Información Importante

La Universidad Santo Tomás, informa que el(los) autor(es) ha(n) autorizado a usuariosinternos y externos de la institución a consultar el contenido de este documento a través del Catálogo en línea de la Biblioteca y el Repositorio Institucional en la página Web de la Biblioteca, así como en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

Se permite la consulta a los usuarios interesados en el contenido de este documento, para todos los usos que tengan **finalidad académica**, nunca para usos comerciales,siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de grado y a su autor.

De conformidad con lo establecido en el Artículo 30 de la Ley 23 de 1982 y elartículo 11 de la Decisión Andina 351 de 1993, la Universidad Santo Tomás informa que "los derechos morales sobre documento son propiedad de los autores, los cuales son irrenunciables,imprescriptibles, inembargables e inalienables."

Bibliotecas Bucaramanga
Universidad Santo Tomás

IMPLEMENTACIÓN DE UN ESTÁNDAR DE CALIDAD PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA INSURCOL LTDA BAJO LA NORMA ISO 27001:2013

MARÍA CAMILA CEPEDA ROJAS

Informe final de práctica empresarial

CLAUDIA MARCELA MARTINEZ
Tutor Empresa

HEIDI PATRICIA CAMACHO GRASS
Tutor Universidad

INSURCOL LTDA

UNIVERSIDAD SANTO TOMÁS BUCARAMANGA
FACULTAD DE INGENIERÍA INDUSTRIAL
DIVISIÓN DE ARQUITECTURA E INGENIERÍAS
BUCARAMANGA
2016

TABLA DE CONTENIDOS

INTRODUCCIÓN 5

1. JUSTIFICACIÓN 6

2. OBJETIVOS 7

2.1 GENERAL 7

2.2 ESPECÍFICOS 7

3. MARCO REFERENCIAL 8

4. PERFIL DE LA EMPRESA 9

4.1 Alcance Organizacional 9

4.2 Clasificación de la información dentro del alcance del SGSI 10

4.3 Alcance y limites a nivel organizacional 10

Redes 10

Activos de la información 10

4.4 Alcance y límites físicos 10

5. ACTIVIDADES REALIZADAS 12

6. APORTES 14

8. LECCIONES APRENDIDAS 18

9. CONCLUSIONES 21

10. REFERENCIAS BIBLIOGRÁGICAS 22

LISTA DE TABLAS

1. TABLA 1: Sedes de Insurcol Ltda. en Colombia……...10
2. TABLA 2: Aportes realizados a la empresa……..13
3. TABLA 3: Lista de lecciones aprendidas……..17

INTRODUCCIÓN

Esta práctica fue desarrollada en Insurcol Ltda., una empresa dedicada a realizar proyectos de ingeniería de origen civil, mecánico, de instrumentación y control en el sector petrolero y de ingeniería a nivel nacional. Tiene sus oficinas principales en la ciudad de Bucaramanga y Bogotá, con presencia en Barrancabermeja, Cartagena y Houston – Estados Unidos.

El objetivo de la práctica realizada en esta empresa, fue implementar un Sistema de Gestión de Seguridad de la Información con el fin de aplicar la NTC ISO 27001:2013 de Seguridad de la Información, como solución a la protección de activos de información de Insurcol Ltda.

Para lograr dicho objetivo se realizaron diferentes actividades como la contextualización de la empresa, identificación de activos de información actuales, identificación vulnerabilidades de los activos, las amenazas que se presentan en la actualidad, se identificaron los riesgos existentes, se identificaron y propusieron mejoras a la infraestructura, equipos y procedimientos de seguridad de la información, además de redactar y normalizar la documentación necesaria para realizar los diferentes procedimientos del sistema.

En el siguiente informe el lector podrá conocer acerca de la Seguridad de la Información, la empresa Insurcol Ltda, las actividades realizadas como parte del desarrollo de la práctica empresarial, los aportes realizados y los resultados obtenidos tanto para la organización como para el practicante, culminando con las conclusiones finales.

1. JUSTIFICACIÓN

La realización de esta práctica fue de vital importancia para el crecimiento profesional del practicante gracias a la aplicación de diferentes áreas de su carrera como calidad, administración, costos, recursos humanos, lecto-escritura, legislación, ética y valores, entre otras, que permitieron día a día ejecutar una metodología de trabajo bajo objetivos y junto a un equipo de trabajo experto en la parte tecnológica, vital para la aplicación y ejecución de conocimientos aprendidos.

Durante la práctica se logró un aprendizaje importante en temas de trabajo en equipo, la aplicación de la NTC-ISO 27001:2013 desde su estudio, análisis de la empresa, estudio de riesgos y vulnerabilidades para luego aplicar metodologías y procedimientos que permitieran a la organización conocer su estado actual y aplicar mejoras a sus procesos para una mayor seguridad de su información.

Para la empresa, la ejecución de la práctica empresarial le permitió identificar sus activos de información y vulnerabilidades que presentan en la actualidad, para así protegerse de una mejor manera con la implementación del Sistema de Gestión de Seguridad de la Información.

2. OBJETIVOS

2.1 GENERAL

Implementar el estándar de calidad de Gestión de Seguridad de la Información en INSURCOL LTDA para el manejo de su información bajo la norma ISO 27001

2.2 ESPECÍFICOS

1. Analizar el estado actual de la empresa en los procesos de seguridad de la información.
2. Establecer las necesidades de Insurcol Ltda. en la seguridad de la información.
3. Apoyar proceso de definición de controles y tratamientos a las necesidades identificadas según la norma ISO 27001.
4. Documentar e implementar procedimientos de seguridad de la información en Insurcol Ltda.

3. MARCO REFERENCIAL

Esta práctica fue realizada bajo la NTC ISO 27001:2013 “Tecnología de la información, técnicas de seguridad, sistemas de gestión de seguridad de la información. Requisitos” a través de la cual se establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información[1]

Dentro de esta norma se establecen siete (7) requisitos a aplicar en la organización para lograr una implementación correcta. El primero es el Contexto de la organización, donde se determina el alcance que va a tener la implementación del sistema de gestión de seguridad de la información en la empresa como herramienta fundamental para cumplir los requisitos de la norma.

El siguiente es Liderazgo, donde se deben establece el compromiso de la dirección en la implementación de este sistema, se definen políticas de seguridad de la información y se asignan las responsabilidades respectivas, seguido de la Planificación, donde se deben establecer los objetivos y planes para lograrlos, además de las acciones para tratar y controlar riesgos y oportunidades encontrados en la organización.

Para el caso del soporte, se deben definir los recursos necesarios para trabajar la seguridad de la información, las competencias del personal encargado de implementar y controlar este sistema, la toma de conciencia por parte de todos los que componen la organización, la comunicación de las actividades en seguridad de la información y toda la información documentada como evidencia de procedimientos y acciones a tener en cuenta el personal responsable.

El siguiente tema a tener en cuenta es la parte de operación, donde se deben planificar y controlar las actividades operativas de la empresa en seguridad de la información, se debe valorar de forma constante los riesgos en seguridad de la información que presenta la organización, y, planear y ejecutar un tratamiento a los riesgos identificados.

Por último la norma establece que debe existir una evaluación de desempeño al SGSI donde se realice un seguimiento, medición, análisis y evaluación a través de la aplicación de auditorías internas y la revisión por dirección con el fin de lograr una mejora continua en el sistema, como el último requisito aplicado de la norma para lograr la implementación idónea del SGSI en la organización.

[1] Generalidades. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. NTC-ISO 27001. Bogotá D.C.: El instituto, 2013. 33p.

4. PERFIL DE LA EMPRESA

Insurcol Ltda. es una Compañía Colombiana, legalmente establecida, fundada el 18 de Agosto de 1988 por el Dr. Álvaro González Rodríguez y Omaira Cárdenas Rodríguez en la ciudad de Bucaramanga. En la actualidad planea y ejecuta proyectos en cuatro líneas principales de Productos y Servicios:

- División de Instrumentación y Control
- División Energética
- División de Desarrollo de Proyectos
- División Metalúrgica.

Se encuentra certificada en la NTC-ISO 9001:2008 Sistema de Gestión de Calidad, NTC-OHSAS 18001:2007 Sistema de Gestión de Seguridad y Salud Ocupacional, NTZ-ISO 31000:2009 Gestión de riesgo. Políticas y directrices, y en la SGE21:2008 Sistema de Gestión Ética y Responsabilidad Social en la cual fue la primera empresa en Latinoamérica en certificarse en dicha norma. El objetivo de la empresa ahora es certificarse en la NTC-ISO 27001:2013 Sistema de Gestión de Seguridad de la Información.

INSURCOL LTDA, cuenta con un equipo financiero, técnico y de gerencia de primera línea. La calidad de los productos que ofrece y la experiencia de su equipo de trabajo conforman una excelente inversión para los clientes existentes y futuros, ostenta una amplia trayectoria en el Suministro, Instalación, Capacitación y Mantenimiento de Sistemas de Control e Instrumentación Electrónica, Sistemas Ininterrumpidos de Potencia (UPS) y Equipos y Elementos de tipo Industrial.

4.1 Alcance Organizacional

El sistema de gestión de seguridad de la información incluye las actividades de prestación de servicio realizadas por INSURCOL LTDA, descritas a continuación:

- **Operación**: Comprende la configuración, administración y monitoreo del hardware y software de la infraestructura tecnológica de la organización, así como la solución de los incidentes que se pueden producir y que alteren el funcionamiento normal de los servicios de tecnología.

- **Soporte**: Comprende el servicio de asistencia técnica para hardware, software u otros dispositivos electrónicos. En general el servicio de soporte sirve para ayudar a resolver las situaciones que puedan presentarse con los usuarios de la organización, mientras hacen uso de servicios, procesos, programas o dispositivos.

4.2 Clasificación de la información dentro del alcance del SGSI

- **Información pública:** Es la información que está disponible para el personal interno y externo de INSURCOL LTDA, como empleados, clientes y/o proveedores en general. Sin ninguna restricción de acceso.
- **Información de uso interno sin restricción de acceso:** Es toda aquella información que se encuentra disponible solo para el personal interno de la compañía (intranet y procesos del sistema de gestión).
- **Información de uso interno con restricción de acceso:** Es la información que se encuentra disponible solo para el personal interno de la compañía con permisos o ciertos niveles de privilegios. (Bases de datos, Código Fuente, formatos, archivos).
- **Información confidencial:** Es toda la información que la empresa procesa durante la realización de sus labores diarias.

4.3 Alcance y limites a nivel organizacional

Redes
El alcance del SGSI de INSURCOL LTDA, incluye las comunicaciones e intercambio de información a través de todas sus redes.

