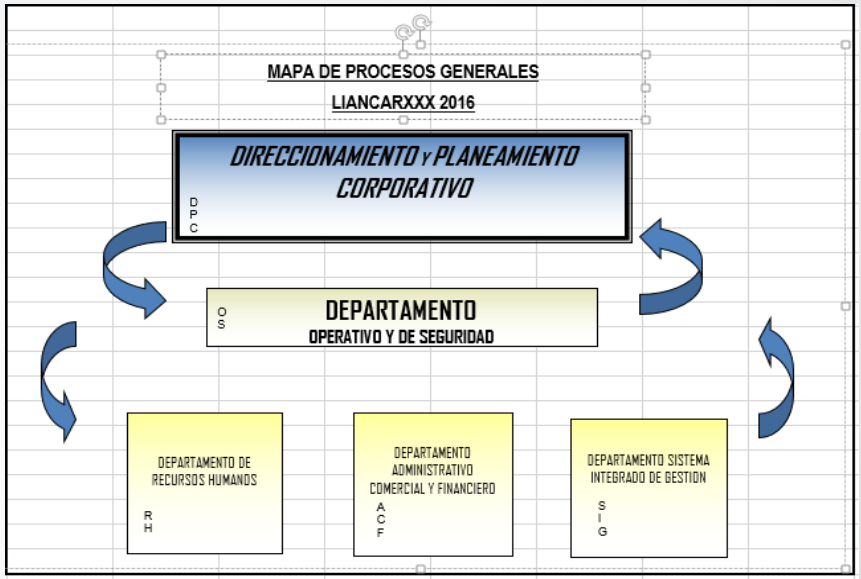
Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Objetivos del Plan Director

Identificar los lineamientos generales que debe seguir la empresa LIANCAR LTDA para mantener un esquema de mejora continua en materia de seguridad de la Información, permitiendo a la empresa conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales en los sistemas y tecnologías de información que soportan los diferentes subprocesos y/o servicios del área de TI de acuerdo al Mapa de procesos.



Mapa de procesos generales

Objetivos específicos

- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura que ofrece el área de TI.
- Definir directrices en temas de seguridad de la información para el área de TI.
- Definir y planificar los planes de acción a realizar (a corto, mediano y largo plazo) teniendo como referencia la diferencia existente entre el nivel de seguridad actual y el nivel de seguridad objetivo.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.

Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Visión Global de los Objetivos de la Seguridad de la Información

rmación de LIANCAR, en las dimensiones de la seguridad de la información de acuerdo a la confidencialidad, onibilidad, 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.

Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Beneficios del Plan Director

- **Gestionar los incidentes de seguridad** que permitan al comité de seguridad tener un soporte sólido para sustentar ante la alta gerencia un plan de inversión en seguridad de la información, donde con evidencias y cálculos claros de los impactos económicos que se pueden presentar ante la materialización de un incidente, es posible presentar **de forma clara las posibles soluciones** para la mitigación correctiva o preventiva de estos eventos no deseados, y de esta forma poder garantizar que la inversión cubra las **brechas de seguridad más importantes** y una medición de la eficacia de sus controles.
- Evitar fugas , destrucción de la información y eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información.
- En caso de **fraudes internos o externos** nos permite entregar al área legal una prueba válida ante un posible proceso administrativo interno o judicial, para lo cual es **conveniente que esta recopilación de evidencias** se realicen cumpliendo las normas legales para este procedimiento.
- Nos permite controlar los ataques de denegación de servicios por software dañino, identificar los dispositivos más vulnerables por la cuales se puedan materializar las amenazas.
- Ayuda a cumplir con los objetivos de **mejorar de manera continua los procesos**, gestionando y midiendo los controles de seguridad, lo que les permite poder determinar cuándo una variación puede **afectar la producción o los servicios** que brindan.
- Obtener una mejor organización en los procesos por medio de la aplicación de las políticas de seguridad de la información.
- Disminución del Impacto de los riesgos y **mayores garantías de continuidad** del negocio basada en la adopción de un plan de contingencias.
- La Mejora de la Imagen de la empresa y aumento de su valor comercial, una mayor confianza por parte de sus clientes, proveedores, accionistas y socios
- Una Mejora del retorno de las inversiones y Un análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial
- Reducción de los costos vinculados a los incidentes.

Voluntad de cumplir con la legislación vigente de protección de datos de carácter personal, servicios de la sociedad e la información, comercio electrónico, propiedad intelectual y en general, aquella relacionada con la seguridad de la información.

Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Ventajas para la Empresa

- El Sistema de Seguridad de la Información se convierte en un **arma competitiva** para el negocio de la empresa porque le permite obtener su **certificación** fortaleciendo la credibilidad con sus clientes
- Se tiene un contenido estructurado de la información en la empresa permitiendo su gestión de mejor manera contando con una serie de buenas prácticas y siguiendo una metodología en la que se haga inventarios de activos, un análisis de los riesgos y gestión de los mismos para saber como afrontarlos.
- Se conoce su nivel de cumplimiento con respecto a los dominios, objetivos y controles de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.
- Al aplicar las normas de Seguridad de la Información, los responsables de TI deben preservar las dimensiones de seguridad ya que es la base por la que se rige la seguridad de la información.
- Los directivos de la empresa LIANCAR comienzan a ser más gestores en atender una serie de pautas que permitan una gestión eficaz de la seguridad de la información y así, proteger y preservar la información por ser su activo más valioso.

Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Esquema del Plan Director

A continuación se da una breve descripción de cómo se definirá el Plan Director de Seguridad de la Información para la Empresa.

Situación Actual

- Contextualización
- Objetivos
- Análisis Diferencial

Sistema de Gestión Documental

- Esquema Documental

Análisis de Riesgos

- Inventario de Activos
- Valoración de Activos
- Dimensión de Seguridad
- Tabla Resumen de Valoración
- Análisis de Amenazas
- Impacto Potencial
- Nivel de Riesgo Aceptable y Riesgo Residual
- Resultados

