UNIVERSITAT OBERTAT DE CATALUNYA ESPAÑA

FICHA DE TRABAJO FINAL DE MASTER

Título del trabajo	**Elaboración de un plan de implementación de la norma ISO 27001:2013**
Nombre del autor	Rubén Darío Zuleta Arango
Nombre del consultor	Antonio José Segovia Henares
Fecha de entrega	10-06-2015
Titulación	MISTIC

RESUMEN. La empresa ficticia Línea S.A.S, requiere mejorar la seguridad de la información empezando desde procesos de sensibilización para empleados, proveedores y clientes. Donde se muestre riesgos, impactos por amenazas y la forma como la empresa puede perder oportunidades de negocio, verse en situaciones legales por delitos informáticos, entre muchas situaciones fundamentadas por malos procedimientos humanos dirigidos a la inestabilidad organizacional fundamentando pérdida de confianza por clientes. Por tanto, la empresa Línea S.A.S reconoce el valor de la información en su razón social sobre la industria de servicios de recreación y alegría en sus parques. Tiene claro la buena práctica de buscar acercarse a un proceso de certificación de la seguridad de la información a través de la norma certificable ISO 27001:2013 y la fijación de políticas y controles de seguridad por etapas con ayuda de la guía de buenas prácticas ISO 27002:2013.

En primera instancia la empresa pretende mitigar los riesgos y los impactos sobre la aplicación ICG desde los puntos de venta localizados en los parques j y pn, para ello se cuenta con el apoyo de la alta gerencia, quien proporcionará los recursos necesarios y tomará decisiones sobre la implementación del sistema de gestión de la seguridad de la información SGSI.

La segunda instancia desarrollar las fases del sistema de gestión de la seguridad de la información, conocer las exigencias de gobierno en línea en materia del SGSI para empezar a establecer los criterios de desarrollo de las fases de auditoria, la forma de trabajo, compromisos, liderazgo y tipo de perfiles a contratar para el desarrollo del SGSI

Otra etapa fundamental consiste en canalizar los procesamientos para implementación del sistema de gestión de la seguridad de la información por el comité de seguridad de la información conformado en la empresa para determinar la forma de ejecución del SGSI, los beneficios que se obtendrán en cada área y la forma como la empresa mejorará la eficiencia de los procesos de la estructura organizacional. Proyectando así, su imagen corporativa a nuevas tendencias financieras, en términos de rentabilidad y solidez financiera. Donde la mirada de los clientes, se enfatizará en la satisfacción y confianza de bienes y servicios obtenidos por calidad. Permitiendo liderazgo competente para enfrentar la globalización del mercado del turismo, haciendo fuerte la estructura organizacional para competir en una era moderna y exigente, donde las tecnologías de la información serán siempre el pilar fundamental y por tanto la seguridad de la información de la empresa deberá significar plena importancia en términos de confidencialidad, alta disponibilidad e integridad de los datos sensibles.

ASTRACT. The fictitious company LINEA S.A.S, requires improving information security processes starting from awareness to employees, suppliers and customers. Where risks, threats and impacts how a company can lose business opportunities, seen in legal situations cybercrime, among many bad situations substantiated by human procedures aimed at organizational instability basing loss of confidence by customers is displayed. Therefore, the company LINEA S.A.S recognizes the value of information in its name on the industry of recreational and joy in their parks. Is clear good practice to seek closer to a certification process of information security through certifiable standard ISO 27001: 2013 and setting security policies and controls in stages using the good practice guide ISO 27002 : 2013.

At first the company intends to mitigate risks and impacts on the CGI application from outlets located in the jy parks pn, for it is has the support of senior management, who will provide the necessary resources and take decisions on the implementation of the management system of information security ISMS.

The second instance developing phases of system management information security, meet the requirements of eGovernment in ISMS to begin to establish the criteria development phases of audit, how to work, commitment, leadership and type of profiles to hire for the development of the ISMS

Another key step is to channel prosecutions for implementation of the management system of information security committee for information security in the company formed to determine how to implement the ISMS, the benefits to be gained in each area and how the company will improve the efficiency of processes of organizational structure. Projecting so, your corporate image to new financial trends, in terms of profitability and financial strength. Where the eye of customers, will emphasize the satisfaction and trust of goods and services obtained by quality. Allowing competent leadership to face the globalization of tourism market, making strong organizational structure to compete in a modern and demanding era where information technology will always be the cornerstone and therefore the information security company shall mean full significance in terms of confidentiality, high availability and integrity of sensitive data.

LISTA DE PALABRAS CLAVES

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.
2. **Procedimiento de Auditorías Internas**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.
3. **Gestión de Indicadores**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.
4. **Procedimiento Revisión por Dirección**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
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 alguien de Dirección.
6. **SGSI.** Sistema de gestión de la seguridad de la información.
7. **SSI**. Seguridad de los sistemas de información.
8. **Nagios**. Es un software libre para monitoreo de redes, permite conocer su estado de funcionamiento y los puntos críticos ante un incidente.
9. **ICG**. Software para equipos cliente pos y manager para el recaudo, inventarios, ventas, facturación y análisis financiero.
10. **SICOF**. Software financiero para las finanzas, contabilidad y presupuesto, tesorería, nómina y gestión humana.
11. **FIREWALL**. Barrera de seguridad para el control de tráfico en la red, aplicaciones, equipos, control de credenciales de usuarios.
12. **AM** programa para la programación del mantenimiento de todas las atracciones y el control de todas las obras civiles que se realizan, generando reportes y costos por obra.
13. **TIMESOFT** Software para control de ingreso y salida del personal operativo de la empresa, reporte y control de horas extras.
14. **MAGERIT** es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas".
15. **Vulnerabilidad** se define en este método de Gestión del Riesgo, como un estado de debilidad o capacidad para resistir un fenómeno amenazante y que al ser explotado afecta el estado de los activos del proyecto, dicho en otras palabras es la potencialidad o 'cercanía' previsible de la materialización de la Amenaza en Agresión.
16. **Impacto** es el daño que causa o puede causar sobre el activo derivado de la materialización de una amenaza.
17. **Riesgo** Es la probabilidad de que las amenazas exploten los puntos débiles (vulnerabilidades)**,** causando pérdidas o daños a los activos e impacto al proyecto o sistema.

Listado de imágenes

Listado de tablas

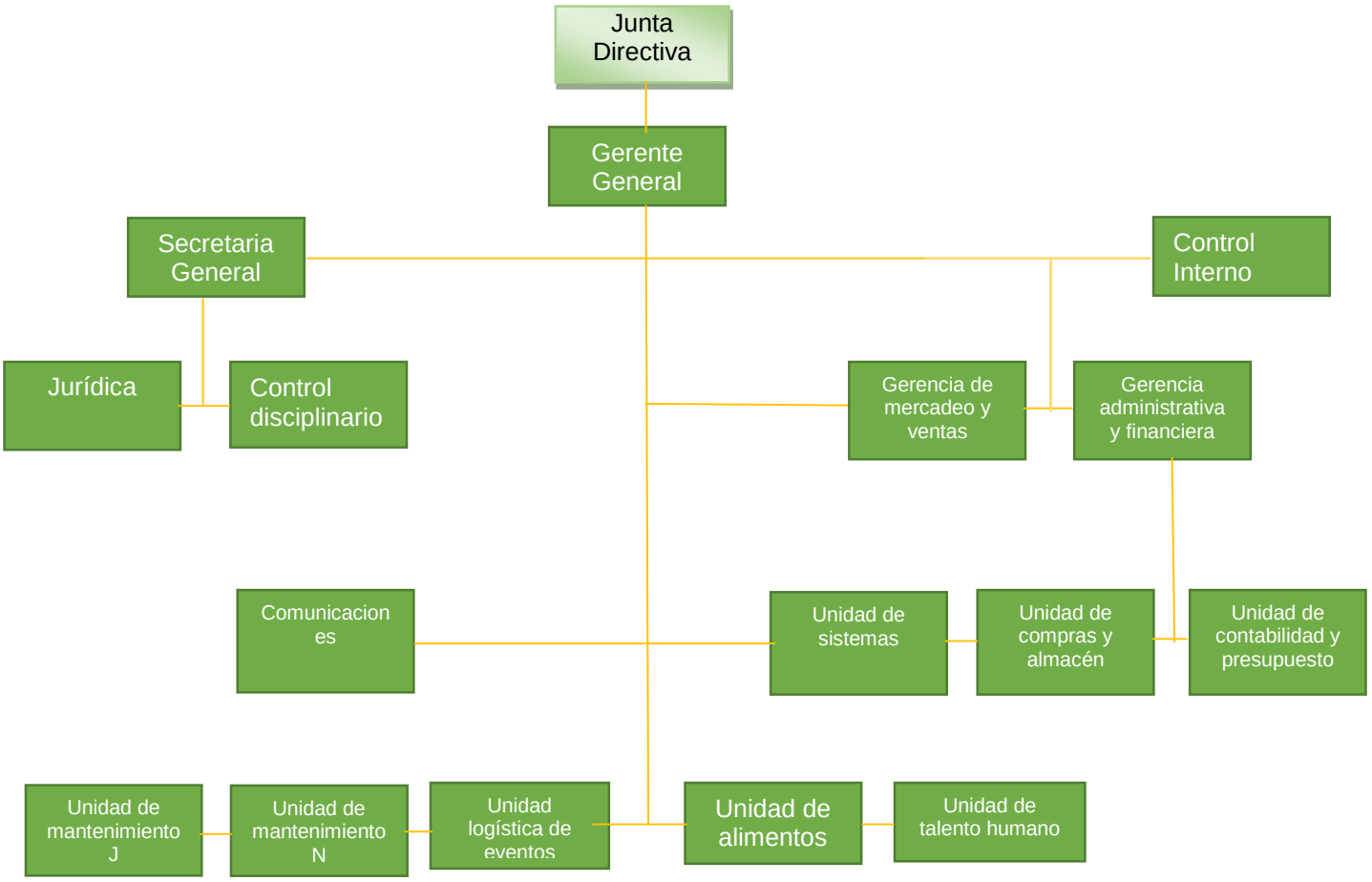
Tabla de Contenido

[1] http://www.pilar-tools.com/magerit/v2/tech-es-v11.pdf

1. **Fase 1: Situación actual: Contextualización, Objetivos y Análisis Diferencial**

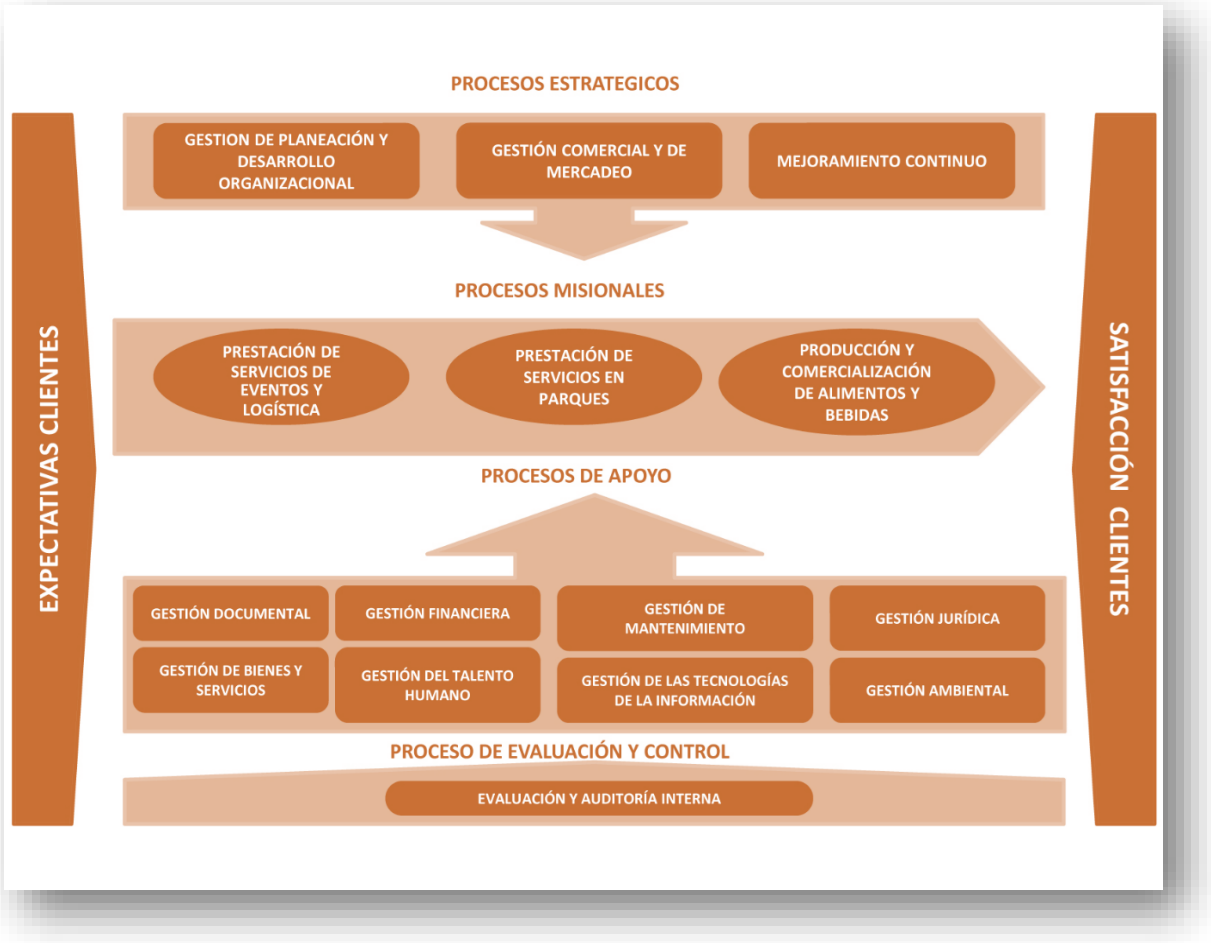
1.1 Introducción. EMPRESA LINEA S.A.S, es un ente público descentralizado del estado Yucatán, desde hace 25 años se ha dedicado a la industria y comercio de bienes y servicios de recreación de la **ciudad Tour**, actualmente cuenta 392 empleados aproximadamente, distribuidos entre el Parque N "Atracciones Mecánicas" y el parque J "Zona Acuática". En cada uno de ellos existen puntos de venta para alimentos y boletería en general. A nivel operativo cuenta con la dependencia de mantenimiento en cargada de soportar las atracciones y mantener el parque aseado y en perfectas condiciones; tiene servicio externo de guardas de seguridad para controlar los accesos y cuidado de los bienes; la parte administrativa consta de las siguientes dependencias: Gerencia General, Secretaria General, Gerencia Financiera, Gerencia de Mercadeo, Administración J, Administración N, contabilidad, costos y presupuesto, tesorería, Jurídica, Control Interno, Control disciplinario, Archivo, compras y almacén, logística, mantenimiento J, mantenimiento N, comunicaciones y talento humano. En la estructura organizacional falta realizar serios ajustes donde se involucre todas las dependencias y el rol de usuario.

Img 1. Estructura organizacional actual



Los procesos de cada dependencia, actualmente se encuentran certificados por el sistema de gestión de la calidad ISO 9001, expedido por el ente certificador, cada año el ente certificador verifica el cumplimiento de los procesos en cada área y otorga las consideraciones necesarias para la continuidad de la certificación.

Img 2, Mapa de procesos del sistema de calidad certificado ISO 9001.



1.1.1 Procesos estratégicos de LINEA S.A.S:

Procesos estratégicos. Son los Dirigidos por la Alta Dirección y son los responsables de analizar las necesidades y condicionantes de la sociedad, del mercado y de los directivos. A través de estos, se define cómo opera el negocio y cómo se crea valor para el cliente / usuario y para la organización. Estos soportan la toma de decisiones sobre planificación, estrategias y mejoras en la organización y proporcionan directrices y límites de actuación para ejecución de los procesos.

Procesos misionales. Son los procesos que tienen contacto directo con el cliente, de hecho son los procesos a partir de los cuales el cliente percibirá y valorará nuestra calidad. Impactan directamente, en el día a día, en los resultados de negocio, el mercado y de los directivos.

Procesos de apoyo. Son los procesos responsables de proveer a la organización de todos los recursos necesarios en cuanto a personas, maquinaria y materia prima, para a partir de los mismos poder generar el valor añadido deseado por los clientes. Su principal cliente es el cliente interno.

Procesos de evaluación y control. Es el encargado de evaluar en forma permanente la efectividad del control interno la eficiencia, la eficacia, la efectividad de los procesos; el nivel de ejecución de los planes y programas; los resultados de la gestión detectando desviaciones,

estableciendo tendencias y generando recomendaciones para orientar las acciones de mejoramiento.