- Red LAN protegida para operaciones de servicio en cada una de las oficinas de Bucaramanga, Barrancabermeja, Bogotá.
- Servicio de VPN para acceso remoto controlado y protegido desde las sucursales y usuarios autorizados.
- Red Wireless para acceso de empleados autorizados.

Activos de la información
El alcance de SGSI de INSURCOL LTDA incluye los activos identificados en INSURCOL LTDA.

- **Infraestructura:** Inmuebles y contenedores.
- **Hardware:** Computador de escritorio, portátiles, servidores, cámaras, DVD, video vean, plotter, quemador de DVD, UPS, fotocopiadoras, Router, aire acondicionado, teléfonos, celulares, avanteles, radios, mini grabadora, switches, biométrico, Impresoras.
- **Software:** SAP, INNOVA, directorio activo, licencias informáticas, telnet.
- **Personal:** Todo el personal que se encuentre contratado en la organización.
- **Intangibles:** Reconocimiento de marca, know how de la empresa.
- **Bases de datos:** Clientes, proveedores y empleados.

4.4 Alcance y límites físicos

El SGSI de INSURCOL LTDA, incluye las siguientes instalaciones donde se desarrollan las diferentes actividades.

Tabla 1: Sedes de Insurcol Ltda. en Colombia

SEDE O SUCURSAL	DIRECCION	TELEFONO
Bucaramanga	Calle 41 21-32	6700100
Barrancabermeja	Transversal 6 # 6B-93 Oficina 404	6221319
Bogotá	Av. Carrera 19 # 39B-56 Teusaquillo	6854240

5. ACTIVIDADES REALIZADAS

Para el desarrollo de esta práctica se realizaron las siguientes actividades clave:

1. Investigación, estudio y capacitación en la NTC-ISO 27001:2013 sus conceptos, aplicaciones y ejemplos referentes a la aplicación de un sistema de gestión de seguridad de la información.
2. Definición de política de seguridad de la información y alcance del mismo en apoyo por la dirección.
3. Modificación de la estructura organizacional en su organigrama, incluyendo un nuevo departamento TI.
4. Aplicación de un análisis GAP[2] (Análisis de Brechas) de la situación actual de la organización frente al cumplimiento de la NTC-ISO 27001:2013. Este análisis fue de vital importancia para identificar que tanto cumplía Insurcol Ltda. al inicio de mi práctica frente buenas prácticas de seguridad de la información. Este análisis se presenta como Anexo 1 en este informe.
5. Identificación de bases de datos confidenciales para la empresa a través de la aplicación de una entrevista dirigida a los coordinadores de área, con el fin de identificar la información confidencial que maneja, su ubicación y acceso para lograr identificar las vulnerabilidades y amenazas que se buscan proteger con el sistema de gestión de seguridad de la información.
6. Identificación de los activos de información de la empresa. Esta actividad fue de vital importancia para la práctica porque se logró tener conocimiento de lo que tiene la empresa en temas de información confidencial junto con alta dirección quienes manifestaron no tener conocimiento de la importancia de la información en su empresa.
7. Aplicación de dos (2) metodologías para el análisis de riesgos. La primera, fue la aplicación de una matriz bajo la ISO 3100[3] de gestión de riesgos evidenciada como anexo 2 en este informe, y la siguiente, fue la aplicación de un análisis de riesgos MAGERIT[4] donde se identificaron los riesgos efectivo e intrínseco real

---

[2] Análisis de brechas: El análisis de brechas es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados de orden local, regional, nacional y/o internacional. Según la Universidad Nacional de Colombia. [Citada el 20 de Diciembre de 2015] Disponible en internet, URL: http://www.ingenieria.unal.edu.co/ACSCI/autoevaluacionacreditacion/docs/NormatividadUNxFactor/Factor%201.%20Misi%F3n,%20Proyecto%20Institucional%20y%20de%20Programa/Ind%205.%20Criterios%20procesos%20de%20autoevaluaci%F3n/Guia_Analisis_Brechas.pdf

[3] INSITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo. Principios y directrices. NTC-ISO 31000. Bogotá D.C.: El instituto, 2011. 12p. MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

[4] La Metodología de análisis de riesgos en los sistemas de información es un proceso de gestión de riesgos de un marco de trabajo para tomar decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información. Esta información se encuentra en GOBIERNO DE ESPAÑA. MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I y II. Ministerio de Hacienda y Administración Pública. 400p.

de la organización representado en dinero, esta evidencia se encuentra como Anexo 2.

8. Capacitación en la estructura documental de Sistema de Gestión Integral de Insurcol Ltda. Para iniciar con la documentación requerida para el sistema de gestión de seguridad de la información.
9. Identificación de necesidades técnicas, tecnológicas y de infraestructura para realizar mejoras pertinentes que permitan a Insurcol Ltda. Proteger de mejor manera sus activos. Esto fue puesto en conocimiento a los gerentes de la empresa los cuales aprobaron la posterior cotización de los cambios para aprobar presupuesto. Los cambios aprobados se muestran como un Anexo 3 en este informe.
10. Redacción de documentos: Se modificaron 7 documentos existentes en la organización (Política de gestión integral, manual de gestión integral, organigrama de Bucaramanga, descripción de responsabilidades, perfil de cargos Bucaramanga parte II, Matriz de habilidades por cargos Bucaramanga parte II, reglamento interno del comité integral de gestión), se crearon 5 nuevos documentos para el sistema de gestión de seguridad de la información (Manual de políticas de seguridad de la información, Declaración de aplicabilidad, Programa de seguridad de la información, continuidad del negocio y gestión de incidentes)
11. Creación de formatos: Se crearon 4 nuevos formatos (matriz análisis de riesgos, matriz de riesgos MAGERIT, consolidado de activos de información y plan de tratamiento del riesgo).
12. Se formalizó la documentación creada y modificada dentro del SGI de Insurcol Ltda. con el área de calidad.

6. APORTES

Tabla 2: Aportes realizados a la empresa

OBJETIVO	APORTE	DOCUMENTO O EVIDENCIA	RESULTADO
Analizar el estado actual de la empresa en los procesos de seguridad de la información.	Aplicación de análisis GAP para conocer su estado actual en seguridad de la información con respecto a los controles de la norma NTC-ISO 27001:2013	Análisis GAP. Ver anexo 4.	Con la aplicación de este análisis se pudo identificar las falencias en seguridad de la información de la empresa como oportunidad de mejora para aplicar el sistema de gestión de seguridad de la información bajo los controles que la norma exige.
Establecer las necesidades de Insurcol Ltda. en la seguridad de la información.	Estudio del estado actual de la empresa en materia de software, hardware y documentación. Junto con el equipo técnico se propuso las mejoras a realizar y se cotizaron los valores a invertir para realizar mejoras	Se presentó un cuadro de mejoras a realizar en la organización junto con su tiempo de implementación y valor aproximados para aprobar cotización. Ver anexo 5.	La subgerencia aprueba los cambios para hacer cotización real de dicha inversión. Luego se presentó la cotización y se decide esperar a tener los recursos suficientes para implementar los cambios en la organización.
Apoyar proceso de definición de controles y tratamientos a las necesidades identificadas según la	Se hizo un análisis detallado de los riesgos identificados con el fin de definir los controles y tratamientos a aplicar en la organización según el Anexo A de la	Declaración de aplicabilidad.	Con este análisis se definieron los controles básicos a tener en cuenta para dar a inicio a la implementación de la norma en la organización. Aunque se documentó, está

norma ISO 27001.	NTC ISO:27001 como requisitos mínimos para implementar el sistema		pendiente su implementación.
Documentar e implementar procedimientos de seguridad de la información en Insurcol Ltda.	Se modificaron 7 documentos del sistema de gestión integral actual de Insurcol Ltda. Se crearon 5 nuevos documentos y 4 nuevos formatos según la norma, para la implementación del sistema de seguridad de la información	Documentos modificados: Política de gestión integral, manual de gestión integral, organigrama de Bucaramanga, descripción de responsabilidades, perfil de cargos Bucaramanga parte II, Matriz de habilidades por cargos Bucaramanga parte II, reglamento interno del comité integral de gestión Documentos creados: Manual de políticas de seguridad de la información, Declaración de aplicabilidad, Programa de seguridad de la información, continuidad del negocio y gestión de incidentes Formatos creados: matriz análisis de	Se entregó en formato digital modificable todos los documentos y formatos al área de calidad con el fin de normalizar en el sistema de gestión integral para su posterior implementación. La implementación no se pudo realizar debido a la programación de auditoría al SGSI realizado por entidad externa en día 18 de diciembre de 2015. Por lo tanto se aplazó su implementación en Insurcol Ltda.

		riesgos, matriz de riesgos MAGERIT, consolidado de activos de información y plan de tratamiento del riesgo. Ver anexo 7.	

7. RECOMENDACIONES

1. Se recomienda a la empresa aplicar la metodología de análisis de riesgos Magerit aplicada y documentada en el Programa de Seguridad de la Información, con el fin de tener un control de los riesgos existentes en cada uno de los procesos del Sistema de Gestión Integral.
2. Se recomienda a Insurcol Ltda. mejorar su infraestructura en temas de seguridad con base en las mejoras presentadas durante la práctica, para controlar de mejor manera su información digital y física a nivel interno, además de protegerla de algún riesgo natural, físico, vandálico o de hacking.
3. Se recomienda a Insurcol Ltda. contratar a personal profesional en seguridad de la información para ser el responsable de planear, hacer, verificar y actuar las actividades definidas en el sistema de gestión de seguridad de la información de la forma correcta ocupando el cargo de Subcoordinador de Seguridad de la Información, teniendo en cuenta que en la actualidad ninguno de los profesionales que se encuentra en la empresa cuenta con el perfil idóneo.
4. Se recomienda a la empresa estar en constante capacitación del personal en seguridad de la información, y actualización de sus sistemas operativos y hardware según el avance tecnológico mundial, para así estar a la vanguardia de metodologías necesarias para proteger su información de nuevos riesgos que se puedan presentar.
5. Es recomendable destinar un presupuesto anual al mantenimiento preventivo
5. de infraestructura (cableado, oficinas), software y hardware con el fin de
5. evitar fallas en los sistemas que manejen información confidencial.
6. Se recomienda socializar de forma constante las Políticas de Seguridad de
5. la Información establecidas en el Manual de Políticas de Seguridad de la
5. Información con el fin de promover una cultura de seguridad en todos los
5. integrantes de la organización.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.
5.