Propuesta Proyectos

- Propuestas
- Resultados

Auditoría de Cumplimiento

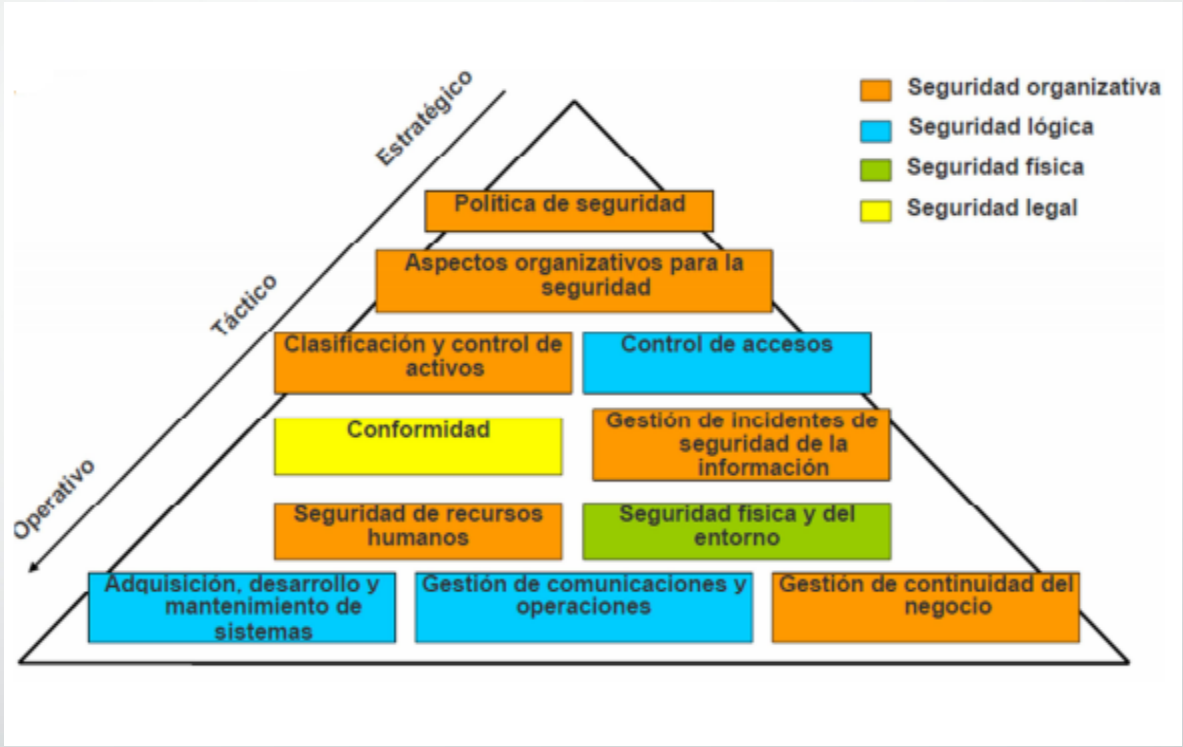
- Metodología
- Evaluación de la Madurez
- Presentación de Resultados

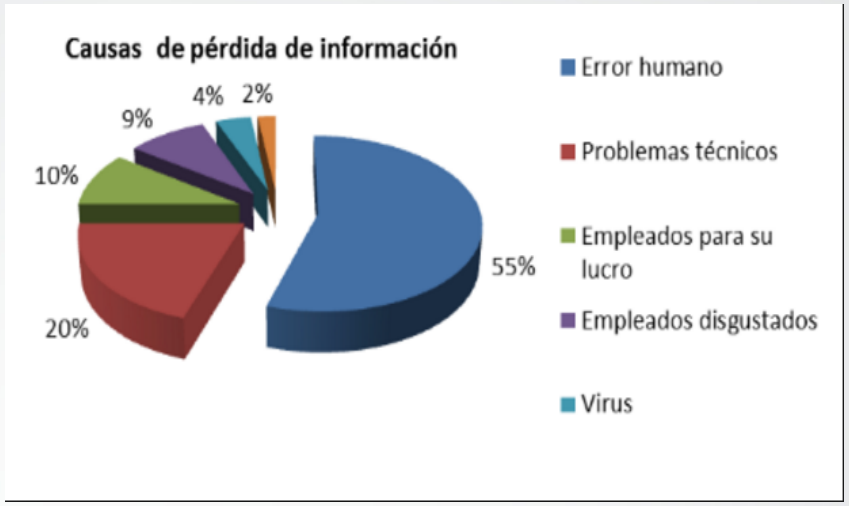
Resultados

Plan Director de Seguridad de la Información para la Empresa LIANCAR LTDA

Marco de Seguridad de la Información

- El marco de seguridad es el conjunto de políticas, normas y procedimientos internos que deben existir para definir y estandarizar los principios, criterios y controles de seguridad necesarios en la empresa, basándose en el riesgo que la dirección está dispuesta a asumir o en otros requisitos como la legislación vigente.





Alcance: Este trabajo tiene como finalidad la definición de un Plan Director de Seguridad para la empresa LIANCAR LTDA, el cual permitirá definir las bases de mejora continua a nivel de seguridad de la información permitiendo conocer el estado actual y definir las acciones necesarias para mitigar los riesgos que se presentan en los activos de información de la organización. Este proyecto se dividirá en las siguientes cinco fases que permitirán identificar:

- El alcance del trabajo y caracterización de la empresa la cual, tiene como objetivo, caracterizar la organización y definir el o los procesos sobre los cuales se desarrollara el presente proyecto.
- La Identificación de los Activos de Información: Una vez identificados el o los procesos a evaluar, se procederá a identificar cuáles son los activos de información que los soportan.
- El Análisis de Riesgos: El análisis de riesgos permitirá identificar la situación actual de la organización y definir los controles para mantener un nivel de riesgo aceptable en la organización
- EL Plan Director de Seguridad define la estrategia de toda la organización a corto, mediano y largo plazo.
- Y en la Presentación de informes, una vez realizado un diagnóstico del estado actual de seguridad y de definir el Plan Director de Seguridad, se procede a presentar los resultados a la alta dirección y a los diferentes sponsors para garantizar así el apoyo en todo los niveles de la organización.

1. Fase: Situación Actual de la Empresa de acuerdo a la Norma 27002:2013

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				

En esta Figura, se denota el nivel de cumplimiento de los 114 controles del Anexo-A, donde se especifica la evaluación de los mismo, el status por código, su significado en porcentaje 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).

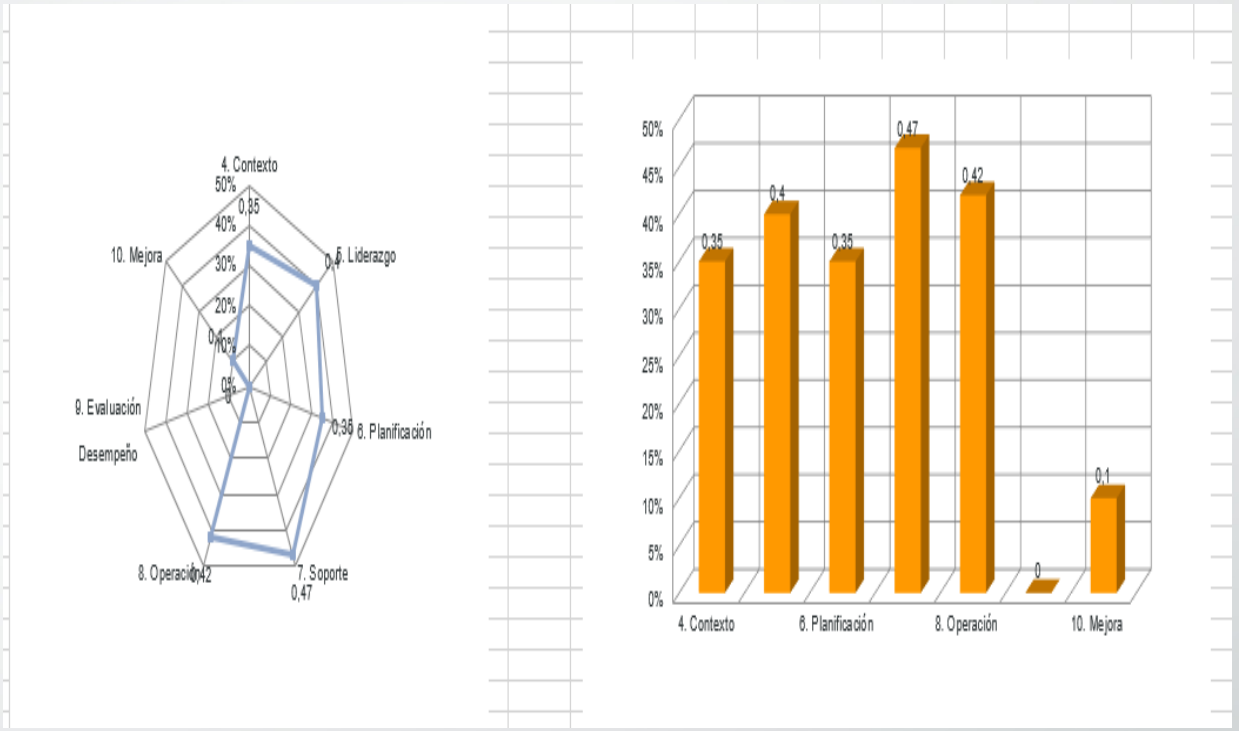
DOMINIO	% DE CUMPLIMIENTO	
A.5-Políticas de seguridad de la información	25,00%	
A.6-Aspectos Organizativos de la Seguridad de la Información	22,00%	
A.7-Seguridad ligada a los recursos humanos	20,00%	
A.8-Gestión de activos	36,50%	
A.9-Control de accesos	28,00%	
A.10-Cifrados	0,00%	
A.11-Seguridad física 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