Se busca una correcta integración del sistema de calidad implementado con el sistema de gestión de la seguridad SGSI, de acuerdo a las exigencias de gobierno en línea del estado **Yucatán**, para el cuidado de la información sensible en términos de disponibilidad, confidencialidad e integridad; donde se implemente el SGSI acorde a la norma internacional certificable ISO 27001/2013, permitiendo con ello fijación de controles de acuerdo al ISO 27002/2013 para identificación y valoración de riesgos por amenazas e impactos en caso de materializarse alguna de ellas, conocer el estado de la seguridad de la información de la organización tanto interno como externamente, selección y aplicación de medidas de control para salvaguardar la información sensible, concienciación del personal de la organización y de la gerencia general sobre el valor y significado que debe tener la información para el fortalecimiento del contexto industrial y comercial que caracteriza a la empresa; poder identificar y controlar las brechas de seguridad, proteger los sistemas de fugas o robos de información no consentidos, elaboración de planes de contingencia para el cuidado de la información ante una posible eventualidad, poder reaccionar y garantizar los servicios sin afectar la productividad y desarrollo de la organización; prevenir posibles intrusiones en los sistemas y aplicaciones de la organización. Se espera lograr una mirada confiable de nuestros clientes, proveedores y empleados de la organización sobre los bienes y servicios ofertados.

1.1.2 Los recursos críticos TIC importantes para proteger en la organización son:

Las personas: Empleados, proveedores y clientes son el recurso más importa a cuidar de acuerdo al nivel de acceso a los recursos TIC de la organización y al uso de la información.

Redes de datos y redes WIFALL, son los medios de comunicación sensibles para las comunicaciones de los parques, sin estos se genera caos en los procesos de la empresa.

Páginas Web administrativa y para los parques de recreación.

Intranet y chat interno, software para comunicación local**.**

EXCHANGE software para correo corporativo de la organización.

PQRSD software WEB para las quejas, reclamos y peticiones de los clientes y empleados.

DOCUMENT aplicación para el registro documental de la empresa.

SICOF programa financiero de la organización compuesto de varios módulos: Contabilidad, presupuesto, almacén y compras, nómina y talento humano.

ICG programa para stock de ventas de los parques por equipos post ICG y un servidor manager ICG encargado de recibir recaudos, brindar estadísticas, balances financieros, actualizaciones de valores de los servicios a comercializar, control de inventario, programación logística, entre otros.

AM programa para la programación del mantenimiento de todas las atracciones y el control de todas las obras civiles que se realizan en los parques, generando reportes y costos por obra.

TIMESOFT Software para control de ingreso y salida del personal operativo de la empresa, reporte y control de horas extras.

SYMANTEC programa para las copias de seguridad.

DLO SYMANTEC software para copias de seguridad de usuarios críticos de jefes y gerentes.

MCAFEE software antivirus corporativo para 138 equipos cliente y 12 servidores.

Directorio activo Sirve para crear, modificar y controlar credenciales de usuarios para los accesos a los equipos cliente y servidores.

Microsoft Hyper-V es un programa de virtualización basado en un hipervisor para los sistemas de 64 bits con los procesadores basados en AMD-V o tecnología de virtualización Intel (el instrumental de gestión también se puede instalar en sistemas x86.

Licenciamiento: Bases de datos Oracle 10g y 11g standard, Software ICG, SICOF, Microsoft Windows versiones profesional 8, 8.1, 7; Licencia de LAN to LAN para conectar los dos parques a nivel local; SYMANTEC para las copias de seguridad, licencia del software financiero SICOF, Licencias ICG para las ventas en los puntos de comercio abiertos al público y usuarios manager para gestión administrativa y financiera de la empresa, licencia de TIMESOFT para el control de accesos de empleados, licencia de AM para la gestión y manejo de los recursos por la dependencia mantenimiento, 150 Licencias antivirus MCAFEE distribuidas entre 138 equipos de cómputo clientes y 12 servidores, licencia firewall marca SONY WALL empleado para controlar tráfico de red en la organización y para ayudar proteger los sistemas de algunas amenazas, licencias del DOCUMENT sistema documental utilizado y controlado desde el archivo para el registro de procedimientos legales.

1.2 [2]Conociendo la ISO/IEC 27002

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la International Organization for Standardization y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013.

Precedentes y evolución histórica. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la International Organization for Standardization y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

Publicación de la norma en diversos países. En España existe la publicación nacional UNE-ISO/IEC 17799, que fue elaborada por el comité técnico AEN/CTN 71 y titulada *Código de buenas prácticas para la Gestión de la Seguridad de la Información*, que es una copia idéntica y traducida del inglés de la Norma Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 se estima que esté disponible en la segunda mitad del año 2006. En Perú la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto del 2004, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe).

En Chile, se empleó la ISO/IEC 17799:2005 para diseñar la norma que establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documento electrónicos de los órganos de la Administración del Estado de la República de Chile, y cuya aplicación se recomienda para los mismos fines, denominado Decreto Supremo No. 83, "NORMA TÉCNICA SOBRE SEGURIDAD Y CONFIDENCIALIDAD DEL DOCUMENTO ELECTRÓNICO".

En Bolivia, se aprobó la primera traducción bajo la sigla NB ISO/IEC 17799:2003 por el Instituto de Normalización y calidad IBNORCA el 14 de noviembre del año 2003. Durante el año 2007 se aprobó una actualización a la norma bajo la sigla NB ISO/IEC 17799:2005. Actualmente el IBNORCA ha emitido la norma NB ISO/IEC 27001 y NB ISO/IEC 27002.

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. Organización de la Seguridad de la Información.
2. Seguridad de los Recursos Humanos.
3. Gestión de los Activos.
4. Control de Accesos.
5. Criptografía.
6. Seguridad Física y Ambiental.
7. Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo;

[2] http://es.wikipedia.org/wiki/ISO/IEC_27002

gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

8. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.
9. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
10. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.
11. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.
12. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.
13. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

1.3 Contextualización. Gestión de tecnologías de la información y la comunicación.

La infraestructura tecnológica está dotada de 12 servidores, 9 de ellos son virtuales por el software Hyper-v y 3 son físicos, los sistemas operativos soportados son Windows 2003 server y Windows 2008 server 64 bits, 138 computadores clientes para todo el personal administrativo con sistema operativo Windows 8 profesional 64 bits, 31 equipos post ICG para las ventas en los parques con sistema operativo Windows 7 64 bits. La topología de red es estrella bus, la conexión local entre parques se contrata por servicio de red LAN to LAN con un proveedor de servicios X, tiene 2 firewall corporativo marca SONYWALL para el control de tráfico de red, tiene 2 swiches capa 3 para la gestión y direccionamiento ip, Se cuenta con varios swiches de fibra para la conectividad, file server para compartir archivos entre usuarios, cuenta con sistema de almacenamiento para las copias de seguridad de la información entre máquinas cliente y servidores con aplicaciones críticas, el internet es 20Mb dedicados para los dos parques, cuenta con servicio de red wifi para los clientes separado del segmento de red de la empresa proporcionado por el municipio x, zona wifi para empleados administrativos, directorio activo para la gestión de cuentas de usuario; clúster de red para alto rendimiento, alta disponibilidad, balanceo de carga y escalabilidad de los sistemas de información y cuenta con un software antivirus MCAFEE corporativo que ayuda a proteger los sistemas de instrucciones, amenazas, visita de sitios maliciosos, eliminación y reporte automático de malware, gestión de funciones desde la consola.

1.3.1 Incidentes soportados: Denegación de servicios DoS de internet, problemas de segmentación de la red cableada UTP categoría 5E, Perdida del servicio Wifi por alta demanda de usuarios y alto tráfico de red ocupando los canales de la frecuencia 2.4 G, perdida de la base de datos de correo corporativo paralizando la empresa por 1 día, swiches de fibra con puertos malos quemados por las sobre cargas eléctricas, mala conectividad en los puntos de venta pos ICG; Algunos servidores tienen pocas características de rendimiento, de alta escalabilidad y disponibilidad de servicios para soportar la demanda de recursos de aplicaciones ICG y SICOF; falta de concienciación de los usuarios sobre el cuidado y manejo de los recursos tic de la organización; pocas medidas de seguridad sobre el control y uso de contraseñas debido a que muchos usuarios se prestan las credenciales; falta concienciación desde la alta gerencia para asumir el valor y cuidado que debe tener la información y lo más crítico la alta rotación de personal ha generado fugas de información importantes, paralización y desarrollo de la empresa en los procesos.

Actualmente se realiza la gestión de mejoramiento de la red cableada a categoría 6A, propuesta de cambio de la telefonía análoga por la de voz sobre ip, integración de AP WIFI desde una controladora gestionada por software, ampliación del almacenamiento para las copias de seguridad, “Web Application Firewall” para el aseguramiento de aplicaciones públicas ante posibles intrusiones por inserción código malicioso y la renovación de servidores para soportar correctamente las aplicaciones SICOF e ICG.

Observar img 3, el montaje de la infraestructura actual Pg 18.

1. 4. OBJETIVOS DEL SGSI ORGANIZACIONAL

Objetivos	Indicador
Elaborar el sistema de gestión de la seguridad SGSI, ajustado a la norma ISO 27001/2013 para el buen funcionamiento de la infraestructura tecnológica y el desempeño adecuado de los procesos.	• Cobertura de las políticas. • Efectividad de la política de cumplimiento.
Implementar un sistema de gestión de la seguridad de la información organizacional para el cumplimiento de las exigencias de gobierno en Línea del estado Yucatán.	• Efectividad de las auditorías o revisiones normativas. • Efectividad de la planificación de la revisión por la dirección.
Mejorar el nivel de concienciación de los usuarios sobre el correcto manejo y uso de la información organizacional.	• Responsabilidad sobre la SI en la organización.
Verificar la seguridad de la información de la estructura organizacional de acuerdo a las políticas de seguridad de la información y a las mejoras de los controles implementados.	• Alcance de la gestión de riesgos de SI. • % de Controles ISO 27002:2013 Implementadas • Existencia y efectividad de políticas, procedimientos y controles para el intercambio seguro de información relevante
Auditar interna y externamente el uso eficiente de la información organizacional.	• Efectividad del SSI para controlar o mitigar los riesgos. • Efectividad de las auditorías o revisiones normativas.
Reforzar y controlar los accesos a los sistemas de información con ayuda de políticas claras y controles de seguridad física.	• Grado de despliegue o efectividad de los controles aplicados. • % de Controles ISO 27002:2013 Implementadas • Eficacia del control de acceso a sistemas y aplicaciones. • Efectividad de las revisiones de seguridad física.
Mejorar la alta disponibilidad, escalabilidad y rendimiento seguro de las aplicaciones y servidores destinados al servicio de las distintas labores organizacionales.	• Existencia y efectividad de estándares, directrices, procedimientos y herramientas de seguridad de redes
Cumplir con las exigencias reglamentarias en la legislación vigente en materia de salvaguardar información sensible de personas, derechos de autor, delitos informáticos, sociedades de la información y la comunicación.	• Efectividad del SSI • Efectividad de la continuidad de la seguridad de la información.

1.4.1 ALCANCE DEL SGSI

La organización desea enfocar el SGSI basado en la norma ISO 27001:2013 principalmente para el programa de ventas ICG y la red de la organización de la siguiente manera:

Los sistemas de información que dan soporte al programa de ventas ICG y la red interna de la Organización, según la declaración de aplicabilidad vigente.

1.4.1.1 Descripción del Alcance. Los procesos tienen un componente liderado por personal operativo y personal administrativo. Interesa enfocar el sistema de gestión de la seguridad de la información, al tratamiento y mejora de incidencias sobre equipos informáticos de la administración de la infraestructura tecnológica de la empresa ligados al programa de ventas ICG y la red interna. Inicia con identificar la infraestructura tecnológica y termina con la identificación de amenazas, valoración y análisis de riesgos, selección y aplicación de controles de seguridad de la información, elaboración de planes de contingencia, recomendaciones monitoreo de la red y recomendaciones generales de aplicabilidad.

Img 3. Red LAN to LAN monitoreada con nagios

1.5 Objetivos del plan director de seguridad de la información.

- Aplicar la normatividad vigente para el manejo y tratamiento adecuado de la información organizacional con apoyo recursos financieros, tecnológicos y humanos necesarios e indispensables para su desarrollo y cumplimiento.

- Elaborar planes de contingencia ante eventualidades inesperadas de seguridad causados voluntaria o involuntariamente desde de la propia organización o aquellos provocados externamente por delincuentes informáticos, accidentalmente por catástrofes naturales y fallos técnicos.

- Implementar controles de seguridad adecuados para la garantía de la seguridad de la información en términos de confidencialidad, integridad, disponibilidad, autorización y no repudio, y trazabilidad.

- Hacer patente el compromiso de la Dirección con la seguridad de la información, para la garantía de continuidad de las actividades de la Organización.

- Definir, desarrollar y poner en funcionamiento los controles técnicos, legales y de gestión necesarios para la garantía del cumplimiento, en todo momento, de los niveles de riesgo aprobados para la Organización.

- Cumplir en todo momento la legislación vigente en materia de protección de datos y sociedad de la información, y evaluación de otros factores de riesgo sobre alteración de la seguridad de los activos de la Organización.

- Crear una “cultura de seguridad” compartida por todo el personal de la Organización.

- Tratar la seguridad de la información como un proceso de mejora continua para la optimización de los controles de seguridad.

1.6 Análisis diferencial de medidas de seguridad existente en la organización y las impartidas por ISO/IEC 27001 e ISO/IEC 27002. Actualmente la empresa cuenta con una certificación ISO 9001 de calidad de los procesos certificada. Entre ellos está la gestión de tecnologías de la información y la comunicación. La cual actualmente, tiene implementada la política de seguridad pero su aplicabilidad radica solo en la gestión de contraseñas, normas de uso de los equipos informáticos, administración de la red de datos, gestión antivirus, sistemas de backup y almacenamiento, plan de mejoramiento continuo de la infraestructura tecnológica, soporte a usuarios y soporte de infraestructura tecnológica.

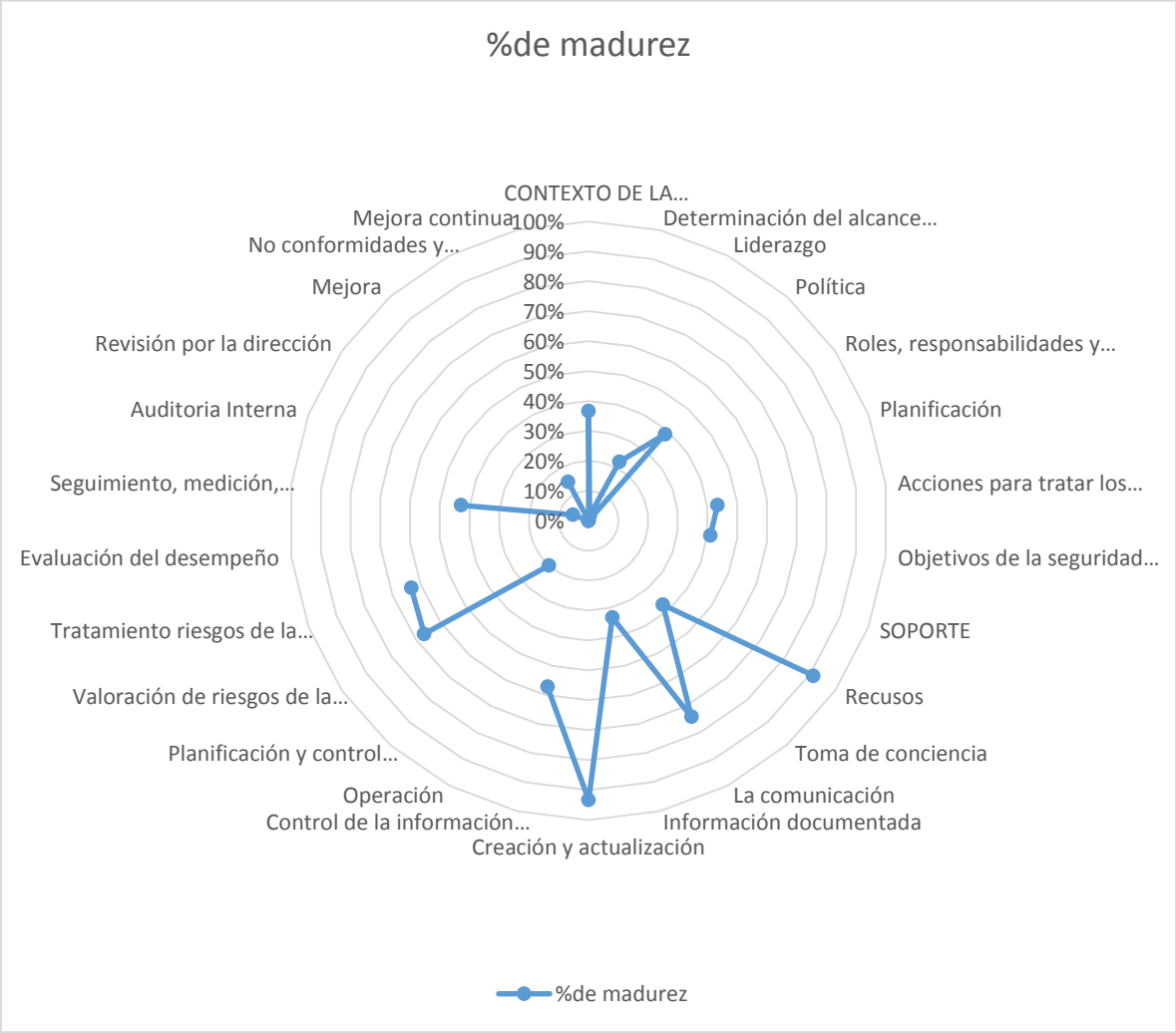
Se diferencia de la guía de aplicabilidad ISO 27002/2013, por ser una guía puntual de controles de seguridad de la información que se pueden aplicar para fortalecer el sistema de calidad actual en la organización y para estructurar, y aplicar las políticas de seguridad de la organización para cumplir con los pilares de la seguridad de la información en términos de confidencialidad, integridad y disponibilidad.

