DISEÑO DE UN PLAN ESTRATÉGICO PARA LA SEGURIDAD DE LA INFORMACIÓN DE CIAS & PROFESIONALES S.A.S

JORGE MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
MOCOA
2017

DISEÑO DE UN PLAN ESTRATÉGICO PARA LA SEGURIDAD DE LA INFORMACIÓN DE CIAS & PROFESIONALES S.A.S

JORGE MUÑOZ

Trabajo de grado para optar por el título de Especialista en Seguridad Informática

Supervisor: Ing. MARTÍN CAMILO CANCELADO RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
MOCOA
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Mocoa, Putumayo _____

DEDICATORIA

Dedico este logro con agrado a Dios, quien es el que permite que todo sea posible.

A mi esposa Liliana Alexandra Villacorte López que me apoyo incondicionalmente es este proceso; a mis hijas Daly Salome y Daniela que son el motivo de mi superación.

A mis padres María del Carmen y Luis Antonio quienes son un ejemplo de vida y enseñanza.

Jorge Muñoz

AGRADECIMIENTOS

Agradezco a DIOS ante todo por la salud y sabiduría con la que me da cada día y por oportunidad que me ha dado de poder estudiar en esta Universidad, por permitir buscar los recursos necesarios para poder terminar este trabajo.

A mi madre María del Carmen Muñoz Campo por todos sus concejos sabios y de su anhelo para estudie pese a todas las dificultades económicas durante mi formación académica y universitaria, ella es una de mis pilares para poder lograr mis metas.

A mi esposa Liliana Alexandra Villacorte
López y mis hijas Daniela Fernanda y Daly Salome que son la razón de mi vida y de todos mis esfuerzos, ellas son el motor de mi existir la razón de que todo lo que hago valga la pena.

A la Universidad Nacional Abierta y a distancia UNAD, por compartir sus conocimientos conmigo, en especial al Ing. Martin Cancelado por su ayuda contribución en mi formación y su ayuda incondicional durante mí proceso de trabajo de grado.

A la empresa Cias & Profesionales S.A.S por permitir realizar este trabajo en la empresa y por su valiosa colaboración incondicional de todos y cada uno de los socios y empleados, los cuales fueron indispensables en este proceso.

A todos mis familiares y amigos que estuvieron presentes en el desarrollo de este proceso, siempre con una voz de apoyo y entisamos a seguir adelante y terminar este proyecto.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Cias & Profesionales S.A.S es una empresa que brindar asesorías jurídicas en las diferentes especialidades del derecho, así como en la administración y recuperación de cartera, bajo los principios calidad y eficiencia, garantizando el reconocimiento y la satisfacción de los clientes. Las efectivas políticas de prestación de servicios establecidas por la empresa desde sus inicios, generaron el crecimiento de la demanda y en consecuencia, el mejoramiento de su infraestructura y de su competente talento humano, el cual interactúa garantizando a nuestros clientes una excelente calidad en los servicios y la seguridad de los activos.

El desarrollo tecnológico evoluciona constantemente, haciendo que el portafolio de servicios sea más amplio y la cobertura en la región se expanda de manera considerable; sin embargo debido a este crecimiento constante la empresa se hace vulnerable a los ataques informáticos para obtener, modificar y eliminar la Información. Por este motivo es necesario la implementación de sistemas de gestión de seguridad informática usando técnicas y metodologías apropiadas puedan proteger la información y evitar posibles ataques.

Este trabajo está enfocado al diseño de un Plan Estratégico para la Seguridad de la Información de Cias & Profesionales, mediante la revisión de la Infraestructura tecnológica, evaluación del riesgo el análisis y políticas de seguridad que contribuyan a prevenir y controlar los riesgos, garantizando la integridad coherencia, confiablidad y disponibilidad de la Información.

PALABRAS CLAVE: Seguridad de la Información. Desarrollo Tecnológico. Vulnerabilidades, amenazas y riesgos. Políticas de seguridad de la información.

ABSTRACT

Cias & Profesionales S.A.S is a company that provides legal advice in the different specialties of the law, as well as in the administration and recovery of debt, under the principles of quality and efficiency, guaranteeing the recognition and satisfaction of the clients. The effective policies of service provision established by the company from its inception, generated the growth of demand and consequently, the improvement of its infrastructure and its competent human talent, which interacts guaranteeing our customers an excellent quality in services and the security of assets.

Technological development is constantly evolving, making the portfolio of services more extensive and coverage in the region to expand considerably; however, due to this constant growth, the company becomes vulnerable to computer attacks to obtain, modify and eliminate the Information. For this reason it is necessary to implement computer security management systems using appropriate techniques and methodologies to protect information and avoid possible attacks.

This work is focused on the design of a Strategic Plan for the Information Security of Cias & Professionals, by reviewing the technological infrastructure, risk assessment, analysis and security policies that contribute to preventing and controlling risks, guaranteeing integrity coherence, reliability and availability of information.

KEYWORDS: Information Security. Technological development. Vulnerabilities, threats and risks. Information security policies.

INTRODUCCIÓN

En la actualidad los avances tecnológicos imponen grandes retos y desafíos orientados a dar respuesta adecuada cuando la Información esté en riesgo, por esta razón las Empresas u Organizaciones deben contar con un Departamento de Sistemas donde se pueda llevar a cabos las acciones pertinentes que incluyan al personal y todos los activos. Además de esto debe contar con políticas con la cual se asegura que la información de la Empresa u Organización.

Pero para que funcione muy bien el Departamento de Sistemas debemos planear primero que todo el Análisis de Riesgos, Amenazas y Vulnerabilidades con los que cuenta la empresa u Organización, realizando este tipo de análisis podemos llegar a estructurar un Plan Estratégico con las políticas de seguridad de la información ligadas a unos buenos planes de mejora continua y así asegurar la continuidad del negocio.

1. TITULO

DISEÑO DE UN PLAN ESTRATÉGICO PARA LA SEGURIDAD DE LA INFORMACIÓN DE CIAS&PROFESIONALES S.A.S

2. **PLANTEAMIENTO DEL PROBLEMA**

En Cias & Profesionales S.A.S, existe información Contable y Jurídica de carácter confidencial y muy importante de clientes que ha depositado su confianza para la Gestión de Cobranza y no se tiene definida Políticas de Seguridad Informática que conserven la confidencialidad, integridad, disponibilidad y autenticidad de la Información.

Diseñar un Plan Estratégico de Seguridad de la Información garantiza que todos o la mayoría de los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

3. FORMULACIÓN DEL PROBLEMA

La cantidad de Información y la importancia de esta, en una Empresa son fundamentales y necesarias para el funcionamiento de todas las Áreas, las cuales están expuestas a vulnerabilidades y amenazas. Por lo anterior se debe plantear si como Empresa está debidamente protegida contra amenazas.

Teniendo en cuenta las razones planteadas, es necesario dar respuesta a la siguiente pregunta:

Que controles se realizan con el fin de asegurar la Información en Cias&Profesionales S.A.S y en qué grado de vulnerabilidad se encuentra este Activo?

4. JUSTIFICACIÓN

Para Cias&Profesionales S.A.S es muy importante contar con un Plan donde se defina las Estrategias, procesos y procedimientos para garantizar la seguridad ante las amenazas que se pueden presentar para poner en riesgo la Integridad de la Información, de igual forma contar con los recursos necesarios para mantener la Infraestructura Tecnológica y así poder actuar antes las necesidades de la Empresa.
La Información es la Columna Vertebral de toda empresa, por lo tanto la seguridad de esta es un factor muy importante para su crecimiento; es por esto que ser conscientes de que el uso de las nuevas tecnologías para guardar Información hace que sea más vulnerable a las diferentes amenazas.

Es muy importante que Cias&Profesionales S.A.S se prepare no solo para prevenir el peligro ante diferentes amenazas, sino también para establecer medidas y políticas que permitan actuar frente a problemas de seguridad de la Información que puedan surgir.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Diseñar un Plan Estratégico de Seguridad de la Información orientado a cumplir con las normas, procedimientos y estándares para proteger todos los Activos y asegurar la continuidad de operaciones o actividades de la empresa Cias&Profesionales S.A.S.

5.2. OBJETIVOS ESPECÍFICOS

- Analizar identificar y valorar todos los activos de Información que tiene Cias&Profesionales S.A.S.

- Identificar las amenazas y vulnerabilidades que tiene Cias&Profesionales S.A.S a través de la revisión de la Infraestructura Tecnológica.

- Realizar un análisis de los controles actuales y determinar la evaluación del riesgo.

- Diseñar políticas de seguridad física, lógica y de comunicaciones para Cias&Profesionales S.A.S, dentro del Plan Estratégico de Seguridad que permitan prevenir y controlar frente a una situación en la cual se comprometa la Información.

6. ALCANCE

El resultado del proyecto será el Plan Estratégico para la Seguridad de la Información, establecidos en las Dependencias de Sistemas, Gestión Financiera y Gestión Documental de la siguiente forma:

- La elaboración del plan de procedimientos a corto plazo y calendario de trabajo en el periodo de tiempo establecido
- La identificación de los todos procesos de información y redes de comunicación.
- La clasificación de toda la información en niveles de importancia.
- Planes de seguridad física, lógica y de comunicaciones.

7. MARCO REFERENCIAL

Para las empresas el estar amenazadas constantemente en sus Activos, puede representar miles o hasta millones de pesos en pérdidas. Esto se debe a las vulnerabilidades en los Sistemas Operativos, Sistemas de Información o acceso a la Información sin aprobación o de manera ilícita, por eso es de gran importancia conocer todos los conceptos y conocimientos para contrarrestar estos posibles ataques.

Las preocupaciones actuales y los riesgos que esto significa son los Ataques realizados con Mezclas de diferentes virus llamados Ataques Híbridos[1], los cuales suelen ser de propagación rápida y basadas en vulnerabilidades de algún Sistema.
Virus como Blaster[2] forma parte de Programas Maliciosos que permite la intrusión a terceros, haciendo que la máquina infectada sea fácilmente atacada por otros virus, o accesos remotos no autorizados. En términos generales, se trata de un problema de seguridad que permite al intruso obtener el control de los equipos en forma remota. Por eso, y con el fin de evitar posibles ataques, es importante tanto a los administradores y responsables de Área de Sistemas la instalación inmediata de los parches proporcionados por Microsoft para corregir dicha vulnerabilidad.[3]

Según estudios realizados[4] sobre las fallas de Seguridad, más del 70% de los funcionarios de entidades son conscientes de la necesidad de la seguridad de la Información y consideran que es un tema crítico para la empresa el otro 30% consideran de muy poco valor los Activos como la Información, esta tendencia muestra que no existe la importancia adecuada y la conciencia del uso de la Información toda vez que los atacantes evolucionan constantemente ya sean por motivaciones financieras, de competencia o simplemente romper los sistemas vulnerables. Lo hace una demanda obligada de mayores esfuerzos para cerrar las puertas tan grandes que existen en temas de seguridad.

Ahora bien según un estudio de la Universidad de Texas, solo el 6% de las empresas que sufren un desastre informático sobreviven. El 94% restante tarde o temprano desaparece. Investigaciones de Gartner Group, aunque más moderadas, respaldan esta tendencia al indicar que dos de cada cinco empresas que enfrentan ataques en sus sistemas dejan de existir. Como se puede observar es importante conocer los

[1] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Seguridad de la Información http://cert.inteco.es/ [Consulta: Lunes, 17 de Noviembre de 2016]
[2] WIKIPEDIA. Definición de Blaster. http://es.wikipedia.org/wiki/Blaster [Consulta: Lunes, 17 de Noviembre de 2016]
[3]NORTON BY SYMANTEC. Jennifer, Agujeros de seguridad. http://es.norton.com/yoursecurityresource/detail.jsp?aid=patch_holes [Consulta: Miercoles, 19 de Noviembre de 2014]
[4] Recursos de Seguridad. http://www.pwc.com/ [Consulta: Miércoles, 19 de Noviembre de 2016]

activos de la empresa y detectar sus vulnerabilidades para asegurar la confidencialidad, disponibilidad e integridad de la información.

La información [5] se convierte cada vez más en uno de los activos más significativos de las organizaciones, razón por la cual se hace más necesaria la protección de esta. Además de esto cada vez son más los riesgos latentes y ataques que sufren las organizaciones a sus sistemas de información así como también son más sofisticados y dañinos estos ataques.

En Colombia, según la encuesta nacional de seguridad informática 2012 2013 [6], (ESI 2012-2013), las organizaciones son más conscientes de la necesidad de tener mecanismos de protección de la información por lo que el porcentaje aumenta año tras año y muestran a los sistemas de gestión de seguridad de la información, SCSI, como el mecanismo de protección más adecuado para el manejo seguro y conveniente de la información organizacional, generando políticas institucionales que buscan asegurar este activo de gran valor de cualquier tipo violación de la seguridad de la información incluyendo ataques de tipo interno o externo a la organización.

7.1. MARCO CONTEXTUAL

7.1.1 Historia

La empresa **CIA'S & PROFESIONALES S.A.S.** inició actividades en Mocoa - Putumayo el 15 de enero del año 2012, cuando sus accionistas, Jorge Muñoz, Claudia Marcela Villacorte López, Liliana Alexandra Villacorte López y Luz Mary Villacorte López decidieron proyectarse como profesionales independientes en asesorías jurídicas, contables, de sistemas y salud ocupacional. Las efectivas políticas de prestación de servicios establecidas por la empresa desde sus inicios, generaron el crecimiento de la demanda y en consecuencia, el mejoramiento de su infraestructura y de su competente talento humano, el cual interactúa garantizando a nuestros clientes una excelente calidad en nuestros servicios. Actualmente la empresa **CIA'S & PROFESIONALES S.A.S**. está consolidada como una empresa dedicada a la prestación de servicios profesionales como, Asesorías jurídicas (recuperación de cartera (Cobros Pre-jurídicos y Jurídicos), asesoramiento y representación jurídica, Liquidación de contratos IPS – EPS, cobro de cartera y conciliaciones ante la superintendencia Nacional de Salud, cuyo espíritu empresarial concentra su esfuerzo en la satisfacción de nuestros clientes.

[5] INTECO, Centro de Documentación. http://inteco.or.cr/esp/centro-documentacion [Consulta: Lunes, 12 de Enero de 2015]
[6] ACIS, Revista de Sistemas. http://www.acis.org.co/revistasistemas/ Lunes, 12 de Enero de 2015]

7.1.2. Ubicación y Localización

La Oficina está ubicada en la calle 7ª # 3ª-46 Barrio José María Hernández, en el municipio de Mocoa capital del Departamento del Putumayo.

Figura 1. Foto Cias & Profesionales S.AS

Fuente: El Autor

Figura 2. Ubicación

Fuente: Google 2017 – datos de Mapas

7.1.3. Descripción de la Entidad

Cias&Profesionales S.A.S, es una empresa creada con el fin de prestar Servicios en diferentes Áreas, se originó la idea por la necesidad de Empleo de personas con perfil Profesional; está integrada por Ingenieros, Abogados, Profesionales en Salud Ocupacional y demás Perfiles.