8. LECCIONES APRENDIDAS

Tabla 3: Lista de lecciones aprendidas

PROBLEMA	POSIBLES SOLUCIONES	SOLUCIÓN	LECCIÓN APRENDIDA	APROBÓ
No se tenía la norma ISO 27001 actualizada	Comprar la norma de manera rápida.	Adquisición de nueva norma con Icontec a través de internet.	A la hora de realizar algún trabajo sobre una norma o ley se debe tener la última actualización de la misma para trabajar sobre la correcta y evitar retrocesos.	Subgerencia
Desconocimiento de la norma y su aplicabilidad en las empresas	- Realizar un curso en la norma NTC-ISO 27001 con SGS o ICONTEC. - Asistir a capacitaciones que se realicen en este tema - Leer y consultar acerca de trabajos realizados bajo la norma por cuenta del practicante.	El practicante tuvo que capacitarse por su cuenta investigando acerca de la NTC-ISO 27001, ejemplos de empresas que la han aplicado y metodologías para su análisis e implementación de controles y tratamientos.	Cuando en una organización los directivos no están dispuestos a invertir recursos en la formación de sus trabajadores, el mismo trabajador debe buscar formarse por sus propios medios con el fin de lograr realizar su labor de la forma correcta.	Subgerencia Tutor de la empresa
Desconocimiento de mejoras técnicas necesarias para una empresa más segura	- Investigación de soluciones técnicas. - Contratar a un experto en seguridad de la información. - Soportarse en los ingenieros del área de sistemas y	Se formó un equipo de trabajo multidisciplinario junto al ingeniero de sistemas y al ingeniero en programación especialista en seguridad de la	Para lograr poner en marcha algún proyecto en una organización, es necesario formar equipos de trabajo multidisciplinarios que aporten ideas y acciones desde su experiencia.	Subgerencia

	programación para conocer las mejoras a realizar	información para identificar falencias en materia técnica para la seguridad y dar posible soluciones.		
Falta de conexión entre sedes de la empresa	- Investigar las posibles soluciones - Contactar a empresas prestadoras del servicio de conexión entre sedes	Se invitó a 3 empresas prestadoras del servicio de interconexión entre sedes a presentar su propuesta y a cotizar.	Se aprendieron las diferentes formas técnicas y tecnológicas de conectar las sedes y controlar desde un software especializado de manera remota.	Equipo de trabajo en Seguridad de la información.
Falta de digitalización de documentos	- Mandar a digitalizar toda la información con una empresa. prestadora de este servicio. - Contratar a 3 personas que se dediquen a digitalizar todo el archivo en físico actual.	El practicante realizó las tres (3) cotizaciones a empresas requeridas por Subgerencia para tomar la decisión, pero se decidió trabajar la actividad con personal contratado directamente y compara los equipos necesarios como una decisión más económica.	Se toma de esta experiencia que antes de tomar alguna decisión de inversión de recursos para mejorar en la empresa se debe realizar un estudio económico de las posibles soluciones para entender cuál es la más viable.	Sugerencia.
Desconocimiento de la forma de documentar según el SGI de Insurcol Ltda.	- Capacitarse en la gestión documental de la empresa y ser evaluada.	La practicante redactó la documentación bajo estándares de otros documentos en	La enseñanza de esta situación para el practicante fue instruirse, conocer y entender las metodologías,	Auxiliar de calidad.

	- Redactar documentos con base en documentación existente	un primer momento, sin conocer la estructura clara. Al ocurrir esto el área de calidad revisó y devolvió la documentación a corrección con el fin de modificar y redactar bajo los parámetros correctos.	parámetros y tipos de documentos que establece cada organización en su sistema de calidad, con el fin de evitar retrocesos por errores en la estructura documental.	
Desarrollo de auditoría externa antes de la implementación del SGSI	- No normalizar ni implementar documentos	No se normalizó ni implementó la documentación redactada y aprobada por la nueva fecha de auditoría al SGI el cual no puede tener implementado un nuevo sistema sin generar evidencias mínimas de 3 meses para la auditoría.	Se aprendió a planificar las actividades de implementación de alguna nueva norma de calidad antes de cualquier auditoría, ya que para las auditorias se requieren evidencias de todos los sistemas de gestión de calidad que la organización quiere implementar.	Auxiliar de Calidad. Tutor de la empresa. Subgerencia.

9. CONCLUSIONES

1. El análisis actual de la empresa realizado con base a la NTC-ISO 27001:2013 y aplicado bajo la metodología de análisis GAP, permitió al practicante conocer las falencias en seguridad de la información existentes en Insurcol Ltda. para dar inicio a gestionar el sistema de gestión de seguridad de la información.
2. Para establecer necesidades técnicas y de infraestructura fue necesario contar con un equipo técnico que apoyara a la identificación y posibles soluciones a las necesidades de mejora. Se conformó un equipo ingeniero de sistemas especialista en seguridad de la información y un programador aparte de la practicante.
3. Se definieron los controles y tratamientos con base al Anexo A de la NTCISO 27001:2013 como actividad clave para establecer las actividades mínimas a realizar la organización para dar inicio a la implementación del Sistema de Seguridad de la Información.
4. Se documentaron los procesos y procedimientos necesarios para implementar el Sistema de Gestión integral, pero no se pudo implementar debido a auditoría externa programada para el 18 de diciembre evitando implementar y evaluar el sistema de gestión de seguridad de la información propuesto por el practicante.

10. REFERENCIAS BIBLIOGRÁGICAS

ACADEMY 27001. Informe: Lista de documentación obligatoria requerida por ISO/IEC 27001. UI. Vladimira Nazora 59, 10000 Zagreb, EPPS Services Ltd., 2014. 9p.

BAUTISTA, Luis Alejandro. Plan de Seguridad de la Información Compañía XYZ Soluciones. Trabajo de grado de máster universitario en Seguridad de las TIC. Barcelona. Universidad Autónoma de Barcelona. 45p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatuaria 1581 de 2012 (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48587. 214p.

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto número 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá D.C., 2013. 11p.

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto número 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamento del Sector Comercio, Industria y Turismo. Bogotá D.C., 2015. 412p.

GOBIERNO DE ESPAÑA. MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I y II. Ministerio de Hacienda y Administración Pública. 400p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. NTC-ISO 27001. Bogotá D.C.: El instituto, 2013. 33p.

INSITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo. Principios y directrices. NTC-ISO 31000. Bogotá D.C.: El instituto, 2011. 12p.

INSURCOL LTDA. Documentación del SGSI. Suministrado por el área de calidad. Bucaramanga. 27 de Agosto de 2015.

PERÚ. LA COMISIÓN DE LA COMUNIDAD ANDINA. Decisión 486 (14, septiembre, 2000). Por la cual se establece el régimen común sobre la propiedad industrial. Lima, 2.000. 61p.

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Seguridad de la información. Política para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas. Bogotá D.C. [Citada el 25 de diciembre de 2015] Disponible en internet, URL: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

ANEXOS

1. ANEXO 1: Glosario

Los conceptos utilizados para el conocimiento, documentación e implementación del Sistema de Gestión de Seguridad de la Información según el glosario de la ISO 27000 establecido por la SGSI Colombia es el siguiente:

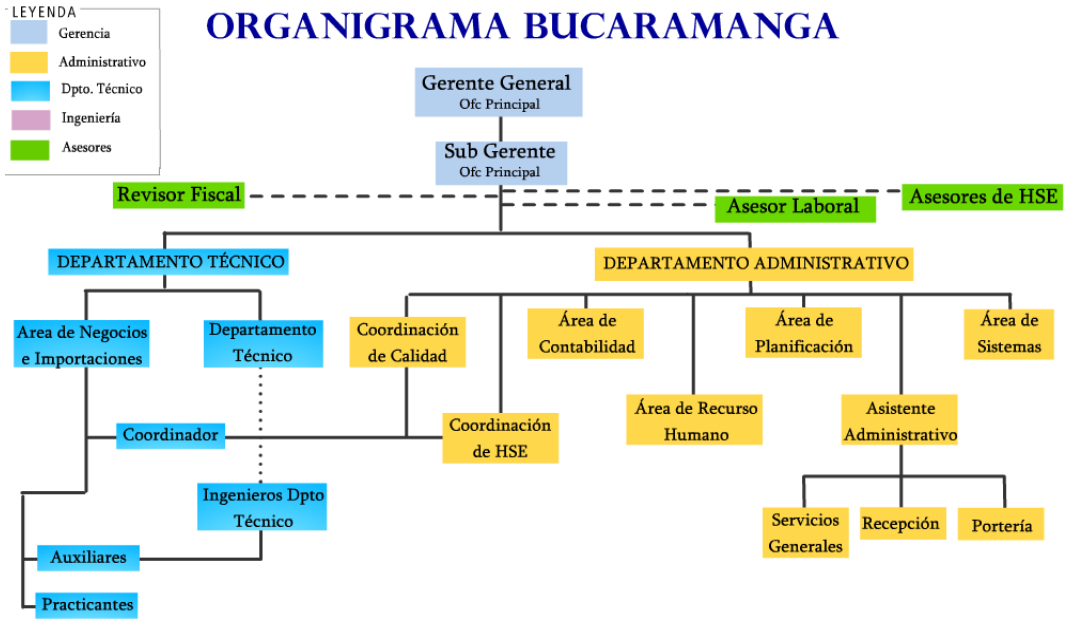
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Operación**: Comprende la configuración, administración y monitoreo del hardware y software de la infraestructura tecnológica de la organización, así como la solución de los incidentes que se pueden producir y que alteren el funcionamiento normal de los servicios de tecnología.
- **Autenticidad**: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de auditoria**: Estudio de evidencias de todas las actividades y acciones que afectan a los activos de información.
- **No repudio**: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- **Legalidad**: Los activos de información cumplen los parámetros legales, normativos y estatuarios de la institución.
- **Soporte**: Comprende el servicio de asistencia técnica para hardware, software u otros dispositivos electrónicos. En general el servicio de soporte sirve para ayudar a resolver las situaciones que puedan presentarse con los usuarios de la organización, mientras hacen uso de servicios, procesos, programas o dispositivos.
- **Información pública:** Es la información que está disponible para el personal interno y externo, como empleados, clientes y/o proveedores en general. Sin ninguna restricción de acceso.
- **Información de uso interno sin restricción de acceso:** Es toda aquella información que se encuentra disponible solo para el personal interno de la compañía (intranet y procesos del sistema de gestión).
- **Información de uso interno con restricción de acceso:** Es la información que se encuentra disponible solo para el personal interno de la compañía con permisos o ciertos niveles de privilegios. (Bases de datos, Código Fuente).

- **Información confidencial:** Esta información está disponible solo para el personal autorizado, con ciertos niveles de acceso y privilegios.
- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Activo:** Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, bases de datos…) que tenga algún valor para la organización.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgos asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. Es una medida que modifica el riesgo.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos.
- **Impacto:** El coste para la empresa de un incidente, que puede o no ser medido en términos estrictamente financieros.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometes las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Tratamiento de riesgos:** Proceso de modificar el riesgo, mediante la implementación de controles.

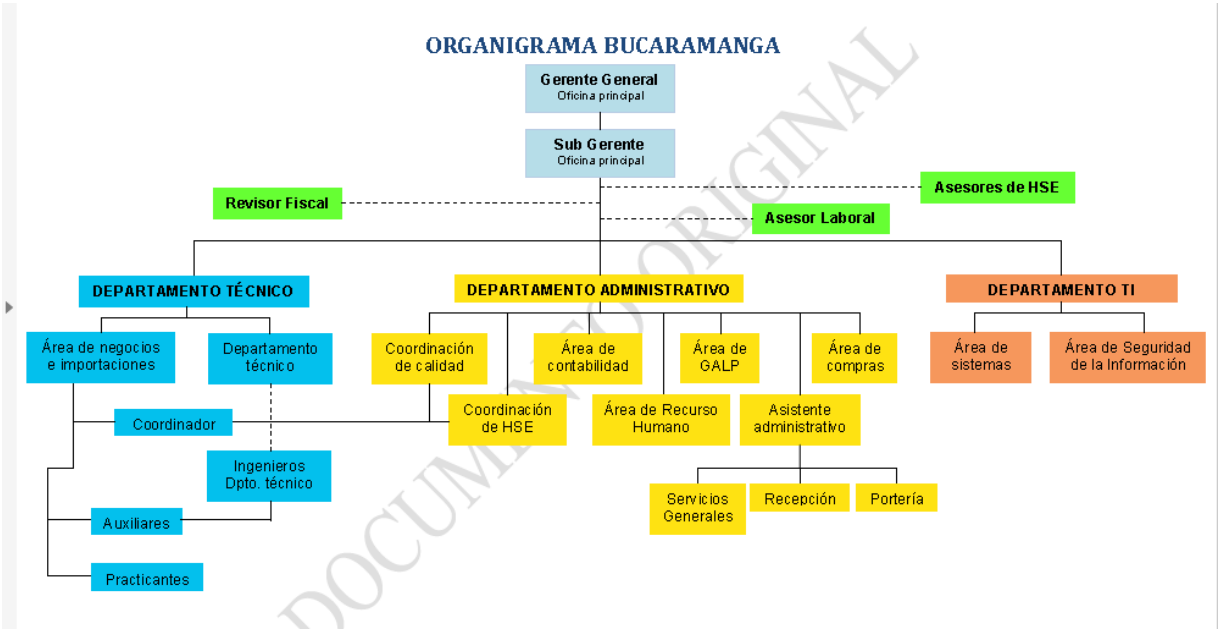
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

2. ANEXO 2. Organigrama

Antes:

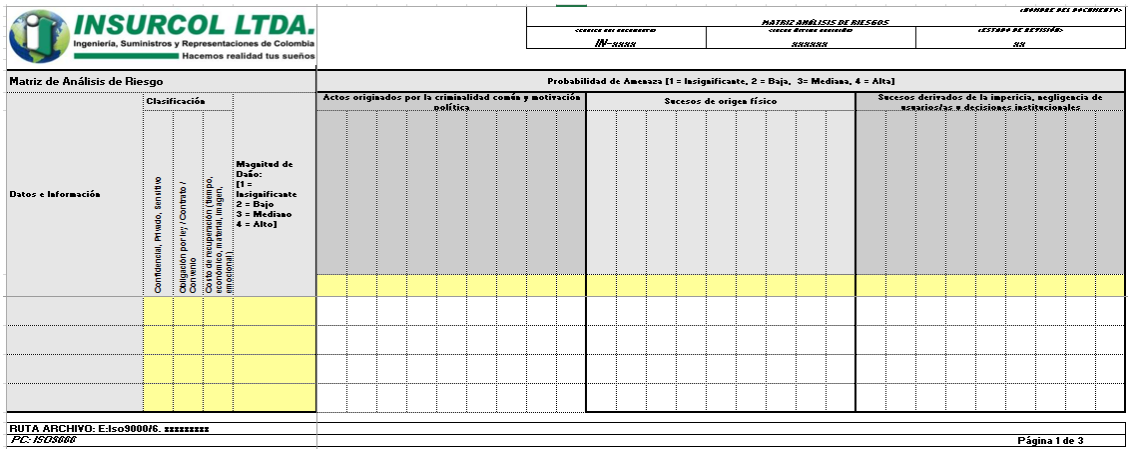


Ahora:



3. ANEXO 3: Metodologías para el análisis de riesgos

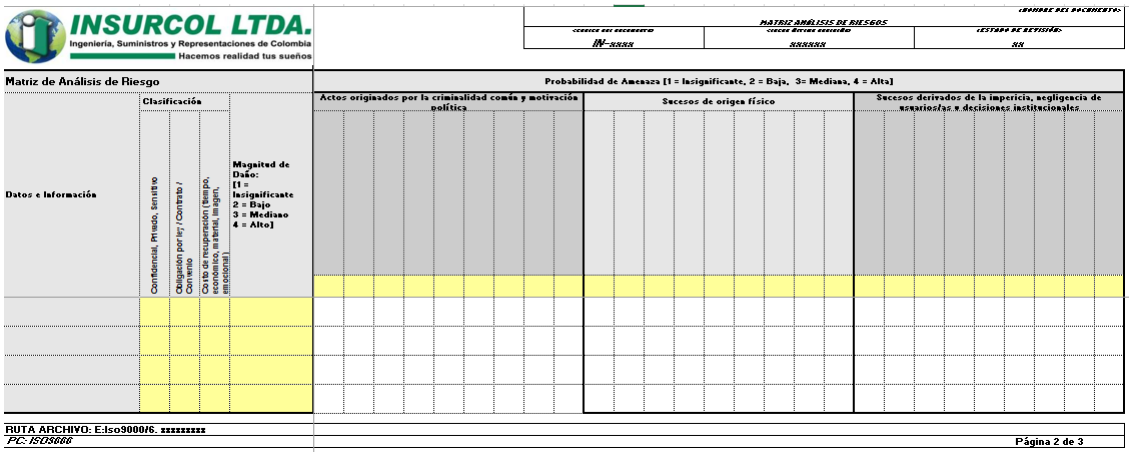
- Matriz de análisis de riesgos


INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia
Hacemos realidad tus sueños

MATRIZ ANÁLISIS DE RIESGOS		
<CÓDIGO DEL DOCUMENTO>	<FECHA ÚLTIMA REVISIÓN>	<ESTADO DE REVISIÓN>
IN-AAAA	AAAAAA	AA

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]		
	Clasificación				Actos originados por la criminalidad común y motivación política	Sucesos de origen físico	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, esfuerzo, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]			

RUTA ARCHIVO: E:\iso9000\6. xxxxxxxxx
PC: ISO8666
Página 1 de 3



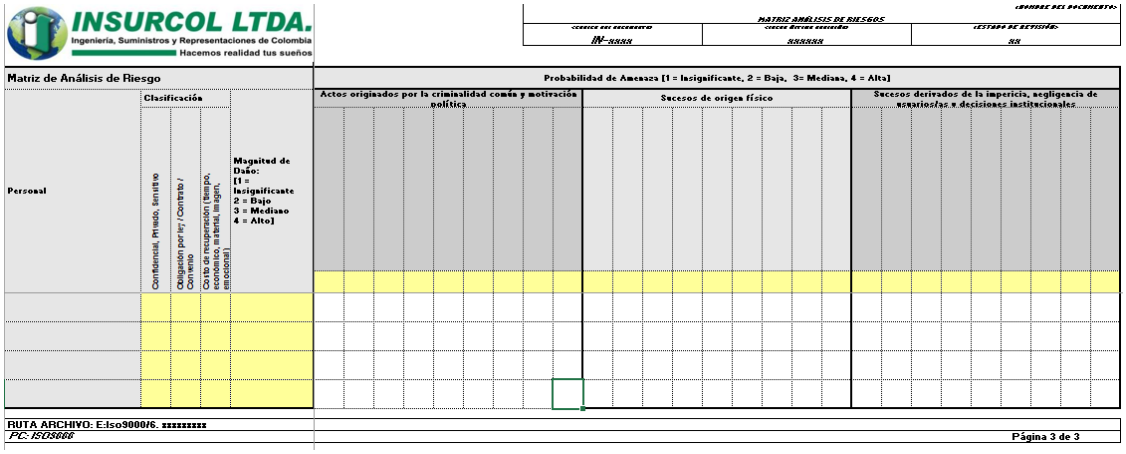
INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia
Hacemos realidad tus sueños

MATRIZ ANÁLISIS DE RIESGOS

<CÓDIGO DEL DOCUMENTO>	<CÓDIGO OTROS>	<ESTADO DE REVISIÓN>
IN-XXXX	XXXXXX	XX

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																			
	Clasificación				Actos originados por la criminalidad común y motivación política									Sucesos de origen físico										
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Cliente	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]																				

RUTA ARCHIVO: E:\Iso9000\6. xxxxxxxxx
PC: ISOS666 Página 2 de 3



INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia
Hacemos realidad tus sueños

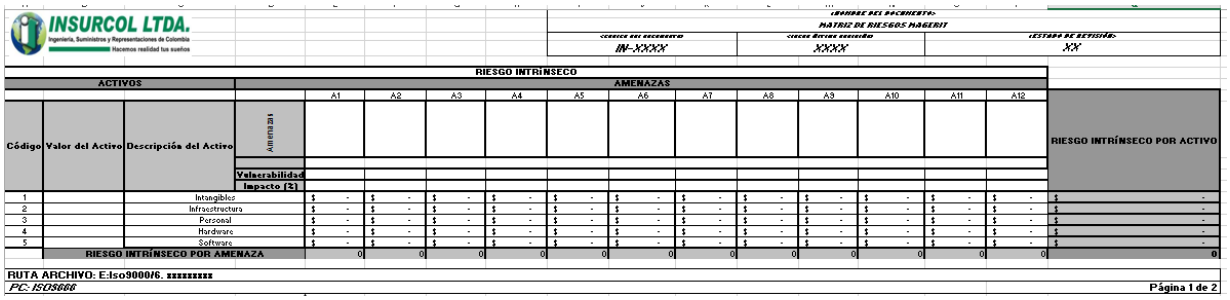
MATRIZ ANÁLISIS DE RIESGOS

<CÓDIGO DEL DOCUMENTO>	<CÓDIGO OTROS>	<ESTADO DE REVISIÓN>
IN-XXXX	XXXXXX	XX

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																			
	Clasificación				Actos originados por la criminalidad común y motivación política									Sucesos de origen físico										
Personal	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Cliente	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]																				

RUTA ARCHIVO: E:\Iso9000\6. xxxxxxxxx
PC: ISOS666 Página 3 de 3

- Matriz de riesgos Magerit



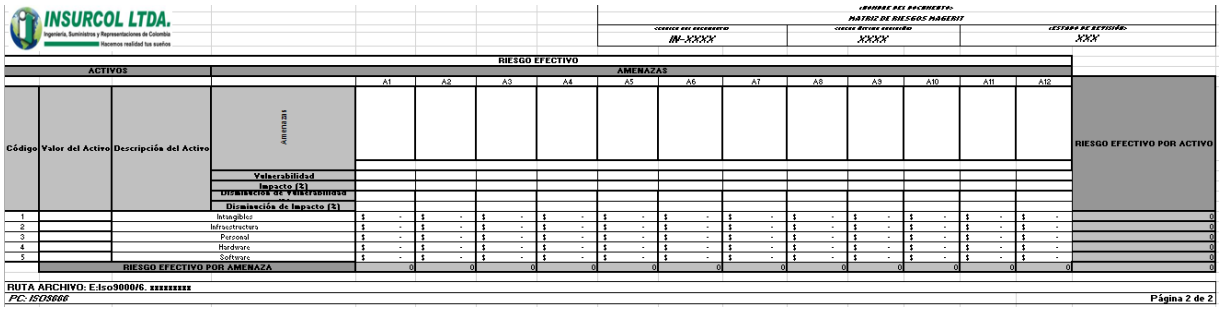
INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia
Hacemos realidad tus sueños

MATRIZ DE RIESGOS MAGERIT

<CÓDIGO DEL DOCUMENTO>	<CÓDIGO OTROS>	<ESTADO DE REVISIÓN>
IN-XXXX	XXXX	XX

			RIESGO INTRÍNSECO													
ACTIVOS			AMENAZAS													
				A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	
Código	Valor del Activo	Descripción del Activo	Amenaza													RIESGO INTRÍNSECO POR ACTIVO
			Vulnerabilidad													
			Impacto (%)													
1		Intangibles	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
2		Infraestructura	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
3		Personal	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
4		Hardware	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
5		Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RIESGO INTRÍNSECO POR AMENAZA			0	0	0	0	0	0	0	0	0	0	0	0	0	0

RUTA ARCHIVO: E:\Iso9000\6. xxxxxxxxx
PC: ISOS666 Página 1 de 2



INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia Ltda.
Hacemos realidad tus sueños

«NOMBRE DEL DOCUMENTO»
MATRIZ DE RIESGOS MAGERIT

«CODIGO DEL DOCUMENTO»	«CODIGO ÚLTIMA VERSIÓN»	«ESTADO DE REVISIÓN»
IN-XXXX	XXXX	XXX

ACTIVOS			AMENAZAS												
				A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
Código	Valor del Activo	Descripción del Activo	AMENAZAS												RIESGO EFECTIVO POR ACTIVO
			Valorabilidad												
			Impacto (I)												
			Disminución de Vulnerabilidad												
			Disminución de Impacto (I)												
1		Intangibles	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	0
2		Infraestructura	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	0
3		Personal	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	0
4		Hardware	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	0
5		Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	0
		RIESGO EFECTIVO POR AMENAZA	0	0	0	0	0	0	0	0	0	0	0	0	0	0

RUTA ARCHIVO: E:\iso9000\6. xxxxxxxxx
PC: ISO9000
Página 2 de 2

4. ANEXO 4: Análisis GAP de la norma.

Resultado del análisis aplicado:

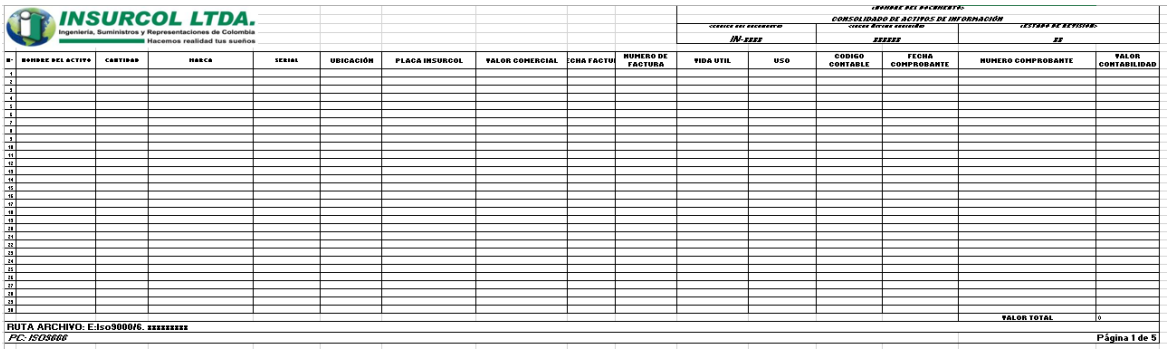
Cantidad	Códigos Status	Significado	Contribución %
3	D	El control se documentó e implementó	2%
9	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetitividad del proceso y mitigar los riesgos.	7%
25	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	19%
84	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	65%
9	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	7%
130			

5. ANEXO 5: Presupuesto de inversión.

PRESUPUESTO DE TECNOLOGIA INSURCOL 2016				
Switches Mejora de RED Insurcol	**Cant.**	**Valor Unitario**	**Valor Total**	**OBSERVACIONES**
Switch Administrable (ya sea de 12-16 o 24 puertos)	5	USD 1.284,71		
SERVIDOR PARA CAMBIOS	**Cant.**	**Valor Unitario**	**Valor Total**	**OBSERVACIONES**
WEB	1	USD 1.957,65	USD 1.957,65	
Directorio Activo	1	USD 1.957,65	USD 1.957,65	
pfsense O firewall	1	USD 1.957,65	USD 1.957,65	
ARCHIVO o NAT	1	USD 1.957,65	USD 1.957,65	
OSSIM	1	USD 1.957,65	USD 1.957,65	
Respaldos	1	USD 1.957,65	USD 1.957,65	
CABLEADO ESCTRUCTURADO CASA1	**Cant.**	**Valor Unitario**	**Valor Total**	**OBSERVACIONES**
nestor ortiz reyes	**1**	**16.467.241**	**16.467.241**	
CABLEADO ESCTRUCTURADO CASA2	**Cant.**	**Valor Unitario**	**Valor Total**	**OBSERVACIONES**
nestor ortiz reyes	**1**	**PTE**	**PTE**	
SERVICIO TECNICO DE L PROVEEDOR DE SERVICIO	**Cant.**	**Valor Unitario**	**Valor Total**	**OBSERVACIONES**
INSTALACIONES E IMPLEMENTACION Y PUESTA EN MARCHA DE LOS SERVICIOS ADQUIRIDOS EJEMPLO: (Directory)	1	$ 2.800.000,00	$ 2.800.000,00	

6. ANEXO 6: Formatos del sistema de seguridad de la información

- Consolidado de activos de información


INSURCOL LTDA.
Ingeniería, Suministros y Representaciones de Colombia
Hacemos realidad tus sueños

CONSOLIDADO DE ACTIVOS DE INFORMACIÓN

#	NOMBRE DEL ACTIVO	CANTIDAD	MARCA	SERIAL	UBICACIÓN	PLACA INSURCOL	VALOR COMERCIAL	FECHA FACTURA	NUMERO DE FACTURA	VIDA UTIL	USO	CODIGO CONTABLE	FECHA COMPROBANTE	NUMERO COMPROBANTE	VALOR CONTABILIDAD
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
														VALOR TOTAL	0

RUTA ARCHIVO: E:Iso9000/6. xxxxxxxxx

PC: ISO5668

Página 1 de 5

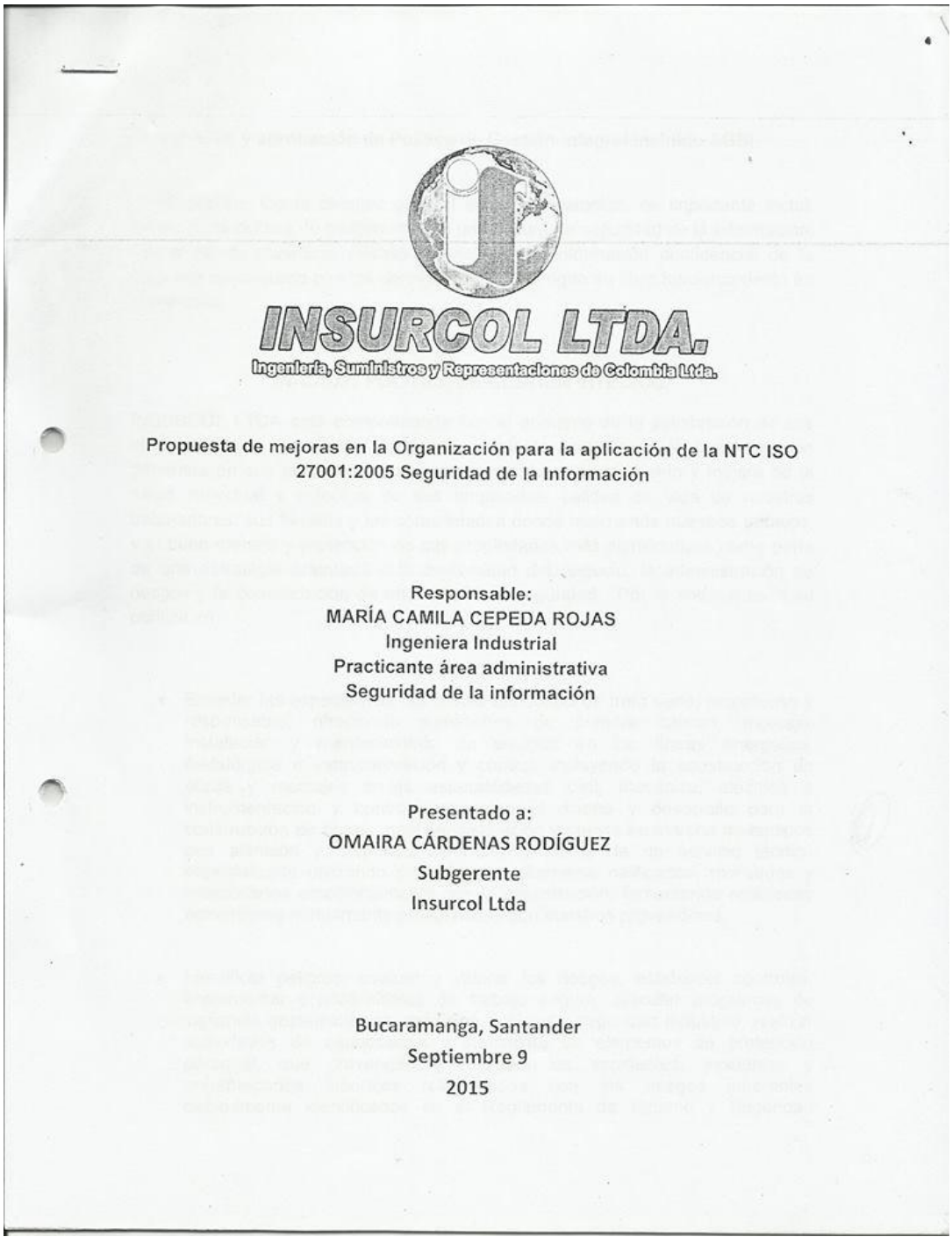
- Control y tratamiento del riesgos

INSURCOL LTDA.	CONTROL Y TRATAMIENTO DEL RIESGO		
	.....	.....	
	M-xxxx	xxxxxx	xx

Nombre del encargado:				Fecha:		
Riesgo(s) identificado(s):						
Área(s) implicada(s):						
Activar vulnerador:	1.		6.		11.	
	2.		7.		12.	
	3.		8.		13.	
	4.		9.		14.	
	5.		10.		15.	
Curar:	1.		6.		11.	
	2.		7.		12.	
	3.		8.		13.	
	4.		9.		14.	
	5.		10.		15.	
Paribler consecuencias:	1.		6.		11.	
	2.		7.		12.	
	3.		8.		13.	
	4.		9.		14.	
	5.		10.		15.	
ACTIVIDADES A REALIZAR						
ACTIVIDAD N°1						
QUÉ						
QUIÉN						
CUANDO						
DONDE						
ACTIVIDAD N°2						
QUÉ						
QUIÉN						
CUANDO						
DONDE						
ACTIVIDAD N°3						
QUÉ						
QUIÉN						
CUANDO						
DONDE						
ACTIVIDAD N°4						
QUÉ						
QUIÉN						
CUANDO						
DONDE						
Responsable:			AUTORIZA:			
Fecha de siguiente seguimiento a las actividades:						
DILIGENCIA						
RUTA ARCHIVO: E:\xx9000\6. xxxxxxxxx						
PC: 150####					Página 1 de 1	

- Matriz de análisis de riesgos: Ver anexo 3
- Matriz de riesgos Magerit: Ver anexo 3

7. ANEXO 7: Informes aprobados por alta gerencia



INSURCOL LTDA.

Ingeniería, Suministros y Representaciones de Colombia Ltda.

Propuesta de mejoras en la Organización para la aplicación de la NTC ISO 27001:2005 Seguridad de la Información

Responsable:
MARÍA CAMILA CEPEDA ROJAS
Ingeniera Industrial
Practicante área administrativa
Seguridad de la información

Presentado a:
OMAIRA CÁRDENAS RODÍGUEZ
Subgerente
Insurcol Ltda

Bucaramanga, Santander
Septiembre 9
2015

1. **Revisión y aprobación de Política de Gestión Integral incluido SGSI**

Justificación: Como directriz general en la organización, es importante incluir dentro de la política de gestión integral una cultura de seguridad de la información, con el fin de minimizar riesgos de violación a información confidencial de la empresa en conjunto con las demás normas que rigen su libre funcionamiento en el mercado.

IN-CAD31 **POLÍTICA DE GESTIÓN INTEGRAL**

INSURCOL LTDA está comprometida con el aumento de la satisfacción de sus clientes, con la protección del medio ambiente previniendo la contaminación generada en sus procesos y con la preservación, mantenimiento y mejora de la salud individual y colectiva de sus empleados, calidad de vida de nuestros trabajadores, sus familias y las comunidades donde realizamos nuestros trabajos, y el buen manejo y protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Por lo anterior basa su política en:

- Exceder las expectativas del cliente brindando un trato serio, respetuoso y responsable; ofreciendo suministros de primera calidad, montaje, instalación y mantenimiento de equipos en las líneas energética, metalúrgica e instrumentación y control, incluyendo la construcción de obras y montajes en las especialidades civil, mecánica, eléctrica e instrumentación y control; así como el diseño y desarrollo para la construcción de obras, montaje, instalación y puesta en marcha de equipos con atención y respuesta oportuna a través de un servicio técnico especializado utilizando profesionales altamente calificados, motivados y relacionados emocionalmente con la organización; fomentando relaciones comerciales mutuamente provechosas con nuestros proveedores.

- Identificar peligros, evaluar y valorar los riesgos, establecer controles, implementar procedimientos de trabajo seguro; ejecutar programas de vigilancia epidemiológica, medicina, higiene y seguridad industrial; realizar actividades de capacitación y suministro de elementos de protección personal, que prevengan y mitiguen los accidentes, incidentes y enfermedades laborales relacionados con los riesgos inherentes debidamente identificados en el Reglamento de Higiene y Seguridad

Industrial, manteniendo condiciones de seguridad adecuadas previniendo y controlando los riesgos potenciales que puedan provocar daños a la propiedad y a la integridad financiera propia y a la de nuestros clientes. Por lo tanto la organización se compromete a asegurar la competencia del personal, para que ejecute tareas que impacten en materia de Seguridad y Salud En el trabajo SST

- Identificar y controlar los aspectos e impactos socio-ambientales significativos, como vertimiento de aguas residuales sanitarias, residuos sólidos, emisión de gases y otros que se presenten en el desarrollo de las actividades; contribuir con la preservación del medio ambiente, previniendo la contaminación del suelo, el aire y el agua; haciendo uso eficiente de los recursos hídricos y energéticos, y asegurando una disposición final adecuada de los desechos. Con el compromiso de la organización, se realizara la disminución de aquellos impactos catalogados como significativos, mediante adiestramiento y capacitación del personal y estableciendo estrategias frente al cambio climático, haciendo un manejo adecuado de las emisiones por fuentes móviles y gases refrigerantes.

- Garantizar tanto en las operaciones como en las relaciones comerciales con proveedores, contratistas, clientes y competidores, el cumplimiento de buenas prácticas comerciales, teniendo en cuenta nuestros principios y valores claramente definidos en el Código de Conducta. Asimismo, INSURCOL LTDA, está comprometida en el cumplimiento de los derechos humanos, en la libertad de expresión, libre desarrollo y demás acciones para el mejoramiento de las condiciones laborales de sus trabajadores, disponiendo de prácticas encaminadas a mejorar y fortalecer las relaciones entre la familia-empleado-empresa, logrando así una estabilidad emocional, familiar y económica de éstos; ejecutando programas de acción social y garantizando el buen uso de los recursos invertidos por sus asociados.

- Proteger, preservar y administrar objetivamente la información de INSURCOL LTDA, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Igualmente, se compromete a cumplir los requisitos específicos y aquellos que aun no estando establecidos, son necesarios para el uso especificado o previsto, de igual forma, requisitos legales, reglamentarios y la normatividad local aplicables y otros que suscriba la organización, enmarcando sus Sistemas de Gestión de Calidad, Ambiente, Seguridad y Salud en el trabajo y ética y responsabilidad social en la filosofía de prevención, de mejoramiento continuo, bienestar y desarrollo de

las partes interesadas y en los lineamientos de las NTC ISO 9001:2008, NTC ISO 14001:2004, NTC OHSAS 18001:2007, SGE 21:2008 y NTC ISO 27001:2005. La Alta Dirección mantendrá permanentemente el respaldo económico a todas las actividades generadas de la implementación, desarrollo, mantenimiento y mejora de los sistemas de gestión. La Gerencia, asesores, profesionales, técnicos, personal administrativo y proveedores de servicios, participarán en los diferentes programas acordados y divulgados en un proceso creativo, prospectivo y persuasivo, para lograr efectividad en el cumplimiento de todos los objetivos del Sistema de Gestión Integral.

OBSERVACIONES:_____

2. **Revisión y aprobación de alcance del SGSI**

Justificación: Es importante establecer el alcance del SGSI para identificar los riesgos de dichos procesos y actividades, su control y tratamiento para una mejora continua en seguridad de la información en Insurcol Ltda.

ALCANCE DEL SGSI

El SGSI en Insurcol Ltda, se llevará a cabo en todas las instalaciones y procesos de la organización que manejen información confidencial para la empresa, donde se identificará la información sensible y los riesgos a los cuales se encuentra expuesta, así mismo, se establecerán los controles y tratamientos con el fin de minimizar los riesgos y controlar su manipulación.

OBSERVACIONES:_____

3. Exposición del análisis GAP

Justificación: Para la identificación el estado actual de Insurcol Ltda frente a la norma ISO 27001:2005, se aplicó el análisis GAP o análisis de brechas, herramienta importante donde se revisa punto a punto de la norma, comparado con los procedimientos, procesos y documentos actuales de la empresa.

Cantidad	Codigos Status	Significado	Contribution %
6	D	El control se documentó e implementó	5%
9	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	7%
26	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	20%
83	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	62%
9	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	7%
133			

OBSERVACIONES:_____

_____

_____

_____

_____

4. Identificación de activos

Justificación: A través de esta actividad, se busca identificar de manera exacta la cantidad de activos de información totales y reales que meneja actualmente Insurcol Ltda, teniendo en cuenta el tipo de activo de información, la cantidad existente y el valor ($) que representa para la empresa. Esta recopilación de datos es una actividad clave para el análisis de riesgos y la aplicación de metodología

OBSERVACIONES:_____

_____

_____

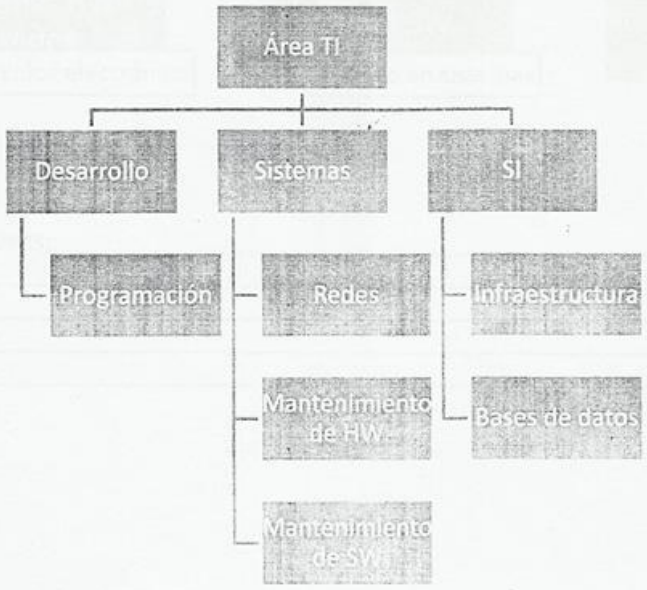
_____

_____

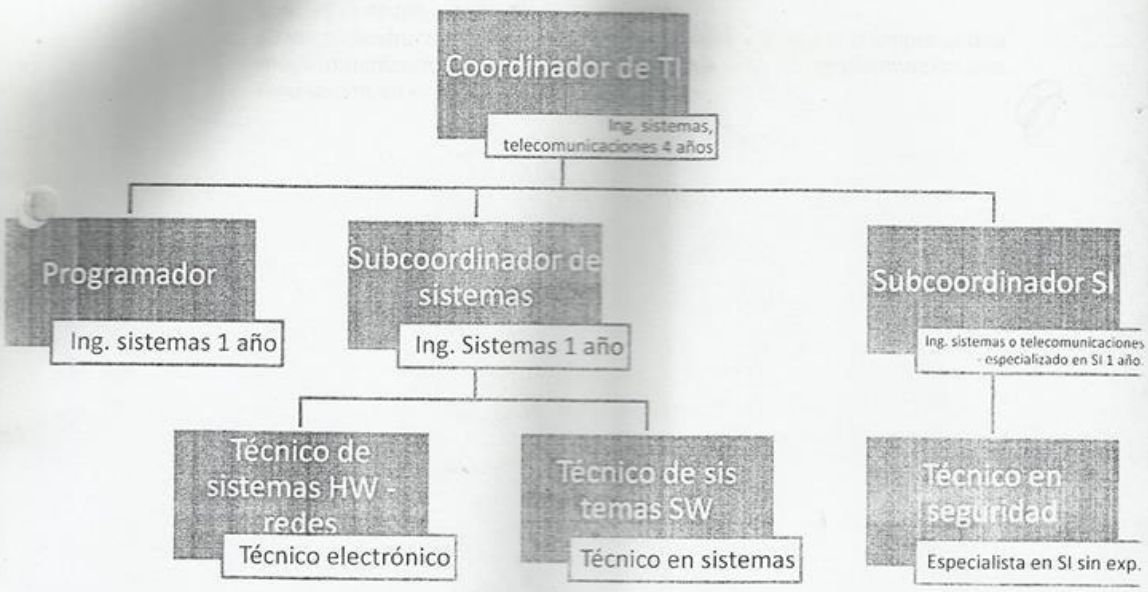
5. Área de TI como una estrategia en la organziación

Justificación: Para la aplicación de la norma ISO 27001:2005 y sus exigencias, es importante entender las herramientas TICS como unas herramientas ESTRATÉGICAS para el flujo seguro de la información a nivel interno y a nivel externo, es por esto que se propone una renovación en el área y sus cargos que la componen, permitiendo adoptar una cultura interna de seguridad.

Organigrama por procesos



Organigrama por cargos



OBSERVACIONES: _____

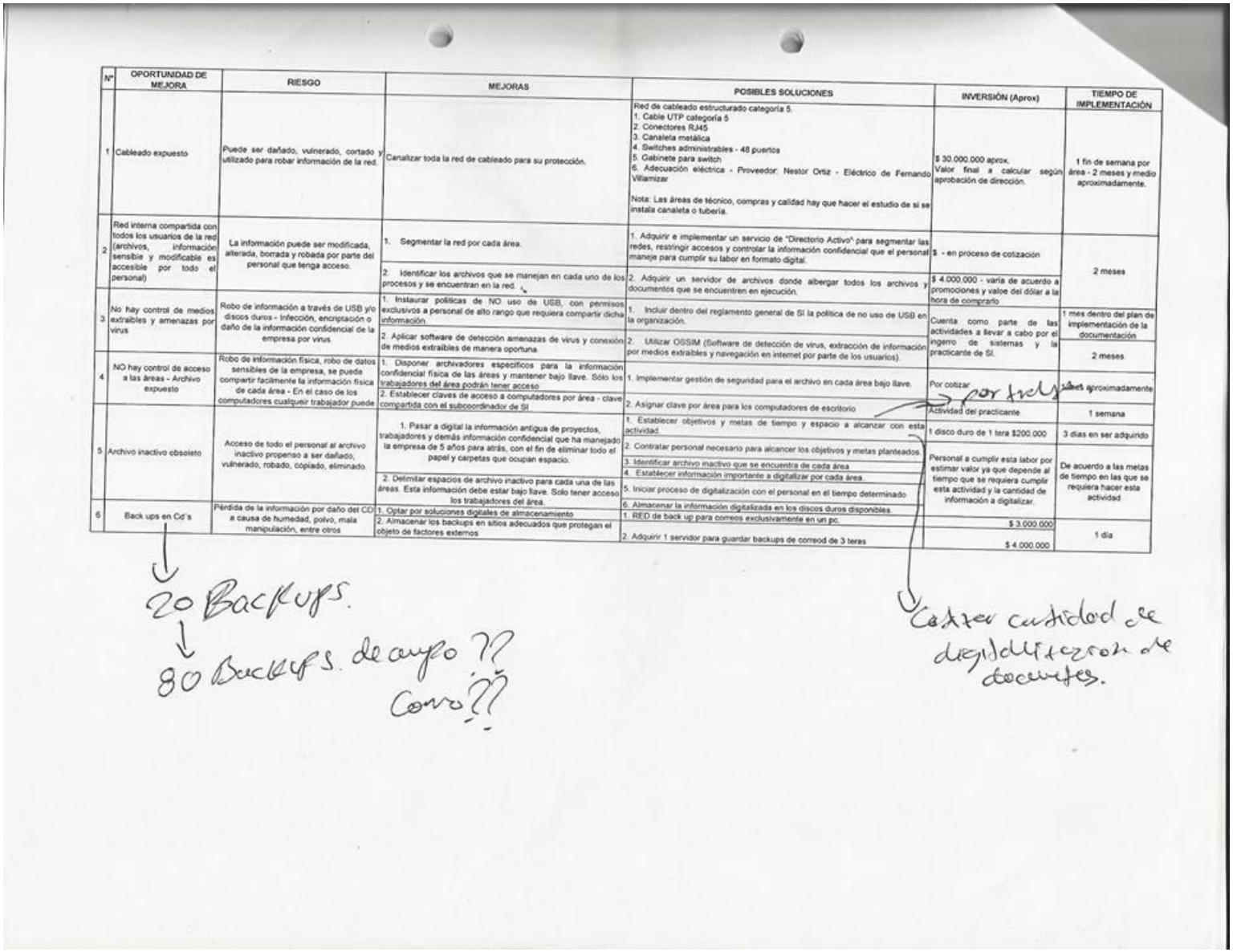
6. RECOMENDACIONES GENERALES

a. Se recomienda adquirir la última versión de la norma ISO 270001:2013
b. Es importante entender que para una aplicación completa de la norma de SI es importante identificar los activos reales y su valor real como pieza clave para su identificación de riesgos, amenazas, vulnerabilidades, controles y tratamientos.
c. Crear o reestructurar un área TI independiente permite a la empresa una mejor organización y control sobre todos los activos de información que intervienen en el flujo seguro de la misma.

Nº	OPORTUNIDAD DE MEJORA	RIESGO	MEJORAS	POSIBLES SOLUCIONES	INVERSIÓN (Aprox)	TIEMPO DE IMPLEMENTACIÓN
1	Cableado expuesto	Puede ser dañado, vulnerado, cortado y utilizado para robar información de la red.	Canalizar toda la red de cableado para su protección.	Red de cableado estructurado categoría 5. 1. Cable UTP categoría 5 2. Conectores RJ45 3. Canaleta metálica 4. Switches administrables - 48 puertos 5. Gabinete para switch 6. Adecuación eléctrica - Proveedor: Nestor Ortiz - Eléctrico de Fernando Villamizar Nota: Las áreas de técnico, compras y calidad hay que hacer el estudio de si se instala canaleta o tubería.	$ 30.000.000 aprox. Valor final a calcular según aprobación de dirección.	1 fin de semana por área - 2 meses y medio aproximadamente.
2	Red interna compartida con todos los usuarios de la red (archivos, información sensible y modificable es accesible por todo el personal)	La información puede ser modificada, alterada, borrada y robada por parte del personal que tenga acceso.	1. Segmentar la red por cada área.	1. Adquirir e implementar un servicio de "Directorio Activo" para segmentar las redes, restringir accesos y controlar la información confidencial que el personal maneja para cumplir su labor en formato digital.	$ - en proceso de cotización	2 meses
			2. Identificar los archivos que se manejan en cada uno de los procesos y se encuentran en la red.	2. Adquirir un servidor de archivos donde albergar todos los archivos y documentos que se encuentren en ejecución.	$ 4.000.000 - varía de acuerdo a promociones y valoe del dólar a la hora de comprarlo	
3	No hay control de medios extraibles y amenazas por virus	Robo de información a través de USB y/o discos duros - infección, encriptación o daño de la información confidencial de la empresa por virus.	1. Instaurar políticas de NO uso de USB, con permisos exclusivos a personal de alto rango que requiera compartir dicha información.	1. Incluir dentro del reglamento general de SI la política de no uso de USB en la organización.	Cuenta como parte de las actividades a llevar a cabo por el ingerro de sistemas y la practicante de SI.	1 mes dentro del plan de implementación de la documentación
			2. Aplicar software de detección amenazas de virus y conexión de medios extraibles de manera oportuna.	2. Utilizar OSSIM (Software de detección de virus, extracción de información por medios extraibles y navegación en internet por parte de los usuarios).		2 meses
4	NO hay control de acceso a las áreas - Archivo expuesto	Robo de información física, robo de datos sensibles de la empresa, se puede compartir facilmente la información física de cada área - En el caso de los computadores cualqueir trabajador puede ingresar a	1. Disponer archivadores especificos para la información confidencial física de las áreas y mantener bajo llave. Sólo los trabajadores del área podrán tener acceso	1. Implementar gestión de seguridad para el archivo en cada área bajo llave.	Por cotizar	1 mes aproximadamente
			2. Establecer claves de acceso a computadores por área - clave compartida con el subcoordinador de SI	2. Asignar clave por área para los computadores de escritorio	Actividad del practicante	1 semana
5	Archivo inactivo obsoleto	Acceso de todo el personal al archivo inactivo propenso a ser dañado, vulnerado, robado, copiado, eliminado.	1. Pasar a digital la información antigua de proyectos, trabajadores y demás información confidencial que ha manejado la empresa de 5 años para atrás, con el fin de eliminar todo el papel y carpetas que ocupan espacio.	1. Establecer objetivos y metas de tiempo y espacio a alcanzar con esta actividad.	1 disco duro de 1 tera $200.000	3 días en ser adquirido
				2. Contratar personal necesario para alcancer los objetivos y metas planteados.	Personal a cumplir esta labor por estimar valor ya que depende al tiempo que se requiera cumplir esta actividad y la cantidad de información a digitalizar.	De acuerdo a las metas de tiempo en las que se requiera hacer esta actividad
				3. Identificar archivo inactivo que se encuentra de cada área		
				4. Establecer información importante a digitalizar por cada área.		
			2. Delimitar espacios de archivo inactivo para cada una de las áreas. Esta información debe estar bajo llave. Solo tener acceso los trabajadores del área.	5. Iniciar proceso de digitalización con el personal en el tiempo determinado		
				6. Almacenar la información digitalizada en los discos duros disponibles.		
6	Back ups en Cd´s	Pérdida de la información por daño del CD a causa de humedad, polvo, mala manipulación, entre otros	1. Optar por soluciones digitales de almacenamiento	1. RED de back up para correos exclusivamente en un pc.	$ 3.000.000	1 día
			2. Almacenar los backups en sitios adecuados que protegan el objeto de factores externos	2. Adquirir 1 servidor para guardar backups de correod de 3 teras	$ 4.000.000	