Seguidamente, en esta Figura determinamos por porcentajes y muestra de los dominios que son pertenecientes a la ISO/IEC 27002:2013 por medio de una tabla y una gráfica radial.

1. Fase: Situación Actual de la Empresa de acuerdo a la Norma 27001:2013

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 normasno 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				

Descripción de los Criterios y valores por requisitos y cláusulas de la ISO/IEC 27001:2013



Cumplimiento de LIANCAR en los Dominios de la ISO/IEC 27001:2013

Ahora, en esta figura realizamos el análisis diferencial utilizando la norma ISO/IEC 27001:2013 donde presenta una descripción de los criterios por su clasificación del estado actual de LIANCAR, tomando como base la valoración de los diferentes dominios establecidos en esta norma, de acuerdo con los datos entregados por la empresa.

El cumplimiento en los dominios de esta norma la visualizamos en esta figura 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.

2. Fase Sistema de Gestión Documental

- **2.1 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.

- Objetivo: Gestionar de manera objetiva la información de LIANCAR con el propósito de definir pautas para asegurar, proteger y preservar la información ofreciendo apoyo y orientación a la dirección con respecto a la seguridad de la información, afirmando el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información de acuerdo con los requisitos del negocio, los reglamentos y las leyes pertinentes.

- Alcance: Esta política de seguridad de la Información se establece para dar cumplimiento a las disposiciones legales vigentes y es de aplicación a todas las dependencias de LIANCAR, a todos sus procesos internos, externos y recursos vinculados a la empresa ya sea por acuerdos con terceros o contratos con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la misma

2. Fase Sistema de Gestión Documental

- **2.2 Procedimiento de Auditorías Internas**: 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.

- **Objetivo:** Verificar el nivel de implantación y eficacia del SGSI en la empresa LIANCAR LTDA conforme a los requerimientos establecidos por la norma ISO/IEC 27001:2013.

- **Alcance:** La auditoría tiene como propósito revisar cada uno de los procesos relacionados al alcance de la norma ISO/IEC 27001:2013 utilizados en la empresa LIANCAR. Los usuarios de este documento son el director o gerente de alta dirección, los subgerentes, y el líder del centro de Tecnología de la empresa y en general, el comité de seguridad de la información de la empresa.
- Esta auditoría comprende la revisión y la evaluación independiente y objetiva, abarcando algunas de las áreas del sistema de información, sus estándares y procedimientos en vigor, para determinar si el sistema salvaguarda los activos, mantiene la integridad de la información y el cumplimiento de los objetivos fijados por la empresa.

2. Fase Sistema de Gestión Documental

- **2.3 Gestión de Indicadores**: La creación de estos indicadores de gestión se orientan principalmente en la medición de la efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de la seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de la mejora continua permitiendo adoptar decisiones oportunas para el avance de la madurez en los tópicos de la seguridad de la información de la empresa LIANCAR.

- **Objetivos:**
- Evaluar la efectividad de la implementación de los controles de seguridad
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la empresa LIANCAR.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.

Servir como insumos al plan de análisis y tratamiento de riesgos

INDICADOR 04 – PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR	IN0-4				
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada po parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**		
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema de la seguridad de información		(VSI07/VSI08)*100	Comité de Seguridad de la Información o en su defecto el Oficial de Seguridad de Información, auditorías internas, atención al usuario, listas de asistencia		
VSI08: Total de personal a capacitar.			Total de funcionarios de la entidad.		
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80-90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

2. Fase Sistema de Gestión Documental

- **2.4 Procedimiento Revisión por Dirección:** La revisión por la Alta Gerencia General al Sistema de Seguridad de la información se realizará una vez al año, en sesión ordinaria del Comité de la Seguridad Informática y Subgerentes de LIANCAR en reunión extraordinaria convocada por el Representante de la Dirección

- **Objetivo:** Establecer los lineamientos para que la Alta Dirección O Gerencia General de LIANCAR, revise el Sistema de la Seguridad de la Información y así asegurar continuamente su conveniencia, adecuación, eficacia, eficiencia y efectividad.

- **Alcance:** Incluye la consolidación de la información requerida para la revisión por la Alta Gerencia General al Sistema de Seguridad de la información, la evaluación de oportunidades de mejora del SGSI y la necesidad de efectuar cambios en el mismo.

5. Descripción de actividades

Nro.	ACTIVIDAD	RESPONSABLE	REGISTRO/DOCUMENTO
1.	**PROGRAMAR Y PLANEAR LA REVISIÓN POR LA DIRECCIÓN AL COMITÈ DE SEGURIDAD DE LA INFORMACIÒN** Una vez al año o cuando se presenten situaciones que puedan afectar el desempeño del Sistema de Seguridad de la información, se programa la revisión gerencial al Sistema de Seguridad de la información Se define la fecha de la revisión. Se realiza la citación al Comité de Seguridad Informática.	Representante de la Alta Dirección Gerente General de LIANCARXXX	Correo electrónico o memorando de citación

2. Fase Sistema de Gestión Documental

- **2.5 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

Perfiles Propuestos

- 1. Personal de seguridad de la información.
- 2. Un representante del área de Tecnología.
- 3. Un representante del área de Control Interno.
- 4. Un representante del área de Planeación.
- 5. Un representante de sistemas de Gestión de Calidad.
- 6. Un representante del área Jurídica.
- 7. Funcionarios, proveedores, y ciudadanos

- **Responsables:** El Comité de Seguridad Informática, compuesto por los representantes de los distintos departamentos de la empresa, así como por el Gerente General de LIANCAR.
- Los funcionarios de la empresa, contratistas o colaboradores de la empresa
- 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.
- El Responsable de Seguridad (RSI) debe coordinar y controlar las medidas de seguridad de la información en cualquiera de sus formas.
- El responsable del Área de Tecnología, que junto con el RSI define las políticas, normas, procedimientos y se encarga de hacerlas cumplir.
- 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

2. Fase Sistema de Gestión Documental

- **2.6 Metodología de Análisis de Riesgos**: Esta metodología se basará en el marco normativo de ISO 27001:2013 para la seguridad de la información y en los dominios existentes en el anexo A de la norma ISO 27002:2013.
- Para el análisis se utilizará la metodología MAGERIT, desarrollada por el Consejo Superior de Administración electrónica de España. Se utilizará tanto el libro I: método, como el libro II: catálogo.

