Información Técnica y Tecnológica, ubicado en las Instalaciones de la Empresa en la ciudad de Bogotá Colombia. Involucra los Servicios de información, técnicos y tecnológicos suministrados por el Centro de Información Técnica y Tecnológica (CITT) de la Empresa MLB como: Los sistemas de almacenamientos de la información, sistemas de comunicaciones, sistemas de seguridad perimetral, sistemas de intercambio de información con Terceros y Clientes.

1.5.2 PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión avala la adecuada implantación, gestión y operación de todo lo referente a la implementación de controles, métricas e indicadores, que permiten establecer un marco adecuado de gestión de la seguridad de la información en cualquier organización.

1.5.2.1 Procedimientos orientadores

- Revisión por la Dirección.
- Procedimiento de acción correctiva, acción preventiva y acción de mejora.
- Instructivo para auditorías internas del SGSI para el MLBSGSI.

1.5.3 OBJETIVOS DE CUMPLIMIENTO

Para el SGSI de la empresa MLB en alineación con el cumplimiento de la política integral, los lineamientos generales y directrices de seguridad de información, se plantea los siguientes tres (3) objetivos:

- Mantener durante todo el ciclo de operación del CITT, la confidencialidad definida por los usuarios, mediante la implementación de controles y mecanismos de manejo de la información acorde con el análisis de riesgos. (Procesos)
- Disminuir el impacto y la ocurrencia de los incidentes de seguridad a través de la gestión de riesgos frente al cumplimiento de la confidencialidad, integridad y disponibilidad. (Tecnología)
- Aumentar la toma de conciencia con relación a los hábitos y comportamientos seguros. (Personas)

1.5.4 LIDERAZGO Y COMPROMISO

Todas las actuaciones del Equipo de Dirección de la empresa MLB y del CITT, conformado por el Director, y Líder del SGSI, así como las de todos los colaboradores del Instituto y del CITT, están enmarcadas en las disposiciones del Código de Buen Gobierno y el Código de Ética de la empresa MLB.

Uno de los compromisos adquiridos por el equipo de dirección, es la implementación del sistema de gestión de seguridad de la información, con el fin de obtener los siguientes beneficios:

- Aspecto organizacional: Compromiso: el registro de las actividades permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización, en todos sus niveles y probar la diligencia razonable de sus administradores.
- Aspecto legal: Conformidad con requisitos legales: el registro permite demostrar que la organización observa todas las leyes y normativas aplicables al alcance.
- Aspecto funcional: Gestión de los riesgos: obtención de un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección. Garantiza también una mejor disponibilidad de los materiales y datos.
- Aspecto comercial: Credibilidad y confianza: los socios, los accionistas y los clientes se tranquilizan al constatar la importancia que la organización

concede a la protección de la información. Una certificación también puede brindar una diferenciación sobre la competencia y en el mercado.

- Aspecto financiero: Reducción de los costos vinculados a los incidentes.
- Aspecto humano: Fortalecer la sensibilización del personal hacia la seguridad y a sus responsabilidades en la organización.

1.5.5 ANÁLISIS DIFERENCIAL

El análisis se realiza teniendo como base el estado actual de la organización basándose en el análisis GAP de MLB, en donde se puede visualizar el nivel de cumplimiento actual en relación con la ISO 27001 y la ISO 27002.
Anexo: GAP 27001- mlb .xlsx, GAP 27002- mlb .xlsx