Se realiza una entrevista en cada dependencia para evaluar el nivel de cumplimiento de la norma ISO 27001:2013 de los apartados del 4 al 10 y lo referente a la guía de controles ISO 27002:2013. En la siguiente tabla del anexo 2, se expone los resultados de la entrevista y se encontrará el estado de la seguridad de la información de la empresa en sus diferentes procesos.

Anexo 1. Análisis diferencial ISO 27001.xls. Consideraciones bajo la norma ISO 27001:2013 y Anexo A de controles para la declaración de aplicabilidad de los controles.

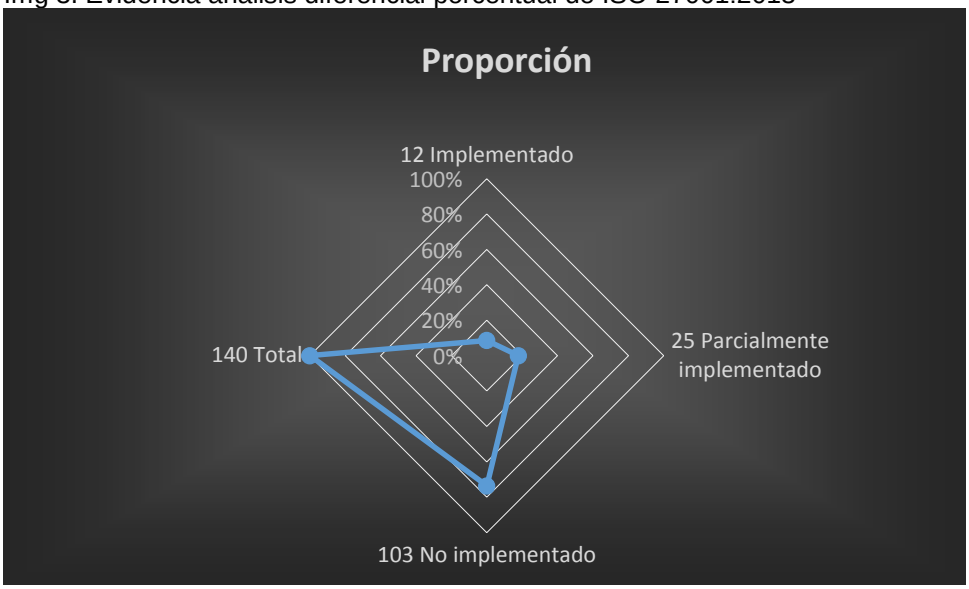
1.6.1 Resultados del análisis diferencial Anexo 1. Análisis diferencial ISO 27001.xls

Img 2. Evidencia de resultados del análisis diferencial de ISO 27001:2013



La img 2, indica el grado de madurez de los procesos de seguridad de la información con respecto a la norma ISO 27001:2013.

Img 3. Evidencia análisis diferencial porcentual de ISO 27001:2013



La img 3, indica cantidad total de criterios considerados de la norma para verificar el estado de cumplimiento organizacional.

1.6.1.1 Conclusiones.

- En la imagen 3, se puede verificar que la empresa cumple con 26 consideraciones de la norma ISO 27001:2013 contempladas en los apartados 4 al 10, donde resulta 12 consideraciones implementadas eficazmente, 25 consideraciones de forma parcial por estar incompletos o le falta grado de madurez y 103 no se cumplen o no hay razón de existencia.

- El análisis diferencial de ISO 27001:2013, permite a la empresa conocer su situación actual sobre el estado de los fundamentos base para iniciar una etapa de implementación del sistema de gestión de la seguridad SGSI.

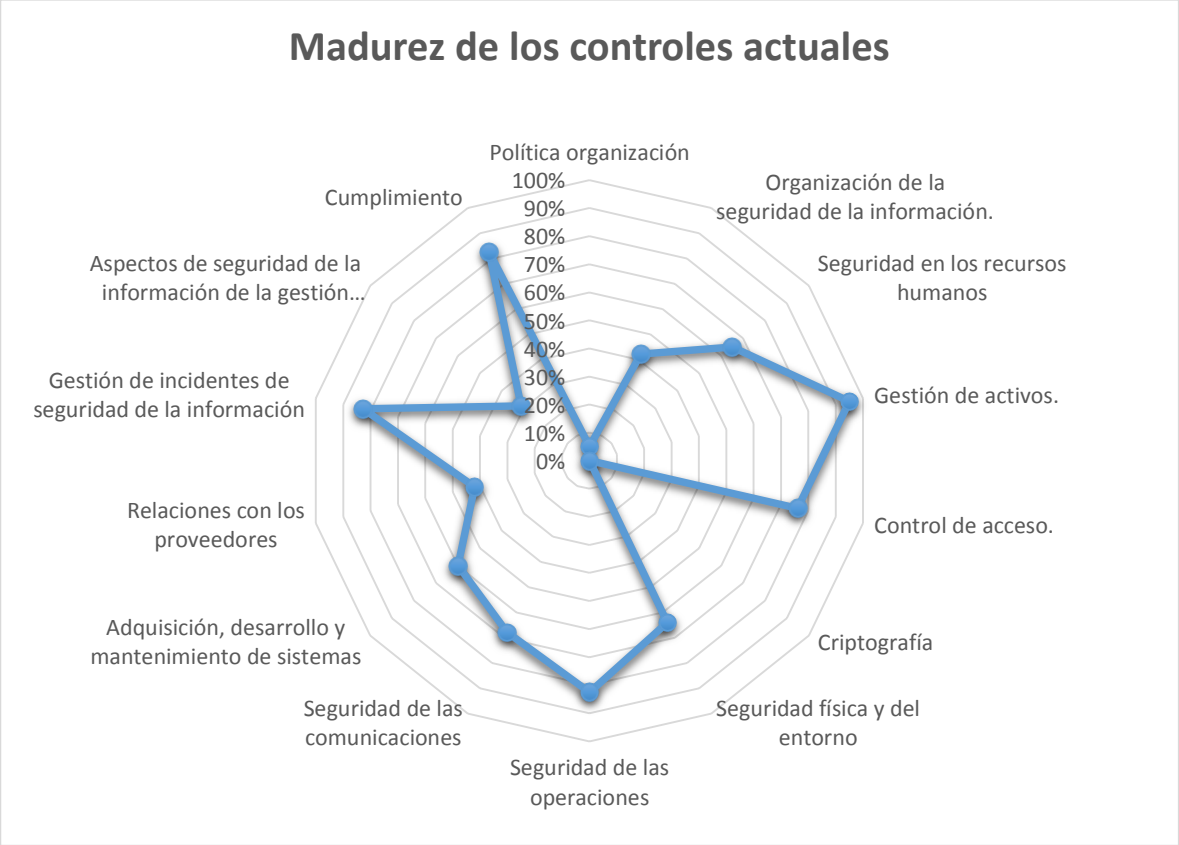
- Los resultados arrojados son pertinentes para determinar los criterios necesarios para enmarcar la importancia y el valor que debe tener la información para una organización. De la imagen 3, 74% de las consideraciones no se han implementado o no se aplican; un 18% se cumple de forma parcial y un 9% se cumplen y se aplican al contexto organizacional.

- Se verifica consideraciones pertinentes al fortalecimiento de los procesos para el cuidado y tratamiento de la información sensible y los apartados para salvaguardar y tratar la información en términos de confidencialidad, disponibilidad e integridad donde muchas de las consideraciones exigidas por la norma aún no están contempladas por la dirección de la empresa.

- El análisis diferencial con base a la norma ISO 27001:2013, ayuda a la toma de conciencia, saber que se está sujeto a riesgos por pérdida o fuga de información y permite establecer los criterios de valorar riesgos de una amenaza que al llegarse materializar puede generar un impacto considerable y crítico para la organización.

Ver Anexo 2. Análisis diferencial ISO 27002.xls, permite indagar sobre el estado inicial de la seguridad de la información de la empresa ficticia LINEA S.A.S.

Img 4. Evidencia análisis diferencial Anexo 2, controles y dominios



La img 4, indica el grado de madurez de los 114 controles de acuerdo a la situación actual de la organización.

Img 5. Evidencia análisis diferencial Anexo 2, controles y dominios

La img 5, indica los porcentajes de madurez de los controles de la organización con respecto a los dominios del ANEXO A de la norma ISO 27001 y la guía de controles ISO 27002 del año 2013.

Conclusión

La img 4 y la img 5. Según guía de controles del anexo A que son también considerados en la guía ISO 27002:2013, indica de 114 controles, la empresa solo tiene optimizados 20 controles y 23 controles son inexistentes por tener inconsistencias en la efectividad de la política de seguridad de la información, por no haber claridad en los procedimientos y por no estar actualizando los procesos; 12 controles están en estado inicial, aún no se aplican puede ser por desconocimiento de la norma, la tranquilidad del personal, por falta de concienciación sobre el valor e importancia que debe tener la información dentro y fuera de la organización o porque son esfuerzos individuales que no tienen en cuenta los criterios del equipo de trabajo de la organización. Se verifica también 14 controles con una efectividad del 90% donde los procesos están implementados, documentados y comunicados, y 45 controles de un 95% de efectividad; por tanto, por ser procesos gestionables y medibles pueden seguirse evaluando con ayuda de indicadores.

2. FASE 2. SISTEMA DE GESTIÓN DOCUMENTAL DEL SGSI

2.1 Esquema documental. Elaboración mínima de documentos exigidos para el cumplimiento de las exigencias de la norma ISO 27001:2013 y para el cumplimiento de un proceso de certificación.

2.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA LINEA S.A.S

2.1.1.1 Propósito. Contribuir al logro de la seguridad de la información por etapas, partiendo de concienciación de la alta dirección y del personal sobre el valor e importancia de la información, uso apropiado de los sistemas de información y de las aplicaciones; hasta la consolidación de una organización sólida y comprometida con el cumplimiento de la legislación vigente en materia de delitos informáticos y sociedad de la información, respecto por los derechos de autor o propiedad intelectual, cumplimiento de los tres pilares de la seguridad de la información en términos de confidencialidad, integridad y disponibilidad para establecimiento de alta confianza y calidad de servicios para empleados, clientes y proveedores.

2.1.1.2 Alcance

Esta política es de aplicación en el conjunto de áreas que componen la Empresa, a sus recursos, a la totalidad de los procesos internos o externos vinculados a través de contratos o acuerdos con terceros y a todo el personal o cualquiera sea su situación contractual.

En particular, los objetivos comprenden:

- Asegurar que los recursos tecnológicos de información y comunicaciones proporcionados o al servicio de la información, se utilicen en forma consistente con la misión de empresa, considerando la ética, los aspectos legales, los valores de honradez y responsabilidad, considerada apropiada, de conformidad con ésta política institucional y leyes aplicables vigentes.

- Asegurar que las interrupciones y perturbaciones en el préstamo de los servicios asociados a los sistemas informáticos y de comunicaciones, ocasionados por uso inapropiado o inaceptable, sean mínimos, al igual que los deterioros y daños ocasionados por mal uso accidental o provocado.

- Dar a conocer a los usuarios que en general, la información electrónica está sujeta a las mismas leyes, regulaciones, políticas y requerimientos aplicables a la información que se comunica en otras formas y formatos escritos, pero también hay múltiples aspectos adicionales por considerar, dada la naturaleza excepcional de la información electrónica.

2.1.1.3 Uso Apropiado

El uso de los recursos informáticos y servicios asociados que se proporcionan a los usuarios debe ser consistente con los fines de la Empresa, igual que ocurre con cualquier otro recurso que se suministra como herramienta de trabajo.

Se espera que las personas actúen responsablemente en la forma como acceden o transmiten información desde o a través de las redes de cómputo de la Empresa. Los usuarios deberán ser responsables de sus acciones y omisiones.

2.1.1.4 Usos inaceptables e inapropiados para la seguridad de la información.

Los recursos informáticos no deberán:

1. Utilizarse para llevar a cabo actividades por fuera de la Ley.

2. Utilizarse para fines particulares en horario laboral.

3. Entregarse a terceros datos o información de los proyectos sin tener la debida autorización de los directivos de la Empresa.

4. Utilizar los recursos sin el respeto por las leyes de Derechos de Autor. Aplicable entre otros, a textos, elementos multimedia (gráficos, fotografías, videos, música, etc), datos y software.

5. Utilizar los recursos de tal forma que no se viole ésta u otras políticas, reglamentos o directrices institucionales.

6. Utilizar los recursos para actividades no relacionadas con la misión y objetivos de la Empresa.

7. Utilizar los recursos en forma inapropiada, poniendo en peligro la información, los recursos o los intereses de la Empresa.

8. Utilizar los recursos en forma inapropiada, interfiriendo con los sistemas de cómputo y telecomunicaciones.

9. Utilizar los recursos sin respetar el trabajo o derechos de otros usuarios.

10. Utilizar recursos sin tener autorización o autoridad para hacerlo; o permitir o facilitar que usuarios no autorizados hagan uso de los recursos de la Empresa.

11. Distribuir datos o información confidencial de la Empresa sin autorización.

12. Difamar de otras personas vía correo electrónico o por otros medios.

13. Alterar configuraciones de software o hardware del sistema sin autorización.

14. Usar, alterar o acceder sin autorización a los datos o a los archivos de otros usuarios, así esa información se encuentre accesible.

15. Leer la correspondencia electrónica ajena, a menos que se esté específicamente autorizado para hacer eso.

16. Prestar las contraseñas personales, los datos o los archivos de otros.

17. Suplantar a otras personas, haciendo uso de una falsa identidad, utilizando por ejemplo cuentas ajenas de correo electrónico.

18. Llevar a cabo actividades particulares en nada relacionadas con los fines institucionales, por ejemplo, utilizar Internet para consulta de páginas con contenidos pornográficos, o utilizar los discos duros de los computadores del Instituto para almacenar archivos de música mp3 o similares.

19. Intentar evitar los mecanismos de seguridad de la red o de control impuestos, perjudicar la funcionalidad de la red, o saltarse las restricciones establecidas por los administradores de la red.

20. Sacar o tomar prestados los recursos de la Empresa sin tener la debida autorización.

21. Utilizar software sin respetar los Derechos de Autor, por ejemplo: Duplicar, instalar o utilizar software en una forma diferente a la permitida o autorizada.

22. Evadir las restricciones o condiciones impuestas en las licencias o términos de uso del software. Instalar software gratuito o software obtenido de Internet sin disponer de algún respaldo legal que claramente autorice su uso, ya sea impreso o digital.

23. Interferir o trastornar deliberadamente el sistema o el trabajo de otros, por ejemplo: Cargar excesivamente un sistema de cómputo o ejecutar códigos dañinos tales como virus.

24. Crear, copiar, enviar o reenviar cadenas de mensajes en nada relacionados con la Empresa.

25. Escribir en papel las contraseñas asignadas o mantenerlas en medios digitales sin protección alguna.

26. Instalar software sin estar debidamente autorizado para ello, sea o no el software de propiedad de la empresa LINEA.

27. Crear, obtener, desplegar, almacenar, copiar o transmitir materiales sexualmente orientados o sexualmente explícitos.

28. Utilizar los recursos informáticos para juegos.

2.1.1.5 Uso de Internet

La empresa LINEA S.A.S y el uso de Internet que se lleva a cabo utilizando las direcciones y nombres de dominio www.linea.mx.ar

- La empresa LINEA, promueve el uso de Internet para que los usuarios puedan llevar a cabo sus labores de una mejor forma y anima a sus empleados, colaboradores y personal de contrato a desarrollar las destrezas necesarias para utilizar esta herramienta en forma efectiva en el desarrollo de las labores institucionales. El uso de Internet debe realizarse únicamente para actividades relacionadas con Empresa, salvo el uso particular eventual, limitado y permitido por fuera del horario laboral.

- Se espera que los funcionarios utilicen Internet para incrementar su conocimiento, para acceder a información técnica y científica y de otros tipos sobre temas de relevancia para empresa, y para comunicarse con colegas y otras personas en el desarrollo del quehacer institucional.

- Es responsabilidad de cada usuario hacer ejercicio de buen juicio cuando se acceda a sitios de Internet y evitar sitios que ninguna relación tengan con el trabajo o que pongan en peligro la buena imagen, los equipos o los recursos de la Empresa.