- **Objetivo:** Utilizar metodología MAGERIT para la gestión de riesgos que permita desarrollar de manera clara y sistemática el análisis y gestión de riesgos de los activos de información de la empresa LIANCAR:

- **Alcance:** El poder realizar un análisis de los riesgos en forma sistemática permite ejecutar diferentes actividades de gestión, como por ejemplo tomar diseñar planes e implementar controles que lleven a la mitigación de los riesgos asociados

2. Fase Sistema de Gestión Documental

- **2.7 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.

- **Objetivo:** Verificar cuales dominios, objetivos de control aplican o no en el estudio de la mitigación de riesgos permitiendo establecer la acción a realizar para su respectivo cumplimiento.

  - **Alcance:** La Declaración de Aplicabilidad se desarrolla luego del tratamiento de riesgos, que a su vez es la actividad posterior a una evaluación de riesgos. El tratamiento tiene como objetivo la definición de las acciones a realizar para **mitigar** aquellos riesgos que han sido identificados y analizados. Existen varias opciones de tratamiento agrupan en categorías como:
  - **Mitigar**. Consiste en implementar algún control que reduzca el riesgo.
  - **Transferir**. Ocurre cuando se delega la acción de mitigación a un tercero.
  - **Aceptar**. Se presenta cuando el impacto generado por un riesgo es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo.

Declaración de Aplicabilidad ISO 27001:2013 para la Empresa LIANCARXXX						
Dominio	Subdominio	Control Actual	Objetivos de Control	Aplica	Acción	Justificación
A.5. POLITICAS DE LA SEGURIDAD DE LA INFORMACION	A.5.1. ORIENTACION DE LA DIRECCION PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION	A.5.1.1	Políticas para la seguridad de la Información	SI	Establecer una política de seguridad de la información	En la empresa LIANCARXXX se han identificado problemas manifestando riesgos en la información, en tal sentido es necesario informar y concientizar a todos los colaboradores y partes interesadas sobre los riesgos a los que están expuestos, así como los controles implementados para evitar la materialización de estos riesgos.
		A.5.1.2	Revisión de las Políticas para la seguridad de la Información	SI	Revisión por la alta gerencia de la empresa LIANCARXX	La política de seguridad de la información de la compañía deberá ser frecuentemente revisada para asegurar su idoneidad con respecto a los riesgos de información. Está política debe ser comunicada a todas las partes interesadas.

Fase 3 Análisis de Riesgos

- Objetivo: Determinar qué factores están afectando de forma directa o indirecta a la empresa LIANCAR, para lograr tener una calidad en la seguridad tanto física como seguridad lógica y lograr cumplir con los objetivos y dimensiones de seguridad entre ellos con la confidencialidad, integridad y disponibilidad.
- Una de las primeras acciones que debe tener LIANCAR es el proceso de análisis de riesgos para mejorar la seguridad de la información, en la cual se deben identificar y determinar la magnitud e identificar las áreas que requieren medidas de protección. De esta manera, iniciamos este proceso de análisis de riesgos a través del inventario de activos, valoración de Activos, amenazas, las vulnerabilidades, determinación del impacto potencial y riesgo residual.

- **Pasos que se deben seguir para el Análisis de Riesgos**

1. **Inventario de Activos**: El primer punto para el análisis es analizar los activos vinculados a la información. 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.

La clasificación de los activos se dará teniendo en cuenta el alcance del proyecto y que serán responsabilidad del área de tecnología en la empresa y sean de software, hardware o personal y que se encuentran relacionados con el proceso misional.

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		

Fase 3 Análisis de Riesgos

- **2. Valoración de los Activos:** El objetivo final es tomar grupo de medidas que garanticen nuestros activos. El sentido común indica que el coste de las medidas no deberá ser superior al coste del activo protegido. Empezaremos por tanto a determinar el valor de los diferentes activos.
- Nos basamos en el análisis que propone MAGERIT en su Libro III (punto 2.1), completándolo con una estimación cuantitativa. En el caso de que el activo presente un valor entre $40.000.000.00 y $50.000.000.00 tendrá una valoración de Alto (A) como se muestra en la tabla "Valoración de los activos de la empresa".
- **3. Dimensiones de Seguridad:** Se tiene en cuenta, la disponibilidad, integridad, confiabilidad, autenticidad y trazabilidad. se ha de tener presente la escala en la que se realizarán las valoraciones. En este caso utilizaremos una escala de valoración de cero a diez valores siguiendo los siguientes criterios visualizados en la tabla "Valoración Dimensiones de Seguridad"

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 LIANCARXXX

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

Fase 3 Análisis de Riesgos

Tabla resumen de valoración

- De forma resumida, lo visto hasta ahora nos debe permitir generar una tabla, donde reflejaremos tanto la valoración de activos de la empresa como los aspectos críticos valorados del cero al diez. 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

"Valoración de los activos y aspectos críticos".

Fase 3 Análisis de Riesgos

4. Análisis de amenazas

- Ahora, estimamos cuán vulnerable son los activos a la materialización de las amenazas, así como la frecuencia estimada de la misma. Para ello nos basamos en las amenazas de MAGERIT (en concreto Libro 2 "Catálogo de Elementos" (Punto 5))[18]. Donde las amenazas están clasificadas en los siguientes grandes bloques:
- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

En la tabla a la derecha mostramos solamente las amenazas de Origen Natural y de origen Industrial. De esta forma, analizaremos para los grupos de amenazas, la dimensión de seguridad que puede afectar y por consiguiente el activo directamente afectado.

En la tabla, tenemos 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					

Amenazas de Origen Natural y de origen Industrial.

Fase 3 Análisis de Riesgos

En definitiva, para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

En consecuencia, esta frecuencia estará en la siguiente escala de valores para hacer la definición de la probabilidad de ocurrencia de la materialización de cada amenaza con respecto a los activos de acuerdo a una frecuencia estimada en días y meses del año según lo propuesto por MAGERIT, observaciones y necesidades de la empresa LIANCAR, como se muestra en la Tabla.

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**

Escala de valores para la probabilidad de Ocurrencia de una Amenaza

Fase 3 Análisis de Riesgos

- 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 para un activo "Computadores".
- En la Tabla vemos que la amenaza que ocurre con mayor frecuencias es la [E8] Difusión de Software Dañino

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	0,2739		60%	50%	40%	

Activo "Computadores".