Figura 3. Estado actual de la ISO 27001

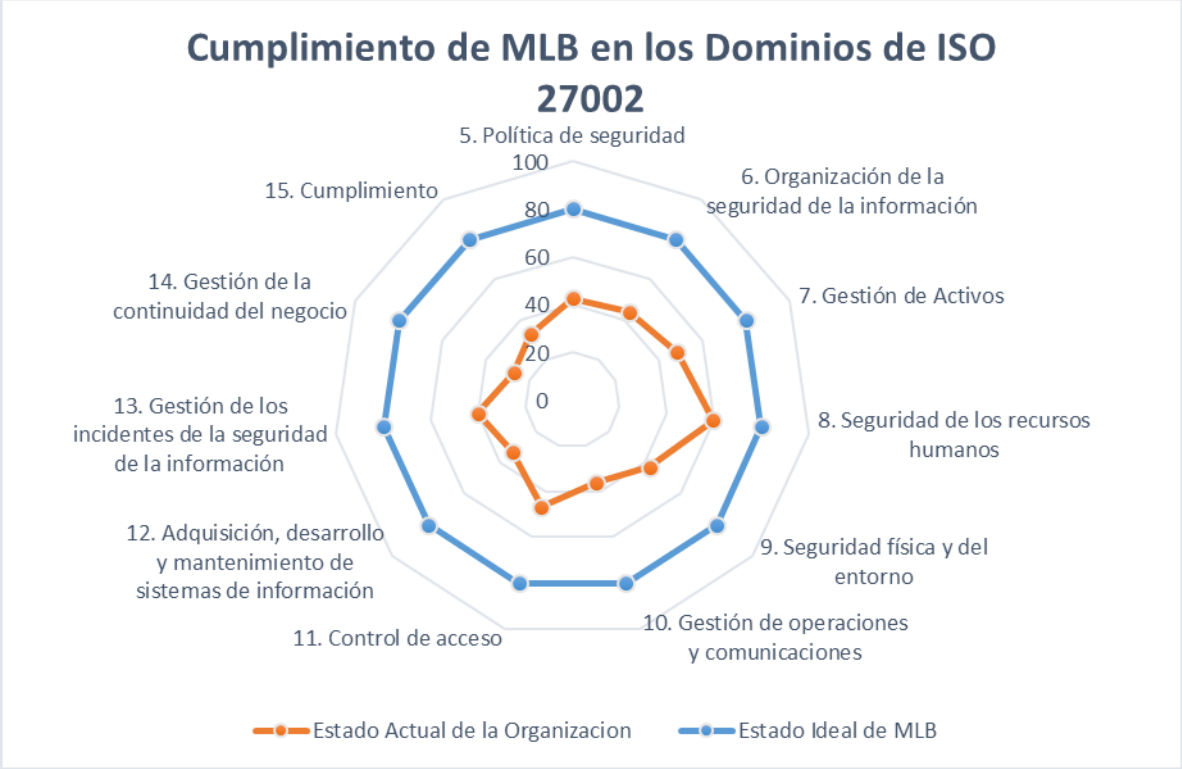

Figura 4. Estado actual de la ISO 27002

Se logra evidenciar el bajo cumplimiento de los diferentes dominios establecidos por la norma ISO 27002