SER CON LA Dra OMAIRA

Octubre 16-2015



Nº	OPORTUNIDAD DE MEJORA	RIESGO	MEJORAS	POSIBLES SOLUCIONES	INVERSIÓN (Aprox)	TIEMPO DE IMPLEMENTACIÓN
1	Cableado expuesto	Puede ser dañado, vulnerado, cortado y utilizado para robar información de la red.	Canalizar toda la red de cableado para su protección.	Red de cableado estructurado categoría 5. 1. Cable UTP categoría 5 2. Conectores RJ45 3. Canaleta metálica 4. Switches administrables - 48 puertos 5. Gabinete para switch 6. Adecuación eléctrica - Proveedor: Nestor Ortiz - Eléctrico de Fernando Villamizar Nota: Las áreas de técnico, compras y calidad hay que hacer el estudio de si se instala canaleta o tubería.	$ 30.000.000 aprox. Valor final a calcular según aprobación de dirección.	1 fin de semana por área - 2 meses y medio aproximadamente.
2	Red interna compartida con todos los usuarios de la red (archivos, información sensible y modificable es accesible por todo el personal)	La información puede ser modificada, alterada, borrada y robada por parte del personal que tenga acceso.	1. Segmentar la red por cada área.	1. Adquirir e implementar un servicio de "Directorio Activo" para segmentar las redes, restringir accesos y controlar la información confidencial que el personal maneje para cumplir su labor en formato digital.	$ - en proceso de cotización	2 meses
			2. Identificar los archivos que se manejan en cada uno de los procesos y se encuentran en la red.	2. Adquirir un servidor de archivos donde albergar todos los archivos y documentos que se encuentren en ejecución.	$ 4.000.000 - varía de acuerdo a promociones y valoe del dólar a la hora de comprarlo	
3	No hay control de medios extraibles y amenazas por virus	Robo de información a través de USB y/o discos duros - Infección, encriptación o daño de la información confidencial de la empresa por virus	1. Instaurar políticas de NO uso de USB, con permisos exclusivos a personal de alto rango que requiera compartir dicha información.	1. Incluir dentro del reglamento general de SI la política de no uso de USB en la organización.	Cuenta como parte de las actividades a llevar a cabo por el ingerno de sistemas y la practicante de SI.	1 mes dentro del plan de implementación de la documentación
			2. Aplicar software de detección amenazas de virus y conexión de medios extraibles de manera oportuna.	2. Utilizar OSSIM (Software de detección de virus, extracción de información por medios extraibles y navegación en internet por parte de los usuarios).		2 meses
4	NO hay control de acceso a las áreas - Archivo expuesto	Robo de información física, robo de datos sensibles de la empresa, se puede compartir facilmente la información física de cada área - En el caso de los computadores cualquier trabajador puede	1. Disponer archivadores específicos para la información confidencial física de las áreas y mantener bajo llave. Solo los trabajadores del área podrán tener acceso	1. Implementar gestión de seguridad para el archivo en cada área bajo llave.	Por cotizar	2 días aproximadamente
			2. Establecer claves de acceso a computadores por área - clave compartida con el subcoordinador de SI	2. Asignar clave por área para los computadores de escritorio	Actividad del practicante	1 semana
5	Archivo inactivo obsoleto	Acceso de todo el personal al archivo inactivo propenso a ser dañado, vulnerado, robado, copiado, eliminado.	1. Pasar a digital la información antigua de proyectos, trabajadores y demás información confidencial que ha manejado la empresa de 5 años para atrás, con el fin de eliminar todo el papel y carpetas que ocupan espacio.	1. Establecer objetivos y metas de tiempo y espacio a alcanzar con esta actividad.	1 disco duro de 1 tera $200.000	3 días en ser adquirido
				2. Contratar personal necesario para alcancer los objetivos y metas planteados.	Personal a cumplir esta labor por estimar valor ya que depende al tiempo que se requiera cumplir esta actividad y la cantidad de información a digitalizar.	De acuerdo a las metas de tiempo en las que se requiera hacer esta actividad
				3. Identificar archivo inactivo que se encuentra de cada área.		
			2. Delimitar espacios de archivo inactivo para cada una de las áreas. Esta información debe estar bajo llave. Solo tener acceso los trabajadores del área.	4. Establecer información importante a digitalizar por cada área.		
				5. Iniciar proceso de digitalización con el personal en el tiempo determinado.		
				6. Almacenar la información digitalizada en los discos duros disponibles.		
6	Back ups en Cd´s	Pérdida de la información por daño del CD a causa de humedad, polvo, mala manipulación, entre otros	1. Optar por soluciones digitales de almacenamiento	1. RED de back up para correos exclusivamente en un pc.	$ 3.000.000	1 dia
			2. Almacenar los backups en sitios adecuados que protegan el objeto de factores externos	2. Adquirir 1 servidor para guardar backups de correod de 3 teras	$ 4.000.000	

20 Backups.

80 Backups. de apoyo ??
Como??

Contar cantidad de digitalizacion de documentos.

8. ANEXO 8: Check list de actividades realizadas en la práctica empresarial

CHECK LIST DE ACTIVIDADES REALIZADAS EN LA PRÁCTICA EMPRESARIAL – INSURCOL LTDA

INSURCOL ANTES DE LOS APORTES	APORTE A LA ORGANIZACIÓN	CUMPLE	NO CUMPLE
No se contaban con políticas de Seguridad de la Información en la empresa	Se definieron las directrices en Seguridad de la Información a tener en cuenta en la organización a través del Manual de Políticas de Seguridad de la Información y la modificación de la Política de Gestión Integral con el fin de implementar acciones para una organización segura.	✓	
No se tenían identificados los activos de información	Se identificó de forma clara los activos de información de la empresa para ser protegidos a través de entrevistas dirigidas a los jefes de área, información suministrada por el área contable y observación. Se creó un formato de Inventario Activos de Información con el fin de llevar un seguimiento ordenado con la información relevante para su tratamiento.	✓	
Desconocimiento de su estado actual frente a la seguridad de la información	Aplicación de análisis GAP para conocer su estado actual en seguridad de la información con respecto a los controles de la norma NTC-ISO 27001:2013, donde se identificó las falencias y mejoras a implementar en la empresa. Con base en esto se creó el documento Declaración de Aplicabilidad donde se establecen los controles que aplican para esta empresa y las mejoras que se darán inicio a implementar con el fin de controlar los riesgos.	✓	

No se conocen los riesgos en Seguridad de la información en la empresa.	Identificación de los riesgos actuales de la empresa donde se identificaron los activos de información, las amenazas, vulnerabilidades e impacto con el fin de establecer qué riesgos presenta la organización y así aplicar metodologías para hacer tratamiento y eliminarlos. Para Este análisis se crearon los formatos Matriz Análisis de Riesgos y Matriz Magerit como parte de las metodologías a aplicar en el documento Programa de Seguridad de la Información donde se establecen todas las actividades a realizar para identificar, dar tratamiento, controlar y verificar los riesgos de información para una mayor seguridad.	✓	
Ausencia de metodologías y actividades documentadas para la seguridad de la información	Se modificaron 7 documentos del sistema de gestión integral actual de Insurcol Ltda. Se crearon 5 nuevos documentos y 4 nuevos formatos según la norma, para la implementación del sistema de seguridad de la información con el fin de definir metodologías y seguimiento a las actividades de la empresa con el fin de mejorar en la seguridad de sus activos de información.	✓	
Desconocimiento del estado actual de infraestructura y equipos para un funcionamiento seguro	Se realizó un análisis de la infraestructura actual de la empresa con el fin de identificar la distribución actual de las áreas, estado de cableado, paredes y techos, conexiones y demás detalles a tener en cuenta para una infraestructura segura. También se realizaron pruebas de los equipos tecnológicos y	✓	

	software que tiene en la actualidad la empresa con el fin de conocer su funcionalidad segura para la información de la empresa. Este análisis dio como resultado un informe presentado a Subgerencia para dar a conocer las mejoras a realizar junto con los valores de inversión a tener en cuenta para realizar el mantenimiento a sus instalaciones y adquirir el software y hardware necesario para salvaguardar su información.		
No tenían en mente cambiar su infraestructura o invertir en tecnología	Se realizó el estudio actual de la empresa en estas áreas y se les presentó las actividades, mejoras y adquisición de equipos necesarios para la organización junto con el valor para ser adquiridos e implementados en la organización.		

Realizado por: María Camila Cepeda Rojas

Aprobado por: Claudia Marcela Martínez

Cargo: Coordinadora de RRHH – Tutor de la practicante en la empresa

OBSERVACIONES: Las actividades de este documento se cumplieron en su totalidad.

INSURCOL LTDA.

Firma de conformidad Tutor de la empresa