Fase 3 Análisis de Riesgos

. **Impacto potencial:** Una vez realizado el análisis de menazas, y dado que conocemos los valores de los diferentes ctivos, 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[19] 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**".
- Para ello, es conveniente determinar la escala de valores que nos permitirán evaluar el nivel de impacto potencial.
- En caso de muy alta (MA), la explotación de la vulnerabilidad puede resultar en altas pérdidas financieras por daños de activos o recursos tangibles impedimento el logro de los objetivos.
- Si es alta (A), consistiría en la pérdida financiera significativa o amenaza con pérdida de imagen de la empresa LIANCAR.
- si es media (M), consistiría 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 estaría sin prejuicios o costos bajos

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.

Fase 3 Análisis de Riesgos

Cálculo del Impacto potencial y Riesgo Potencial

- 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).
- 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 potencial sumando todos los impactos potenciales generados por cada amenaza. En la tabla , en la fila de "Riesgo potencial" vemos la determinación de este riesgo.

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 dañino	3,287		55%	90%	80%		$45.000.000,00	$133.123.500,00
	[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

Fase 3 Análisis de Riesgos

- **6. Cálculo para el Nivel de Riesgo Aceptable**

- 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.
- La empresa LIANCAR, en consenso con la alta gerencia, el director del centro de tecnología y el encargado de las finanzas establecieron un nivel de riesgo aceptable de $1.822.763,00 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 la tabla, Decisión del Control o salvaguarda para el Activo "Computadores" 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

Decisión del Control o salvaguarda para el Activo Computadores

Fase 3 Análisis de Riesgos

Cálculo para el Riesgo Residual

- Para cada una de las amenazas que fueron identificadas y cuyo impacto potencial de riesgo supera el riesgo aceptable establecido por la empresa LIANCAR, 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 a la derecha, vemos los salvaguardas que se aplicaron a las amenazas para el activo "Computadores" de la empresa.
- 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.
- 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 acumulando sobre los activos inferiores, o repercutido sobre los activos superiores.

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

Fase 4 Propuesta de Proyectos

Llegados a este punto, conocemos el nivel de riesgo actual en la empresa, por lo que es el momento de plantear proyectos que mejoren el estado de la seguridad. Los proyectos que se mencionan y tratan a continuación son el resultado del análisis de riesgos elaborado para la empresa LIANCAR

Propuesta de Sensibilización y Capacitación

- **Objetivo:** Diseñar la campaña, 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.
- **Instrumentos de Sensibilización**

Presentaciones , Medios audiovisuales, Afiches , Fondos de pantalla. Folletos, Portal de ingreso al correo de la empresa y página web.

- **Diseño del plan de sensibilización Básico, Técnico y Jurídico.**

En esta etapa se diseñaran las estrategias para sensibilizar a todos los funcionarios de la empresa actores de LIANCAR. Para ello se utilizarán diferentes estrategias, las cuales serán seleccionadas y planteadas en este proyecto.

Especificaciones

2.5.1 Nivel básico: Dirigido a todos los empleados, usuarios y terceros de la empresa LIACARXXX, este nivel solamente maneja temas básicos como:

- Contraseñas
- Internet
- Acceso físico

2.5.2 Nivel Técnico: En este nivel se profundiza más en los conceptos técnicos y se abordan con mayor complejidad, está, dirigido a los empleados, contratistas, gestión humana, la Dirección administrativa y Financiera que formen parte de LIANCARXXX. Comprende los siguientes temas:

- Contraseñas seguras
- Internet
- Ingeniería social
- Políticas de escritorio limpios
- Accesos a aplicaciones y servicios
- Accesos físicos

2.5.3 Nivel jurídico: Está dirigido a todos los directivos profesionales de la empresa LIANCARXXX, Gestión humana, Dirección administrativa y Financiera, que deban conocer aspectos de la normativa en legislación informática colombiana.

- Protección de datos personales
- Delitos informáticos

Fase 4 Propuesta de Proyectos

- En la propuesta según el análisis de riesgos de la empresa LIANCAR, sobre el Plan de Capacitación tenemos:
- **Objetivo:** desarrollar los siguientes cursos de capacitación en seguridad de la información para la empresa LIANCAR
- **Alcance**
- Está dirigido al gerente o subgerentes, personal administrativo, empleados, usuarios normales que tengan o no conoci

- En la figura de la derecha, se encuentran 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. Por ello. Es necesario establecer un conjunto de cursos básicos, intermedios y avanzados precisamente porque el personal o empleados no tienen una cultura sobre la seguridad de la información.

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			

Fase 4 Propuesta de Proyectos

El plan de concienciación está orientado a disminuir el nivel de riesgo presente con respecto al control, de salvaguarda [E.7] Deficiencias en la organización, y [E.19] Fugas de información, las cuales fueron identificadas en todo el personal de la empresa LIANCAR.

- Durante esta fase se revisará y diseñará los cursos relacionados con seguridad de la información para personal clave, así como talleres prácticos para otros actores de la comunidad involucrada (administrativos, proveedores, clientes, funcionarios).
- En el nivel técnico también se tendrá el curso sobre Seguridad avanzada en Windows y Unix con una duración de 40 horas cada uno.

3. Ejecución del plan

De acuerdo con lo planeado, la ejecución del plan de capacitación tendrá una duración de 6 meses donde se entregará las memorias y documentos respectivos como soportes del plan de capacitación, esta fase durará 3 meses.

En este tiempo, se ejecutarán los siguientes cursos de capacitación que fueron diseñados y planeados anteriormente y que fueron entregados a la alta gerencia.

Nivel básico: Se obtendrá conocimientos básicos en Seguridad de la Información y definiciones en:

- Conocimientos básicos en la norma ISO /IEC 27001
- Conocimientos básicos en informática y tecnología.
- Conocimientos en análisis de riesgos

Nivel Técnico: Se obtendrá conocimientos adquiridos en el curso sobre:

- Fundamentos de Seguridad de la Información.
- Introducción a la Norma ISO 17799, ISO/IEC 27002.
- Introducción a la Norma BS 7799-2, ISO/IEC 27001.
- El Sistema de Gestión de Seguridad de la Información – SGSI.
- Los Dominios de Control.
- Identificación de la aplicabilidad de los mecanismos de control.
- Definición e implementación de la estrategia.
- El proceso de Análisis de Riesgos.
- Factores críticos de éxito en la implementación del SGSI.

Fase 4 Propuesta de Proyectos

Como **segunda propuesta** según el análisis de riesgos de la empresa LIANCAR, tenemos el plan de continuidad del Negocio.
Objetivo: Proteger los procesos críticos y operativos del negocio, su talento humano, la tecnología, la información y el conocimiento contra desastres naturales o fallas mayores por la interrupción de las operaciones en la empresa LIANCAR, disminuyendo el impacto en las pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad debido a que los recursos de la empresa no están disponibles.

- Como **segunda propuesta** según el análisis de riesgos de la empresa LIANCAR, tenemos el plan de continuidad del Negocio.
- **Alcance**
- El plan de continuidad del negocio está circunscrito a la dependencia del centro de Tecnología de la empresa LIANCAR, y busca generar las pautas que permitan restituir en el menor tiempo posible la operatividad del negocio que incluye los servicios críticos prestados a las diferentes oficinas por el centro de tecnología, en caso de que el centro principal quede sin alguna operatividad a causa de un evento que impida su funcionamiento de manera parcial o total de la empresa.

4. Condiciones del PCN

(1) Datos generales de la empresa
(2) Planos de la empresa
(3) Evaluación y análisis de riesgos
(4) Croquis señalando la distribución de equipo contra incendio y sus inspecciones
(5) Números de teléfonos para emergencia
(6) Ubicación de equipo y Manual de primeros auxilios
(7) Brigadas existentes en la empresa
(8) Programa de capacitación al personal
(9) Programa de simulacros
(10) Programa y Bitácora de Mantenimiento a Maquinaria y Equipo
(11) Manuales y procedimientos de actuación por tipo de riesgo
(12) Revisa los fondos disponibles: Se debe revisar los fondos que tenga disponibles o que se tendría en el momento de una interrupción del negocio.
(13) Reconocer las condiciones financieras de la empresa en caso de una emergencia y preparar las medidas necesarias con anticipación para evitar la quiebra aun cuando se interrumpan los ingresos. Si se suspenden las operaciones de la empresa, se perderán ingresos pero se seguirá teniendo los gastos corrientes como salarios y renta.
(14) Estimar los costos de recuperación, paso seguido es evaluar los gastos que debe incurrir la empresa como resultado del desastre y durante el periodo de interrupción.
(15) Croquis señalando rutas de evacuación, salidas de emergencia y puntos de reunión

Fase 4 Propuesta de Proyectos

- En la figura encontramos las amenazas, los 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 para el Plan de Continuidad del Negocio.

	[I.1] Fuego	Los extintores existentes no cumplen los requisitos exigidos, no hay una adecuada actualización en sus recargas en forma permanente.	Disponibilidad	Generación plan de Procesos	Alto	
	[I5] avería de origen físico o lógico.	Falencia en Servicios básicos como: (energía, agua y alcantarillado, entre otros) de soporte para continuidad.	Disponibilidad	Establecimiento grupos de respuesta. Estudio, diseño e implementación Centro de Datos alterno	Medio Alto	
	[I.6] Corte del suministro eléctrico.	No existe una planta de generación de energía como emergencia	Disponibilidad			
	[I.12] Sobrecarga eléctrica.	La Ups que tienen sólo tiene autonomía de una (1) hora.	Disponibilidad			
	[I13] fluctuación eléctrica.	Alteración del funcionamiento de los equipos y los datos almacenados en forma magnética	Disponibilidad			
Plan de continuidad del negocio	[N.1] Fuego	Los extintores existentes no cumplen los requisitos exigidos, no hay una adecuada actualización en sus recargas en forma permanente.	Disponibilidad			Alto
	[N.2] daños por agua.	Falencia en Servicios básicos como: (energía, agua y alcantarillado, entre otros) de soporte para continuidad.				
	[N.3] Inundación.	La empresa está ubicada cerca al rio Bogotá, por lo que puede presentarse inundaciones.				
	[N.4] Siniestro mayor.	Cambios frecuentes ambientales y climáticos				
	[N.5] Fenómeno sísmico.	Cambios frecuentes ambientales y climáticos				
	[A.18] Destrucción de información.	No existe un monitoreo y trazabilidad de la información y del software utilizado en la empresa				
	[A.26] Ataque destructivo.	No presenta mecanismos para realizar pruebas de intrusión de Hacking ético o Ingeniería social ni de cualquier tipo de pruebas al sistema				

Fase 4 Propuesta de Proyectos

LIANCAR LTDA | SGSI | Versión:

6. Metodología

La metodología recomendada y que puede utilizar la empresa LIANCARXXX para el desarrollo de la GCN está apoyada en ISO 22301:2012, que propone un proceso comprendido desde el inicio del proyecto hasta la definición de la estructura de respuesta ante incidentes. Entre estas fases se desarrollarán las que no se ha elaborado durante el proceso del plan del SGSI de la siguiente forma:

6.1 Inicio del Proyecto

Esta fase se realizó con el propósito de estructurar el proyecto para la GCN, de forma tal que se encuentre adecuadamente organizado y controlado durante su ejecución para cumplir los objetivos estipulados previamente en el proyecto.

6.2 Definir la política de continuidad

La GCN se debe apoyar en una política claramente definida, precisa y posteriormente aprobada de manera formal por la empresa LINCXARXXX.

6.3 Compromiso de la alta gerencia

Una vez se realice la aprobación de la política por parte de la alta gerencia de la empresa LIANCARXXX para la realización del proyecto, se debe también validar la existencia de los recursos financieros, humanos y logísticos requeridos tanto para la etapa de diseño como para la etapa de implementación de la GCN; así como velar porque se logren los objetivos ya definidos al decidir implementar este proyecto.

6.4 Análisis de impacto al negocio

El Análisis de Impacto al Negocio (BIA), tiene como función principal determinar

Planes o Estrategias de continuidad

En esta fase, de Estrategias de continuidad del negocio, tiene como objetivo principal analizar los diferentes esquemas o estrategias de continuidad operacional según los escenarios de riesgo definidos, de tal forma, que estas estrategias cumplan con los requerimientos reflejados por el Análisis de Impacto de Negocio y la Evaluación de Riesgos de Continuidad. Los recursos según la norma ISO 22301: 2012 que deben de ser considerados son: personas, información, edificios, equipamiento, tecnologías, transporte, finanzas, y proveedores, entre otros.

En la empresa LIANCARXXX, después de discutir diferentes alternativas decidió contar con un centro de réplica como "estrategia de sitio alterno" ubicado en la sede de la ciudad de Medellín, el cual le permita trasladar en el menor tiempo posible la operación para continuar con sus actividades. Esta decisión fue tomada con anterioridad por la alta gerencia y el centro de tecnología. Anotamos, que esta sede es propiedad de LIANCARXXX por tanto, los recursos técnicos y humanos para su adecuación se vienen contemplando con anterioridad y se encuentran en fase de instalación y configuración.
Después se realizará un replicación online y restauración de backusps.

Otra estrategia es, cuando el colaborador que ejecuta los procesos no puede asistir a trabajar para desarrollar las actividades propias de su cargo. En este caso, se debe establecer la siguiente cadena de comunicación:

- El colaborador ausente activa la Cadena Telefónica y se comunica con el Jefe inmediato.
- El Jefe inmediato comunica el evento al Jefe del Área y activa la contingencia por "Ausencia de Personal". Distribuye procesos claves y asigna funciones al colaborador Back - up. De ser necesario, solicita al Comité de Seguridad de la Información, la reasignación de perfiles.
- El Jefe inmediato confirma al Jefe del Área la continuidad exitosa de los procesos.

Fase 4 Propuesta de Proyectos

Ahora, en caso de presentarse una contingencia Tecnológica, cuando el hardware y/o software presenta fallas, o por interrupción prolongada de telecomunicaciones, se implementará una estrategia en forma estructurada para los aplicativos e infraestructura de la empresa ver tabla Nro1.