1.5.6 ESTRUCTURA ORGANIZACIONAL DEL SGSI

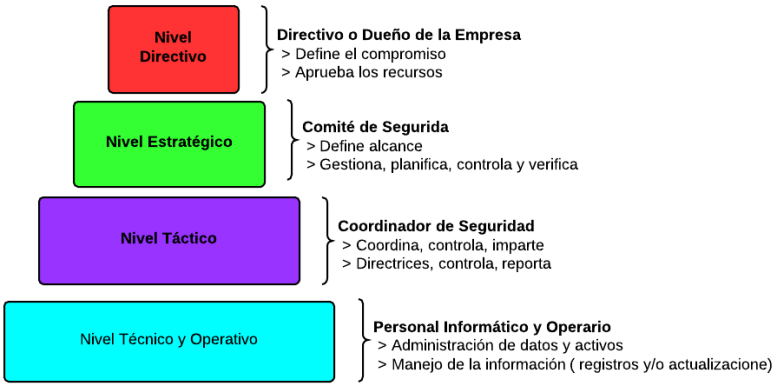

Figura 5. Estructura organizacional

1.5.6.1 ORGANIGRAMA FUNCIONAL

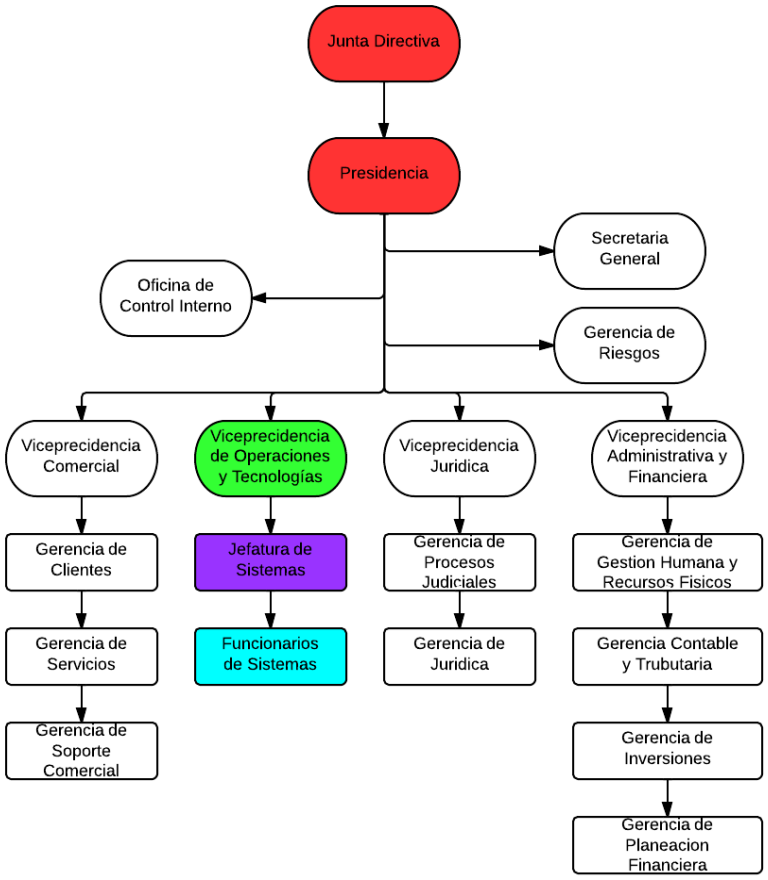

Figura 6. Organigrama funcional de MLB

1.5.7 DIAGRAMA DE RED ACTUAL

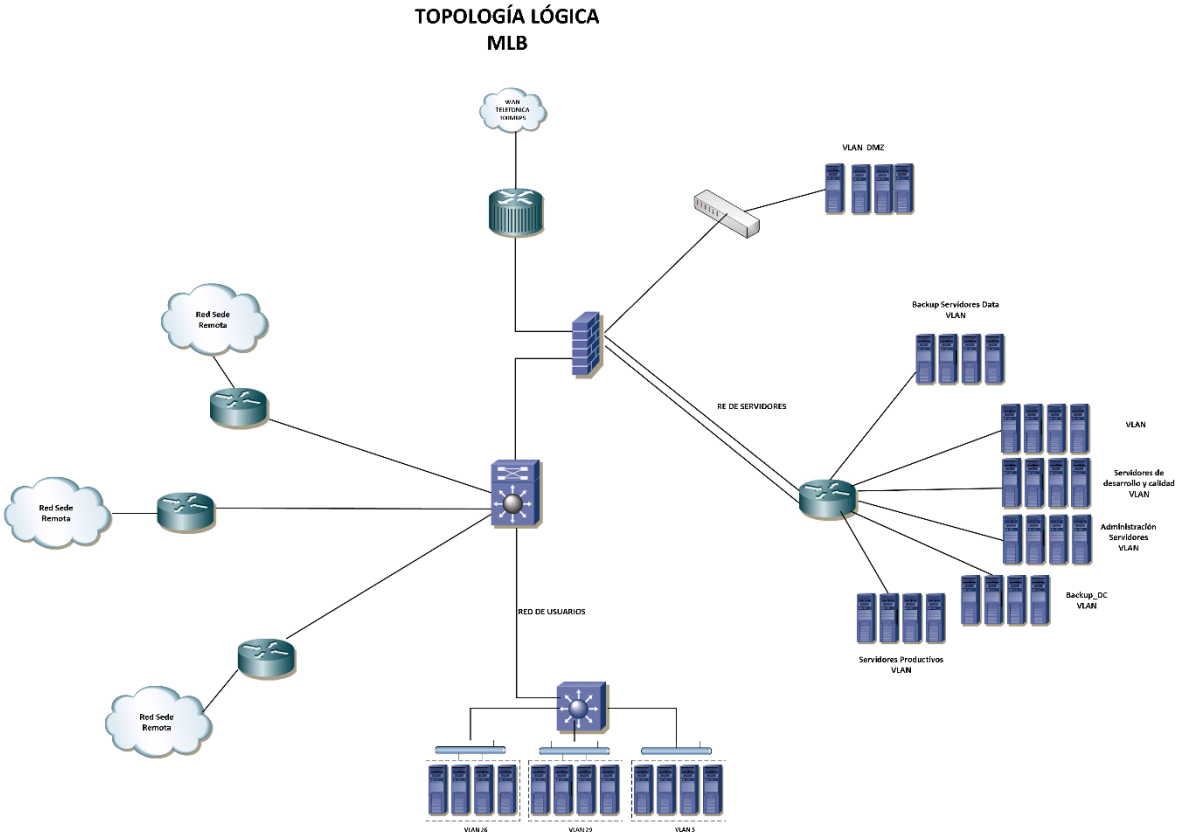

Figura 7. Diagrama de red actual

2 FASE 2: SISTEMA DE GESTIÓN DOCUMENTAL

2.1 POLÍTICAS

MLB integra la administración de Seguridad de los Activos de Información en las políticas generales contenidas en el directorio de políticas y por lo tanto estos documentos hacen parte de la normativa que regula la administración de la Seguridad de sus activos. Busca que con su divulgación que toda comunidad: Funcionarios, contratistas, terceros y directivos conozcan el marco normativo de forma individual y colectiva, brinden su apoyo para que la Empresa administre, utilice y disponga de información con niveles adecuados de seguridad.

Estos documentos permiten establecer las políticas sobre las cuales se debe direccionar el desarrollo de la seguridad de información para MLB y los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información en la Empresa.

2.2 PROCEDIMIENTOS DE AUDITORIAS

Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos y es conforme con los requisitos de la norma ISO 27001:2006 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información.

Describir las actividades requeridas para llevar a cabo una auditoría interna del Sistema de Gestión de Seguridad de la información - SGSI del Centro de Información Técnica y Tecnológica, con el fin de determinar si los objetivos de control definidos, los controles implementados, los procesos establecidos y procedimientos definidos, cumplen los requerimientos de la norma NTC-ISO/IEC 27001 y acatan las políticas, lineamientos y directrices, emitidos por la organización.