7.1.4. Empleados

Ahora la empresa cuenta con 7 funcionarios de Planta y con 10 Operadores Comisionistas en los municipios del Putumayo.

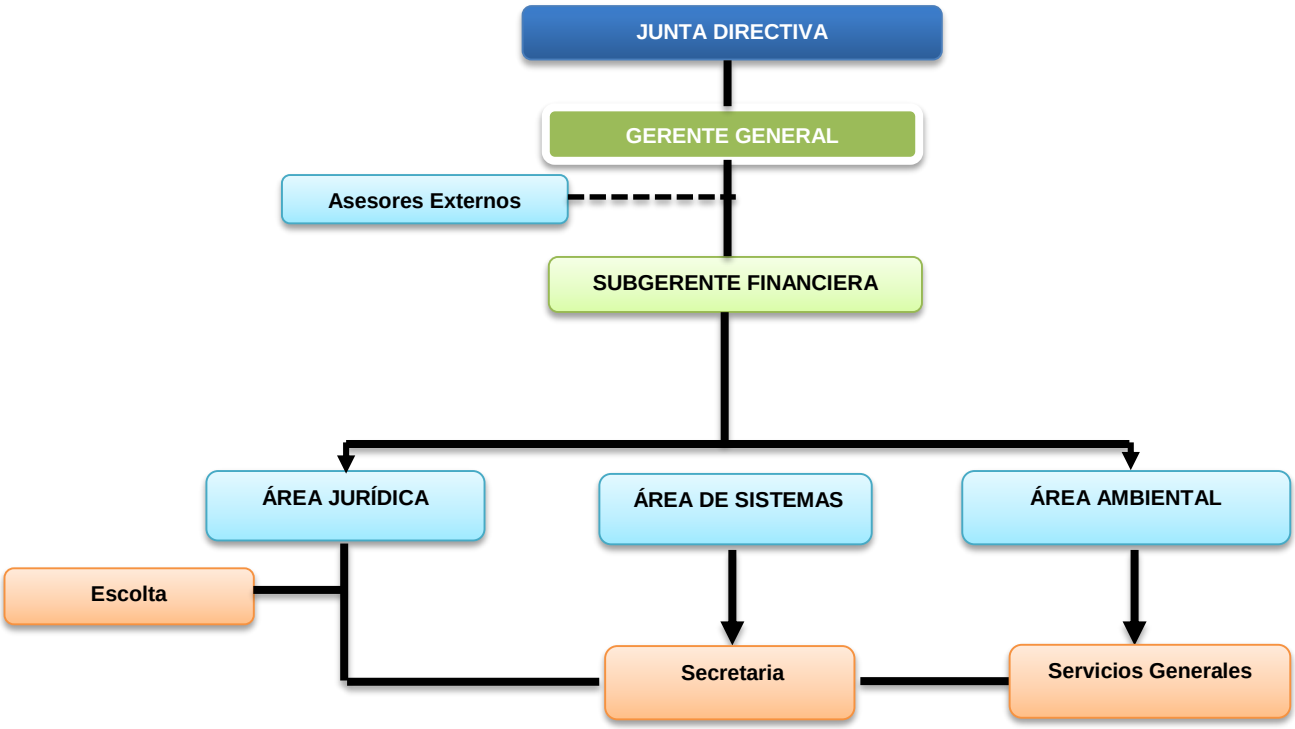
7.1.5. Funcionalidades

Cias&Profesionales S.A.S ubicada en Mocoa como sede central, en el cual se encuentran todos los activos tangibles e intangibles.

Cias&Profesionales S.A.S posee un sistema de cableado estructurado CAT 6 con 20 puntos de red, los cuales están distribuidos de forma estratégica. La red inalámbrica de la entidad dispone de una controladora Cisco.

7.1.6. Estructura Organizacional

Figura 3. Organigrama



Fuente: Portafolio de servicios Cias&Profesionales S.A.S

7.1.7. Plataforma Estratégica

7.1.7.1. Misión

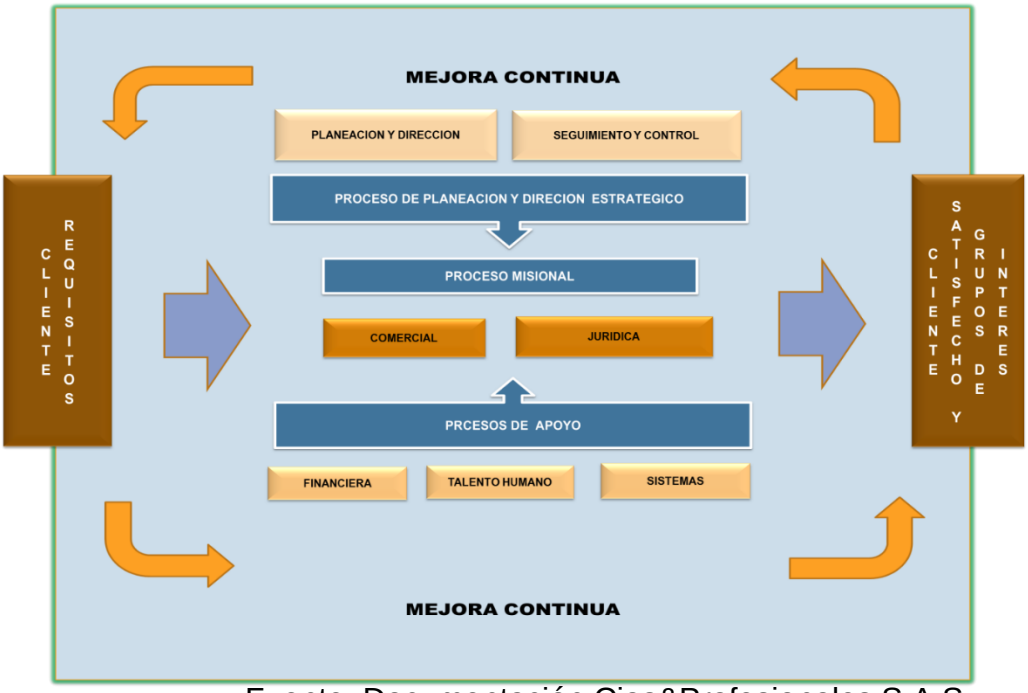
Brindar asesorías jurídicas en las diferentes especialidades del derecho, así como en la administración y recuperación de cartera, bajo los principios calidad y eficiencia, garantizando el reconocimiento y la satisfacción de nuestros clientes.

7.1.7.2. Visión

CIA´S & PROFESIONALES S.A.S, para el año 2018 será una empresa líder en el Departamento del Putumayo y con proyección nacional, reconocida por su calidad y eficiencia en la prestación de servicios de asesorías jurídicas en las diferentes especialidades del derecho, así como en la administración y recuperación de cartera. Siendo su pilar fundamental de éxito, la utilización de tecnologías y sistemas integrales, que permitan satisfacer las necesidades de nuestros clientes y partes interesadas.

7.1.7.3. Mapa de Proceso

Figura 4. Mapa de Procesos



Fuente: Documentación Cias&Profesionales S.A.S

7.2. MARCO TEÓRICO

La Planificación estratégica de la Seguridad de la Información, es el proceso de estudiar, analizar y decidir las mejores estrategias de incorporación y uso de los sistemas informáticos (SI) y de las SGSI (Sistema de Gestión de Seguridad de la Información) en una Empresa.

ISO (International Organization for Standardization): La ISO es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios, consumidores) acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros. Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

La ISO garantiza un marco de amplia aceptación mundial a través de sus 3.000 grupos técnicos y más de 50.000 expertos que colaboran en el desarrollo de estándares.

Para el caso de la seguridad de la información, la ISO y la IEC han creado un conjunto de normas para facilitar la implantación de Sistemas de Gestión de Seguridad de la Información -SGSI. Entre estas normas están las siguientes:

NORMA ISO/IEC 27000: Recoge los términos y definiciones empleados en el resto de normas de la serie, con esto se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas. Además, incluye una visión general de la familia de normas en esta área, una introducción a los sistemas de Gestión de Seguridad de la información y una descripción del ciclo de mejora continua.

NORMA ISO/IEC 27001: Es la norma principal de la serie. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo,

especifica los requisitos para implementar controles y medidas de seguridad adaptados a las necesidades de cada organización.

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoria externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standards Institution) BS7799- Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.

NORMA ISO/IEC 27002: Es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Para ello describe 11 áreas de actuación, 39 objetivos de control o aspectos a asegurar dentro de cada área y 133 controles o mecanismos para asegurar los distintos objetivos de control.

ISO/IEC 27003: Information technology - Security techniques - Information security management system implementation guidance" - provee información práctica y una guía de implementación de la norma ISO/IEC 27001.

ISO/IEC 27004 : Information technology - Security techniques - Information security management measurements" provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001.

ISO/IEC 27005:2008: Information technology - Security techniques - Information security risk management" – provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001.

ISO/IEC 27006:2007: Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems" – establece los requerimientos para Organismos que prestan servicios de auditoría y certificación.

ISO/IEC 27007: Information technology - Security techniques - Information security management systems - Auditor guidelines" - provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.

7.2.1. Estándares de Seguridad Informática

Para garantizar el éxito en la gestión de la información, se toman en cuenta los referentes que brindan los estándares para su seguridad. Con esto se espera que la información se proteja celosamente y se garantice la implantación de las estrategias que propician la integridad, la confidencialidad y la disponibilidad de ésta hacia los clientes. Entre estos estándares se encentran:

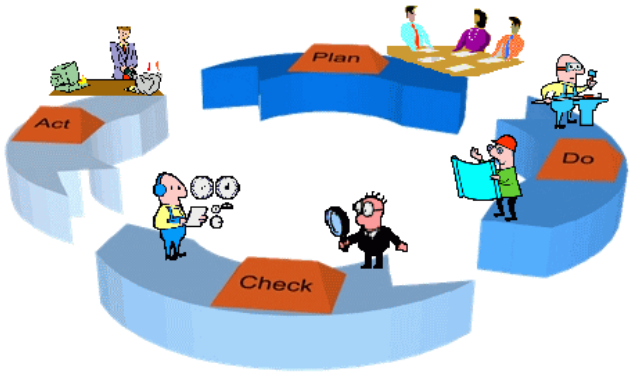
ITIL: Biblioteca de Infraestructura de Tecnologías de Información, como conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

COBIT: Objetivos de control para la información y la tecnología relacionada; concebida como un marco creado por ISACA para la tecnología de la información (TI) y el Gobierno de TI.

7.2.2. ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

Figura 5. PDCA



Fuente: JJ Consultores. http://jjconsultores.com.ar/?p=625

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.

- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI

PLAN (PLANIFICAR): ESTABLECER EL SGSI.

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Definir una política de seguridad que:

- Incluya el marco general y los objetivos de seguridad de la información de la organización
- Considere requerimientos legales o contractuales relativos a la seguridad de la información
- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI
- Establezca los criterios con los que se va a evaluar el riesgo
- Esté aprobada por la dirección.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

Identificar los riesgos:

- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios
- Identificar las amenazas en relación a los activos
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas
- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información

- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados
- Estimar los niveles de riesgo
- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- Aplicar controles adecuados
- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan
- Transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

La empresa deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información
  - Identificar brechas e incidentes de seguridad
  - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
  - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores
  - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- También revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- De igual manera se debe medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, entre otros.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

- La empresa deberá regularmente:
- Implantar en el SGSI las mejoras identificadas.

- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Hay que tener en cuenta que no tiene que haber una secuencia estricta de las fases, sino que puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

7.3. MARCO LEGAL

Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 603 de 2000, se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. Ver esta ley.

Ley Estatutaria 1266 del 31 De Diciembre De 2008, Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Ley 1341 Del 30 de Julio de 2009, Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley Estatutaria 1581 de 2012, Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos

establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

8. DISEÑO METODOLÓGICO

8.1. Fuentes de Información

Las fuentes necesarias para obtener la información para llevar a cabo este proyecto son las siguientes:

Primaria: Se obtuvo información mediante las técnicas de recolección de información como son la encuesta. Esta encuesta se llevó a cabo por medio de una serie de preguntas con diferentes opciones de respuesta, donde se pretende conocer el nivel de conocimiento sobre la Seguridad de la Información.

Secundaria: Las fuentes secundarias utilizadas para el desarrollo del proyecto, está la revisión de los documentos, consultas a páginas web, de igual las normas, estándares, modelos y metodologías vigentes relacionadas con la seguridad de la información.

8.2. Técnicas e Instrumentos de Recolección de Datos

El proyecto se apoyó en las siguientes herramientas con el fin de llevar a cabo las diferentes fases:

Técnicas: Se realizaron procesos de análisis documental, estadísticas, y una serie de encuestas y entrevista a las personas involucradas con los procesos de seguridad de la información de administración departamental.

Instrumentos: Para el desarrollo del proyecto se plantearon las siguientes herramientas:

Encuestas: Se desarrollaron una serie de encuestas\cuestionarios dirigidos a las personas que esta vinculados laboralmente con la empresa; con el fin de y lograr determinar vulnerabilidades, conductas y el conocimiento que tenían los empleados sobre las políticas de seguridad de la información de la entidad. Este proceso se realizó mediante documento físico y se entregó a los empleados de la empresa.

Observación y visitas de campo: Se utilizó las visitas de campo a las diferentes áreas de la entidad así como también la observación para registrar patrones de conducta de los funcionarios y de los sistemas de información.

Revisión documental: Se realizó la revisión de la toda la documentación referente a la Sistemas de Seguridad de la Información; NTCISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, la Metodología MAGERIT entre otros documentos que se incluyen en las referencias bibliográficas.

8.3. Línea de Investigación

La Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI de la UNAD ha definido líneas de investigación por cada cadena de formación, de acuerdo al tema de estudio de este proyecto se encuentra dentro de la siguiente línea:

CADENA DE FORMACIÓN	LÍNEA
CADENA DE FORMACIÓN DE SISTEMAS	GESTIÓN DE SISTEMAS

8.4. Población

La población de Cias & Profesionales está conformada por quince (15) empleados de los cuales dos (2) son de nómina y tienen cargos directivos incluida la gerente, también cuenta con dos (2) empleados que laboran en el área de sistemas de Información.