Aplicativos	Infraestructura		
SI&SI Correo electrónico Sistema Contable Backups Office otros Software de Bases de Datos	Red	Red Lan	Switches Centro Cableado
		Comunicaciones	Hub Firewall
	Centro de Computo	PBX-ETB	Rotuters
	Servidor	Bases de Datos	Enlaces
		Sistema Operativo	Sistema de Incendio
		Servidor	Sistema eléctrico
		Hardware	Ups

Tabla Nro. 1 Infraestructura de la empresa

6.6 Desarrollo del plan

En esta fase se definirán los grupos necesarios para un desarrollo adecuado del plan, además de 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 restauración a la normalidad.

6.6.1 Disparo de alarma: Es el punto fundamental para el éxito del plan de continuidad del negocio y estará a cargo del líder de PNC. En este momento las sedes de la empresa LIANCARXXX, cada una tendrán un tiempo de respuesta.

6.6.2 Plan de Respuesta: Las acciones que deben llevar a cabo para la ejecución del plan en la empresa deben estar orientadas a la protección de las personas, al control de las amenazas, a la protección de los activos ofreciendo notificaciones de acción pública y registrando las acciones que se van realizando.

6.6.3 Plan de Respaldo: En la empresa LIANCARXXX siempre se pretende mantener el servicio dentro de los niveles requeridos para ello, detectará los recursos necesarios para ejecutar las acciones requeridas fijando un tiempo para activarlas. Además, identificar el personal implicado en el PCN y un registro de estas acciones.

6.6.4 Plan de recuperación: La gestión de la continuidad de negocio requiere de una estructura organizacional, encargada de promover el desarrollo de los lineamientos definidos. Dado que el Comité de PNC realiza el monitoreo a la gestión del Sistema de Riesgo Operativo, también es responsable de administrar la continuidad de la operación de la empresa. A continuación en la Tabla Nro. 2, se mencionan los integrantes del comité, su rol y responsabilidad frente a este Plan.

Comité del PNC	Roles de Contingencia
Gerente General y Oficial	Director de Continuidad
Jefe de Riesgos	
Asistente Administrativa	
Secretaría General	Líder de Administración

Planes de escenarios y Pruebas

En esta fase, se realizarán las pruebas pertinentes para verificar que el plan funciona de manera correcta y oportuna.

D) TIPO DE PRUEBAS

En la siguiente Tabla Nro. 3, se ilustra la metodología que se debe utilizar para la realización de las pruebas del plan de continuidad de negocio de la empresa LIANCARXXX.

TIPO DE PRUEBA	TECNICA UTILIZADA	OPERACIÓN
Integrada	• Creación de un escenario • Seguimiento en vivo de todas las estrategias de recuperación • Con previo aviso. • Apoyo de los proveedores de recuperación	Prueba integrada con todos los elementos que hacen parte del plan de contingencia.
Componentes	• Creación de un escenario • Seguimiento de las estrategias de recuperación • Con previo aviso.	Se ejecutan las estrategias y procedimientos de recuperación de cada uno de los componentes de la infraestructura tecnológica.
Escritorio	• Con previo aviso. • Creación de un escenario.	Se realiza un ejercicio de papel de un escenario de desastre que toma lugar en un salón de conferencia.

Tabla Nro. 3 Metodología para las pruebas.

En lo referente al plan de la continuidad de la empresa, denotamos, 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]. 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.

Fase 4 Propuesta de Proyectos

Plan de Mitigación de riesgos

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.

Pasos para realizar la mitigación del riesgo

Seleccionar los controles apropiados para los riesgos que se han analizado y se han determinado tratar sobre el Catálogo de Buenas Prácticas de la ISO/IEC 27002 (133 controles posibles), pero pueden añadirse otros que la empresa considere necesario.

Diseñar los procedimientos para implantar los controles aunque sean controles técnicos es necesario procedimientos de instalación, uso y mantenimiento.

Verificar que los controles estén correctamente implantados.

Selección de Controles

Los controles seleccionados e implantados para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos como por ejemplo [E.1] Errores de los usuarios se ha aplicado el salvaguarda "Programas de Capacitación permanentes", [E.2] Errores del administrador se ha aplicado el control "Capacitación y actualización, Redundancia" y así con los otros riesgos.

Nombre del Proyecto	Amenazas identificadas	Riesgos Identificados	Dimensión afectada	Acciones	impacto	Prioridad desarrollo
		ético o Ingeniería social ni de cualquier tipo de pruebas al sistema				
Plan de mitigación de riesgos	[A.14] Interceptación de información (escucha).	Existen falencias en los Controles de acceso a la red interna y externa, segregación en redes y controles para asegurar servicios de la red.	Confiabilidad	Bloqueo de puertos de comunicación empleados por software. Inspección de tráfico, bloqueo de tráfico. Inspección y medición del tráfico para control de canal. Establecimiento de políticas de uso de software, políticas de intercambio de información y actualización de políticas de uso de TI.	Medio	Alto
	[A.18] Destrucción de información	No existe un monitoreo y trazabilidad de la información y del software utilizado en la empresa	Disponibilidad		Medio	
	[E.8] Difusión de software dañino	No existen Soluciones de protección contra malware	Disponibilidad, Integridad		Medio	

Tabla 13. Relación de proyectos con riesgos identificados por encima del valor aceptable, con las diferentes acciones a realizar.

Fase 4 Propuesta de Proyectos

Plan de Mitigación de Riesgos

Para que las medidas adoptadas sean efectivas, la dirección debe adoptar y mantener un compromiso con los planes de seguridad de la dicha empresa. Entre las principales actuaciones que han de tener el respaldo directo de la dirección están:

Establecer una política de seguridad

Definir directrices claras para el tratamiento de la información

Promover una estructura de clasificación de la información

Definir normas de etiquetado de soportes

Establecer procedimientos que regulen las comunicaciones y relaciones con terceros y

Asegurar el cumplimiento de todos los aspectos legales que obliguen a la empresa en materia de tratamiento de la información. En la figura de la derecha detallamos un ejemplo de los pasos que se deben realizar para mitigar los riesgos

.

8.23 Controles contra código malicioso

Los errores generados en el software instalado en la aplicación, pueden ser aprovechados por software malicioso para producir daños en el sistema, este hecho amenaza la integridad y la confidencialidad de los datos y debe ser gestionado adecuadamente. Los virus informáticos son aplicaciones o trozos de código que aprovechan estos errores.

8.23.1 Implantación de Medidas

Se debe establecer una política de protección del sistema de información que incluya la instalación en todos los equipos de un software antivirus. Se deben adoptar medidas de seguridad complementarias a la instalación de un antivirus, como son establecer una planificación de actualizaciones del mismo, formar y concienciar al personal para que eviten la ejecución de archivos o lectura de mensajes no reconocidos, recomendando la eliminación de los mismos. También se debe contemplar en las medidas la prohibición de instalación de software sin licencia, ya que dicho software podría encubrir al software malicioso (virus, troyanos, etc.), así como el uso de software no autorizado específicamente por la empresa.