2.3 GESTIÓN DE INDICADORES

Los indicadores reflejarán cuáles fueron las consecuencias de acciones tomadas en el pasado en el marco de una organización. El objetivo principal es que los indicadores sienten las bases para acciones a tomar en el presente y en el futuro.

Es importante que los indicadores reflejen los datos veraces y fiables, ya que el análisis de la situación, de otra manera, no será correcto. Por otra parte, si los indicadores son ambiguos, la interpretación será complicada.

Se implementarán indicadores de gestión para mantener monitorizado y actualizado del SGSI, los cuales permitirán controlar el funcionamiento de las medidas de seguridad implementadas, eficacia y eficiencia.

2.4 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

Asegurar una adecuada planeación y corrección de las desviaciones en el cumplimiento de los objetivos, estableciendo los requisitos mínimos, los responsables y los mecanismos para gestionar la Revisión por parte de la Dirección de los procesos y el macro de procesos del Sistema de Gestión de Seguridad de la Información de MLB.

El Sistema de Gestión de Seguridad de la Información de MLB contempla una evaluación periódica, sistemática y estructurada del SGSI de MLB a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de las desviaciones en el cumplimiento de los objetivos y como tal, incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la organización, promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.

Este procedimiento hace parte del Sistema de Gestión de Seguridad de la Información de MLB; es aplicable a todos los funcionarios responsables por el seguimiento y evaluación del SGSI, de la organización y a los Representantes de la Dirección.