8.5. Muestra

Para obtener la información se aplicó una encuesta a los empleados y se tomó una muestra con el nivel de confianza de 80% de la población total. Para calcular el tamaño de la muestra se realizó la siguiente fórmula:

$$n = \frac{K^2 NPQ}{(N-1)\,E^2 + K^2 PQ}$$

$$n = \frac{(1.28^2)\,(15)\,(0.25)}{(15-1)(0.05^2) + (1.28^2)\,(0.25)}$$

n= 13.82 ≈ 14 Empleados

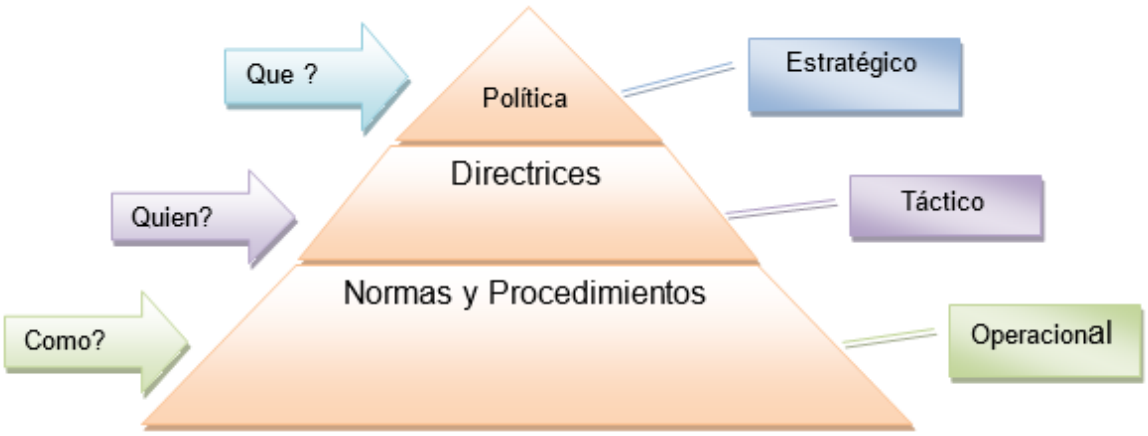
N: Tamaño de la población.
K: El nivel de confianza (para este caso, 80%, es decir, α = 0.05 y K = 1.28).
PQ: La varianza de la población. Se asume la mayor posible
(PQ = 0.25, esto es: P Para = 0.5 y Q = 0.5).
E: El error muestra o error de estimación (E = 0.05).

Los valores de **K** más utilizados y sus niveles de confianza son:

Valor de *k*	1,15	1,28	1,44	1,65	1,96	2,24	2,58
Nivel de confianza	75%	80%	85%	90%	95%	97,5%	99%

Se realiza el cálculo para el grupo de población y como resultado tenemos: 14 empleados.

Figura 6. Diseño Preliminar



Fuente: El autor

Un plan estratégico de seguridad de la Información está asentado en una serie de políticas de seguridad elaboradas previo a una evaluación de los riesgos que indicará el nivel de seguridad en el que se encuentre la Cias&Profesionales S.A.S. Estas políticas deben ser elaboradas considerando las características de la Empresa, su organización, ubicación, sus activos y la tecnología que posee la empresa.

8.6. Evaluación de los Riesgos

Con la evaluación de los riesgos podremos identificar las causas de los riesgos potenciales a los que está expuesta la organización y cuantificarlos para que la gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos, en los diferentes puntos de análisis.

Los pasos para realizar una valoración de riesgos son los siguientes:

8.6.1. Identificar los riesgos.

En este paso se identifican los factores que introducen una amenaza para la Empresa. Existen muchas formas para identificar los riesgos pero para este análisis, se utilizara los cuestionarios elaborados para cada fin como son evaluar la seguridad física, lógica, redes y recursos humanos; los mismos serán respondidos por los miembros del área de sistemas, Gestión Financiera y Gestión Documental.

Una vez identificados los factores de riesgo, con la ayuda de los integrantes de las área antes mencionadas se procede a la aprobación de los mismos dando a cada uno de ellos su valor de importancia y determinando así los de mayor relevancia.

8.6.2. Determinación de los controles existentes.

Después de identificar las causas de los riesgos que afectan a la Empresa, se determinará que riesgos el área de sistemas tiene bajo control y cuáles no, para así determinar las medidas a tomar sobre estos.

8.6.3. Análisis de riesgos.

Una vez que se hayan identificado los riesgos, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

8.6.3.1. Valoración de riesgos

Estando ya identificados los riesgos, debemos proceder a valorarlos mediante una escala como la que se presenta a continuación.

- Riesgo alto: Son todas las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.
- Riesgo medio: Serán exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.
- Riesgo bajo: Exposiciones a pérdidas que no causan un gran impacto financiero.

8.6.3.2. Crear la matriz de riesgos

Una vez que le hemos dado un criterio de importancia a cada factor de riesgo procedemos a confrontarlos con los activos informáticos mediante la elaboración de una matriz, en la cual valoramos cada activo de acuerdo a cada factor de riesgo siguiendo la escala de riesgo Alto, Medio y Bajo; para finalizar y obtener un peso o riesgo evaluado de un recurso procedemos a realizar la siguiente operación: por cada activo realizamos una sumatoria de cada uno de los resultados obtenidos de multiplicar la valoración del activo con respecto a cada factor de riesgo por la ponderación de cada factor de riesgo. Y así determinaremos según el mayor valor

cuál es el más vulnerable y a raíz de estos resultados podremos determinar qué frecuencia de revisión deberá tener.

8.7. Políticas de seguridad

Las políticas de seguridad informática serán fijadas mediante mecanismos y procedimientos que deberá adoptar la empresa para salvaguardar sus sistemas y la información que estos contienen.

Deberán ser elaboradas a medida para así recoger las características propias de la organización.

Las políticas en su contenido incluirán:

- Generalidades, dentro de este punto se incluirá: objetivo, alcance, responsabilidad, medidas a tomar en caso de incumplimiento de la política.
- Estructura de la política.- Seguridad física, seguridad lógica, seguridad en redes y seguridad en los recursos humanos.
- Para diseñar la política nos basamos en las normas y estándares de seguridad informática como son COBIT e ISO 17799.

8.8. Plan de Estratégico de Seguridad de la Información

Este plan será elaborado por la organización basándose en las políticas que se crearon a raíz del análisis de riesgo que han sido fundamentadas en las normas y/o estándares de seguridad ya mencionados.

Este plan debe ser realizado tomando en cuenta las actividades que podrá llevar a cabo la organización en un corto, mediano y largo plazo para concientizar a los recursos humanos e implantar medidas en cuanto a seguridad.

9. RECURSOS DISPONIBLES

Humanos: Para la elaboración del Trabajo se cuenta con los siguientes Profesionales:

Liliana Alexandra Villacorte Contadora Publica quien a su vez es la Gerente General de la Empresa, Luz Mary Villacorte, Profesional en salud Ocupacional Encargada

del Área de Gestión Humana y Jorge Muñoz Profesional en Ingeniería de Sistemas es el Encargado del Área de Sistemas de Cias&Profesionales S.A.S.

Físicos: Los recursos físicos con los que se cuenta para este proyecto son:

- Local Propio ubicado en la Zona Comercial de Mocoa – Putumayo.
- Infraestructura de Oficinas del Local.

Tecnológicos:

- Servidor
  - Sistema Operativo: Windows Server 2008 R2
  - Características físicas:
    - Memoria RAM: 12GB (3 x 4GB)
    - Disco Duro 1.000 G.
    - Servidor HP ProLiant ML30 Gen9
  - Procesador: Intel® Xeon ® 3.3 Gz.
- Router: ADSL, ZTE Modelo W-300, ADl, inalámbrica
- Computador de Mesa
  - Sistema Operativo: Windows 7
  - Características físicas:
    - Memoria RAM: 4GB (2 x 2GB)
    - Disco Duro 500 G
    - Compac
  - Procesador: Intel® Core I7 ®.
- Sistema de Información Ciasoft® donde se almacena la Información de los clientes de la Empresa, basado en PHP y MySQL

10. CRONOGRAMA DE ACTIVIDADES

Diseño de un Plan Estratégico para la Seguridad de La Información de Cias&Profesionales S.A.S	

Diseñar un Plan Estratégico de Seguridad de la Información orientado a cumplir con las normas, procedimientos y estándares para proteger todos los Activos y asegurar la continuidad de operaciones o actividades de la empresa Cias&Profesionales S.A.S.

Fase del proyecto	Comienzo	Fin	Fase del proyecto	Comienzo	Fin
[Fase 1]	12/01/2015	18/02/2015	Inventario de Activos	12/01/2015	18/02/2015
[Fase 2]	19/01/2015	08/02/2015	Evaluación, Identificación de Riesgos	19/01/2015	08/02/2015
[Fase 3]	09/02/2015	01/03/2015	Determinación de los controles existentes	09/02/2015	01/03/2015
[Fase 4]	02/03/2015	24/03/2015	Análisis de riesgos	02/03/2015	24/03/2015
[Fase 5]	25/03/2015	15/04/2015	Valoración del riesgos	25/03/2015	15/04/2015
[Fase 6]	16/04/2015	17/05/2015	Matriz de Riesgos	16/04/2015	17/05/2015
[Fase 7]	18/05/2015	21/06/2015	Desarrollo e Implantación de las Políticas de Seguridad	18/05/2015	21/06/2015

Enero

L	M	X	J	V	S	D
			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	31	

Febrero

L	M	X	J	V	S	D
						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	

Marzo

L	M	X	J	V	S	D
						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	31					

Abril

L	M	X	J	V	S	D
		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			

Mayo

L	M	X	J	V	S	D
				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	31

Junio

L	M	X	J	V	S	D
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					

11. DESARROLLO DEL PLAN ESTRATÉGICO DE SEGURIDAD

11.1. Diagnostico Situacional

De acuerdo a la información obtenida por la Empresa se evidencia que la Oficina de Sistemas de Información no cuenta con inventario de Activos, se registra mediante hoja de cálculo la Información de los Equipos de Cómputo, referencias y características generales.

Cias&Profesionales SAS cuenta con un pequeño centro de datos donde se encuentra swiches, routers, servidor de datos y aplicaciones configurado mediante virtualización.

Según la información recolectada los funcionarios no conocen la importancia de la seguridad de la Información, lo cual se hace evidente por el manejo de memoria USB externas para guardar la información. De igual forma la empresa no cuenta con Políticas de Seguridad para el personal que labora.

El principal riesgo de seguridad es el uso inadecuado de los Activos por parte de los funcionarios toda vez que todos sin excepción pueden acceder sin controles de seguridad a la Información.

Figura 7. Oficina de Sistemas de Información

Fuente: Autores

11.2. Metodología para el análisis y evaluación del Riesgo

Para desarrollar este proyecto se utiliza la metodología de análisis y gestión de riesgos denominada MAGERIT, esta cual fue elaborada por el Consejo Superior de Administración Electrónica de España, actualizada en 2012 a la versión 3; la metodología contempla diferentes actividades relacionadas con los activos que tienen la organización. MAGERIT proporciona un método de evaluación y gestión del riesgo relacionada con la seguridad de la información, conforme a los requerimientos y lineamientos de los estándares internacionales en específico con la serie ISO/IEC 27000; busca los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

11.3. Inventario de Activos

Esta tarea es crítica por que un buen inventario permite realizar las siguientes tareas:

- Establecer las dependencias entre los activos
- Permite valorar a los activos
- Ayuda a identificar y valorar las amenazas
- Escoge que salvaguardas serán necesarias para proteger el sistema

Según información levantada en el inventario realizado, actualmente la empresa cuenta con los siguientes activos, para su funcionamiento:

11.3.1. Servicios Internos

Para los funcionarios, de la empresa se presta los siguientes servicios:

Tabla 1. [IS] Servicios Internos

Código	Nombre	Proceso	Propietario del Activo
[INTERNET_CS]	Internet de 15 M de Velocidad.	Red de datos	Área de sistemas
Fuente: Realizado con PILAR 5.4.5			

11.3.2. Equipos

El hardware incluye toda infraestructura tecnológica tenemos los siguientes:

Tabla 2. [HW] Equipos

Código	Nombre	Proceso	Áreas Asociadas
[SDB_CS]	Servidor de base de datos y aplicaciones PROLIANT ML30 G9	Servidor de Archivos Servidor Aplicaciones (BD MySQL)	Área de sistemas
[ROUTER_CS]	Router Dlink Dir 300[7]	Red de datos	Área de sistemas
[PRINT_CS]	Impresoras de Uso común	Red de datos	Todas las Áreas
[PC_CS]	Equipos de computo	Herramientas de trabajo	CIAS&PROFESIONALES S.A.S
Fuente: Realizado con PILAR 5.4.5			

11.3.3. Soporte de Información

En la empresa se utilizan los siguientes soportes de información.

Tabla 3. [MEDIA] Soportes de Información

Código	Nombre	Proceso	Áreas Asociadas
[USB_CS]	USB medio de trasporte de Activos como la Información	Herramientas de trabajo	Área de sistemas
Fuente: Realizado con PILAR 5.4.5			

[7] (D-Link Corporation, 2012)

11.3.4. Comunicaciones

A través de los siguientes medios de transporte de información tenemos.

Tabla 4. [COM] Comunicaciones

Código	Nombre	Proceso	Áreas Asociadas
[TEL_CS]	Telefonía IP	Red de datos	Área de sistemas
[WIFI_CS]	Red Wifi	Red de datos	Área de sistemas
[LAN_CS]	Red LAN	Red de datos	Área de sistemas
[IEX_CS]	Internet	Red de datos	Área de sistemas
Fuente: Realizado con PILAR 5.4.5			

La empresa cuenta con los siguientes equipos auxiliares.

Tabla 5. [AUX] Equipamiento Auxiliar

Código	Nombre	Proceso	Áreas Asociadas
[SWITCH_CS]	Switch	Red de datos	Área de sistemas
[SISVG_CS]	Sistema De Vigilancia de 4 Cámaras 7/24	Red de datos	Área de sistemas
[RACK_CS]	Rack	Red de datos	Área de sistemas
[GAB_CS]	Gabinete Piso	Red de datos	Área de sistemas
[CAB_CS]	Cableado	Red de telefónica y Datos	Área de sistemas

Código	Nombre	Proceso	Áreas Asociadas
[OE_CS]	Otros Equipos	Red de datos	Área de sistemas
Fuente: Realizado con PILAR 5.4.5			

11.3.5. Aplicaciones (Software)

El software de base (sistema operativo, software ofimático, software utilitario, otro) tenemos los siguientes.

Tabla 6. [SW] Aplicaciones (Software)

Código	Nombre	Proceso	Áreas Asociadas
[SHS_CS]	Aplicativo Empresarial V2.0	Software para el manejo de la Información de CIAS&PROFESIONALES S.A.S	Todas las Áreas
[WO_CS]	Software Contable 7.0.29	Software de manejo de información contable y financiera.	Contabilidad Tesorería
[OS_CS]	Sistema Operativo	Sistema Operativo del Servidor de Datos y Aplicaciones	Gestión de Sistemas
[OFF_CS]	Herramientas Ofimáticas	1 Licencia de Office 2010 Pyme	Todas las Áreas
[AV_CS]	Antivirus Eset Endpoint 5.0.2126.6	1 Licencia de Antivirus para 20 computadores	Sistemas y Planeación
[OTR_CS]	Otros Software y Licencias	Licencia de Sistemas Operativos y otras aplicaciones	Todas las Áreas
Fuente: Realizado con PILAR 5.4.5			

11.3.6. Personal

El personal involucrado en esta investigación esta los siguientes:

Tabla 7. [P] Personal

Código	Nombre	Propietario del activo	Áreas Asociadas
[GG_CS]	Gerente General	CIAS&PROFESIONALES S.A.S	Gerencia
[RAS_CS]	Responsable del área de sistemas	CIAS&PROFESIONALES S.A.S	Oficina de Sistemas
[SP_CS]	Operador de Base datos y aplicaciones	CIAS&PROFESIONALES S.A.S	Oficina de Sistemas
[GFC_CS]	Gerente Financiera y de Contabilidad	CIAS&PROFESIONALES S.A.S	Gestión Financiera
[AC_CS]	Auxiliar de Contabilidad	CIAS&PROFESIONALES S.A.S	Gestión Financiera
[OP_CS]	Operadores	CIAS&PROFESIONALES S.A.S	Todas las Áreas
Fuente: Realizado con PILAR 5.4.5			

11.3.7. Instalaciones

La infraestructura donde se localiza los sistemas de información y comunicación, está ubicado en Mocoa Putumayo Barrio José María Hernández Cl. 3ª N 7 ª -14.

Tabla 8. [L] Instalaciones

Nombre	Proceso (Funciones Generales)	Propietario del activo	Áreas Asociadas
[OFC_CS]	Oficina	CIAS&PROFESIONALES S.A.S	Todas las Áreas
Fuente: Realizado con PILAR 5.4.5			

11.4. Valoración de activos

Para contemplar en la valoración de activos cada una de estas dimensiones, es necesario definir unos criterios de valoración que nos permitan ubicar la posición en que se encuentra cada activo frente a cada dimensión. A continuación se relacionan los criterios que se podrían tener en cuenta para valorar los activos con respecto a cada dimensión de seguridad.

Para cada valoración conviene tomar en consideración la siguiente información:

- Dimensiones en las que el activo es relevante
- Estimación de la valoración en cada dimensión

Tabla 9. Criterios de Valoración

Niv	Criterio
1	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto(-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo(+)
1	Bajo
0	Depreciable
Fuente: Herramienta PILAR 5.4.5	

Se evalúan los activos en una escala de 0 a 10 de la siguiente forma

Tabla 10. Escala de Valoración

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización
Fuente: Herramienta PILAR 5.4.5	

Dimensiones

[D] Disponibilidad

[I] Integridad de los datos

[C] Confidencialidad de los datos

[A] Autenticidad de los usuarios y de la información

[T] Trazabilidad del servicio y de los datos

Tabla 11. Valoración de Activos

Activos	[D]	[I]	[C]	[A]	[T]
Servicios Internos					
Internet de 2 M de Velocidad.	[7]			[7]	[7]
Aplicacion					
Aplicativo Empresarial V2.0		[9	[9]	[9	[9]
Software Contable					[7]
Sistema Operativo					[7]
Herramientas Ofimática					[7]
Antivirus Eset Endpoint 5.0.2126.6					[7]
Otros Software y Licencias					[5]
Equipo					
Servidor de base de datos y aplicaciones		[9	[9]	[9	[9]
Router Dlink Dir 300[8]					[6]
Impresoras de Uso común					[7]
Equipos de computo					[7]
Comunicacion					
Telefonía IP		[7]			
Red Wifi					[7]
Red LAN					[7]
Internet		[7]	[7]		
Equipos					
Switch	[7]				
Sistema De Vigilancia de 4 Cámaras 7/24	[7]				
Rack	[7]				
Gabinete Piso	[7]				
Cableado	[7]				
Otros Equipos	[7]				
Soportes de Información					
USB		[7	[7]		
Instalacione					
Oficina			[8]		
Persona					
Gerente General			[8]		
Responsable del área de sistemas			[8]		

[8] (D-Link Corporation, 2012)

Activos	[D]	[I]	[C]	[A	[T]
Operador de Base datos y aplicaciones			[7]		
Gerente Financiera y de Contabilidad			[8]		
Auxiliar de Contabilidad			[7]		
Operadores			[6]		
Fuente: Herramienta Pilar 5.4.5					

11.5. Vulnerabilidades, Amenazas y Riesgos

Una vez realizado trabajo de campo en Cias & Profesionales SAS, se da a conocer el siguiente estudio de amenazas vulnerabilidades y riesgos.

11.5.1. Identificación de las Vulnerabilidades

11.5.1.1. Vulnerabilidades Físicas

Dentro de las visitas se puedo establecer que los activos físicos no tienen seguridad, haciendo fácil la modificación, alteración hurto o destrucción de los mismos. No hay zonas restringidas para el centro del cableado y el servidor.

Existe carencia de un centro de datos con las condiciones físicas adecuadas de acuerdo a los estándares que la norma que los regula (ANSI/TIA/EIA-568), hay disposición desorganizada de cables de energía y de red.

La protección física de las herramientas informáticas es de gran importancia, así como del servidor que puedan contener información crítica y sensible, de esta manera lograr garantizar la continuidad del servicio.

Figura 8. Disposición del Cable de red

Fuente: Autores

Figura 9. Disposición del Cable Eléctrico

Fuente: Autores

Figura 10. Gabinete en mal estado

Fuente: Autores

11.5.1.2. Vulnerabilidades Naturales

La ubicación Geográfica de la cuidad de Mocoa hace que la humedad sea muy alta, situación que provoca alto grado de corrosión y provoca una vulnerabilidad relativa puesto que en centro de datos no cuenta con equipos de climatización que permitan controlar la humedad

Figura 11. Paredes con humedad

Fuente: Autores

Figura 12. Deterioro de la pared

Fuente: Autores

11.5.1.3. Vulnerabilidades de Hardware y Software

Se evidencia que hay que la entidad no cuenta con políticas y formatos (listas de chequeó) que les permitan registrar y tramitar de manera adecuada las nuevas configuraciones o cambios que se realicen en servidores, equipos de cómputo, firewall, y otros dispositivos del centro de datos.

En la área donde está ubicada la Empresa son muy problemas eléctricos; a pesar de contar con 1 UPS no cuenta con un raspado total de los equipos de cómputo.

No existe un medio definido para la eliminación o reutilización de equipos; el estudio realizado se demuestra que la empresa no cuenta con procesos documentados sobre cómo realizar la destrucción de los equipos de cómputo y medios que ya no se usen.

11.5.1.4. Vulnerabilidades de Dispositivos o Medios

Para el personal que ya no labora en la empresa, no existe un medio definido para la devolución de Dispositivos y medios de almacenamiento sin el borrado de seguridad que amerite según el caso.

11.5.1.5. Vulnerabilidades de Comunicaciones

De acuerdo a los registros, permitió realizar una verificación de seguridad en la red mediante el análisis de los puertos abiertos en servidores y equipos de cómputo.

No se aplica periódicamente pruebas de red con Sniffer que les permita el diagnóstico remoto y la revisión de la configuración de puertos y el tráfico de la red de datos.

11.5.1.6. Vulnerabilidades de Personal

El factor humano compromete la seguridad de los activos de la empresa, porque no hay estrategias que permitan capacitar y concientizar a los funcionarios del uso de las buenas prácticas y de las políticas de Seguridad de la empresa.

11.5.2. Identificación y valoración de Amenazas

Las amenazas están clasificadas en cuatro grupos:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataque intencionados

Esta actividad consta de 2 sub-tareas:

- Identificación de las amenazas
- Valoración de la amenazas

11.5.2.1. Identificación de las amenazas

Las amenazas están clasificadas de la siguiente manera:

[N] Desastres naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.16] Introducción de falsa información
[E.17] Degradación de la información
[E.18] Destrucción de la información
[E.19] Divulgación de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal

[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 12. Identificación de Amenazas de los Activos

Activos	Amenazas
INTERNET DE 2 M DE VELOCIDAD	[A.7] Uso no previsto
SERVIDOR DE BASE DE DATOS Y APLICACIONES PROLIANT ML30 G9	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [E.2] Errores del administrador del sistema / de la seguridad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.11] Acceso no autorizado
IMPRESORAS DE USO COMÚN	[I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.11] Acceso no autorizado
EQUIPOS DE COMPUTO	[N.2] Daños por agua [N.*] Desastres naturales [I.*] Desastres industriales [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [A.6] Abuso de privilegios de acceso
ROUTER DLINK DIR 300	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado

Activos	Amenazas
USB	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información
TELEFONÍA IP	[I.8] Fallo de servicios de comunicaciones [E.9] Errores de [re-]encaminamiento [E.15] Alteración de la información [E.19] Fugas de información [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha)
RED WIFI	[I.8] Fallo de servicios de comunicaciones [E.9] Errores de [re-]encaminamiento
RED LAN	[I.8] Fallo de servicios de comunicaciones [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [A.5] Suplantación de la identidad del usuario [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado
INTERNET	[I.8] Fallo de servicios de comunicaciones [E.15] Alteración de la información
SWITCH	[I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad
SISTEMA DE VIGILANCIA	[I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad
RACK	[I.3] Contaminación medioambiental
GABINETE PISO	[I.3] Contaminación medioambiental
CABLEADO	[I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad
OTROS EQUIPOS AUXILIARES	[I.3] Contaminación medioambiental

Activos	Amenazas
APLICATIVO EMPRESARIAL	[I.5] Avería de origen físico o lógico [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
WORD OFFICE	[I.5] Avería de origen físico o lógico [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario
SISTEMA OPERATIVO	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21]Errores de mantenimiento / actualización de programas (software) [A.7] Uso no previsto
OFIMÁTICA	[E.1] Errores de los usuarios [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino
ANTIVIRUS ESET ENDPOINT	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21]Errores de mantenimiento/ actualización de programas (software)
OTROS SOFTWARE	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21]Errores de mantenimiento / actualización de programas (software)
GERENTE GENERAL	[E.28.1] Enfermedad [E.28.2] Huelga [A.29] Extorsión [A.30] Ingeniería social (picaresca)
RESPONSABLE DEL ÁREA DE SISTEMAS	[E.4] Errores de configuración [E.19.3] A personas externas que no necesitan conocerlo [A.29.2] Ataque desde el interior

Activos	Amenazas
OPERADOR DE BASE DATOS Y APLICACIONES	[E.4] Errores de configuración [E.19.3] A personas externas que no necesitan conocerlo [A.29.2] Ataque desde el interior
GERENTE FINANCIERA Y DE CONTABILIDAD	[E.28.1] Enfermedad [E.28.2] Huelga [A.29] Extorsión [A.30] Ingeniería social (picaresca)
AUXILIAR DE CONTABILIDAD	[E.28.1] Enfermedad [E.28.2] Huelga [A.29] Extorsión [A.30] Ingeniería social (picaresca)
OPERADORES	[A.29] Extorsión [A.30] Ingeniería social (picaresca) [E.28.1] Enfermedad
Fuente: Realizado con PILAR 5.4.5	

11.5.2.2. Valoración de las amenazas

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

Tabla 13. Degradación

MA	MUY ALTA	Es Casi seguro que la amenaza afectara la seguridad
A	ALTA	Es Probable que la amenaza afectara la seguridad
M	MEDIA	Es posible que la amenaza afectara la seguridad
B	BAJA	Es improbable que la amenaza afectara la seguridad
MB	MUY BAJA	Es impensable que la amenaza afectara la seguridad
Fuente: Herramienta Pilar 5.4.5		

Tabla 14. Probabilidad

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARO
Fuente: Herramienta Pilar 5.4.5	

Tabla 15. Valoración de Amenazas

Activos	Amenazas	P	[D]	[I]	[C]	[A	[T]
INTERNET	[A.7] Uso no previsto	MA	M	M	M	-	-
SOFTWARE EMPRESARIAL	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	B	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	B	B	M	-	-
	[A.5] Suplantación de la identidad del usuario	P	A	A	A	-	-
SOFTWARE CONTABLE	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	B	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	B	B	M	-	-
	[A.5] Suplantación de la identidad del usuario	P	A	A	A	-	-
HERRAMIENTAS OFIMÁTICA	[E.1] Errores de los usuarios	P	M	M	M	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	B	-	-	-
	[A.8] Difusión de software dañino	PP	B	B	B	-	-
ANTIVIRUS	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	M	-	-	-
SISTEMAS OPERATIVOS	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[E.1] Errores de los usuarios	PP	M	M	M	-	-
	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	B	M	M	-	-

Activos	Amenazas	P	[D]	[I]	[C]	[A	[T]
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	B	-	-	-
	[A.7] Uso no previsto	P	B	B	B	-	-
OTROS SOFTWARE Y LICENCIAS	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	PP	B	B	B	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	-	-	-
SERVIDOR DE BASE DE DATOS Y APLICACIONES	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.3] Contaminación medioambiental	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[I.7]Condiciones inadecuadas de temperatura o humedad	MA	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	MA	-	A	A	-	-
	[A.23] Manipulación del hardware	MA	A	-	A	-	-
IMPRESORAS DE USO COMÚN	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	PP	-	M	M	-	-
EQUIPOS DE COMPUTO	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.*] Desastres industriales	P	B	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-

Activos	Amenazas	P	[D]	[I]	[C]	[A	[T]
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Uso no previsto	P	M	B	M	-	-
ROUTER DLINK	[N.1] Fuego	PP	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	[A.11] Acceso no autorizado	PP	-	B	B	-	-
TELEFONÍA IP	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.10] Errores de secuencia	P	-	M	-	-	-
	[E.15] Alteración de la información	P	-	A	-	-	-
	[E.19] Fugas de información	P	-	-	M	-	-
	[A.7] Uso no previsto	P	-	M	M	-	-
	[A.9] [Re-]encaminamiento de mensajes	P	-	-	M	-	-
	[A.10] Alteración de secuencia	P	-	M	-	-	-
	[A.12] Análisis de tráfico	P	-	-	A	-	-
	[A.14] Interceptación de información (escucha)	P	-	-	A	-	-
RED WIFI	[I.8] Fallo de servicios de comunicaciones	P	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	B	-	-
RED LAN	[I.8] Fallo de servicios de comunicaciones	PP	B	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.10] Errores de secuencia	P	-	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	P	-	M	M	M	-
	[A.9] [Re-]encaminamiento de mensajes	P	-	-	M	-	-

Activos	Amenazas	P	[D]	[I]	[C]	[A	[T]
	[A.10] Alteración de secuencia	P	-	M	-	-	-
	[A.11] Acceso no autorizado	PP	-	M	-	-	-
INTERNET	[I.8] Fallo de servicios de comunicaciones	P	A	-	-	-	-
	[E.15] Alteración de la información	P	-	B	-	-	-
SWITCH	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	A	-	-	-	-
CABLEADO	[I.3] Contaminación medioambiental	PP	A	-	-	-	-
	[I.4] Contaminación electromagnética	MR	B	-	-	-	-
GABINETE	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
SISTEMA DE VIGILANCIA	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	A	-	-	-	-
RACK	[I.3] Contaminación medioambiental	PP	A	-	-	-	
OTROS	[I.3] Contaminación medioambiental	P	M	-	-	-	
USB	[E.15] Alteración de la información	PP	-	B	-	-	-
	[E.19] Fugas de información	PP	-	-	B	-	-
	[A.15] Modificación de la información	PP	-	B	-	-	-
	[A.19] Revelación de información	PP	-	-	B	-	-
OFICINA	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[N.*.4] Terremotos	P	M	-	-	-	-
	[N.*.9] Tsunamis	P	M	-	-	-	-
	[N.*.11] Calor extremo	MA	B	-	-	-	-
	[I.*] Desastres industriales	P	B	-	-	-	-
	[A.27] Ocupación enemiga	P	MA	-	A	-	-
	[A.11] Acceso no autorizado	P	-	A	M	-	-
	[A.27] Ocupación enemiga	P	M	-	M	-	-
GERENTE	[E.28.1] Enfermedad	P	M	M	M	-	-
	[E.28.2] Huelga	PP	B	-	-	-	-

Activos	Amenazas	P	[D]	[I]	[C]	[A	[T]
GENERAL	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
RESPONSABLE DEL ÁREA DE SISTEMAS	[E.4] Errores de configuración	P	-	A	-	-	-
	[E.19.3] A personas externas que no necesitan conocerlo	P	-	A	-	-	-
	[A.29.2] Ataque desde el interior	P	M	M	M	-	-
OPERADOR DE BASE DATOS Y APLICACIONES	[E.4] Errores de configuración	P	-	A	-	-	-
	[E.19.3] A personas externas que no necesitan conocerlo	P	-	A	-	-	-
	[A.29.2] Ataque desde el interior	P	M	M	M	-	-
GERENTE FINANCIERA Y DE CONTABILIDAD	[E.28.1] Enfermedad	P	M	M	M	-	-
	[E.28.2] Huelga	PP	B	-	-	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
AUXILIAR DE CONTABILIDAD	[E.28.1] Enfermedad	MA	M	-	-	-	-
	[E.28.2] Huelga	MR	B	-	-	-	-
	[A.29] Extorsión	PP	M	B	M	-	-
	[A.30] Ingeniería social (picaresca)	P	M	M	M	-	-
OPERADORES	[E.28.1] Enfermedad	PP	M	-	-	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	M	M	M	-	-
Fuente: Realizado con PILAR 5.4.5							

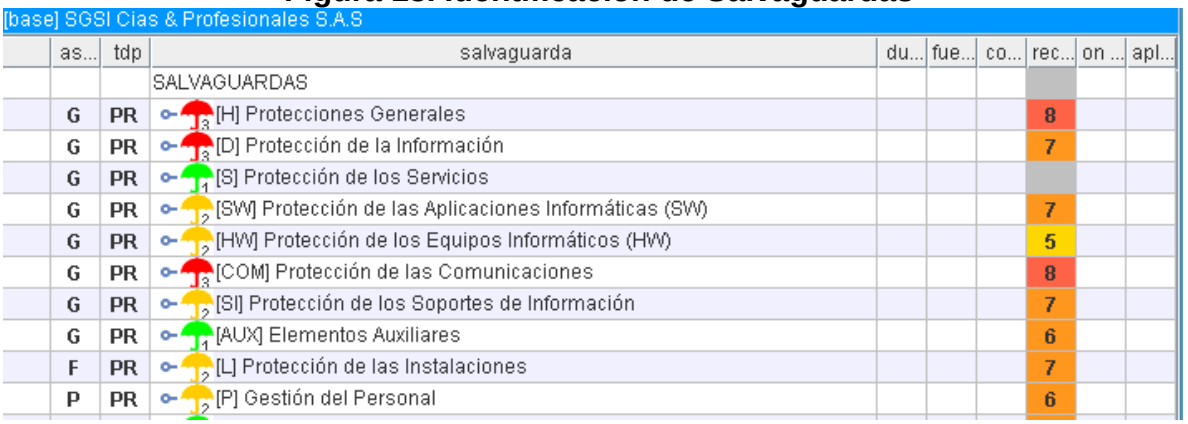
11.5.3. Caracterización de las Salvaguardas

Se procede a identificar las salvaguardas efectivas para la empresa junto con la eficacia que tiene cada una de ellas para mitigar el riesgo.

11.5.3.1. Identificación de las salvaguardas

En esta tarea contaremos con la ayuda de la herramienta PILAR 5.4.5 que nos ayuda a la elección de salvaguardas de cada activo para contrarrestar las amenazas identificadas en los pasos anteriores.

Figura 13. Identificación de Salvaguardas



Fuente: Pilar 5.4.5

La información detallada de Salvaguardas está adjuntas en el anexo A.

11.5.4. Gestión de Riesgos

Después de análisis de Riesgos se procede a la Gestión de Riesgos

11.5.4.1. Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de amenaza

Tabla 16. Niveles de Riesgo

Valor	Nivel
9	Nivel 9
8	Nivel 8
7	Extremadamente crítico
6	Muy crítico
5	Critico

Valor	Nivel
4	Muy Alto
3	Alto
2	Medio
1	Bajo
0	Despreciable
Fuente: Herramienta Pilar 5.4.5	

Tabla 17. Riesgo Potencial

Activos	[D]	[I]	[C]	[A]	[T]
Servicios Internos					
Internet	{4,2}	{5,4}	{5,4}	-	-
Equipamiento					
Aplicaciones					
Aplicación Empresarial	-	{6,6}	{6,6}	-	-
Software Contable	-	{5,4}	{5,4}	-	-
Ofimática	-	{5,4}	{5,4}	-	-
Antivirus	-	{5,4}	{5,4}	-	-
Sistema Operativo	-	{5,4}	{5,4}	-	-
Otros Software y Licencias	-	{4,5}	{4,5}	-	-
Equipos					
Servidor de base de datos y aplicaciones PROLIANT ML30 G9	-	{6,6}	{6,6}	-	-
Router Dlink Dir 300	-	{3,6}	{3,6}	-	-
Impresoras de Uso Común	-	{4,5}	{4,5}	-	-
Equipos de computo	-	{1,8}	{1,8}	-	-
Comunicaciones					
Telefonía IP	-	{3,3}	-	-	-
Red WIFI	-	-	{4,5}	-	-
Red LAN	-	{4,5}	{6,6}	{4,5}	-
Internet	-	{4,5}	-	-	-
Elementos Auxiliares					
Switch	{4,5}	-	-	-	-
Sistema De Vigilancia de 4 Cámaras	{2,4}	-	-	-	-
Rack	{3,3}	-	-	-	-
Gabinete Piso	{3,3}	-	-	-	-
Cableado	{3,3}	-	-	-	-
Otros Equipos	{2,1}	-	-	-	-
Soportes de Información					
USB	-	{1,8}	{1,8}	-	-
Instalaciones					
Oficina	-	-	{6,6}	-	-
Gerente General					
Responsable del área de sistemas	-	-	{4,8}	-	-
Operador de Base datos y	-	-	{3,3}	-	-
Gerente Financiera y de	-	-	{3,3}	-	-
Auxiliar de Contabilidad	-	-	{6,0}	-	-

Activos	[D]	[I]	[C]	[A]	[T]
Operadores	-	-	{3,0}	-	-
Fuente: Realizado con PILAR 5.4.5					

El nivel de riesgo este se divide en cuatro zonas:

•Bajo: El nivel de riesgo es bajo, y por lo tanto es necesario emplear Salvaguardas adicionales.

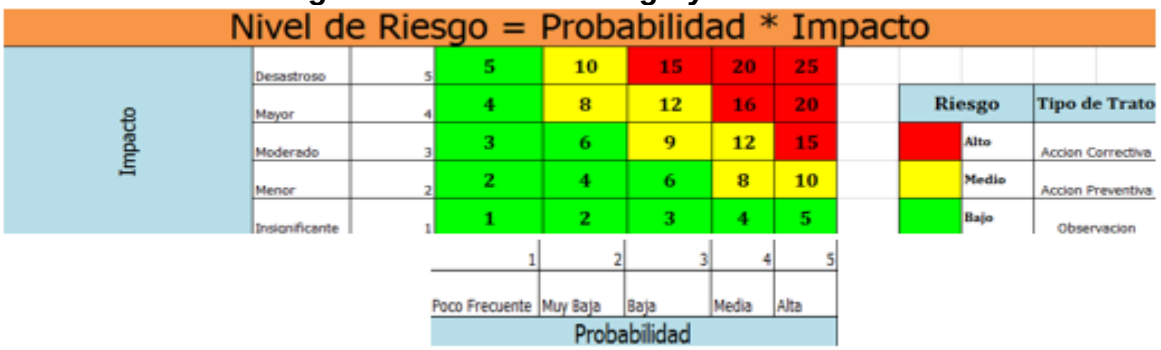
•Medio: El nivel de riesgos es medio y se deberá de poner en consideración si se deben implantar salvaguardas para evitarlos.

•Alto: El nivel de riesgos es alto aquí es una obligación implantar las Salvaguardas necesarias para mitigar riesgos.

•Crítico: Aquí el nivel de riesgo es crítico lo que realmente es preocupante porque se deben utilizar obligatoriamente salvaguardas adicionales para minimizarlos

Podremos hacer uso de la metodología MAGERIT para hacer la evaluación del riesgo teniendo en cuenta los activos y las amenazas identificadas:

Figura 14. Nivel de Riesgo y Probabilidad



Fuente: Metodología MAGERIT.

11.5.5. Calificación del Riesgo

Se gestionan los activos con riesgos críticos:

Internet: Este activo pertenece a la capa de Servicios Internos, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee es el uso no previsto que afecta en la disponibilidad (4,0) y en la confidencialidad e integridad (4,8) si se llega a materializar esta amenaza no podrían ejecutar tareas diarias como el envío de emails

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- La medida que se deben de tomar es el de restricción de páginas como son redes sociales, descargar programas para que el uso de Internet solo sea para actividades de trabajo y no para distracciones de empleados.
- Además no hay nada que garantiza la protección de los servicios como es el aseguramiento de la disponibilidad para ello se deberían adquirir dispositivos accesible (cortafuegos, servidores) para soportar la máxima carga prevista.

Aplicativo Empresarial: pertenece a la capa de Aplicaciones, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.
La mayor amenaza a la que se enfrenta este activo es la de Suplantación de la identidad del usuario que sufre la integridad y con confidencialidad (4,2).

Esta amenaza nace a partir a que el sistema no cuenta con una clave de acceso permitiendo que cualquier trabajador interno o individuo externo, indague en la información perteneciente a la empresa.
Si se llega a materializar esta amenaza podría ser víctimas de robo de información o de generar datos erróneos en la información perjudicando el desempeño de las actividades de la mayoría de los empleados
Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Debería existir claves confidenciales para acceder al sistema
- Mejorar la protección de la aplicación con privilegios de acceso de acuerdo al puesto de trabajo y a la información que maneja.

Antivirus: pertenece a la capa de Aplicaciones, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.
La amenaza a la que está expuesto este activo: Difusión de software dañino que perjudica a las dimensiones con niveles altos de riesgo que son la integridad (3,2) y la confidencialidad (3,2). Una de las principales razones es que la mayoría de veces cuando hacen uso de dispositivos externos como memory flash no la hacen analizar por el antivirus provocando la propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- La medida que se debe tomar es la adquisición de software óptimo para evitar la propagación de virus.
- También es que por lo menos una cuatro veces al mes el antivirus sea actualizado para que pueda contra restar cualquier software dañino.

- que en lo posible de colocar dispositivos externos en las máquinas para así evitar que pueda ser infectadas.

Sistema Operativo: pertenece a la capa de Aplicaciones, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

Posee las siguientes amenazas que tienen como resultado niveles altos de riesgo en:

Errores de los usuarios y Difusión de software dañino, que indisponen a las dimensiones de integridad (3,1) y confidencialidad (3,1). Este tipo de errores se da por el mal del uso de esta aplicación, lo que pueda generar inhabilitado el sistema operativo. Puede disponer de antivirus, pero si este no se actualiza constantemente no puede detectar posibles formas de contagio existentes. Vulnerabilidades de los programas (software) afecta a la integridad (3,0) y la confidencialidad (3,0). Nunca se podrá garantizar que software es 100% ya que puede aparecer con ciertos errores de fábrica y por tal motivo hay que tomar en cuenta esta amenaza.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- La adquisición de software con licencia.
- Además de la instalación de parches y actualizaciones que son muy necesarios.
- Control de acceso al sistema operativo: con el uso de claves de usuario.

Servidor de Base de Datos: este activo pertenece a la capa de Equipos, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza que tiene como resultado un nivel alto de riesgo es la: Manipulación de hardware que afecta a la confidencialidad (3,8), esta amenaza está latente porque no existe un lugar adecuado donde solo ingrese el personal autorizado permitiendo que cualquier empleado pueda hacer mal uso de este equipo quedando totalmente inseguro. Si esta amenaza se materializa podría causar graves daños para la empresa ya que se encuentra almacenada información importante y no hay redundancia.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente

- Es de trasladar el servidor hacia un cuarto donde se toman todas las medidas de seguridad necesarias como es el control de accesos.
- La resguardar la seguridad física para ser frente amenazas como desastres naturales.

Equipos de Cómputo: este activo pertenece a la capa de Equipos, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:

La amenaza que tiene un nivel de riesgo alto es el uso no previsto que afecta

principalmente confiabilidad (3,2) y la integridad (1,8).
Esta es una amenaza muy común ya que algunos empleados pueden instalar programas que no tengan ninguna relación con el trabajo sino que son para su interés personal como juegos, programas personales o almacenamiento de datos personales. Retrasando sus actividades de acuerdo al puesto de trabajo en el que se están desempeñando.
La medida para reducir el riesgo actual (current) de este activo, es la siguiente:

- Crear cuentas de usuario y administrador para así poder instalar el software adecuado necesario para las jornadas de trabajo.

Red LAN: este activo pertenece a la capa de Comunicaciones, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:
Las amenazas que son: errores de [re]-encaminamiento y [Re]- encaminamiento de mensajes, que posee un nivel de riesgo alto (3,5) que afecta a la confidencialidad.
Si estas amenazas llegan a materializarse puede causar perdida en la confidencialidad de información. Ya que son víctimas de un atacante que intercepta la información. Existe un mal estado en la red donde se encuentra conectado a equipos de un lugar a otro pero no se ha seguido ninguna norma de seguridad para evitar este tipo de ataques.
Las medidas para reducir el riesgo actual (current) de este activo, es la siguiente:

- Se deberían implementar protecciones criptográficas para la confidencialidad de los datos intercambiados.
- Dispositivos Físicos y emplear servicios certificados.
- Además de realizar mantenimientos regulares del estado de la red
- LAN.

Cableado: Este activo pertenece a la capa de Equipos Auxiliares, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:
La amenaza que es de Contaminación medioambiental que posee un nivel de riesgo alto en la disponibilidad (3,0). Esta amenaza se da por la deplorable instalación del cableado y equipos interrelacionados exponiéndoles a daños físicos por el polvo y suciedad.
Las medidas para reducir el riesgo actual (current) de este activo, es la siguiente:

Para la protección de cableado se debería tener lo siguiente:

- Disponer de planos actualizados del cableado.
- Etiquetar todos los elementos de cableado.
- Evitar rutas a través de áreas públicas.

- Controlar todos los accesos al cableado.
- Separar el cableado de alimentación del de comunicaciones para evitar interferencias.
- Proteger contra daños o interceptaciones no autorizadas

Personal que son todo el personal que se encuentra en la empresa que son: Gerente General, Responsable del área de sistemas, Operador de Base datos y aplicaciones, Gerente Financiera y de Contabilidad, Auxiliar de Contabilidad y Operadores; las principales amenazas que posee el personal que labora en esta empresa son la ingeniería social y extorción.

La primera amenaza se cumple por que los empleados saben la clave de los demás para acceder a su computador de esta manera se puede sustraer, modificar y destruir de la información. Originando a que la segunda amenaza que puede ser utilizada como extorción o como abuso de buena fe para beneficio propio del atacante.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente:

- Crea una normativa relativa a la gestión de personal (en materia de seguridad)
- Crear procedimientos relevantes se seguridad: emergencias, incidencias
- Prevención y Reacción frente a extorción
- Prevención y reacción frente ataques de ingeniería social

12. CONCLUSIONES

- En la actualidad de la era digital, el uso de las tecnologías de información es un aspecto importante que requieren las Empresas u organizaciones para cumplir mejor su misión u objetivos propuestos; por lo que la gestión correcta de los riesgos de tales tecnologías, juega un papel fundamental en la protección de los activos de información.

- Al revisar las vulnerabilidades vs riesgos se puede evaluar la seguridad de un sistema de información, la cual nos da un diagnostico actual y se pueden tomar decisiones para la mejora de la seguridad en la información.

- La información es el activo más valioso de cualquier empresa, por lo cual se debe diseñar las estrategias que conlleve a mitigar el impacto de los posibles riesgos cerrando las brechas de los mismos, para lograrlo se puede determinar a partir de la matriz de la clasificación de los riesgos.

- Para el diseño de los controles informáticos se pueden plasmar a partir del estado actual de la empresa y mediante los aportes de todos los integrantes o profesionales en el tema se llegan a común acuerdo para el trabajo colaborativo.

- El factor humano es el mayor riesgo de seguridad, porque a pesar de que tengamos un buen sistema de seguridad sería inútil para resguardar nuestros activos informáticos si los funcionarios no hacen uso de las buenas prácticas y de las políticas de Seguridad de la empresa.

- Gracias a la metodología MAGERIT donde se siguió una serie de pasos estructurados para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la empresa donde se supo escoger que medidas serán necesarias para mitigar el riesgo.

- La herramienta PILAR 5.4.5 fue de gran ayuda en este Plan toda vez que ayudo en la valoración de los riesgos en diferentes etapas potencial, situación actual y objetivo. Gracias a este software se supo de manera directa que mecanismos de seguridad se tienen que implementar en esta empresa.

- Después de haber realizado este trabajo la empresa obtendrá un documento encaminado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa.

13. RECOMENDACIONES

- Se recomienda que se realice una revisión periódica de las amenazas y riesgos teniendo en cuenta que la tecnología evoluciona constantemente y deben ser controlados para evitar futuros problemas.

- Se sugiere a la gerente de la empresa que contrate al personal adecuado para implementar las salvaguardas que fueron escogidas en el análisis de riesgos.

- Para reducir los riesgos que existen en los activos de la empresa se deberían pensar en crear una Dependencia de Gestión Documental.

- Asimismo de capacitar al personal para que se cumplan las normas de seguridad que se emplearon en la gestión de riesgos.

14. BIBLIOGRAFÍA

Academia Latinoamericana de Seguridad Informática (2011), Introducción a la seguridad Informática (1ra Ed).

Artículos de seguridad y amenazas informáticas para el usuario común, que no posee grandes conocimientos, pero al que le interesa mantener segura su pc. [En línea] [Consultado 12 de Enero de 2016].Disponible en Internet: http://infoobera.blogspot.com/

BRUNA López Ignacio - Licenciado en derecho de las nuevas tecnologías - Diplomado en Dirección de Seguridad de la Información - Auditor CISA (Certified Information Systems Auditor) por ISACA, Confidencialidad, Integridad y Disponibilidad de la Información. [En línea] [Consultado 11 de Enero de 2016]. Disponible en Internet: http://www.belt.es/expertos/experto.asp?id=2245

ISO-27001: Los controles (Parte I) [En línea] [Consultado 28 de Febrero de 2016]. Disponible en Internet: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

ISO 27001: Los controles (Parte II) - ISO27000.es. [En línea] [Consultado 28 de Febrero de 2016]. Disponible en Internet: www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

ISO/IEC 27002:2005.Dominios (11), Objetivos de control (39) y Controles (133). [En línea] [Consultado 28 de Febrero de 2016]. Disponible en Internet: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

Definición ISO 27000. [En línea] [Consultado 29 de Marzo de 2016]. Disponible en internet: http://es.wikipedia.org/wiki/ISO/IEC_27000-series

Definición ISO 27001. [En línea] [Consultado 29 de Marzo de 2016]. Disponible en internet: https://seguinfo.wordpress.com/category/estandares/page/6/

Definición ISO 27002. [En línea] [Consultado 29 de Marzo de 2016]. Disponible en internet: http://es.wikipedia.org/wiki/ISO/IEC_17799

Definición MAGERIT. [En Línea] [Consultado 2 Abril de 2016]. Disponible en internet: http://es.wikipedia.org/wiki/Magerit

DEJAN Kosutic, Information security & business continuity academy, conceptos básicos sobre ISO/27001. [En línea] [Consultado 19 de Abril de 2016]. Disponible

en internet:http://www.iso27001standard.com/es/que-es-la-norma-iso-27001#documentos

ISO/27001 & ISO/22301, controles del Anexo A de la Norma ISO/27001, Información registrada en el blog en la fecha octubre 20 de 2010 [En línea] [Consultado 21 de Abril de 2016]. http://blog.iso27001standard.com/es/tag/anexo-a/

Documento con contenido relacionado a la Norma ISO/27000 [En línea] [Consultado 22 de Abril de 2016]. Disponible en internet: http://www.iso27000.es/download/doc_iso27000_all.pdf

Estándar Internacional ISO/IEC 27001 primera edición 2005-10-15 Tecnología de la Información-Técnicas de Seguridad-Sistemas de gestión de seguridad de la información-Requerimientos [en línea] [Consultado 30 de Abril de 2016]. Disponible en Internet: http://www.calameo.com/books/0002626419b16f25c055d

Estándar Internacional ISO/IEC 17799 segunda edición 2005-06-15 Tecnología de la Información-Técnicas de Seguridad-Código para la práctica de la gestión de la seguridad de la información [en línea] [Consultado 30 de Abril de 2016]. Disponible en Internet: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

GÓMEZ Ricardo, Pérez Diego Hernán, Donoso Yesid, Herrera Andrea metodología y gobierno de la gestión de riesgos de tecnologías de la información [en línea] [Consultado 30 de Abril de 2016]. Disponible en Internet: http://revistaing.uniandes.edu.co/pdf/A10%2031.pdf

Ing. JORGE Martin Figueroa Profesor, Alumnas Gutiérrez Medina Claudia, Guevara Angeldonis Catherine Universidad San Martin de Porres curso de Seguridad y Auditoria de Sistemas de Información ISO/IEC FDIS 27001 [en línea] [Consultado 30 de Abril de 2016]. Disponible en Internet: http://www.gigabytesperu.com/trabajos/ISOIEC%20FDIS%2027001.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI).Bogotá: ICONTEC, 2006. 257p. 005.8/I59

JULIA H. Allen, Software Engineering Institute, Homeland Security, Build Security In, Setting a higher standard for software assurance, Plan-Do-Check-Act [En línea] [Consultado 1 de Mayo de 2016]. Disponible en Internet: https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/574-BSI.html

Magerit - v.2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de

Información, Gobierno de España. [En línea] [Consultado 2 de Mayo de 2016]. Disponible en Internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225129 3651550991&langPae=es&detalleLista=PAE_1276529683497133

Ministerio de Comunicaciones de la República de Colombia, Gobierno en Línea, Modelo de Seguridad de la Información-Sistema SANSI-SGSI [En línea] [Consultado 18 de Mayo de 2016]. Disponible en Internet: http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

ORCI, Consultoría aplicada, capacitación/conferencias, tecnología, gestión de servicios. ISO/IEC 27002. [En línea] [Consultado 19 Mayo de 2016] http://www.orcilatam.com/index.php?option=com_content&view=article&id=143&It e mid=191

Anexo A. Encuesta

Cias&Profesionales S.A.S
NIT 900.585.341 - 1

Asesores y Consultores

ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN

1. Seguridad General			
Los equipos de cómputo de su empresa, ¿tienen instalado antivirus?	SI X	NO	N/S
El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?	SI	NO	N/S X
Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?	SI X	NO	N/S
Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?	SI X	NO	N/S
Ha perdido información en su equipo de cómputo?	SI X	NO	N/S
Cuál cree que fue el motivo (si es el caso) de la perdida de la Información?	Virus	Falla X	Otro
2. Comunicaciones			
¿En su empresa se trabaja con conexión vía Internet?	SI X	NO	N/S
Si tiene conexión sin cables (WIFI), ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión?	SI	NO	N/S X
La información es almacenada dentro del disco duro de su equipo de cómputo?	SI	NO X	N/S
Se realiza copia de seguridad de los datos de la empresa?	SI	NO	N/S
3. Programas			
Ha detectado programas no licenciados en su equipo de cómputo?	SI	NO X	N/S
Algún técnico es el encargado de instalar/desinstalar los programas y aplicaciones informáticas en su empresa?	SI X	NO	N/S
4. Internet			
Hace uso de las redes Sociales?	SI X	NO	N/S
Su equipo tiene restricción para ingreso a sitios web?	SI	NO X	N/S
Conoce algún tipo de ataques Informáticos en la Web?	Spoofing	Malware	Ciberacoso

5. Observaciones
La información se guarda en el servidor pero todos tenemos acceso y se puede eliminar. Los equipos no tienen restricciones

Anexo B. Resultados de Encuesta

La información fue recolectada mediante encuesta y se realizó el análisis cualitativo y cuantitativo mediante el registro unificado de las respuestas, con una tabulación y su respectiva deducción de los diferentes aspectos.

Los equipos de cómputo de su empresa, ¿tienen instalado antivirus?

Tabla 18. Instalación de Antivirus

Respuesta	Frecuencia	%
SI	13	93
NO	1	7
N/S	0	0
TOTAL	**14**	**100**

Figura 15. Instalación de Antivirus

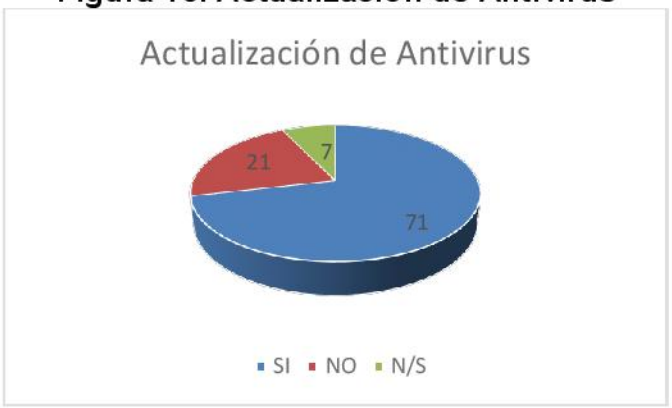
Fuente: Autores

El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

Tabla 19. Actualización de Antivirus

Respuesta	Frecuencia	%
SI	**10**	**71**
NO	**3**	**21**
N/S	**1**	**7**
TOTAL	**14**	**100**

Figura 16. Actualización de Antivirus



Fuente: Autores

Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

Tabla 20. Mantenimiento Informático

Respuesta	Frecuencia	%
SI	9	64
NO	0	0
N/S	5	36
TOTAL	**14**	**100**

Figura 17. Mantenimiento Informático

Fuente: Autores

Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Tabla 21. Riesgo Potencial

Respuesta	Frecuencia	%

SI	3	21
NO	10	71
N/S	1	7
TOTAL	**14**	**100**

Figura 18. Programas de descarga

Fuente: Autores

Ha perdido información en su equipo de cómputo?

Tabla 22. Pérdida de Información

Respuesta	Frecuencia	%
SI	6	43
NO	8	57
N/S	0	0
TOTAL	**14**	**100**

Figura 19. Pérdida de Información

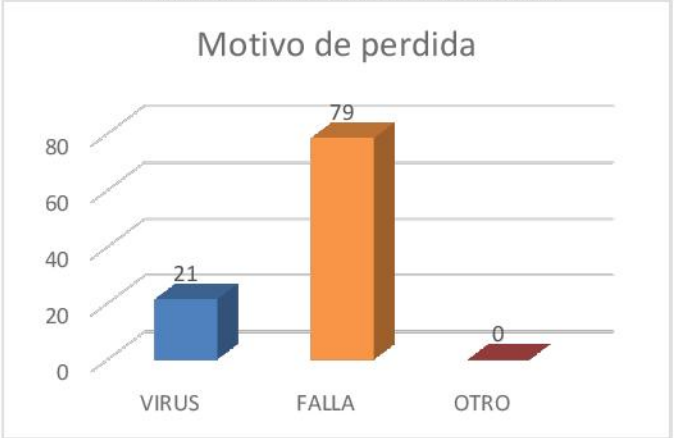
Fuente: Autores

Cuál cree que fue el motivo (si es el caso) de la perdida de la Información?

Tabla 23. Motivo de pérdida

Respuesta	Frecuencia	%
VIRUS	3	21
FALLA	11	79
OTRO	0	0
TOTAL	**14**	**100**

Figura 20. Motivo de pérdida



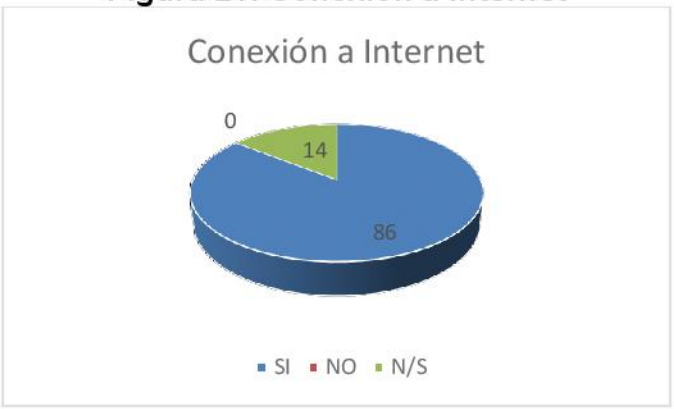
Fuente: Autores

En su empresa se trabaja con conexión vía Internet?

Tabla 24. Conexión a Internet

Respuesta	Frecuencia	%
SI	12	86
NO	0	0
N/S	2	14
TOTAL	**14**	**100**

Figura 21. Conexión a Internet



Fuente: Autores

Si tiene conexión sin cables (WIFI), ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión?

Tabla 25. Seguridad WIFI

Respuesta	Frecuencia	%
SI	3	21
NO	10	71
N/S	1	7
TOTAL	**14**	**100**

Figura 22. Seguridad WIFI

Fuente: Autores

La información es almacenada dentro del disco duro de su equipo de cómputo?

Tabla 26. Almacenamiento de Información

Respuesta	Frecuencia	%
SI	3	21
NO	10	71
N/S	1	7
TOTAL	**14**	**100**

Figura 23. Almacenamiento de Información

Fuente: Autores

Se realiza copia de seguridad de los datos de la empresa?

Tabla 27. Copias de Seguridad

Respuesta	Frecuencia	%
SI	5	36
NO	6	43
N/S	3	21
TOTAL	**14**	**100**

Figura 24. Copias de Seguridad

Fuente: Autores

Ha detectado programas no licenciados en su equipo de cómputo?

Tabla 28. Licencias

Respuesta	Frecuencia	%
SI	3	21

NO	9	64
N/S	2	14
TOTAL	**14**	**100**

Figura 25. Licencias

Fuente: Autores

Algún técnico es el encargado de instalar/desinstalar los programas y aplicaciones informáticas en su empresa?

Tabla 29. Técnico de Mantenimiento

Respuesta	Frecuencia	%
SI	12	86
NO	0	0
N/S	2	14
TOTAL	**14**	**100**

Figura 26. Técnico de Mantenimiento

Fuente: Autores

Hace uso de las redes Sociales?

Tabla 30. Redes Sociales

Respuesta	Frecuencia	%
SI	10	71
NO	4	29
N/S	0	0
TOTAL	**14**	**100**

Figura 27. Redes Sociales

Fuente: Autores

Su equipo tiene restricción para ingreso a sitios web?

Tabla 31. Uso restringido

Respuesta	Frecuencia	%
SI	2	14
NO	10	71
N/S	2	14
TOTAL	**14**	**100**

Figura 28. Uso Restringido

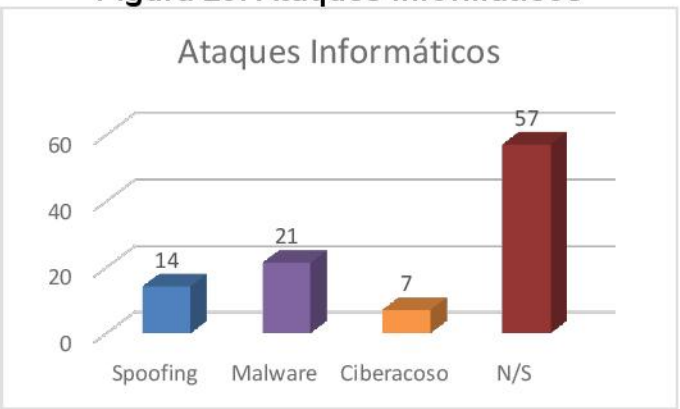
Fuente: Autores

Conoce algún tipo de ataques Informáticos en la Web?

Tabla 32. Ataques Informáticos

Respuesta	Frecuencia	%
Spoofing	2	14
Malware	3	21
Ciberacoso	1	7
N/S	8	57
TOTAL	**14**	**100**

Figura 29. Ataques Informáticos



Fuente: Autores

Anexo C. Análisis de Resultado de Encuesta

Pregunta 1. Los equipos de cómputo de su empresa, ¿tienen instalado antivirus?

A partir de los resultados obtenidos mediante esta pregunta se evidencio que un gran número (93%) de los encuestados conocen que su equipo de cómputo tiene Antivirus y de ahí la importancia que esté asegurada la Información.

Pregunta 2. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

Según las respuestas obtenidas con esta pregunta se concluyeron que el 71% de los encuestados dice conocer que los equipos tienen actualizado el antivirus y se conoce la importancia y la necesidad de proteger sus datos, el 21% de los encuestados no conocen si esta actualizado y tan solo el 7% no saben de las actualizaciones.

Pregunta3. Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

Esta pregunta el 64% informa que si se hace mantenimiento a los equipos de cómputo, pese a que debería llegar al 100% toda vez que los mantenimientos periódicos deben ser imprescindible para prevenir errores graves en el funcionamiento del mismo.

Pregunta 4. Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Con este resultado del 21% se evidencia que algunos equipos de cómputo están con grave riesgo de ´perdida de Información, los programas descargados suelen tener virus y programas dañinos, por lo que se recomienda no descargar ningún software sin licencia en los equipos de la empresa.

Pregunta 5. Ha perdido información en su equipo de cómputo?

Mediante la respuesta obtenida en esta pregunta se puede observar de manera preocupante que aproximadamente la mitad de los encuestados (43 %) han perdido información importante de sus equipos de cómputo, se puede evidenciar que existe

la necesidad de crear unas políticas y controles a riesgos tan inminentes como la perdida de información.

Pregunta 6. Cuál cree que fue el motivo (si es el caso) de la perdida de la Información?

Según la respuesta afirmativa de la anterior se plantea otra pregunta, de la cual se evidencio que la perdida de información fue en un menor porcentaje por Virus informático (21%) y por fallas Físicas de los equipos de cómputo (79%) en esta ocasión se evidencia la necesidad de servicio técnico prestado por parte del personal encargado.

Pregunta 7. En su empresa se trabaja con conexión vía Internet?

Al revisar las respuestas obtenidas con esta pregunta se concluyó que el 86% de los encuestados dice trabajar con conexión a internet, al activar el trabajo on-line en la empresa, se debe extremar las precauciones de seguridad del sistema informático y de las comunicaciones.

Pregunta 8. Si tiene conexión sin cables (WIFI), ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión?

Con el 43% que afirma que no hay seguridad se observa el riesgo de tener una red WIFI sin protección ni seguridad es lo mismo que dejar una puerta abierta para que entre cualquier persona sin autorización

Pregunta 9. La información es almacenada dentro del disco duro de su equipo de cómputo?

Al responder esta pregunta los encuestados manifestaron que no se guarda en su equipo con el 71%, sin embargo de manera verbal manifestaron que hacen guardan la Información en su disco duro guardar información, tener datos de la empresa distribuidos en los equipos es peligroso debido al descontrol que hay sobre dichos datos, además de que no se implementan en ningún tipo de copia de seguridad

Pregunta 10. Se realiza copia de seguridad de los datos de la empresa?

Según las respuesta obtenidas con esta pregunta se concluyó que cerca del 36% de los encuestados dice conocer la importancia y la necesidad de de las copias de

seguridad, pero de manera preocupante el 43% afirman que no y se se evidencia una falta de conocimiento del tema

Pregunta 11. Ha detectado programas no licenciados en su equipo de cómputo?

Cerca del 21% nos informan que tienen instalados en sus equipos programas no licenciados, es recomendable que se supervise la instalación de programas en los equipos de cómputo de la empresa, ya sea previamente, o en modo de mantenimiento y control periódico

Pregunta 12. Algún técnico es el encargado de instalar/desinstalar los programas y aplicaciones informáticas en su empresa?

A partir de los resultados obtenidos mediante esta pregunta se evidencio que un gran número (86%) de los empleados indican que hay personal técnico encargado de la instalación de los programas

Pregunta 13. Hace uso de las redes Sociales?

Con los resultados obtenidos se observa que más del 71% de los empleados hace uso de las redes sociales, se desea con esta pregunta es interrogar qué tan vulnerables pueden ser los encuestados al momento de compartir información y cuidar sus datos. Se puede evidenciar que el 29% no hace uso de estos servicios la mayoría por desconocimiento y el temor de exponer sus datos.

Pregunta 14. Su equipo tiene restricción para ingreso a sitios web?

Se evidencia que el 71% pueden ingresar a cualquier sitio de internet sin ninguna restricción, lo que ratifica la necesidad de crear unas políticas y controles a riesgos tan inminentes como la perdida de información

Pregunta 15. Conoce algún tipo de ataques Informáticos en la Web?

Con las opciones de ataques o vulnerabilidades que se pueden presentar en la actualidad con respecto a la seguridad de la información; se concluyó lo siguiente, 21% solo reconoce a los virus informático como es el Malware, 14% Spoofing y 7% Ciberacoso, con un 57% se evidencia que es muy poco el conocimiento que tiene con respectos a tipos de ataques informáticos que son muy comunes en la actualidad.

Anexo D. Salvaguardas

Protecciones Generales.

Se requiere autorización previa para acceso a la Información y a los Activos. La razón se escogió esta salvaguarda es porque cualquier persona puede acceder a los activos incluso los más importantes y es una amenaza debido a que se exponen los activos como Datos/ Información, Servicios, Aplicaciones (software), Equipos (hardware), Redes de comunicaciones y Soportes de información Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad

Hacer frente a las siguientes amenazas:

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Difusión de software dañino
- Errores de [re]-encaminamiento
- Errores de secuencia
- Alteración de la información
- Fugas de información
- Vulnerabilidad de los programas (software)
- Errores de mantenimiento /actualización de programas (software)
- Suplantación de la identidad del usuario
- Abuso de privilegios de acceso
- Uso no previsto
- [Re-]encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Modificación de la información
- Revelación de información y Manipulación de hardware.

Herramienta contra código de dañino.

La empresa posee herramientas contra código dañino pero no siempre esta actualizado, o se encuentran caducados lo que hace fácil la propagación de virus, troyanos, etc. Por eso se escogió las siguientes salvaguardas:

- El programa se actualiza regularmente
- La base de datos de virus se actualiza regularmente
- Se revisan los programas y servicios de arranque del sistema

Aseguramiento de la Disponibilidad.

Dentro de este grupo de salvaguardas tenemos:

- Se han previsto protecciones frente ataques de denegación de servicio(DoS)

- Procedimientos Operativos
- Se toman medidas frente a ataques originados en las propias instalaciones

Protecciones de las Aplicaciones Informáticas.

Se seleccionó las siguientes salvaguardas ya que la empresa no posee estas normas de seguridad como son:

- Se dispone de normativa sobre el uso autorizado de las aplicaciones
- Se dispone de normativa relativa al cumplimiento de los derechos
- Se controla la instalación de software autorizado y productos con licencia
- Se dispone de procedimientos para realizar copias de seguridad
- Se dispone a crear las políticas de Seguridad de la Empresa

Perfiles de seguridad.

Se encuentra a medias porque solo existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema pero gracias a esta salvaguarda podemos hacer frente a estas amenazas:

Errores de los usuarios, Difusión de software dañino, Vulnerabilidad de los programas (software), Errores de mantenimiento/actualización de programas (software) y Uso no previsto

Se debería tratar de cumplir con lo siguiente:

- Seguridad de los ficheros de datos de la aplicación
- Se protegen los ficheros de configuración
- Seguridad de los mecanismos de comunicación entre procesos

Donde se asegura las dimensiones de seguridad como confidencialidad e integridad

Se debe de llevar un Control de versión de toda actualización de software, ayuda a saber que cualquier software que posea la empresa esté libre de errores y hacer frente amenazas como son: Vulnerabilidades de los programas (software) y Errores de mantenimiento / actualización de programas (software).

Protección de los Equipos Informáticos (HW)

A continuación las salvaguardas adecuadas para la protección de los equipos.

- Se dispone de normativa sobre el uso correcto de los equipos
- Se dispone de procedimientos de uso de equipamiento
- Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la empresa minimiza amenazas como son: Errores del administrados del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

Además se debe de tener en cuenta con estas salvaguardas al momento de utilizar los equipos como son:

- Protección física de los equipos: son mecanismos que la empresa no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el Servidor de Datos
- Para evitar accesos innecesarios
- Para evitar acceso no autorizados
- Seguridad del equipamiento de oficina
- Después de evaluar las salvaguardas antes mencionadas se debe implantar las siguientes salvaguardas:
- Se evalúa el impacto en la confidencialidad de los datos
- Se evalúa el impacto en la integridad de los datos
- Ninguna de estas salvaguardas posee la empresa como son:
- Se priorizan las actuaciones encaminadas corregir riesgos elevados
- Se mantiene en todo momento la regla de "seguridad por defecto"
- Se debe de controlar: Reproducción de documentos

Protección de las comunicaciones.

Se han escogido las siguientes salvaguardas para minimizar riesgos:

Se deben de aplicar perfiles de seguridad : para garantizar la comunicación en la empresa y para hacer frente amenazas como: Errores de [re] – encaminamiento, Errores de secuencia, Alteración de la información, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia y Acceso no autorizado, además proteger las dimensiones de seguridad : integridad , confidencialidad y autenticidad.

- La empresa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado
- Ni siquiera de mecanismos como son :
- Comprobación de origen y destino
- Mecanismos de control
- No tiene ninguna: Seguridad de los servicios de red

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear siguiente salvaguardas:

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas anti spyware
- Se deshabilitan las "cookies" en los navegadores

- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del trafico
- Se toman medidas frente a la inyección de información espuria
- S aplica la regla de "seguridad por defecto"
- Se requiere autorización para que medios y dispositivos que tengan
- acceso a redes y servicios

Protección de los Soportes de Información.

Para proteger el único activo se han escogido las salvaguardas más apropiadas:

- Proteger en uso de contenedores cerrados
- Se dispone de normativa de relativa a la protección criptográfica de los contenidos

Elementos Auxiliares.

Se asegura la disponibilidad como:

- Siguiendo las recomendaciones del fabricante o proveedor
- Continuidad de operaciones: para asegurar las disponibilidad de los equipos auxiliares además para contrarrestar la amenaza de contaminación medioambiental
- Climatización: La adecuada climatización de cada equipo ayuda a enfrentar la amenaza que tiene la mayoría de estos componentes que es: Condiciones inadecuadas de temperatura o humedad.

Protección de las Instalaciones.

- Se dispone de normativa de seguridad para la seguridad de las instalaciones.
- Se dispone de áreas específicas para equipos informáticos , para protegerlos de la manos criminales
- Además de la Protección del perímetro y reforzar la Vigilancia en las instalaciones de la empresa.
- Protección frente a explosivos

Gestión del Personal.

Se deben de crear las siguientes normas de seguridad

- Se dispone de normativa relativa a la gestión de personal (materia de seguridad)
- Se dispone de procedimientos para la gestión de personal (materia de seguridad)

- Creación de normas del personal: Propio y Subcontratado
- Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
- Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos , frente ataques de cómo Extorsión y Ataque desde el interior
- Procedimientos relevantes de seguridad: Emergencias, incidencias.

Después de haber realizado esta tarea tendremos la Declaratoria de Aplicabilidad que es documento formal donde constan las salvaguardas necesarias para proteger al sistema.

Anexo E. Políticas de Seguridad de la Información

En atención a la privacidad y complejidad de la información que se administra en Cias & Profesionales SAS, se hace necesario implementar políticas y prácticas de seguridad para optimizar el uso de los recursos tecnológicos que soportan la gestión de la empresa, orientados a optimizar el uso de estos recursos por parte de los usuarios y responsables de los mismos.

Las buenas prácticas de seguridad tienen como propósito orientar a los usuarios frente a las responsabilidades que deben asumir en la seguridad, confidencialidad y salvaguarda de la información y recursos tecnológicos que se encuentren a su cargo.

La política y prácticas de seguridad de la información establecidas, son de obligatorio cumplimiento para los empleados y contratistas de Cias & Profesionales SAS, ante su infracción, se aplicaran los procedimientos sancionatorios administrativos, disciplinarios y penales que correspondan.

1. NORMATIVIDAD Y DOCUMENTOS DE REFERENCIA

- **ISO 27000**, Estandarización de vocabulario, terminología y definiciones del sistema de seguridad de la información.
- **180 27002**, Actualmente la ISO 17799, establece directrices y principios generales para mejorar la gestión de la seguridad de la información.
- **Ley 527 de 1999**, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- **Ley 1273 de 2009**, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

2. OBJETIVOS

- Consolidar la cultura de seguridad de la información, desarrollada para Cias & Profesionales S.A.S.
- Implementar buenas prácticas para la protección de la información en la red de datos (LAN) de la Empresa.
- Crear la cultura de la seguridad de la información y concientizar sobre los riesgos del hurto o difusión no autorizada de información, vulneración o sabotaje a las redes.
- Definir estándares de seguridad, frente a la administración y uso de la información y los recursos tecnológicos.

3. NORMAS DE SEGURIDAD DE PROTECCIÓN DE LA INFORMACIÓN A NIVEL INFORMÁTICO

Los empleados de Cias & Profesionales SAS, deben conocer la importancia del correcto uso de las herramientas tecnológicas y sus activos, como bases de datos, equipos de cómputo, comunicaciones, software, documentos reservados y clasificados, entre otros.

Ante los avances tecnológicos, se facilita el hurto de datos protegidos, en dispositivos móviles, fáciles de transportar u ocultar, lo que incrementa el riesgo y vulnerabilidad de la información, en consecuencia, la política de seguridad de la información establece una serie de medidas y buenas prácticas para el control al acceso a la información, la administración y control de usuarios, supervisión al uso y trasmisión de la información.

Administración de usuarios: Define los parámetros para la asignación y uso claves de ingreso a los recursos informáticos, parámetros sobre la longitud, frecuencia de cambio y vigencia de las contraseñas.

Perfil de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con un módulo que permita definir y asignar roles y/o perfiles, definiendo las acciones permitidas por cada uno de éstos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario gestione la administración de usuarios.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los empleados y contratistas, son de uso personal e intransferible y están bajo la responsabilidad exclusiva de cada empleado.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

3.1. Las siguientes son las normas de seguridad de la información a nivel informático:

- Los servidores y contratistas son responsables de la información entregada para el ejercicio de su función y deberán cumplir los lineamientos dados por la Empresa, con el propósito de proteger y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
- Los empleados y contratistas no deben suministrar información de la entidad a entes externos sin autorización.
- Los integrantes de la entidad que utilicen recursos Informáticos, tiene la responsabilidad de asegurar la integridad, confidencialidad, disponibilidad y confiabilidad de la información que administra, en especial si está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.
- Abstenerse de hacer uso de dispositivos de almacenamiento con puertos USB, tarjetas de memoria (SO, MMC, Micro SO, Mini SD, Memory Stick, Micro drive, entre otros) que se encuentran ubicados en los computadores o que puedan ser adaptados a los mismos, sin la autorización del Área de Sistemas de Información.

- Con el propósito de evitar daño en los equipos, estos deben estar conectado a una fuente de energía regulada y con protección de UPS.
- Los puertos USB, serán de uso restringido en los equipos de cómputo, su habilitación debe solicitarla el Responsable de Área de Sistemas de Información
- Evitar el envío y transporte de información de la Empresa mediante equipos electrónicos y tecnológicos que a través de sistemas de interconexión inalámbrica permitan la transmisión y almacenamiento de datos, tales como: agendas digitales, iPod, iPad, BlackBerry, PDA's, PALMS, equipos electrónicos que contengan sistemas infrarrojos, wireless o bluetooth y celulares inteligentes, entre otros.
- Abstenerse de realizar actividades que puedan alterar el desempeño de los sistemas de información y por ende generar posibles pérdidas o daños en la misma, como la instalación de software no licenciado, esta conducta igualmente genera riesgos, como el ingreso de virus, instalación de software espías, hurto o divulgación no autorizada de información.
- La administración de cambios (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, deberá ser solicitada mediante comunicación escrita o correo electrónico al Área de Sistemas de Información, por el usuario de la información.
- El uso de la identidad informática de cada empleado (claves, usuarios, contraseñas) es personal e intransferible.
- Abstenerse de hacer uso inadecuado de la red de datos (WANG y LAN) de Cias & Profesionales SAS, para obtener, almacenar y difundir en los equipos de cómputo, material pornográfico, mp3, videos y películas comerciales, cadenas de correos no autorizados.
- En sitios definidos como críticos por la información que se administra, restringir el ingreso de equipos de telefonía celular que cuenten con sistemas de grabación y almacenamiento de datos o imágenes.
- Abstenerse de efectuar la conexión de equipos de cómputo personales, a la red de datos de Cias & Profesionales SAS.
- En las oficinas donde se encuentren dispositivos de red como switch, tomas reguladas, canaletas, punto de red y otros, los empleados deben tener el cuidado de no desconectarlos; apagados; ni colocar objetos pesados sobre las canaletas; se deben proteger de caída de líquidos, evitar conectar equipos como grabadoras, cargadores y otros.
- Abstenerse de retirar equipos de cómputo que pertenecen a Cias & Profesionales SAS y que contienen información del mismo, sin autorización y conocimiento del Área de Sistemas de Información, a fin de verificar la actividad que se realizará y el tipo de información que contiene.
- Abstenerse de dejar portátiles, computadores de escritorio encendidos en horas no laborables, elevando con esto los niveles de riesgo frente a una posible pérdida o difusión no autorizada de información.
- Está totalmente prohibido el uso de dispositivos personales para acceso a Internet en la Oficina, por el grado de inseguridad y vulnerabilidad que representa

para Cias & Profesionales SAS. Solo está autorizado el uso de banda ancha contratada por la Empresa.

- Las impresoras adquiridas en Cias & Profesionales SAS deben ser aptas para trabajar en red (conectadas a un punto de red y no a un computador), si está conectada a un computador debe ser compartida a otros equipos.
- No ejecutar acciones tendientes a eludir o violar el Protocolo de Seguridad de la información.

Cuentas y contraseñas

- A los empleados y contratistas que laboren en Cias & Profesionales SAS y que se les asigne un equipo de cómputo, se creara una cuenta con clave de acceso, la cual tiene definido el perfil del usuario para adicionar, modificar, borrar y consultar información.
- La contraseña es personal, por lo tanto no debe ser compartida ni revelada y debe ser cambiada periódicamente.
- La contraseña debe tener mínimo ocho caracteres, preferiblemente compuesta de letras, números y símbolos.
- La contraseña no debe ser la misma para todos los servicios utilizados (Ciasoft, Word Office, correo, inicio de sesión, entre otros.)
- No se recomienda usar como contraseña el nombre, apellido, número de documento, fechas que se relacionen con el usuario, ni ninguna palabra que aparezca en un diccionario de cualquier idioma.
- Cuando el empleado deja el sitio de trabajo, debe cerrar las aplicaciones que se estén ejecutando.
- Cuando el empleado se retire de Cias & Profesionales SAS, el Responsable de la dependencia deberá informar al Área de Sistemas de Información, para realizar las correspondientes copias de seguridad y cambios de usuarios.

Correo electrónico

- Mantener la lista de correos electrónicos actualizada y depurada, eliminando las cuentas inactivas.
- El responsable de dependencia informara al Área de Sistemas de Información las novedades del personal de su área para realizar los procedimientos correspondientes. (De eliminación, creación o modificación de la cuenta de correo)
- Abstenerse del envío y recepción de datos e información de Cias & Profesionales SAS a través de correos electrónicos personales, los cuales no poseen las características de seguridad requeridas.
- Uso adecuado del correo, descargar los correos continuamente, archivar o eliminar los correos de las carpetas de correos ya leídos y enviados, descargar la carpeta de mensajes eliminados periódicamente.
- La cuenta de correo no debe ser utilizada para enviar y reenviar correos como presentaciones, bromas, video clips, cadenas, pornografía entre otros. Cuando

sean recibidos este tipo de mensajes deben eliminarse inmediatamente, para evitar la contaminación con posibles virus.

- No abrir archivos o ejecutar programas adjuntos a los correos si no se conoce el remitente o el asunto.
- La recepción de archivos de audio y video, se encuentra bloqueada, para evitar congestionar el servidor de correo, o el canal dedicado.

Copias de seguridad

- Es responsabilidad del usuario realizar las copias de seguridad de la información que administra.
- Para la realización de copias de seguridad deberá solicitar soporte técnico al Área de Sistemas de Información, para realizar el correspondiente procedimiento.
- Se deben realizar copia de seguridad de los datos del computador asignado, en forma mensual o en intervalos de tiempo acordes con la necesidad del usuario y de la criticidad de la información.

3.2. Las siguientes son las normas de seguridad de la Información a nivel físico:

- La información que está consignada en documentos físicos debe ser protegida en lugares que dificulten el acceso a personal no autorizado.
- Ningún empleado podrá destapar equipos o impresoras para realizar cualquier clase de mantenimiento o instalación de hardware o software.
- No descuidar documentos que contengan información, ya que esto ocasionaría la consulta, copia o pérdida de la información por parte de personas no autorizadas.
- Es obligación de cada uno de los empleados destruir o desechar correctamente la documentación, evitando la posible reconstrucción de la misma.
- Los empleados deben tener especial cuidado en la seguridad de las gavetas en cada uno de los puestos de trabajo, dejándolos bajo llave cuando se ausente de su puesto de trabajo.
- Los documentos impresos que contengan información, deben ser guardados de forma segura, no deben ser abandonados en lugares públicos o de fácil acceso a personas ajenas a dicha información.

4. VIOLACIONES A LA POLÍTICA DE SEGURIDAD INFORMÁTICA

Son consideradas violaciones a la Política de Seguridad de la Información, aquellas acciones desarrolladas por los empleados de Cias & Profesionales SAS que van en contravía de las normas de seguridad establecidas. En este sentido se consideran las siguientes violaciones:

4.1. Nivel Informático

- Usar dispositivos de almacenamiento en los computadores, cuya autorización no haya sido otorgada por al Área de Sistemas de Información.
- Utilizar equipos electrónicos o tecnológicos que a través de sistemas de interconexión inalámbrica, sirvan para transmitir y almacenar datos.
- Almacenar o enviar información a través de correos electrónicos personales.
- Difundir información a través de correos de Cias & Profesionales SAS, sin las medidas de seguridad, cifrado de datos y sin cumplir los protocolos establecidos para dicho fin.
- Instalar programas o software en los computadores, cuya aplicación no esté autorizada por el Área de Sistemas de Información.
- Ingresar celulares con sistemas de grabación y almacenamiento de datos o imágenes, a las Áreas con restricciones de acceso especiales.
- Almacenar, transportar y portar información de Cias & Profesionales SAS en medios de almacenamiento extraíbles y computadores personales, sin las medidas de seguridad informática.
- Conectar computadores portátiles u otros sistemas electrónicos personales a la red de datos.
- Extraer de las instalaciones computadores portátiles o de escritorio, que contengan información de Cias & Profesionales SAS.
- Permitir el acceso a la red de datos a empleados no autorizados o particulares.
- Dejar los computadores encendidos en horas no laborables.
- Activar puertos USB de acceso, en los computadores sin la autorización del Área de Sistemas de Información.
- Almacenar información de Cias & Profesionales SAS en lugares distintos a la red de datos de la Empresa
- Ingresar a carpetas de información de otros procesos, usuarios, grupos o áreas, sin la debida autorización.
- Archivar información, sin la utilización de claves de seguridad o cifrado de datos.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos.
- Enviar información por correo, copia impresa o electrónica de archivo y documentos sin la debida autorización y sin la utilización de los protocolos establecidos para su difusión.
- Realizar actividades no autorizadas que puedan degradar el desempeño de los sistemas y por ende generar posibles pérdidas o daños de la información almacenada.
- Los equipos serán configurados por el al Área de Sistemas de Información, en el escritorio es obligatorio el uso del fondo de la Empresa, de acuerdo a lo dispuesto por la Gerencia de Cias & Profesionales SAS.
- El Área de Sistemas de Información a través del Grupo de Desarrollo de software son los responsables de desarrollar e implementar los aplicativos requeridos para la gestión de la Empresa.
- Mantener en los equipos música, videos, imágenes, juegos, reproductores de música, MP3, MP4, emuladores de Windows, software de módems inalámbricos,

programas compatibles con teléfonos móviles y todos los demás que no estén autorizados por el Área de Sistemas de Información.

- Hacer uso de la red de datos, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico y ofensivo, cadenas de correos, correos masivos no autorizados, software o códigos maliciosos o cualquier tipo de información que no esté acorde con las buenas costumbres y la ética.
- Manipulación y apertura de los equipos de cómputo e impresoras, lo cual es de facultad exclusiva del Área de Sistemas de Información.

4.2. Nivel Físico

- Descuidar documentación en lugares de fácil acceso, sin las medidas apropiadas de seguridad, que garanticen su protección.
- Dejar rastros de información consignadas en apuntes, agendas, libretas, entre otros.
- Destruir o desechar de forma incorrecta la documentación que contenga información.
- Ignorar la seguridad de las gavetas en los puestos de trabajo, asignados para el desarrollo de su actividad laboral.
- Entregar, enseriar o divulgar información a personas o entidades-no autorizadas.

5. APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad es de cumplimiento de los empleados de Cias & Profesionales SAS en la totalidad de dependencias, por lo cual se deben tener en cuenta las siguientes instrucciones de cumplimiento y despliegue:

- El contenido del presente protocolo es de obligatorio cumplimiento por parte de los empleados.
- Es compromiso de los Responsables de las diferentes Áreas, verificar que el personal bajo su liderazgo cumplan con la Política de Seguridad de la Información al interior de las diferentes dependencias así:
- Los Responsables de Área deberán nombrar una persona que realice las funciones de control y supervisión del cumplimiento de las Políticas de Seguridad de la información.
- Generar espacios para la socialización de las Políticas de Seguridad de la información.
- Supervisar personalmente las acciones que permitan la aplicación del protocolo de seguridad de la información
- Realizar labores de prevención, detección y neutralización de posibles actos de violación a la política y por ende la pérdida alteración o divulgación no autorizada de información.

Dra. LILIANA ALEXANDRA VILLACORTE LÓPEZ
Gerente Cias & Profesionales SAS

V.Bo. Ing. JORGE MUÑOZ
Área de Sistema de Información

Elaborado por: Ing. JORGE MUÑOZ
Revisado por: Dra. LILIANA ALEZXANDRA VILLACORTE LÓPEZ
Fecha de elaboración: 01/06/2017
Archivo: D: //DRIVE/CIAS/SGSI

Por cada tonelada de papel son 17 árboles que desaparecen.

Antes de imprimir este documento piense bien si es necesario hacerlo. La protección del medio ambiente es un compromiso de todos.