8.23.2 Normativa

La implantación de normas de protección contra código malicioso está reflejada en la norma ISO 27002:2013 en el objetivo 12.2.1 en donde, se debe poner en marcha medidas para la detección, prevención y recuperación del sistema frente a código malicioso, así como procedimientos de concienciación de los usuarios. Objetivo 7.2.2 ISO27002:2013.

En la empresa LIANCARXXX, los usuarios utilizan CD's y USB fuera de la empresa en los equipos del sistema de información de la empresa. Se debe definir un procedimiento de instalación y actualización de antivirus en la empresa, desarrollando actuaciones de formación y concienciación complementarias a usuarios, para evitar la entrada de código malicioso en el sistema. Para hacer esto realidad, la empresa decide instalar en todos los equipos un antivirus y mantenerlo actualizado, y establece normas para que cualquier soporte que se utilice (que no pertenezca a la empresa) primero se escanee con dicho antivirus. También establece normas para que solo el software legal y autorizado por la empresa sea instalado en los equipos del sistema de información.

FASE 5: AUDITORÍA DE CUMPLIMIENTO

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 controly 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 deben analizarse 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.

		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 INFORMAC	L2		59%

Tabla No. 15, Control de Auditoría

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la tabla Nro. 14, que se basa en el Modelo de Madurez de la Capacidad (CMM):

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

Tabla Nro. 14, Modelo de Madurez de la Capacidad (CMM)

FASE 5: AUDITORÍA DE CUMPLIMIENTO

EVALUACIÓN DE LA MADUREZ

Ahora, como la efectividad de los controles se encuentra distribuida en la representación de la tabla No. 13, vemos los controles de seguridad en detalle, visualizando la Madurez CMM de los controles ISO.

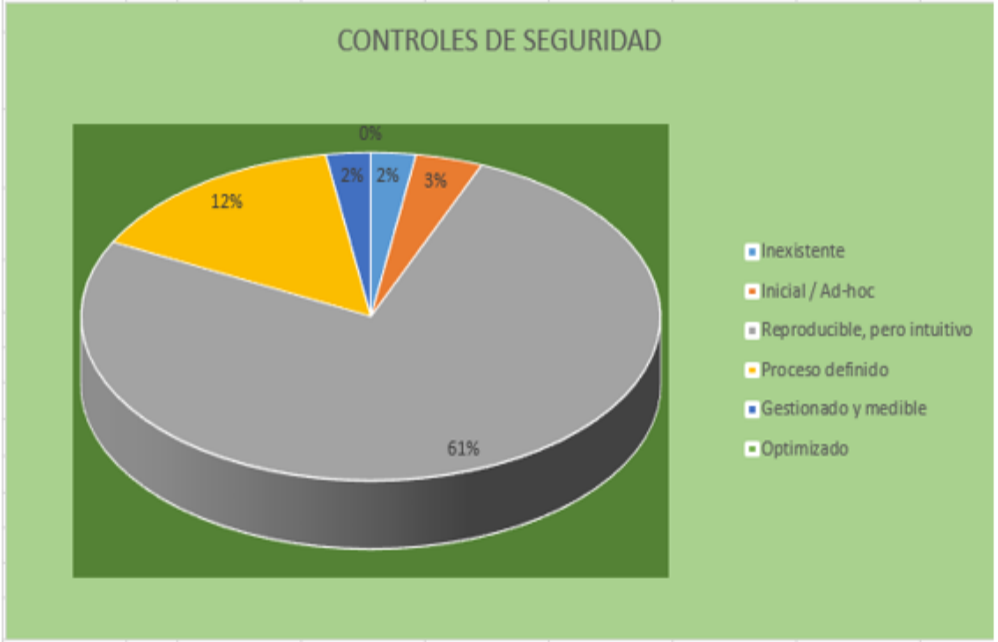


Figura No. 13, Porcentaje de Madurez de los Controles de Seguridad ISO

De acuerdo con los resultados de los dominios analizados y sus respectivos valores diferenciales, se puede concluir que la empresa LIANCARXXX, se encuentra a mitad del camino con un nivel de cumplimiento general del 46% como se detalla en la tabla No. 16.

No.	DOMINIO	VALOR ACTUAL (2017)	VALOR ANALISIS DIFERENCIAL 2016	VALOR DESEADO A TRES AÑOS
5	5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	58%	10%	95%
6	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	59%	10%	95%
7	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	61%	15%	95%
8	8. GESTIÓN DE ACTIVOS	59%	30%	95%
9	9. CONTROL DE ACCESOS	74%	15%	95%
10	10.CIFRADOS	50%	0%	95%
11	11. SEGURIDAD FÍSICA Y AMBIENTAL	84%	40%	95%
12	12. SEGURIDAD EN LA OPERATIVA	79%	20%	95%
13	13. SEGURIDAD EN LAS TELECOMUNICACIONES	71%	15%	95%
14	14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	59%	25%	95%
16	16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71%	20%	95%
17	17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA CONTINUIDAD DEL NEGOCIO	62%	25%	95%
18	18. CUMPLIMIENTO	46%	10%	95%
		64%		

Tabla No. 16, Nivel de cumplimiento de la empresa

Una visión más detallada es la que se presenta como 'diagrama de radar' en la figura No. 14, que mostraría el nivel de cumplimiento por capítulo ISO. Anticipándonos a las medidas, será interesante comparar el estado actual con el estado deseado.

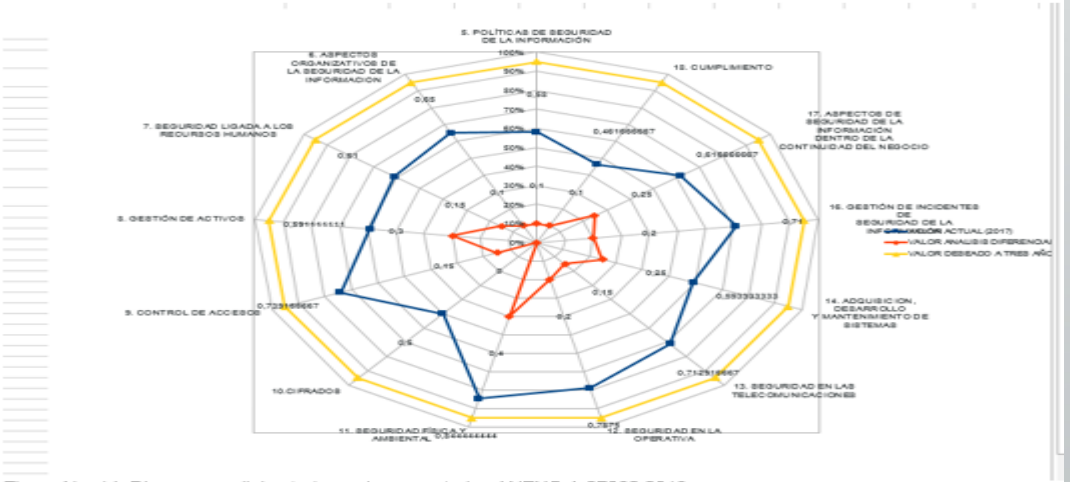


Figura No. 14. Diagrama radial estado madurez controles ANEXO A 27002:2013.