2.5 GESTIÓN DE ROLES Y RESPONSABILIDADES

El Sistema de Gestión de Seguridad de la Información de MLB define los diferentes roles y funciones de los diferentes participantes del SGSI en MLB, estos roles están alineados y cumplen con la funciones necesarias para poder llevar a satisfacción el desarrollo y ejecución del SGSI basado en la norma ISO 27001:2005.
Entre estas definiciones de roles y responsabilidades se podrán identificar alguno de los siguientes items:

- Quien es el responsable de la ejecución de cada hito
- Quien toma las decisiones, solo o conjuntamente con otros
- Quien gestiona los recursos y controla el progreso del trabajo
- Quien debe ser informado
- Quien debe ser consultado
- Quien debe participar
- Quien debe dar apoyo o dotar de infraestructura al equipo
- Quien asegura la calidad de los resultados

2.6 METODOLOGÍA DE ANÁLISIS DE RIESGO

El análisis del riesgo es una de las actividades más relevantes en la implementación, mantenimiento y mejoramiento de un Sistema de Gestión de Seguridad de la Información (SGSI) debido a que es la herramienta que permite identificar las amenazas a las cuales se encuentran expuestas los activos críticos, estimar la frecuencia de la materialización de estas amenazas y valorar los impactos que tendrían para la Organización esa materialización. Por su parte el tratamiento del riesgo permite analizar, evaluar y definir el manejo que se le debe dar a los riesgos identificados y tomar las acciones de control y mejora necesarias para disminuir los impactos de la organización a un nivel aceptable.

De esta manera, el análisis y tratamiento de los riesgos permite asegurar la continuidad de la operación del negocio previniendo y minimizando el impacto de los incidentes de seguridad de una Organización.

MLB actualmente se encuentra en la fase de mantenimiento y mejoramiento del SGSI, razón por la cual se realizará la actualización y reevaluación de los riesgos de la Organización teniendo en cuenta los requerimientos establecidos en los estándares ISO 27001 e ISO 27005. La metodología empleada para la valoración de riesgo en la presente Consultoría de Seguridad, está alineada con el ejercicio anterior de riesgos desarrollada por MLB, con el fin de que los análisis sean comparables y repetibles, de tal manera que los niveles de impacto, probabilidad y matriz de evaluación de riesgo fueron tomados de la misma manera.

3 FASE 3: ANÁLISIS DE RIESGOS

3.1 METODOLOGÍA DE VALORACIÓN DE RIESGOS

Establecer los criterios, condiciones y actividades a desarrollar para la clasificación, manejo y gestión de los activos de información de MLB.

La realización del inventario y clasificación de los activos de información hace parte de la debida diligencia que a nivel estratégico ha definido MLB con respecto a la seguridad de los activos de información, y tiene como fin dar cumplimiento a tres puntos principales de la norma técnica colombiana NTC ISO/IEC 27001 en el ítem “Gestión de Activos”:

- **Inventario de Activos:** Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de los mismos dentro de la organización.

- **Directrices de Clasificación:** La información debe clasificarse en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
- **Propiedad de los Activos:** Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la organización.

Todos los activos de información que se encuentren dentro del inventario son considerados propiedad de MLB, sin embargo se asignará un responsable para cada activo, los cuales serán los Vicepresidentes, Gerentes, Jefes de Oficina o Subgerentes de área.

4 FASE 4: PROPUESTA DEL PROYECTO

La propuesta da respuesta a la solicitud formulada por MLB en el sentido de realizar una consultoría en seguridad de la información, buscando implementar las principales etapas dentro de un Sistema de Gestión de Seguridad de la Información SGSI, frente a los estándares internacionales ISO 27001:2005 y orientada a sentar las bases fundamentales para una posterior certificación ISO/IEC 27001.

El proyecto comprende el levantamiento de Información y valoración de riesgos de la actual plataforma tecnológica de MLB.

Definición del Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo a las normas internacionales ISO27001 e ISO/IEC 17799:2005 según los controles requeridos para mitigar los riesgos encontrados.
Definición del Plan de Concientización para los colaboradores de MLB.