- El uso de la conexión a Internet debe realizarse sin interferir con el trabajo de los demás, debe ser legal, en particular, observando respeto por las leyes de derechos de autor.

2.1.1.6 Seguridad

- El acceso y uso de Internet se debe realizar utilizando una compuerta segura, equipada de un cortafuegos (firewall) que controle todo paquete entrante o saliente y que impida conexiones entrantes no autorizadas a las redes de datos de la Empresa.

- Los servicios de red institucionales debidamente autorizados, que se habiliten para su acceso desde Internet, deben colocarse en operación solo después de aplicar unas medidas de seguridad básicas (por ejemplo, para ciertos servicios mediante el uso de conexiones encriptadas).

- Cuando se requiera acceder remotamente a los equipos de la empresa Linea, se deberán utilizar conexiones seguras, evitando servicios tales como Telnet, ftp y otros que se sabe son de alto riesgo.

- Los servicios de red o conexiones autorizados desde la propia organización hacia Internet incluyen: consultas web (http y https), correo electrónico, conexiones remotas tipo ssh o telnet, transferencia de archivos vía FTP, consultas DNS, sincronización de tiempo y copias remotas usando rsync. Otros servicios y conexiones se irán autorizando de acuerdo a necesidad y conveniencia institucional.

- No está permitido conectarse a Internet utilizando equipos diferentes a los que se encuentran oficialmente en servicio, así por ejemplo, no está permitido conectar o usar los módems de los PCs de los usuarios para ese propósito.

- Tenga en cuenta que cualquier documento que se envía a través de Internet puede caer en manos de terceros, por lo tanto, actúe de acuerdo a las políticas de confidencialidad de la empresa.

2.1.1.7 Responsabilidades de los administradores

Son responsabilidades de los administradores de las redes de datos de la Empresa LINEA S.A.S:

- Instalar y configurar apropiadamente los dispositivos de protección necesarios para que el acceso a Internet se realice siempre de forma segura.

- Velar siempre que el acceso a Internet se realice de forma segura.

- Instalar y configurar los servidores intermediarios (proxies) y software adicional necesario que permita controlar el uso de la conexión a Internet.

- Realizar pruebas que demuestren que las redes de datos institucionales se encuentran seguras, protegidas de accesos remotos no autorizados.

- Verificar que la conexión a Internet se utilice de acuerdo a lo contratado con los proveedores del servicio de Internet.

- Por seguridad, el Administrador no debe conectarse a Internet desde cuentas privilegiadas para llevar a cabo actividades que pueden efectuarse desde cuentas no privilegiadas de usuarios, tales como consultar páginas web, acceder a un servidor FTP, etc.

2.1.1.8 Responsabilidades de los usuarios

Los usuarios son responsables por:

Es responsabilidad de cada usuario utilizar los recursos informáticos en forma apropiada, de la manera detallada descrita, en beneficio de los intereses de la empresa.

Cada usuario es responsable de leer, documentarse y comprender está y demás políticas informáticas institucionales, para darles cabal cumplimiento.

- Seguir las políticas de seguridad y procedimientos para su uso de los servicios de Internet y, abstenerse de cualquier práctica que podría poner en peligro los sistemas de cómputo, la información o los datos de la Empresa.

- Verificar que el software antivirus institucional se encuentre en ejecución y vigilante en forma permanente.

- Familiarizarse con cualquier requisito necesario para acceder, proteger y utilizar datos, incluyendo materiales protegidos por Leyes de Privacidad, materiales con Copyright y obtención de datos confidenciales.

- Como funcionarios públicos, actuar de tal forma que siempre se refleje positivamente sobre la Empresa.

2.1.1.9 Correo electrónico

- No está permitido el envío de datos o información confidencial no autorizados vía Internet.

- Cuando necesite enviar información confidencial por correo electrónico vía Internet, considere comunicarla por teléfono o por correo normal.

- Las cuentas de correo electrónico que se asignan a los usuarios son exclusivamente para uso oficial, salvo el envío o recepción eventual de mensajes breves de sólo texto.

- La lista global de direcciones debe ser creada con los nombres y los dos apellidos de las personas, y los correos deben tener una estructura estandarizada en su creación.

- Cuando una persona deje de trabajar en la empresa, la cuenta de correo de esta persona debe ser bloqueada inmediatamente y deshabilitada en un tiempo máximo de 1 mes; no sin antes realizar un respaldo de la misma.

- Está prohibido abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, ya que pueden contener virus u otros códigos dañinos.

- Todo usuario debe supervisar que el software antivirus institucional siempre se encuentre en ejecución permanente, para minimizar los riesgos de activación de virus ya sea al enviar o al revisar el correo recibido.

- No está permitido que los usuarios compartan sus contraseñas de sus cuentas de correo.

2.1.1.10 Privacidad y supervisión

La empresa LINEA S.A.S, se reserva el derecho de revisar los archivos de correo electrónico de los usuarios en cualquier momento, ya sea para verificar el cumplimiento de las políticas Institucionales, por razones de seguridad, por razones técnicas o para otros propósitos legítimos de la Empresa.

En particular, la privacidad no se puede garantizar dado que, en el cumplimiento de su deber, los administradores de los sistemas de correo pueden necesitar supervisar las transmisiones u ocasionalmente observar los contenidos de los mensajes de correo de los usuarios.

Por otro lado, por la naturaleza excepcional de la información electrónica, los usuarios no deberían tener expectativas de privacidad.

2.1.1.11 Responsabilidades de los usuarios frente al uso del correo electrónico.

Es deber y responsabilidad de todos los usuarios utilizar en forma apropiada el servicio de correo electrónico proporcionado por la empresa para el cumplimiento de su deber. En particular, observar los debidos cuidados en la selección y manejo de contraseñas, no dejar sesiones de trabajo abiertas y otras precauciones y conductas que impidan usos indebidos de terceras personas.

2.1.1.12 Responsabilidad de los administradores de los sistemas de correo.

- Actuar de manera ética cuando en el cumplimento de sus deberes necesiten mirar los correos de los usuarios, por ejemplo, inspeccionando al nivel menos invasivo posible.

- Responder a los correos de los usuarios en forma apropiada y oportuna.

- No deben borrar ningún archivo de usuario que se encuentre almacenado en los sistemas de cómputo al servicio de la Empresa sin el permiso de su propietario, a menos que la presencia del archivo interfiera con la operación del sistema.

- Pueden por razones de seguridad o por usos inaceptables, deshabilitar temporalmente las cuentas de correo de los usuarios.

2.1.1.13 Las responsabilidades y deberes de los administradores de sistemas informáticos de la empresa LINEA S.A.S.

- Orientar y configurar los sistemas que administran de tal forma que en cualquier momento se pueda identificar a los usuarios que acceden o usan un determinado recurso informático.

- Realizar revisiones periódicas a los computadores personales y estaciones de trabajo de los usuarios que se encuentren bajo su cuidado, para verificar que solamente se esté utilizando en ellos software legal autorizado y que el uso que se les da a estos equipos esté acorde a las políticas institucionales.

2.2. PROCEDIMIENTOS DE AUDITORIAS INTERNAS.

2.2.1 Objetivo. Definir el alcance de los procedimientos para las auditorías internas

2.2.2 Ámbito. Se incluye los sistemas de gestión de la seguridad organizacional donde el responsable es el analista de seguridad de la información organizacional.

2.2.3 Planificación. Las auditorías internas se deben realizar por lo menos una vez al año, el equipo auditor debe ser independiente de las áreas que va auditar, debe contar con el acompañamiento del analista de la seguridad de la información organizacional y con el apoyo de la alta dirección. Se debe verificar por etapas y lapsus de tiempo la revisión de las políticas y controles implementados.

Se debe realizar auditorías de caja negra sin conocimiento de los procesos que se requieran auditar y otras de caja blanca donde el auditor tiene información suministrada por el equipo de seguridad de la organización

Las auditorías internas deberán comprobar la efectividad y madurez de los controles, objetivos y políticas de seguridad; comprobar las debilidades de seguridad y fortalecer al equipo de seguridad de la información sobre las mejoras posibles para evitar riegos frente amenazas.

Se debe otorgar a los administradores de la seguridad de la información sobre los mecanismos de seguridad implementados son adecuados o no, aspectos a mejorar, identificación y control de amenazas.

Los auditores deben plasmar en una acta la planificación detallada de las auditorías que se van a realizar durante el año para que la dirección de la organización pueda llevar seguimiento de igual manera para futuras auditorias planear los procedimientos a seguir.

2.2.4 Responsables:

Dirección General de la organización.

- Responsable de la aprobar el programa de auditorías internas.

Representante de la dirección.

- Conocer el procedimiento de auditorías Internas
- Revisión del plan de Auditorías;
- Actualizaciones del plan de auditorias
- Revisión de informes de las auditorias por la dirección general de la empresa.

Responsable de Seguridad de la Información

- Elaboración y actualización del procedimiento de auditorías internas
- Planificación de las auditorías internas
- Revisión de los informes de las Auditorías Internas
- Determinación de medidas para acometer las no conformidades

2.2.5 Equipo Auditor

- Ser independientes de las áreas que va auditar.
- Firmar acuerdos de confidencialidad sobre la información sensible suministrada.
- Formación de los auditores:
- Profesional en informática o áreas afines
- Profesional con certificaciones comprobadas en ISO 27001:2013 con sólidos conocimientos en implementación de un SGSI.
- Formación para realizar auditorías internas
- Experiencia mínima de 1 año sobre auditorías internas
- Persona con conocimiento de la organización auditar
- Capacidad para comunicarse y hablar en público
- Capacidad para elaborar y preparar informes
- Ser imparcial y responsable.
- Capacidad y habilidad para verificar registros y datos
- Persona con compromiso con el desarrollo y ejecución de las actividades establecidas para el SGSI organizacional.

2.2.6 Programación

El responsable de la seguridad de la información organizacional debe fijar acuerdos con las áreas que se van a intervenir y con el equipo auditor para acordar el cronograma de actividades y fechas en que se va a desarrollar los procedimientos de la auditoria.

Se debe fijar un instructivo que indique:

- Fechas y hora de auditoria
- Áreas a intervenir
- Tipos de procesos a evaluar
- Fijación del tipo de solicitudes
- Tiempo para la auditoria.

El auditor o equipo auditor debe llevar lo necesario para el desarrollo de las labores como: formulario, documentos de soporte, entre otros.

El equipo auditor debe realizar:

- Revisiones de documentación
- El responsable de seguridad de información y las áreas auditadas deben suministrar la información necesaria para cumplimiento de las labores.
- Preparación de la auditoria interna
- Socialización del programa de auditoria interna con suficiente tiempo de antelación para que sea revisado por la dirección general de la empresa y por las áreas a intervenir.

2.2.7 Ejecución

- Auditoria de las áreas en fechas acordadas
- Realización de reunión de apertura con la dirección general y áreas a intervenir.
- Socialización del tipo de auditoria y procedimientos a realizar.
- Apoyo del personal de la organización para que colaboren con los procedimientos de auditoria y con la información solicitada.
- Los auditores deben ser claros con los procedimientos.

- Los auditores deberán entregar informe técnico para el personal de TI y uno ejecutivo para la alta dirección y el resto del personal auditado.
- Fijar reunión de cierre y socialización de resultados.

Cuando el equipo Auditor considere finalizada su tarea, deberá presentar un Informe con los resultados obtenidos de la auditoría. El informe deberá incluir:

- Nombre del equipo auditor y/o auditor líder
- Fecha de la auditoría
- Procesos auditados
- Responsables de las actividades o procesos
- Objetivos, alcances y criterios
- Hora de inicio y duración de la auditoría
- Hallazgos y no conformidades encontradas
- Oportunidades de mejora
- Requerimiento de acciones correctivas.
- Nombre, cargo y firma de la persona responsable del auditado
- Firma de los Auditores

El informe de auditoría debe emitirse en un plazo máximo de cinco días hábiles después de su ejecución. Dirección debe exigir la entrega de este informe.

2.3 GESTIÓN DE INDICADORES

Los indicadores se determinan a partir de los controles seleccionados de cada dominio de la norma ISO 27001:2013, se elabora una tabla de Excel donde se define el tipo de dominio, métrica asociada, y etapa de medición.

Se define las siguientes consideraciones para el valor umbral:

Color	%Umbral	Descripción
Amarillo	75% o más	Cumple meta
Rojo	Menos de 45%	No cumple meta
Verde	De 45% o menos 75%	Cumple meta a término medio

Tabla 1. Valor umbral para los indicadores

El valor umbral es un valor que permite la toma de decisiones cuando una meta frente a un indicador no se cumple o para indicar que también estamos en el cumplimiento de los controles.

Ver Anexo 3. Gestión de indicadores.xls

2.4 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN.

La dirección de la organización LINEA S.AS. Tendrá como compromiso la revisión del sistema de gestión de la seguridad de la información a intervalos planificados para medir la conveniencia, la adecuación y la eficacia de mejora continua.

A continuación se relaciona procedimiento:

Fecha	**Tipo de revisiones**	**Estado de las revisiones**	**Consideraciones externas**	**Consideraciones internas**

Retroalimentación				
No conformidades	**Acciones correctivas**	**Seguimiento**	**Resultados**	**Cumplimiento de objetivos**
Retroalimentación de partes interesadas				
Valoración de riesgos	**Estado plan de tratamiento de riesgo**	**Oportunidades de mejora continua**	**Decisiones**	**Conclusiones**

Las reuniones se realizaran en las instalaciones de la empresa LINEA S.AS, se acordará fecha y hora de reunión para socialización del sistema de gestión de la seguridad, la reunión no podrá exceder de 2 horas, el informe debe ser puntual y concreto en relación con el objeto de los servicios acordados relacionados con los lineamientos de la política de seguridad de la información organizacional y el alcance del SGSI pactado. Las

2.4.1 FICHA DE PROCESO

RECURSOS	DESCRIPCIÓN	RESPONSABLE
Instalaciones de la empresa, recursos humanos y económicos.	Se establece acuerdos por parte de la dirección general de la empresa sobre el proceso de implementación del SGSI.	Gerente general de la organización, responsable de la seguridad de la información, responsable de las áreas auditadas.
Entradas	**Interacciones**	**Salidas**
Amenazas en los sistemas cliente y servidores de aplicaciones. Resultados de las actividades de análisis y tratamiento de riesgos.. Conocimientos de técnicas y productos de seguridad. Resultados de auditorias Cambios que puedan afectar los sistemas Catálogos de productos y servicios de seguridad. Procedimientos de mejora continua. Indicadores de procesos y servicios.	Procedimientos para la mejora continua. Supervisión de cumplimiento de las auditorías internas. Proceso de monitorización, evaluación y resultados.	Actas de reuniones Disponibilidad de recursos Objetivos para los indicadores Destinación de tiempos y recursos humanos. Evaluación de actividades y procesos. Relación de programas de seguridad.
Indicadores	**Riesgos**	**Documentos**
Cumplimiento con los requerimientos del SGSI. Resultados del SGSI Adaptación de las políticas y objetivos del SGSI a la organización.	Incumplimiento del alcance del SGSI. SGSI no cumpla con la exigencias de gobierno en línea Los resultados no sean los esperados por malos procedimientos para evaluar la situación actual de la organización. Auditores irresponsables con bajos criterios para orientar los procesos de la organización.	Informe final del SGSI Actas de reuniones Contratos Pólizas de cumplimiento Documentación de auditores.

Tabla 2. Procedimiento de revisión por la dirección.

Se expone las consideraciones que deben ser revisadas por la dirección para el cumplimiento del alcance planteado en el SGSI.

2.5 Composición del Comité de Seguridad de la información.

- **Gerente administrativo y financiero. E**ncargado de tomar las decisiones, asignar recursos, establecer las tareas a cada dependencia de acuerdo al rol y credenciales que tenga dentro de la organización.

- **Responsable de la seguridad de la información o Profesional analista de sistemas de información** los cuales deben de presidir dicho comité puesto que son las personas que realmente manejan el tema sobre seguridad de la información.

- **Responsable de Informática.** encargado de administrar la plataforma tecnológica**.** Muchas de las decisiones que se puedan dar van de la mano con el desarrollo de las tecnologías dentro de la organización y porque realmente son muy pocos los procesos manuales.

- **Responsable de Seguridad Física del edificio, y asuntos generales.** Se entrega la responsabilidad a los jefes administradores de los parques.

- **Responsable del Departamento Jurídico.** Es el encargado de aplicar la ley en todos los procesos legales de la empresa y de defender los intereses y bienes de la misma.

- **Responsable de Calidad**. Es el líder encargado de llevar una continuidad de mejora y cumplimento de los procesos de acuerdo a los lineamientos del sistema de gestión de la calidad ISO 9001 de la organización y de los procesos requeridos para el sistema de gestión de la seguridad de la organización SGSI.

- **Líderes de las áreas de negocio** (**directores o gerentes de cada dependencia). L**a seguridad de la información organizacional, es un tema de todas las personas que hacen parte de una organización. Por tanto es indispensable los líderes de cada dependencia comprendan como es el beneficio y uso de medidas de control en cada una de las áreas, donde ellos mismos aprenden aportar ideas para mejorar los controles y las medidas de seguridad que se generen para la organización.

  Es imprescindible que en el Comité de Seguridad se encuentre personal del Comité de Dirección. De esta forma se garantizará el apoyo directo de la Dirección.

Roles

- RESPONSABLE: Gerente General, Gerente Administrativo y Financiero
- LÍDER: Jefe Unidad de Sistemas.
- EJECUTORES: Profesional analista de sistemas de información, Profesional administrativo, técnico administrativo, Auxiliar Administrativo y practicante (según disponibilidad).

2.6 Declaración de la aplicabilidad

Se realiza una verificación de los controles para determinar si aplica o no aplica para alcanzar los objetivos propuestos para el SGSI de LINEA S.A.S.

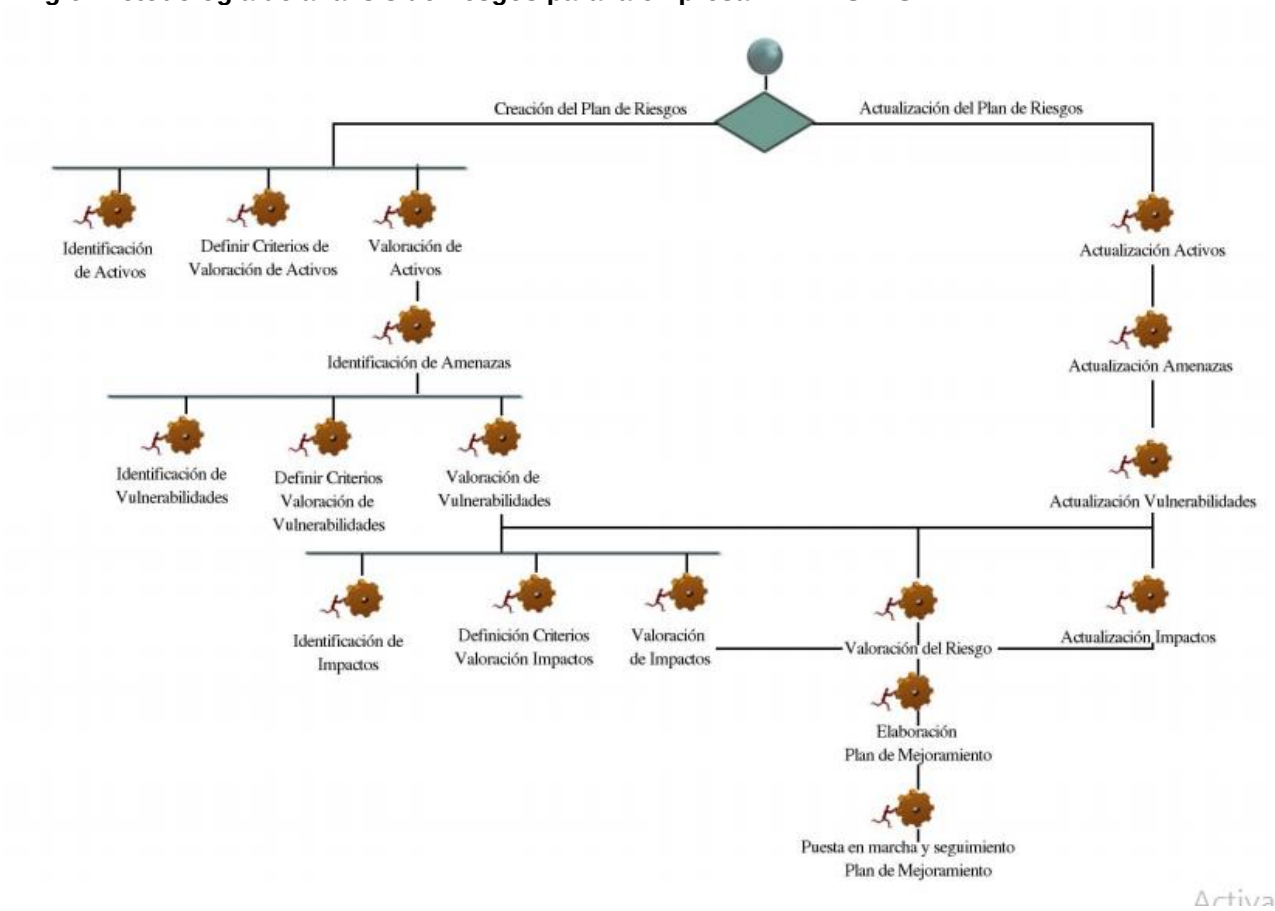
Ver Anexo 4. Declaración de la aplicabilidad.xls

2.7 Metodología de análisis de riesgos

Se define la metodología de análisis y gestión de riesgos Magerit, la cual es una metodología elaborada por el Consejo Superior de Administración Electrónica español, para dar respuesta al análisis de riesgos que pueden generar las tecnologías de la información organizacional. Por tanto, se pretende aplicar de acuerdo a los controles a implementar en la empresa LINEA S.A.S para el tratamiento de riesgos por amenazas.

Se va utilizar la metodología de riesgos Magerit, las etapas a desarrollar serán:

[3]Img 6. Metodología de análisis de riesgos para la empresa LINEA S.A.S



[3] http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

2.7.1 Identificación de Activos. Permite la gestión de riesgos organizacional. Los activos a proteger han de tener asignado un propietario en la compañía. A cada propietario de los activos debe tener unas medidas para tratamiento de los riegos.

Los tipos de activos identificables para el análisis de riesgos:

- **Físicos**: Activos de Hardware como: ordenadores, teléfonos móviles, Tablets, Impresoras, entre otros.
- **Lógicos**: Activos de software, como los sistemas operativos, utilidades, instalación de aplicaciones de terceros, entre otros.
- Personas: Personal de la organización, proveedores, visitantes.
- **Entorno e Infraestructura**: Elementos de la infraestructura tecnológica, red de datos, red eléctrica, entre otros.
- **Intangibles:** Elementos no materiales de la organización (confianza de los clientes, experiencia, "know-how" entre otros).
- **Los datos que se manejan**: especificaciones y documentación de los sistemas, código fuente, manuales del operador y del usuario, datos de prueba.

2.7.2 Identificación de amenazas. Son asociadas a los activos una vez se haya detectado los activos importante en la empresa LINEA S.A.S, se debe iniciar la respectiva identificación de la amenazas a los que están expuestos los sistemas de información en especial las identificadas en el servidor ICG de la compañía

Relación a seguir: Activo – Amenaza

La identificación de amenazas se analiza con los siguientes criterios:

- Perdida de continuidad de servicios de red, ICG, alteración de bases de datos SQL, intrusiones a sistemas por salto de privilegios por usuarios mal intencionados.
- Requerimientos legales, contractuales de la organización, las soluciones realizadas e implementadas, entre otros.
- Hallazgos de amenazas en sistemas de información.
- Servidores de puntos de venta ICG afectados por virus informáticos.
- Identificación y tratamiento de amenazas por el personal de TI.
- Socialización de riesgos de la información al personal de la organización.
- Programas de sensibilización y concienciación sobre el valor y cuidado de la información.

Registro de Riesgos: Identificación de amenazas

Se registrarán todos aquellos riesgos que tengan una probabilidad no nula de ocurrir en el período de un año y que, de materializarse, tendrían un efecto negativo en activos de información de la organización.

El registro de riesgos se hará en el documento "Mapa de riesgos" que está bajo la responsabilidad del Responsable de Seguridad de la Información y con el soporte de la persona o personas que hubieran identificado la vulnerabilidad.

En el momento del registro de riesgos se identificarán:

- Activo o tipo de activo afectado y su propietario
- Vulnerabilidad del activo
- Amenazas que pueden explotar la vulnerabilidades
- Probabilidad o frecuencia con la que las amenazas podrían materializarse
- Impacto esperado en caso de materializarse la amenaza
- Alternativas de tratamiento de los riesgos.

Importante analizar otros criterios de riesgo cuando una amenaza llegue a materializarse.

2.7.3 Valoración de activos. Se define criterio para otorgar a los activos un valor que puede ser cualitativo, cuantitativo o ambos.

[4]Valoración Cualitativa:

Escala de valoración	Valor	Descripción
MB: Muy bajo	1	No importante en los procesos prácticos
B: Bajo	2	Importancia menor
M: Medio	3	Importante para el proyecto
A: Alto	4	Altamente importante para el proyecto
MA: Muy alto	5	Muy importante para el logro de objetivos del SGSI.

Tabla 3. Valoración cualitativa de los riesgos por amenazas

Valoración cuantitativa:

Escala de valoración	Escala cuantitativa	Descripción
Muy Alto = MA	5	$ 5.000.000
Alto = A	4	$ 3.001.000
Medio = M	3	$ 1.501.000
Bajo = B	2	$ 500.000
Muy Bajo = MB	1	$ 300.000

Tabla 4. Valoración cualitativa de los riesgos por amenazas

Si se toma en cuenta tanto la escala cuantitativa como cualitativa se deben promediar riegos haciendo relevancia en aquellos con valor mayor a 3

2.7.4 Identificación y valoración de las Vulnerabilidades. Se identifican las amenazas y se valoran de acuerdo a la frecuencia de ocurrencia.

FRECUENCIA / ARO (Annualized Rate of Occurrence)			
EF	0,9973	Extremadamente frecuente	Menos que 1 día
MF	0,1425	Muy Frecuente	Menos que 1 semana
F	0,0329	Frecuente	Menos que un mes
FN	0,0055	Frecuencia Normal	Menos que medio año
PF	0,0027	Poco Frecuente	Menos que un año
EPF	0,0003	Extremadamente Poco Frecuente	Menos que diez años

Tabla 5. Frecuencia de ocurrencia de amenazas.

La forma como se realiza el cálculo es de la siguiente manera:

Ejemplo:
Si tengo la frecuencia de que ocurra una vulnerabilidad 1 vez cada semana y partiendo de que el año tiene 52 semanas, entonces el cálculo sería: número de semanas/número de días año 52/365=0,142465

La relación a considerar es: Activo-amenaza-vulnerabilidad-valoración-probabilidad de ocurrencia

Sirve para estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

[4] http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

2.7.5 [5]Identificación y valoración de impactos. La organización valora los impactos frente amenaza de acuerdo a los siguientes criterios:

IMPACTO						
TÉCNICOS					ORGANIZACIONALES	
Pérdida de confidencialidad	Pérdida de integridad	Pérdida de disponibilidad	Trazabilidad	Autenticidad	Pérdidas económicas	Pérdida de imagen

Calificación de los daños

5	Muy alto **(MA)**	Daño muy grave para el proyecto
4	Alto **(A)**	Daño grave al proyecto
3	Medio **(M)**	Daño importante al proyecto
2	Bajo **(B)**	Daño menor al proyecto
1	Muy Bajo **(MB)**	Daño despreciable

Tabla 6. Calificación de los daños generados por los riegos.

2.7.5.1 Criterios para evaluar los impactos por activo. Se otorga un nivel de daño o riesgo que puede causar una amenaza en un activo, para ello se determina una escala de degradación del activo, los valores para determinar la disminución de los impactos y de las vulnerabilidades representadas por una amenaza.

IMPACTO / EF (Exposure Factor)

C	Crítico	90%	90% de degradación
A	Alto	75%	75% de degradación
M	Medio	50%	50% de degradación
B	Bajo	20%	20% de degradación

DISMINUCIÓN DEL IMPACTO

MA	Alta	90%
A	Media	60%
M	Baja	30%
B	Nula	0%

DISMINUCIÓN DE LA VULNERABILIDAD

MA	Alta	90%
A	Media	60%
M	Baja	30%
B	Nula	0%

Tabla 7. Valores para los impactos a considerar para evaluar los riesgos.

[5] http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

Fase 3: Análisis de Riesgos. Se verifican, valoran los activos de la organización LIENA S.AS se procede a buscar los riesgos asociados a causa de una amenaza y sus impactos.

3.1 Inventario de activos

					Categoría						
Id	**Activo**	Responsable	Criticidad	Valoración	Físicos	Lógicos	Entorno e infraestructura	Datos	Personal	**Servicios**	**Misión**
AC-1	Gerencia general	Junta directiva de la organización	MA	5					X	Encargado de dirigir y asignar recursos para el funcionamiento de la organización.	Presidir reuniones del consejo directivo y tomar decisiones.
AC-2	Personal administrativo y financiero	Gerente administrativo y financiero	A	4					x	Gestiona, aprueba y asigna los recursos para el funcionamiento de la organización.	Verificar y controlar el estado de las finanzas de la organización
AC-3	Secretaria General	Gerente General	A	4					x	Verifica la contratación y controla los gastos e inversiones de la organización	Vigilar que los estados financieros de la organización se realicen de forma correcta conforme la ley y estatutos organizacionales.
AC-4	Personal de control interno	Jefe de control interno	A	4					X	Controla y verifica que los funcionarios de la organización cumplan con sus funciones de forma correcta.	Controlar e intervenir en los procedimientos legales de la empresa y en las diferentes áreas de gestión administrativa.
AC-5	Personal de comunicaciones, mercadeo y logístico	Jefe de comunicaciones	A	4					X	Encargada de los medios audiovisuales y comunicaciones, imagen corporativa de la empresa, realización de eventos y comercio para la empresa.	Proyectar y vender la imagen corporativa.
AC-6	Personal de TI	Jefe de sistemas	MA	5					x	Gestiona y garantiza la seguridad de la información y el funcionamiento de la infraestructura de TI.	Garantizar la seguridad de la información y el funcionamiento de los recursos TIC.

AC-7	Personal de operaciones	Jefe de mantenimiento	MA	5					x	Responsable del mantenimiento de los parques y operaciones de las atracciones.	Garantizar la disponibilidad de los servicios a los clientes de la empresa.
AC-8	Servidor de backup	Analista de seguridad de la información	A	4	X					Equipo con Windows 2008 server r2, aplicación Symantec para backups	Permite salvaguardar información sensible de bases de datos y de usuarios críticos.
AC-9	Servidor de antivirus	Analista de seguridad de la información	A	4	X					Equipo con Windows 2008 server y software antivirus MCAFEE	Permite el control de software malicioso.
AC-10	Servidor de desarrollo	Desarrollador de aplicaciones	A	4	X					Equipo para probar desarrollos de aplicaciones nuevas	Permitir el ensayo previo de nuevas instalaciones de aplicaciones.
AC-11	Servidor ICG	Encargado de la infraestructura	A	4	X					Permite el recaudo financiero de las ventas	Servidor para la administración financiera de los datos ICG.
AC-12	Servidor SICOF	Encargado de la infraestructura	MA	5	X					Permite la gestión de las finanzas de la organización.	Ayudar a los procedimientos financieros de la organización.
AC-13	Servidor DOCUMENT	Encargado de la infraestructura	A	4	X					Permite la gestión documental de la empresa para todos los procesos.	Contribuir a la documentación digital del archivo y agilidad en los procedimientos organizacionales.
AC-14	Servidor de virtualización	Encargado de la infraestructura	MA	5	X					Dispositivo de hardware que integra todas las máquinas virtuales con ayuda de la aplicación de virtualización hyper-v	Contribuir a la virtualización de equipos de alto rendimiento para mejorar la escalabilidad, crecimiento y alta disponibilidad de los servicios.
AC-15	Servidor de directorio activo	Encargado de la infraestructura	A	4	X					Ayuda a la gestión de usuarios.	Mejorar los niveles de gestión de usuarios para control de roles y credenciales para operar los equipos informáticos
AC-16	Servidor AM	Encargado de la infraestructura	M	3	X					Servidor destinado para manejo de la aplicación AM de contracciones civiles y control de activos.	Permitir la gestión de activos por obras civiles en la aplicación AM.
AC-17	Servidor TIMESOFT	Encargado de la infraestructura	A	4	X					Servidor para control de acceso de empleados temporales	Ayudar a la gestión del control de usuarios temporales en los parques de la organización.

AC-18	Servidor de intranet	Encargado de la infraestructura	A	4	X					Permite la interacción de los procesos institucionales.	Agilizar la comunicación y la interacción con los procesos de la empresa y el sistema de calidad.
AC-19	Cuarto de telecomunicaciones	Encargado de la infraestructura	MA	5	X					Lugar para salvaguardar los sistemas de información de la empresa	Permitir la integración, la gestión y salvaguardar la información sensible.
AC-20	Swiches capa 2 y 3	Encargado de la infraestructura	A	4	X					Permiten el direccionamiento del tráfico de red	Permitir la gestión de servicios de red.
AC-21	FIREWALL	Analista de seguridad de la información	MA	5	X					Permite el control de tráfico de la red.	Gestionar la seguridad de la red y permisos a nivel de rol de usuario.
AC-22	Equipos pos ICG	Encargado de la infraestructura	A	4	X					Hardware destinado para las recaudo y registro de ventas	Permitir la gestión financiera en puntos de venta.
AC-23	Datafonos	Personal de soporte técnico	A	4	X					Permitir pagos por transacciones electrónicas	Manejar los pagos electrónicos de clientes.
AC-24	Computadores portátiles y de escritorio	Personal de soporte técnico	MA	5	X					Contribuye al de desarrollo y construcción de la información organizacional por procesos.	Permitir por rol de usuario procesar, guardar y salva guardar la información sensible de la organización.
AC-25	Tablets	Personal de soporte técnico	M	3	X					Acceso a Internet a usuarios invitados	Permitir la interacción de usuarios invitados a la red de internet para el registro de tareas y navegación entre aplicaciones de internet.
AC-26	Celulares	Personal de soporte técnico	A	4	X					Recepción y realización de llamadas de voz, chat y mail para gestión de proyectos de la empresa.	Permitir el vínculo de clientes a los negocios de la empresa y la comunicación organizacional.
AC-27	Memorias usb, sd	Personal de soporte técnico	A	4	X					Son importante para la portación de información	Permitir el acceso a la información.
AC-28	Discos duros	Personal de soporte técnico	MA	5	X					Almacenar la información de los usuarios.	Permitir salvaguardar la información
AC-29	Almacenamiento SAN	Encargado de la infraestructura	MA	5	X					Gestionar la alta escalabilidad de los recursos de almacenamiento y servicios para servidores.	Escalar el rendimiento de los servicios por los servidores activos para las labores y cumplimiento de los procesos de la empresa.

AC-30	Now How	Gerente general	MA	5				X		Conocimiento de servicios de diversión y alegría para chicos y grandes mediante simuladores 7D, 4D, 5D, atracciones mecánicas, zona acuática, eventos y logística, mercadeo.	Conocimiento y estrategias para el comercio de servicios de diversión y recreación.
AC-31	Documentos financieros	Gerencia administrativa y financiera	MA	5				x		Evidencia la información de los estados de las finanzas por las negociaciones, inversiones, gastos y cuentas por cobrar.	Permitir los registros de las finanzas corporativas.
AC-32	Documentos del archivo	Jefe del archivo	MA	5				X		Registro de toda la información de la empresa	Permitir guardar las evidencias de la información procesada de empleados, clientes, proveedores y de todos los demás procesos.
AC-33	Documentos del sistema de calidad ISO 9001	Jefe de calidad	A	4				X		Se registra la gestión de los procedimientos y procesos de calidad por dependencia para cumplimiento de la norma.	Auditar los procesos de la compañía para cumplir con el estándar de calidad ISO 9001.
AC-34	Documentos del área de mercadeo y logística.	Gerencia de mercadeo y logística	A	4				X		Registro de la gestión de mercados para el comercio de servicios de recreación y logística de eventos.	Registrar los negocios para cumplimiento de metas y trazabilidad de los procesos.
AC-35	Documentos del área de sistemas	Jefe de sistemas	MA	5				X		Evidencia de información de los sistemas.	Salvaguardar el registro de evidencias de operación y uso de la red y seguridad informática para los procesos de la empresa.
AC-36	Documentos de registro de operaciones de las atracciones mecánicas y acuáticas.	Jefe de mantenimiento	MA	5				X		Información sensible de las operaciones en los parques de recreación.	Salvaguardar el registro de operación para el control de procesos.
AC-37	Manuales de operaciones de redes y seguridad de la información	Jefe de sistemas y analista de la seguridad de los sistemas de información.	MA	5				X		Gestión de procedimientos y seguridad de los sistemas de información.	Gestionar la confidencialidad, la integridad y disponibilidad de la información organizacional.

AC-38	Registro de logs de sistemas y claves de seguridad de la información.	Analista de seguridad de la información	MA	5				X		Procesamiento de información sensible para uso de administradores de TI.	Permitir información sensible para la gestión de TI por administradores del sistema.
AC-39	Sistema de seguridad perimetral	Analista de seguridad de la información	A	4	X					Control de acceso	Impedir los accesos no autorizados a los sistemas de información y áreas restringidas.
AC-40	Planta de teléfono	Personal de soporte técnico	A	4	X					Registro las comunicaciones por voz	Permitir la comunicación para la gestión de procesos.
AC-41	Red eléctrica	Jefe de mantenimiento	A	4			X			Suministro de energía eléctrica para los sistemas de información y para la infraestructura organizacional.	Permitir el fluido eléctrico para los equipos y sistemas de información en las diferentes dependencias de la empresa.
AC-42	Cableado estructurado vertical y horizontal	Personal de soporte técnico	A	4			X			Permite la conectividad a la red de datos.	Brindar conectividad a los depósitos de red.
AC-43	Puesto de trabajo	Personal de soporte técnico	M	3			X			Destino de los lugares de trabajo para cada rol de usuario.	Garantizar puestos de trabajo para cada funcionario de la empresa.
AC-44	Aplicación documental	Jefe de archivo	A	4		X				Permite la gestión documental de la empresa.	Garantizar la trazabilidad, disponibilidad, integridad y confidencialidad de la información organizacional.
AC-45	Software financiero	Jefe de sistemas	MA	5		X				Gestión y control de las finanzas.	Permitir la gestión administrativa y control de las finanzas.
AC-46	Software para ventas ICG	Jefe de sistemas	A	4		X				Ayuda al control de operaciones y registros de ventas para el recaudo financiero.	Gestionar causaciones de las ventas.
AC-47	Software para el sistema de inventario	Jefe de sistemas	A	4		X				Ayuda al control y gestión de bienes.	Controlar y salvaguardar los bienes de la organización.
AC-48	Aplicación antivirus	Analista de seguridad de la información	A	4		X				Control y gestión de amenazas de software por intrusos o gestión de eventos por operaciones maliciosas en la red.	Garantizar la seguridad de la información en los equipos informáticos por amenazas de red y software malicioso o dañino.

AC-49	Sistemas operativos	Personal de soporte técnico	A	4		X				Ayuda al trabajo de los usuarios para ejecutar sus tareas y procesamiento de información.	Permitir el procesamiento de información.
AC-50	Aplicación web	Desarrollador de aplicaciones	A	4		X				Permitir la publicación de información.	Gestionar los niveles de servicios al público.
AC-51	Bases de datos	Desarrollador de aplicaciones	MA	5		X				Importa por su contenido y disponibilidad de información.	Permitir el almacenamiento y escalabilidad de los datos,

Tabla 8. Activos de la empresa LINEA S.AS

3.2 Dimensiones de seguridad de los activos. Se otorga un valor a cada activo y se dimensiona de acuerdo a la criticidad del activo para los sistemas de información de la organización.

[6]Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

3.2.1 [D] Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].

3.2.2 [I] Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].

3.2.3 [C] Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].

3.2.4 [T] Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

3.2.5 [A] Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

valor	criterio	
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Tabla 9. Valores asociados a las dimensiones de seguridad de la información.

[6] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VTwEUiF_Oko

Con los criterios asociados para dimensionar la seguridad de la empresa LINEA S.A.S se verifica el estado de seguridad de cada activo.

3.5 TABLA RESUMEN DE VALORACIÓN. A continuación de observa la evaluación de los pilares de la seguridad de la información para cada activo de la empresa LINEA S.A.S

Id	Activo	Criticidad	DIMENSIONES DE SEGURIDAD				
			C	D	I	T	A
AC-1	Gerente General de la organización	MA	5	10	0	10	10
AC-2	Personal administrativo y financiero	A	6	10	7	5	10
AC-3	Secretaria General	A	5	5	0	10	10
AC-4	Personal de control interno	A	10	10	5	10	8
AC-5	Personal de comunicaciones, mercadeo y logístico	A	3	4	6	9	10
AC-6	Personal de TI	MA	10	5	6	3	10
AC-7	Personal de operaciones	MA	10	6	5	9	9
AC-8	Servidor de backup	A	8	7	5	4	0
AC-9	Servidor de antivirus	A	2	10	8	5	10
AC-10	Servidor de desarrollo	A	5	0	10	2	10
AC-11	Servidor ICG	A	10	10	10	5	10
AC-12	Servidor SICOF	MA	10	7	10	10	10
AC-13	Servidor DOCUMENT	A	8	10	10	10	10
AC-14	Servidor de virtualización	MA	10	10	10	10	10
AC-15	Servidor de directorio activo	A	10	8	10	7	10
AC-16	Servidor AM	M	4	6	10	5	10
AC-17	Servidor TIMESOFT	A	10	10	10	7	10
AC-18	Servidor de intranet	A	0	10	8	3	10
AC-19	Cuarto de telecomunicaciones	MA	10	8	10	10	10
AC-20	Swiches capa 2 y 3	A	5	10	10	8	10
AC-21	FIREWALL	MA	8	10	10	10	10
AC-22	Equipos pos ICG	A	5	10	10	10	10
AC-23	Datafonos	A	9	5	10	10	10
AC-24	Computadores portátiles y de escritorio	MA	5	8	10	9	10
AC-25	Tablets	M	0	2	4	4	10
AC-26	Celulares	A	10	7	10	10	8
AC-27	Memorias usb, sd	A	3	5	10	3	7
AC-28	Discos duros	MA	9	7	10	10	10
AC-29	Almacenamiento SAN	MA	10	10	10	10	10
AC-30	Now How	MA	10	10	10	8	10

AC-31	Documentos financieros	MA	6	8	10	10	10
AC-32	Documentos del archivo	MA	3	10	10	10	10
AC-33	Documentos del sistema de calidad ISO 9001	A	4	7	10	8	10
AC-34	Documentos del área de mercadeo y logística.	A	4	10	10	6	10
AC-35	Documentos del área de sistemas	MA	7	8	10	10	10
AC-36	Documentos de registro de operaciones de las atracciones mecánicas y acuáticas.	MA	10	7	10	10	10
AC-37	Manuales de operaciones de redes y seguridad de la información	MA	10	7	10	10	10
AC-38	Registro de logs de sistemas y claves de seguridad de la información.	MA	10	8	10	10	10
AC-39	Sistema de seguridad perimetral	A	7	8	10	10	10
AC-40	Planta de teléfono	A	4	9	8	6	8
AC-41	Red eléctrica	A	6	10	10	7	10
AC-42	Cableado estructurado vertical y horizontal	A	2	10	10	4	10
AC-43	Puesto de trabajo	M	0	7	9	4	8
AC-44	Aplicación documental (document)	A	8	10	10	10	10
AC-45	Software financiero SICOF	MA	10	10	10	10	10
AC-46	Software para ventas ICG	A	9	10	10	10	10
AC-47	Software para el sistema de inventario AM	A	6	8	10	8	10
AC-48	Aplicación antivirus MCAFEE	A	8	10	10	10	10
AC-49	Sistemas operativos WINDOWS	A	7	8	10	9	10
AC-50	Aplicación web JOOMLA	A	8	9	10	10	10
AC-50	Información almacenada base de datos	MA	10	10	10	10	10

Tabla 10. Dimensiones de la seguridad de la información por activo

3.6 Análisis de amenazas. Se presenta a continuación un catálogo de amenazas posibles según Magerit sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

.

Las amenazas se pueden clasificar de acuerdo a los siguientes criterios establecidos por Magerit:

Nº	Amenazas		Descripción
1	AM-01	Incendio	Posibilidad de que el fuego queme las instalaciones de la infraestructura tecnológica y otras dependencias de la empresa LINEA S.A.S
2	AM-02	Desastre natural	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, entre otros. Pudiendo afectar zona de TI y funcionamiento de la empresa.
3	AM-03	Ataque físico	Vandalismo, terrorismo, acción militar, salto de privilegios en los sistemas.
4	AM-04	Fallo / avería de equipo	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema
5	AM-05	Avería climatización	Cuarto de TI expuesto a altas temperaturas pudiendo afectar las operaciones.
6	AM-06	Fallos suministro eléctrico	Alteración o ausencia del servicio eléctrico podría significar pérdidas importantes de productividad en la empresa y más aún si no existe una contingencia.
7	AM-07	Robo personal interno	Muchos usuarios roban las pertenencias o activos de otros usuarios y no hay un control sobre ello.
8	AM-08	Robo personas externas	Existe personas ajenas a la empresa que ingresan sin ser autorizados y roban activos importantes que afectan el now how de la empresa y la fuga no consentida de información.
9	AM-09	Ataque informático	La probabilidad de que un intruso o un usuario escalen privilegios para afectar la zona de TI y llevar acabo sus acciones desconocidas.
10	AM-10	Indisponibilidad física	La carencia de espacios para el personal genera pérdidas importantes de productividad y de ingresos para la empresa.
11	AM-11	Indisponibilidad lógica	Muchos espacios no están acondicionados por falta de asignación de recursos y de personal calificado para implementar los requerimientos.
12	AM-12	Indisponibilidad personal	La no disponibilidad de personal para las diferentes labores y actividades puede afectar significativamente la continuidad de los servicios de TI en la empresa y de otras labores por dependencias.
13	AM-13	Errores humanos	Los errores humanos en las operaciones sueles ser frecuentes, lo que genera alteración y detrimento patrimonial.
14	AM-14	Indisponibilidad de comunicaciones	Es frecuente que muchos sistemas de comunicaciones al tiempo actual no deberían operar por ser analógicos y por no soportar la demanda de usuarios actuales.
15	AM-15	Error de diseño	En comunicaciones y en planos de construcciones las adecuaciones y planeaciones no son adecuadas, lo que genera a futuro perdida en patrimonio.
16	AM-16	Acceso no autorizado a sistemas	No existen controles actos para hacer cumplir la política organizacional sobre control de usuarios a cuartos de TI.
17	AM-17	Divulgación no autorizada	No hay controles por actas de confidencialidad sobre información confidencial.
18	AM-18	Fallo en copias	Las copias de seguridad fallan por falta de almacenamiento y configuración adecuada de los agentes y credenciales de las bases de datos.
19	AM-19	Ingeniería inversa	Hay personal que trata de sacar información confidencial mediante técnicas de ingeniería social basas en la confianza de personas.
20	AM-20	Fallos de software	Son habituales por una mala parametrización, filtros para los accesos no adecuados y vulnerables ataques informáticos.
21	AM-21	Carencia de mantenimiento software	Las inspecciones y tratamiento técnico a los programas son pocos y no eficaces.
22	AM-22	Fallo en las comunicaciones	Las operaciones para comunicaciones son regular debidas que no se planea adecuadamente las inversiones y los diseños para las implementaciones.
23	AM-23	Eliminación no autorizada	Errores humanos en la manipulación de equipos, programas, e información.

24	AM-24	Pérdida de información	Evidente cuando se daña un servidor, existe un robo por un extraño o cuando hay un pare inesperado de los servicios de la empresa.
25	AM-25	Coacción	Existe personal obligado hacer cosas en contra su voluntad comprometiendo gravemente los intereses organizacionales.
26	AM-26	Extravío de documentos	Se puede perder fácilmente información de una dependencia no hay controles de accesos claros.
27	AM-27	Negligencia	La pereza y el desconocimiento de los procesos hacen que se alteren.
28	AM-28	Difusión a personas no autorizadas	Comentarios no adecuados a terceros que comprometen el now how organizacional.
29	AM-29	Manipulación de equipamiento	Manipulación no adecuada del equipamiento por desconocimiento o por capricho.

Tabla 11. Relación de amenazas

Ver Anexo 5, AnálisisDeRiesgos-Magerit.xls

El valor de riesgo intrínseco se calcula = valor del activo* frecuencia de ocurrencia de la amenaza* por el impacto que puede generar en caso de materializarse.
Riesgo intrínseco diario por activo= es la suma de todos los riesgos intrínsecos diarios por activo
Riesgo anual por activo= riesgo intrínseco diario por activo / números de días del año (365).
Riesgo diario por amenaza= suma de todos los riesgos diarios de cada activo por amenaza.
Riesgo intrínseco anual por amenaza= riesgo diario por amenaza* 365 días del año

3.7 Impacto potencial. Ver anexo 5, AnálisisDeRiesgos-Magerit.xls, donde se podrá observar el impacto potencial por amenazas que sobrepasen el 50% de degradación. Los valores del impacto potencial se pueden apreciar en la tabla **12.**

El impacto potencial representativo para la estimación de riesgos se relaciona en la siguiente tabla:

IMPACTO / EF (Exposure Factor)			
C	Crítico	90%	90% de degradación
A	Alto	75%	75% de degradación
M	Medio	50%	50% de degradación
B	Bajo	20%	20% de degradación

Tabla 12. Tabla de valores para evaluar impacto generado por amenazas.

El impacto potencial estimado para los riesgos de la empresa LINEA S.A.S va desde el valor 50% hasta 90%, siendo 50% un impacto moderado o medio sobre los activos de la empresa, 75% impacto alto y 90% muy alto. Todo depende qué tan representativo es el activo para la organización y qué tan riesgoso sería que le ocurran daños al activo. Por determinación planteada desde el nivel de riego aceptable por la dirección de la empresa, solo se tendrán en cuenta los efectos críticos medios, altos y muy altos de las amenazas sobre el activo.

3.7.1 [7]La degradación [del valor] de un activo. Cuando un activo es víctima de una amenaza, una parte de su valor se pierde. Intuitivamente, se habla de un "porcentaje de degradación del activo", de forma que se puede perder entre un 0% y un 100%.

[7] http://www.pilar-tools.com/magerit/v2/tech-es-v11.pdf

Para calcular el impacto potencial se tiene en cuenta el valor del activo y el % de degradación que puede tener frente a una amenaza considerada en la tabla 12**.**

3.8 Nivel de riesgo aceptable y riesgo residual

3.8.1 Valoración de riesgo aceptable

Se define el nivel de riesgo aceptable de acuerdo a los valores reflejados en Alto, medio, bajo, y nulo o despreciable, debido a los criterios establecidos por la dirección de la organización para mitigar las amenazas que puedan representar riesgos y pérdidas de valor importantes, donde interesa tratar los riesgos con probabilidad de ocurrencia muy altos; los demás niveles de riegos serán considerados como aceptables.

Impacto/Perdidas

Probabilidad		Leves	Moderadas	Graves
	Muy Alto (MA)	Alto	**Muy Alto**	**Muy Alto**
	Alta (A)	Medio	**Alto**	**Alto**
	Medio (M)	Bajo	Medio	Alto
	Baja (B)	Bajo	Bajo	Medio
	Nulo (N)	Null	Null	Null

VALORACIÓN DE ACTIVOS			
MA	$	5.000.000	Muy Alto
A	$	3.001.000	Alto
M	$	1.501.000	Medio
B	$	500.000	Bajo
MB	$	300.000	Muy Bajo

Tabla 13. Nivel de riesgo aceptable por la dirección.

Los riegos bajos son importantes tratar pero por falta de asignación de recursos, la alta dirección opta sólo por tratar riesgos en estado muy alto.

3.8.2 Riesgo residual. Es una medida del estado presente, entre la inseguridad potencial (sin Salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Según Magerit, dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores. Las salvaguardas seleccionadas permiten determinar cuán eficaces son frente al riesgo.

En el caso de la empresa **LINEA S.A.S**, el nivel de riesgo aceptable se determina por el **riesgo controlado diario por activo = Riesgo Intrínseco diario por activo – El riesgo efectivo diario por activo.**

3.8.2.1 Salvaguardas: Son medidas de aseguramiento que se tienen en cuenta para mitigar los riesgos por amenazas, estas salvaguardas por activo tienen un costo y otro valor por la cantidad de amenazas consideradas**.**

Cálculos:

3.8.2.1.2 Valor Salvaguarda por activo= valor cuantitativo de activo / número de activos considerados

3.8.2.1.3 Coste salvaguarda por amenaza= Valor Salvaguarda por activo / número de amenazas consideradas.

Para ello existen dos tipos fundamentales de controles de seguridad o salvaguardas:

3.8.2.1.4 Preventivas. Son aquellas medidas de seguridad que reducen las vulnerabilidades (La frecuencia de ocurrencia).

Nueva vulnerabilidad = Vulnerabilidad × Porcentaje de disminución de vulnerabilidad

3.8.2.1.5. Correctivas. Son aquellas medidas de seguridad que reducen el impacto de las amenazas.

Nuevo impacto = Impacto × Porcentaje de disminución de impacto

[8]La decisión entre realizar un análisis de riesgos intrínseco o residual depende de si una organización pretende analizar, si la inversión que ha realizado en seguridad ha sido la correcta o si, por el contrario, lo que pretende es estudiar la situación real en la que se encuentra. Lo más habitual es realizar el análisis de riesgos residual, puesto que, si una organización ya posee unas medidas de seguridad implantadas y pretende mejorar su seguridad, deberá contemplar estas soluciones teniendo en cuenta la situación actual en la que se encuentra, ya que, aunque la inversión no haya sido la correcta, no podrá recuperarla.

En este caso la empresa tiene unos controles implementados y otros no implementados, por tanto se analiza los riesgos intrínsecos y el riesgo residual de los activos, ver img 8

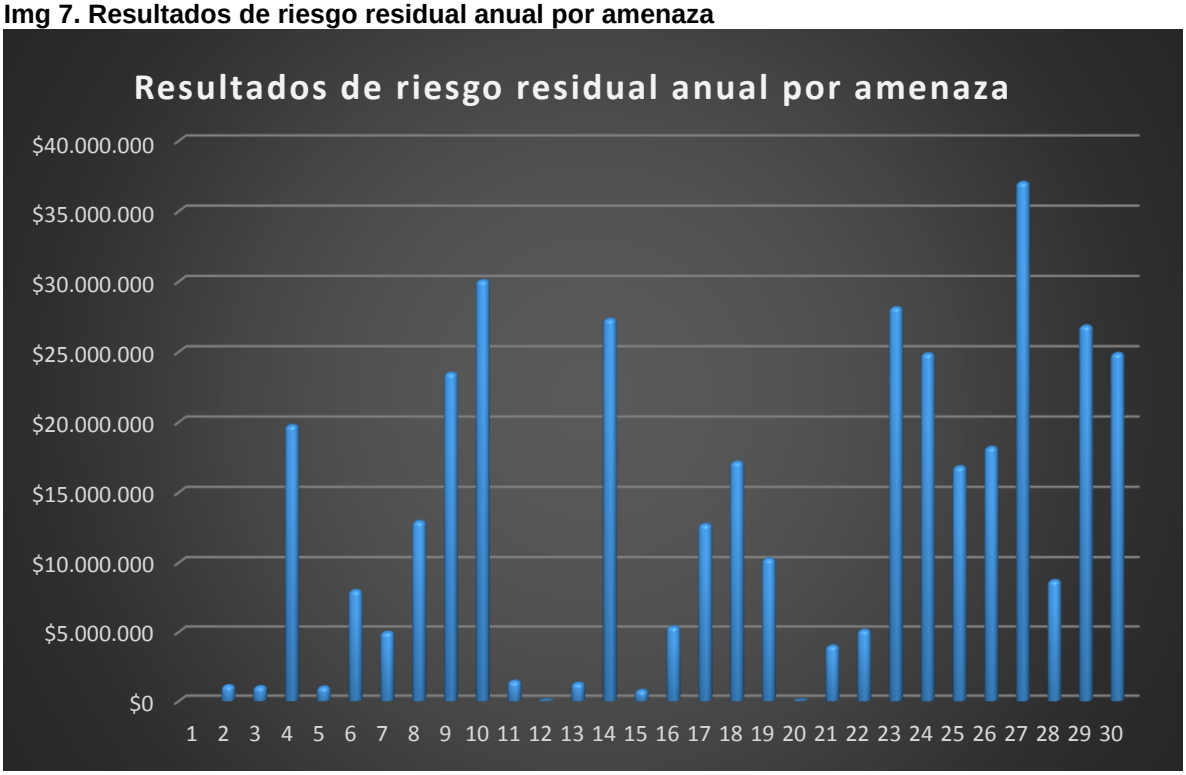
Ver Anexo 5, AnálisisDeRiesgos-Magerit.xls

[8] Módulo 2. Análisis de riesgos.pdf_ Universitat Oberta de Catalunya, Asignatura SGSI.

3.9 RESULTADOS

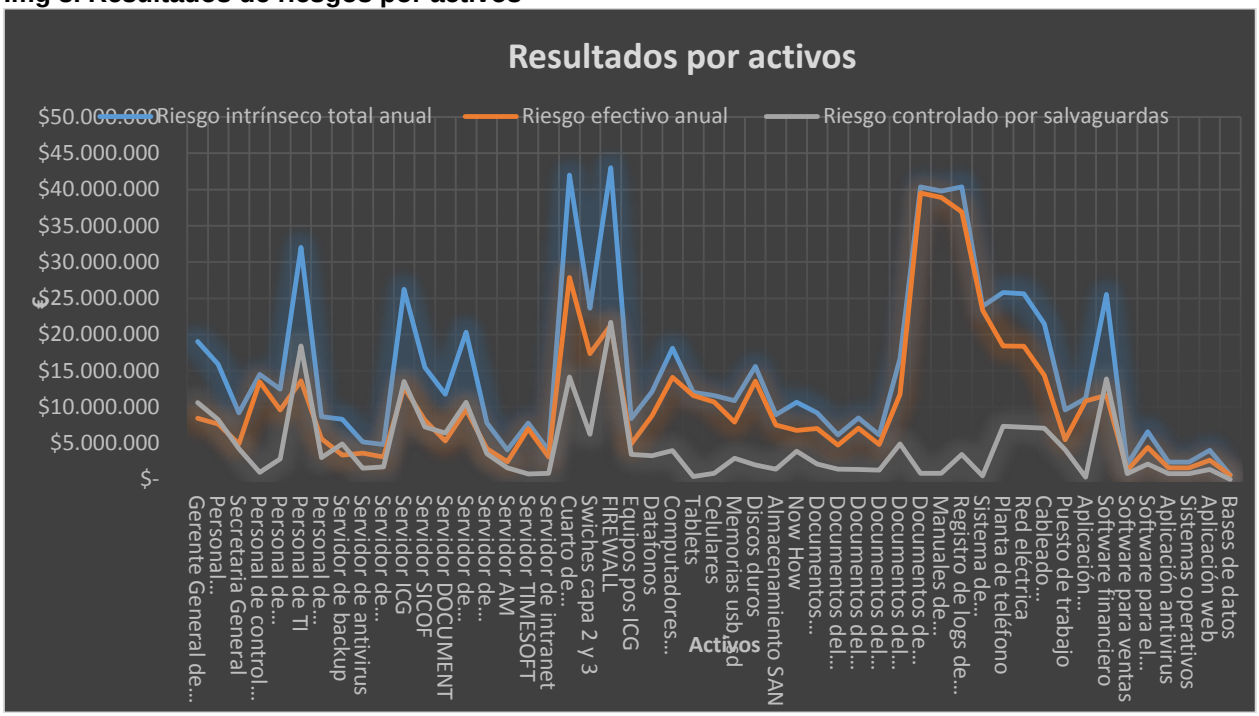
Ver anexo 5, AnálisisDeRiesgos-Magerit.xls

Img 7. Resultados de riesgo residual anual por amenaza



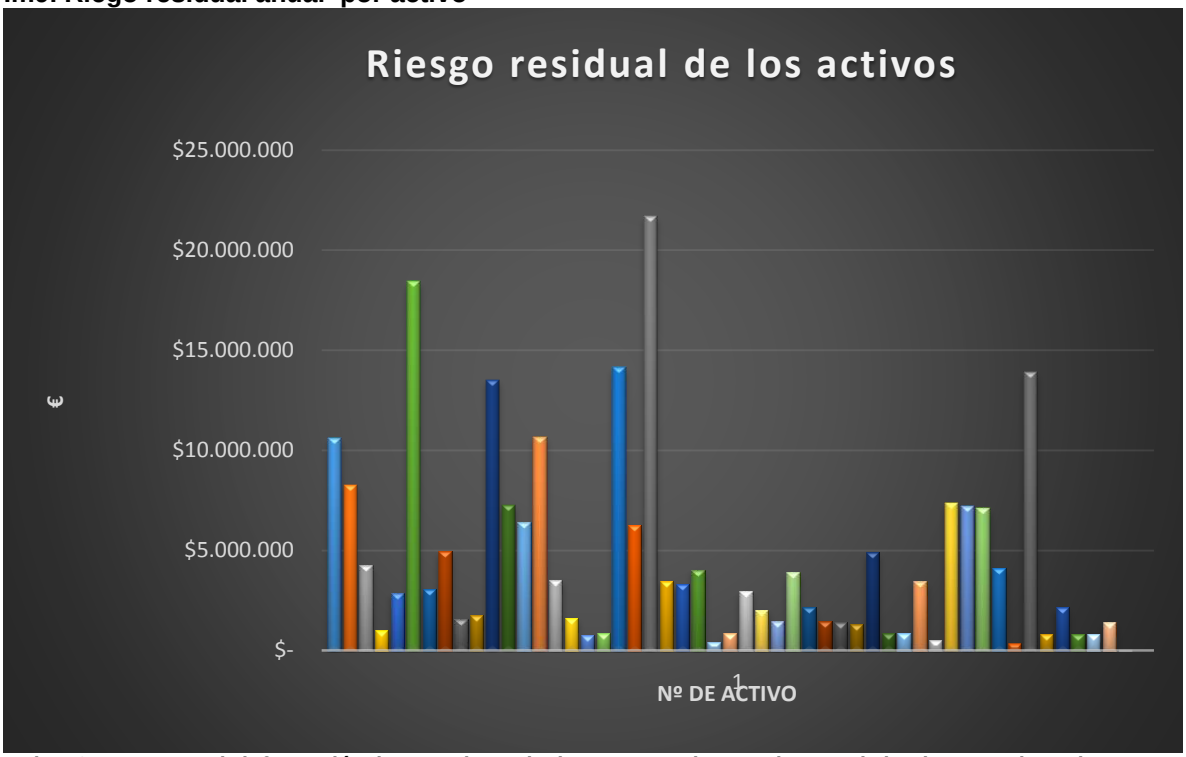
La img 7. Indica el riesgo controlado por las salvaguardas anuales por amenaza, donde al comparar con los resultados de la gráfica con los del anexo de Excel llamado **FASE 3, AnálisisDeRiesgos-Magerit.xls**, se puede ver que el riesgo residual más alto tiene un valor de **$ 37065498** y el más pequeño es de **$793866** y en otros casos los controles no surtieron efecto dando un valor de cero. Esto indica para los casos de activos con amenazas que generan riesgos y perdidas económicas muy altos para la empresa hay que implementar otras medidas de control para que el riesgo residual sea adecuado.

Img 8. Resultados de riesgos por activos



En la img 8, se puede apreciar el riesgo intrínseco total, riesgo efectivo y el riesgo controlado anual. Donde al observar las variaciones del riesgo intrínseco son muy altas y los controles actuales no son capaces de mitigar los impactos generados por las amenazas posibilitando su materialización, daños y pérdidas medias desde el activo gerente hasta el servidor de intranet, luego los riesgos se elevan pasando por el firewall, y luego retoman un impacto moderado o medio hasta el activo de documentos de sistema. Después los riesgos efectivos crecen exageradamente y los controles lo mitigan hasta el activo aplicación documental retornando nuevamente un valor medio de criticidad y por último los riesgos minimizan hasta el activo de bases de datos.

Im9. Riego residual anual por activo



La img 9. Representa la información de tratamiento de riesgos por salvaguardas anual, donde se puede ver los costos de los controles asociados para mitigar los riesgos que generan las amenazas en los activos de la empresa LINEA S.A.S.

4 FASE 4: PROPUESTAS DE PROYECTOS

4.1 Introducción. La empresa LINEA S.A.S ha considerado importante relacionar los proyectos destinados a la mitigación de los impactos generados por amenazas sobre los activos de la empresa. Dentro de las consideraciones importantes, está en verificar el nivel de riesgo aceptable por la dirección general de la organización para elaborar los proyectos de activos críticos por los riesgos causados y determinados a partir de la metodología de análisis de riesgos Magarit.

4.2 Elaboración de propuestas. Se determinan los activos críticos de acuerdo al nivel de riesgo aceptable comparado al nivel de riesgo efectivo, determinar el tipo de proyectos a realizar.

Los proyectos parten de los activos afectados por amenazas más críticas. Por tanto se evaluó el riego residual anual por activo para conocer el riego aceptable y el tipo de riesgo a tratar.

Nº	Código	Nombre	Valor Riesgo residual por activo anual	Riesgo No Aceptable
1	AC-01	Gerente General de la organización	$ 10.610.873	MA
2	AC-02	Personal administrativo y financiero	$ 8.267.976	MA
3	AC-06	Personal de TI	$ 18.423.941	MA
4	AC-11	Servidor ICG	$ 13.517.127	MA
5	AC-12	Servidor SICOF	$ 7.263.195	MA
6	AC-13	Servidor DOCUMENT	$ 6.429.300	MA
7	AC-14	Servidor de virtualización	$ 10.668.620	MA
8	AC-19	Cuarto de telecomunicaciones	$ 14.130.507	MA
9	AC-20	Swiches capa 2 y 3	$ 6.235.208	MA
10	AC-21	FIREWALL	$ 21.701.041	MA
11	AC-40	Planta de teléfono	$ 7.366.834	MA
12	AC-41	Red eléctrica	$ 7.226.464	MA
13	AC-42	Cableado estructurado vertical y horizontal	$ 7.089.560	MA
14	AC-45	Software financiero	$ 13.902.410	MA

Tabla 14. Identificación de riesgos no aceptables

4.3 Determinación de las salvaguardas para tratar el riesgo residual anual con nivel de criticidad muy alto.

Código Salvaguardas	Descripción	Responsable
SG-01	Concienciación y capacitación sobre aspectos esenciales para la seguridad de la información organizacional	Líder de proyecto
SG-02	Concienciación sobre la seguridad de la información y manejo correcto de los recursos TIC (Tecnologías de la información y la comunicación)	Líder de proyecto
SG-03	Formación en seguridad de la información de las tecnologías de la información y comunicación.	Líder del proyecto
SG-04	Adquisición y mejorara de los recursos de software y hardware seguro.	Personal de TI
SG-05	Actualización de software y capacitación de personal para evitar errores operacionales y fugas de información.	Proveedor y personal de TI
SG-06	Licenciamiento y mejoras de código seguro para la estabilidad, escalabilidad y cuidado de la información.	Proveedor y personal de TI

SG-07	Perímetro de seguridad mediante cámaras y software especializado para monitoreo de intrusos y software malicioso.	Personal de TI
SG-08	Barrera de seguridad con cámaras y acondicionamiento de espacios y medios para el trabajo de la infraestructura.	Personal de TI
SG-09	Configuración estable y segura de swiches para soportar las operaciones de la organización.	Personal de TI
SG-10	Configuración segura y adecuada para control de tráfico y protección de los accesos a los sistemas.	Personal de TI
SG-11	Actualización de planta de teléfono para la gestión y control de llamadas.	Personal de TI
SG-12	Adecuación y mejora de la carga eléctrica para el soporte de las operaciones de la infraestructura tecnológica.	Personal de TI
SG-13	Cambio del cableado de red, certificación para evitar las intermitencias, latencias del trabajo operacional por usuarios.	Personal de TI
SG-14	Seguridad para las operaciones financieras	Analista de seguridad

Tabla 15. Salvaguardas para tratar los riesgos

4.4 Presentación de propuestas. Se proponen varias propuestas para mejorar los estados de la seguridad de la información de la empresa LINEA S.A.S, permitiendo así mejorar la aplicabilidad de los controles de acuerdo a los indicadores establecidos para el cumplimiento del SGSI.

AC-1. Dirección general de la organización

Salvaguarda	SG-01
Descripción - Objetivo	Capacitar a la alta dirección de la empresa sobre la importancia de la seguridad de la información.
Responsable	Líder del proyecto
Activos a proteger	AC-01
Valor	$7.000.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Contratación de líder de seguridad de la información ○ Verificación de conocimientos y experiencia, certificación de auditorías internas ISO 27001:2013 ○ Planeación de actividades ○ Inicio y fin de la capacitación ○ Entrega de memorias y certificación. ○ Otras recomendaciones de seguridad de la información.
Indicador	Cobertura de las políticas, responsabilidad de la SI en la organización, efectividad de la planificación de la revisión por la dirección.
Fecha Inicio	14-05-2015
Fecha Finaliza	29-05-2015

Tablas 16. AC-1 Dirección general de la organización

AC-2. Personal administrativo y financiero

Salvaguarda	SG-02
Descripción - Objetivo	Capacitar al personal administrativo y financiero sobre la importancia de la seguridad de la información y de los dispositivos TIC de uso financiero.
Responsable	Líder del proyecto
Activos a proteger	AC-02
Valor	$6.000.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Contratación de líder de seguridad de la información ○ Verificación de conocimientos y experiencia, certificación de auditorías internas ISO 27001:2013 y auditoría técnica de seguridad de la información. ○ Planeación de actividades ○ Inicio y fin de la capacitación ○ Entrega de memorias y certificación. ○ Entrega de informes para la dirección y otro técnico para el personal de TI.
Indicador	Existencia y efectividad de políticas, procedimientos y controles para el intercambio seguro de información relevante.
Fecha Inicio	14-05-2015
Fecha Finaliza	25-05-2015

Tabla 17. AC-2. Personal administrativo y financiero

AC-06 Personal de TI

Salvaguarda	SG-03
Descripción - Objetivo	Formar y certificar al personal de TI en seguridad de la información de las tecnologías de la información y la comunicación.
Responsable	Líder del proyecto
Activos a proteger	AC-06
Valor	$20.000.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Contratación de líder de seguridad de la información ○ Verificación de conocimientos y experiencia, certificación de auditorías internas ISO 27001:2013, Ethical Hacking y auditoría técnica de seguridad de la información. ○ Planeación de actividades ○ Inicio y fin de la capacitación ○ Entrega de memorias y certificación. ○ Entrega de informes para la dirección y otro técnico para el personal de TI.
Indicador	Eficacia del control de acceso a sistemas y aplicaciones, efectividad de la continuidad de la seguridad de la información
Fecha Inicio	20-05-2015
Fecha Finaliza	,,26-07-2015

Tabla 18. AC-06 Personal de TI

AC-11 Servidor ICG

Salvaguarda	SG-04
Descripción - Objetivo	Adquirir software ICG actualizado y licenciado con los componentes de hardware óptimos para la alta disponibilidad, escalabilidad y rendimiento de forma segura.
Responsable	Proveedor y personal de TI
Activos a proteger	AC-11
Valor	$75.500.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Solicitud de propuesta con proveedores de ICG y TI. ○ Evaluación de propuestas ○ Elaboración de contrato de servicios con proveedores. ○ Planeación para licenciamiento y adaptación a nuevo hardware. ○ Adaptación de mejoras ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de rendimiento y seguridad de la información.
Indicador	Grado de despliegue o efectividad de los controles aplicados, garantía de instalaciones para el procesamiento de información, Efectividad de la continuidad de la seguridad de la información
Fecha Inicio	22-06-2015
Fecha Finaliza	22-07-2015

Tabla 19. AC-11 Servidor ICG

AC-12 Servidor SICOF

Salvaguarda	SG-05
Descripción - Objetivo	Actualizar y auditar el servidor SICOF.
Responsable	Proveedor y personal de TI.
Activos a proteger	AC-12
Valor	$55.500.000
Porcentaje de reducción del riesgo	%75
Actividades	○ Solicitud de propuesta con proveedores de SICOF. ○ Evaluación de propuestas ○ Elaboración de contrato de servicios con proveedores. ○ Planeación para implementación de mejoras ○ Adaptación de mejoras ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de rendimiento y seguridad de la información.
Indicador	Grado de despliegue o efectividad de los controles aplicados, garantía de instalaciones para el procesamiento de información.
Fecha Inicio	27-06-2015
Fecha Finaliza	28-08-2015

Tabla 20. AC-12 Servidor SICOF

AC-13 Servidor Document

Salvaguarda	SG-06
Descripción - Objetivo	Licenciar y mejorar la seguridad de la aplicación y servidor document.
Responsable	Proveedor y personal de TI.
Activos a proteger	AC-13
Valor	$40.500.000
Porcentaje de reducción del riesgo	%75
Actividades	○ Solicitud de propuesta con proveedores de Document y personal de seguridad de la información para auditar la seguridad de la aplicación. ○ Evaluación de propuestas ○ Elaboración de contrato de servicios con proveedores. ○ Planeación para implementación de mejoras ○ Adaptación de mejoras ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de rendimiento y seguridad de la información.
Indicador	Grado de despliegue o efectividad de los controles aplicados, garantía de instalaciones para el procesamiento de información, Efectividad en las pruebas de los desarrollos.
Fecha Inicio	29-07-2015
Fecha Finaliza	29-08-2015

Tabla 21. AC-13 Servidor Document

AC-14 Servidor de virtualización

Salvaguarda	SG-07
Descripción - Objetivo	Mejorar la seguridad perimetral y monitoreo de la red para evitar intrusiones e instalación de código malicioso.
Responsable	Personal de TI.
Activos a proteger	AC-14
Valor	$30.600.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Solicitud de propuesta con proveedores de sistemas de seguridad perimetral y sistemas de monitoreo de redes. ○ Evaluación de propuestas ○ Elaboración de contrato de servicios con proveedores. ○ Planeación para implementación de mejoras ○ Adaptación de mejoras ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de las implementaciones.
Indicador	Grado de despliegue o efectividad de los controles aplicados, garantía de instalaciones para el procesamiento de información, Efectividad de los controles contra código malicioso.
Fecha Inicio	01-06-2015
Fecha Finaliza	04-07-2015

Tabla 22. AC-14 Servidor de virtualización

AC-19 Cuarto de telecomunicaciones

Salvaguarda	SG-08
Descripción - Objetivo	Mejorar la seguridad perimetral y acondicionar el cuarto de TI de acuerdo a la normatividad vigente para las operaciones óptimas y seguras.
Responsable	Personal de TI.
Activos a proteger	AC-19
Valor	$70.800.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Solicitud de propuesta con proveedores de sistemas de seguridad perimetral y de infraestructura tecnológica. ○ Evaluación de propuestas ○ Elaboración de contrato de servicios con proveedores. ○ Planeación para implementación de mejoras ○ Adaptación de mejoras ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de las implementaciones.
Indicador	Garantía de instalaciones para el procesamiento de información, efectividad de las revisiones de seguridad física.
Fecha Inicio	06-06-2015
Fecha Finaliza	09-07-2015

Tabla 23. AC-19 Cuarto de telecomunicaciones

AC-20 Swiches capa 2 y 3

Salvaguarda	SG-09
Descripción - Objetivo	Mejorar la configuración y seguridad de los swiches capa 2 y capa 3 para la correcta gestión de redes de datos.
Responsable	Personal de TI.
Activos a proteger	AC-20
Valor	$6.800.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Capacitar al personal de TI en configuración de swiches capa 2 y capa 3. ○ Buscar entidad formadora ○ Estudiar propuestas de formación. ○ Planeación de la formación. ○ Prueba piloto en red experimental ○ Implementación de necesidades. ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de las implementaciones.
Indicador	Garantía de instalaciones para el procesamiento de información, efectividad del procedimiento de mantención de equipos.
Fecha Inicio	10-07-2015
Fecha Finaliza	08-08-2015

Tabla 24. AC-20 Swiches capa 2 y 3

AC-21 FIREWALL

Salvaguarda	SG-10
Descripción - Objetivo	Configurar y mejorar la seguridad de la información y la gestión de usuarios en las redes.
Responsable	Personal de TI.
Activos a proteger	AC-21
Valor	$30.300.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Verificar manual de procedimientos ○ Realización de propuestas de mejora y configuración del firewall. ○ Analizar propuestas. ○ Planeación de las mejoras. ○ Implementación de necesidades. ○ Pruebas y puesta en marcha ○ Seguimiento y evaluación de las implementaciones.
Indicador	Efectividad de la continuidad de la seguridad de la información.
Fecha Inicio	08-08-2015
Fecha Finaliza	08-09-2015

Tabla 25. AC-21 FIREWALL

AC-40 Planta telefónica

Salvaguarda	SG-11
Descripción - Objetivo	Adquirir de nuevo sistema telefónico para la gestión y control de llamadas.
Responsable	Personal de TI.
Activos a proteger	AC-40
Valor	$84.300.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Adquirir propuestas con proveedores ○ Análisis de propuestas. ○ Elaboración de contrato. ○ Planeación de la implementación. ○ Implementación de la propuesta. ○ Verificación y validación de la funcionalidad. ○ Seguimiento y mejoras.
Indicador	Efectividad en la implementación de los planes de continuidad del negocio.
Fecha Inicio	08-09-2015
Fecha Finaliza	09-10-2015

Tabla 26. AC-40 Planta telefónica

AC-41 Red eléctrica

Salvaguarda	SG-12
Descripción - Objetivo	Adaptar y mejorar la carga eléctrica para el soporte de las operaciones de la infraestructura tecnológica
Responsable	Personal de TI.
Activos a proteger	AC-41
Valor	$51.300.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Adquirir propuestas con proveedores ○ Análisis de propuestas. ○ Elaboración de contrato. ○ Planeación de la implementación. ○ Implementación de la propuesta. ○ Verificación y validación de la funcionalidad. ○ Seguimiento y mejoras.
Indicador	Efectividad en la implementación de los planes de continuidad del negocio.
Fecha Inicio	09-10-2015
Fecha Finaliza	09-11-2015

Tabla 27. AC-41 Red eléctrica

AC-42 Cableado estructura horizontal y vertical

Salvaguarda	SG-13
Descripción - Objetivo	Cambiar cableado de red de datos para evitar las intermitencias, latencias del trabajo operacional por usuarios
Responsable	Personal de TI.
Activos a proteger	AC-42
Valor	$101.500.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Adquirir propuestas con proveedores ○ Análisis de propuestas. ○ Elaboración de contrato. ○ Planeación de la implementación. ○ Implementación de la propuesta. ○ Verificación y validación de la funcionalidad. ○ Seguimiento y mejoras.
Indicador	Efectividad en la implementación de los planes de continuidad del negocio.
Fecha Inicio	09-10-2015
Fecha Finaliza	09-11-2015

Tabla 28. AC-42 Cableado estructura horizontal y vertical

AC-45 Software financiero

Salvaguarda	SG-14
Descripción - Objetivo	Licenciar y mejorar las aplicaciones financieras por código seguro para la estabilidad, escalabilidad y cuidado de la información.
Responsable	Analista de seguridad de la información.
Activos a proteger	AC-45
Valor	$40.600.000
Porcentaje de reducción del riesgo	%90
Actividades	○ Adquirir propuestas con proveedores ○ Análisis de propuestas. ○ Elaboración de contrato. ○ Planeación de la implementación. ○ Implementación de la propuesta. ○ Verificación y validación de la funcionalidad. ○ Seguimiento y mejoras.
Indicador	Efectividad en la implementación de los planes de continuidad del negocio.
Fecha Inicio	10-11-2015
Fecha Finaliza	10-12-2015

Tablas 29. AC-45 Software financiero

Ver Anexo 6, Diagrama de Gantt, donde se socializa los tiempos, líder, y actividades a ejecutar para el cumplimiento de las propuestas.

5 Fase. Auditoria de cumplimiento

5.1 Introducción. Hasta hora se ha analizado el contexto organizacional, identificación de los activos y riesgos asociados a cada activo por amenazas utilizando la metodología de análisis de riesgos Magerit. Ahora se va evaluar el estado de cumplimiento de los controles de la organización y las no conformidades presentadas de acuerdo al nivel de criticidad hallado en el proceso de auditoría de cumplimiento**.**

5.2 Metodología. Para evaluar el grado de madurez de los controles se parte de la relación de 114 controles, 35 objetivos de control, 14 dominios presentes en la guía ISO 27002:2013.

Los aspectos relacionados con las salvaguardas que permitieron reducir los niveles de riesgos a los que estaban expuestos los activos de la empresa LINEA S.A.S, los cuales son el punto de partida para determinar la efectividad de los controles teniendo presente los siguiente criterios del ISO 27002:2013

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

5.3 Informe de auditoría de cumplimiento, ver Anexo 7, informe de auditoría de cumplimiento.pdf, en el anexo se relaciona el objetivo de la auditoria, los hallazgos, las no conformidades, fortalezas de la empresa, oportunidades de mejora, conclusiones, recomendaciones.

6 Fase. Objetivos de la fase

El objetivo genérico de esta fase es la generación de la documentación, que deberá incluir como mínimo los siguientes aspectos:

- Resumen ejecutivo: breve descripción en que se incluya la motivación, enfoque del proyecto y principales conclusiones extraídas.

- Memoria descriptiva: donde se incluirá un detalle del proceso, incluyendo como mínimo la descripción de la empresa en estudio, el análisis de riesgos realizado, el nivel de cumplimiento de la empresa actualmente, un plan de acción para mejorar la seguridad, la cuantificación de la mejora que supondrá el plan y los aspectos organizativos que conviene abordar para hacer viable el plan.

- Una presentación a la dirección planteada para un tiempo de 1h en que se expongan los principales resultados del estudio, se plantee el plan de acción y los aspectos organizativos relevantes.

6.1 Entregables

Para poder superar el proyecto se debe entregar los siguientes documentos:

- Resumen ejecutivo
- Memoria de Proyecto. Figurarán como anexos:
  - Objetivos del Plan Director e Informe Análisis Diferencial
  - Resultados del análisis de riesgos
  - Nivel de cumplimiento de la ISO basado en el análisis de los 114 controles planteados por la norma.
  - Proyectos planteados a la dirección, detallando el coste económico de los mismos, su planificación temporal y su impacto sobre el cumplimiento normativo de la ISO/IEC 27002:2013 en los diferentes dominios.
  - Esquema documental indicado en el apartado 2.2
  - Presentación de resultados del proyecto y video.

Bibliografía

- ISO/IEC 13335-1:2004 – Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for Information and communications technology security management.
- Magerit versión 3, metodología de análisis y gestión de riesgos de sistemas de información; https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/.
- ISO/IEC 27001:2013 Information technology Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534

LISTA DE ANEXOS

Anexo 1, Análisis diferencial ISO 27001.xls

Anexo 2, Análisis diferencial ISO 27002.xls

Anexo 3, Gestión de indicadores.xls

Anexo 4, Declaración de la aplicabilidad.xls

Anexo 5, AnálisisDeRiesgos-Magerit.xls

Anexo 6, Diagrama de Gantt.xls

Anexo 7, informe de auditoría de cumplimiento.pdf

Anexo 8, Objetivos del plan director de seguridad de la información.pdf

Anexo 9, Informe de análisis diferencial.pdf

Anexo 11, Nivel de cumplimiento ISO 27002.xls

Anexo 12, Proyectos planteados a la dirección

Anexo 13, Esquema documental apartado 2.2

Anexo 14, Presentación de resultados del proyecto y video en present@_uoc