5 FASE 5: AUDITORIA

Verificar que el SGSI haya sido establecido e implementado de acuerdo a los requisitos de ISO/IEC 27001
Los requisitos de MLB y los legales y reglamentarios.
Confirmar que en MLB que haya sido implementado eficazmente el sistema de gestión de acuerdo a lo planeado y confirmar que el SGSI es capaz de alcanzar los objetivos de la política de la organización.

CONCLUSIONES

- En la elaboración y desarrollo del proyecto se evidencia que se ha logrado con satisfacción lo propuesto:
- Implementar y administrar eficientemente el Sistema de Gestión de Seguridad de la Información en MLB.
- Asignar responsabilidades de acuerdo a los roles asignados por la empresa.
- Establecer los objetivos de seguridad para una protección apropiada y consistente soportándolos procesos del centro de información técnica y de tecnología de la empresa MLB.
- Apropiación y seguimiento e integración de las políticas general y el manual de Gestión Segura de la Información.
- Conocimiento y divulgación de la cultura en Seguridad de la información hacia toda la empresa.
- Disminuir el impacto y la ocurrencia de los incidentes de seguridad a través de la gestión de riesgos frente al cumplimiento de la confidencialidad, integridad y disponibilidad. (Tecnología)
- Generación de las buenas prácticas en los controles en cuanto a seguridad de la información.
- Delimitación en los sistemas de almacenamiento de la información.

ANEXOS

SGSI-REG GAP 27001- mlb v1.xlsx
SGSI-REG GAP 27002- mlb v1.xlsx
SGSI-POL Política de Adquisicion, Desarrollo y Mantenimiento de Sistemas v1.doc
SGSI-POL Política de Control de Acceso v1.doc
SGSI-POL Política de Cumplimiento v1.doc
SGSI-POL Política de Gestion de Activos v1.doc
SGSI-POL Política de Gestion de Continuidad v1.doc

SGSI-POL Política de Gestion de Incidentes v1.doc
SGSI-POL Política de Gestion de Operaciones y Comunicaciones v1.doc
SGSI-POL Política de Organizacion de la Seguridad de la Informacion v1.doc
SGSI-POL Política de Seguridad Fisica v1.doc
SGSI-POL Política de Seguridad Recursos Humanos v1.doc
SGSI-POL Políticas Generales de Seguridad de la Informacion v1.doc
SGSI-GUIA Gestión de Roles y Responsabilidades v1_2.doc
SGSI-MET Indicadores v1_1.doc
SGSI-MET Metodología de Análisis de Riesgos v1_2.doc
SGSI-PROC Procedimiento Revision por la Direccion v1_1.doc
SGSI-PROC Procedimientos de Auditorías Internas v1_2.doc
SGSI-REG Plantilla Indicadores mlb v1.xlsx
SGSI-REG SOA mlb v1.xlsx
SGSI-PROC Procedimiento de gestion de activos v1_1.doc
SGSI-REG Activos mlb.xlsx
SGSI-REG Matriz de Riesgos.xlsx
SGSI-PROP Propuesta mlb.doc
SGSI-REG Cronograma Proyecto.mpp
SGSI-AI Auditoria.doc
SGSI-REG CMM 27002- mlb v1.xlsx

REFERENCIAS

Introducción al Sistema de Gestión de Seguridad de la Información - SGSI
http://www.iso27000.es/sgsi.html

Historia de la ISO 27000
http://www.iso27000.es/iso27000.html

Presentación de documentos y elaboración de presentaciones
http://materials.cv.uoc.edu/cdocent/NR64BN4TZTOGMDE0V2D7.pdf?ajax=true

Redacción de textos científicos
http://materials.cv.uoc.edu/cdocent/_D_CBBU62JZTHQ9CQQGJ.pdf?ajax=true

Sistema de Gestión de Seguridad de la Información
http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO 27001 Normas y estándares
http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/

Guía de implementación del SGSI

http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/61_leccin_26_auditoras_internas_del_sgsi.htmlg

Organización interna del SGSI
https://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html

Implementación de un SGSI organizacional
http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf