DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA LA EMPRESA PC DIGITAL LTDA USANDO ISO/IEC 27001:2013

KHAANKO NORBERTO RUIZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA LA EMPRESA PC DIGITAL LTDA USANDO ISO/IEC 27001:2013

KHAANKO NORBERTO RUIZ RODRIGUEZ

Monografía para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Proyecto
Ing. HERNANDO JOSE PEÑA HIDALGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

DEDICATORIA

A ti Dios, por ser el hacedor que este paso en mi vida sea posible, y darme las fuerzas para poder lograrlo y culminarlo.

A mi padre que desde el cielo guía mis pasos, y gracias a sus palabras, orientación, y su ejemplo como persona y profesional, puedo ver más cerca la consecución de una de mis metas.

A mi madre que, gracias a sus consejos, paciencia y sabiduría, han logrado forjar a una persona mejor tanto personal como profesionalmente.

A mi Esposa y mis hijos, a quienes les brindare infinidad de consejos y experiencias para que sus sueños se puedan lograr, como ahora lo logro yo.

AGRADECIMIENTOS

Agradezco a todos y cada uno de los docentes de la Universidad Nacional y a Distancia UNAD, por su labor que se ve reflejada, en la culminación de esta etapa académica.

A mi Director de Proyecto el Ingeniero Hernando José Peña Hidalgo quien me acompañó en cada etapa de la formación de este proyecto con su conocimiento y experiencia, gracias por sus comentarios y aportes en el transcurso de este proyecto.

A nuestra Institución por brindarnos la oportunidad de hacer parte de una gran familia de grandes profesionales.

CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

TITULO

“DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA LA EMPRESA PC DIGITAL LTDA USANDO ISO/IEC 27001:2013”

INTRODUCCION

Hoy en día es vital la organización de los componentes de tecnologías de la información y por ende es vital que una organización o empresa tenga dicha organización para que sea relevante ante la competencia.

Los nuevos estándares de calidad, hacen que cada compañía propenda por resaltar su calidad ante las demás, y solo aquellas con un completo orden y control en sus activos tecnológicos y que cuenten con políticas de seguridad, serán quienes sobresalgan en el campo laboral. Teniendo en cuenta esta situación el presente documento muestra el diseño de un sistema de seguridad de la información para la empresa PC DIGITAL LTDA que le permita tener control sobre sus activos y gestionar los riesgos a nivel informático que puedan presentarse.

El lograr la articulación de un proceso de seguridad de la información efectivo en cualquier tipo de compañía sea cual sea su labor, se genera desde la planificación y la estructuración de un sistema que nos permita tener procedimientos, políticas y revisiones a el sistema para mantenerlo, todo esto se consigue con el ciclo PHVA (Planear, Hacer, Verificar, y Actuar)[1]

[1] Norma Técnica Colombiana NTC – ISO/IEC 27001

1. DEFINICION DEL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA.

El crecimiento exponencial y el nivel de utilización de las herramientas tecnológicas de las compañías actualmente, hacen que la seguridad de la información sea un componente vital para el crecimiento a la par de las mismas, para lo cual se deben tener claras las guías de acción precisa para la administración de las tecnologías de la información y comunicaciones, mediante la formulación de estrategias y proyectos que garantizaran los mejores resultados en su labor.

Pc Digital Ltda. Es una compañía con más de 12 años en el sector informático, que presta servicios de mantenimiento preventivo y correctivo, así como de consultoría y desarrollo de Software, también presta asesoramiento en adquisición de equipos de cómputo a usuario final Help Desk. El sistema de gestión de seguridad informática es vital para esta compañía puesto que no se tiene claridad sobre los tipos de riesgos que se enfrentan y no se tiene un nivel de seguridad que permita garantizar la seguridad de los activos.

1.2 FORMULACION DEL PROBLEMA.

¿Cómo el Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, permitirá establecer políticas y procedimientos de seguridad Empresa PC Digital Ltda.?

2. JUSTIFICACIÓN

El presente estudio tiene como finalidad, el diseño del Sistema de Gestión de Seguridad de la Informática en PC DIGITAL LTDA.

PC DIGITAL LTDA necesita la implementación de un sistema de seguridad de la informática para salvaguardar los activos más importantes: la información, los procesos que la administran y el recurso humano. La confidencialidad, integridad y disponibilidad de la información, son elementos primordiales para mantener los niveles de rentabilidad, competitividad e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar los beneficios económicos.

PC DIGITAL LTDA. Como empresa de sector tecnológico y con bastante tiempo de experiencia, debe tener para sí, todo el apoyo documental y de procesos que garanticen el mantenimiento de la compañía como un PYME en Colombia, el establecimiento de este tipo de compañías y la fragilidad del mercado, hacen que cualquier tipo de diferencia entre ellas marque una gran diferencia, a la hora de ofrecer sus productos y estableces sus clientes.

Para cualquier tipo de cliente conocedor de estándares de calidad es grato saber que la compañía que contrato cumple con protocolos y gestión documental tratando se ser lo más organizada posible.

El sistema de gestión de seguridad de la información le brindara a PC Digital Ltda. La capacidad de conocer que activo tecnológico posee y cuál es el riesgo que tiene cada uno de sus activos así mismo pondrá un esquema de seguridad y confiabilidad para sus clientes los cuales podrán confiar en que los procesos que se manejen en PC Digital tienen políticas claras de seguridad de la información.

3. OBJETIVO GENERAL

Diseñar de un sistema de gestión de seguridad informática para la empresa PC Digital Ltda. Usando la norma técnica ISO/IEC 27001:2013.

3.1 OBJETIVOS ESPECÍFICOS.

- Identificar los activos tecnológicos con los que cuenta la Empresa PC Digital Ltda. Mediante el estándar de la norma técnica ISO/IEC 27001:2013.

- Identificar los riesgos, amenazas, vulnerabilidades de cada uno de los componentes tecnológicos así mismo clasificar el riesgo y adoptar medidas para analizar el impacto en la integridad, confiabilidad y disponibilidad de la información en la empresa PC Digital mediante la norma técnica ISO/IEC 27001:2013.

- Definir la política de seguridad, para el manejo de la información basados en la norma ISO/IEC 27001:2013

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO.

La información es el activo más valioso en cualquier tipo de compañía, por ello el manejo de la esta debe tener, los estándares más elevados de seguridad para su uso. Evitando así posibles daños de la información causando la no confiabilidad en la misma. Produciendo perdidas que pueden ser catastróficas para la compañía u organización.

La seguridad de la información busca crear, estrategias, procesos, directrices para el buen uso de los elementos que las Tics, buscando con ello que la información como activo valioso de la compañía, sea infranqueable y confiable.

Todo gerente de la información debe tener cuatro palabras básicas o claves en la actividad o rol que se desempeña en el área como son: activación, capacitación, ejecución y explotación. Así como que es un activo informático, la clasificación de los mismos que es un riesgo, como clasificarlos y una metodología de análisis.[2]

El diseño de un Sistema de gestión de seguridad de la información permite identificar amenazas y vulnerabilidades y los riesgos a que están expuestos los activos de una organización, permitiendo establecer normas y controles adecuados para proteger el activo más valioso en cualquier compañía, y de este modo garantizar la continuidad de todos los procesos de la compañía.[3]

Figura 1 Procesos SGSI

[2] SGSI – Blog especializado en Sistemas de Gestión de seguridad de la información - Disponible en http://www.pmg-ssi.com/2014/02/implementacion-de-un-sgsi-etapa-3-ejecucion/

[3] Portal de ISO 27001 en español – Recuperado el 15 de marzo de 2017- Disponible en http://www.iso27000.es/sgsi.html

Fuente http://www.iso27000.es/sgsi.html

4.1.1 Activo

Cualquier tipo, cosa o demás elemento material e inmaterial que tenga valor para la compañía.[4]

4.1.2 Riesgo

Es la cantidad de perdidas tras la ocurrencia de explotación de una amenaza o vulnerabilidad.

4.1.3 Valoración de riesgo

Es un proceso global que permite el análisis y evaluación de los riesgos de la entidad frente a sus activos.

4.1.4 Gestión de riesgo

Es uno de los mecanismos que permite el análisis, diseño e implementación, así como el de evaluar y planificar los eventos que puedan llegar a desencadenar un desastre en la compañía o entidad, ya sean estos de orden interno o externo.

4.1.5 Margerit Versión 3

Es una metodología que se denomina Proceso de gestión de los riesgos, ella implementa el proceso de gestión de riesgos dentro de un contexto de trabajo para que se te tomen decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información y comunicación.[5]

La metodología es una herramienta vital que permite administrar de manera eficiente todos los activos, dando como primera fase el levantamiento o recolección de datos de todos los activos su valoración y sugiriendo controles necesarios para evitar o poder mitigar la gran cantidad de riesgos que se puedan derivar.

---

[4] Banco terminológico. Activo de Información. Disponible en: http://banter.archivogeneral.gov.co/vocab/?tema=5

[5] Magerit – Versión 3.0. Metodología de Análisis y Gestión del Riesgos de los Sistemas de Información. – Gobierno de España – Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

4.1.6 Norma Técnica Colombiana NTC-ISO/IEC 27001

Esta norma nos especifica los lineamientos para establecer, implementar, mantener, y realizar la mejora continua de un SGSI (Sistema de Gestión de Seguridad de la Información), dentro del marco de una organización.[6]

4.1.7 Guía Técnica Colombiana GTC-ISO/IEC 27003

Esta guía tiene como fin enfocar los aspectos más relevantes, críticos y necesarios para la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información), de acuerdo con la norma ISO/IEC 27001:2005 (NTC-ISO/IEC 27001:2006). Esta está prevista para ser aplicada por cualquier organización que se encuentre implementado un SGSI. [7]

4.2 MARCO CONCEPTUAL.

4.2.1 Amenaza

Es toda aquella circunstancia, evento o probabilidad de la ocurrencia de un imprevisto que puede originarse de forma intencional o natural; las amenazas se representan en factores de riesgo externo o interno que pueden explotar vulnerabilidades existentes en la compañía.

4.2.2 Ciclo PHVA

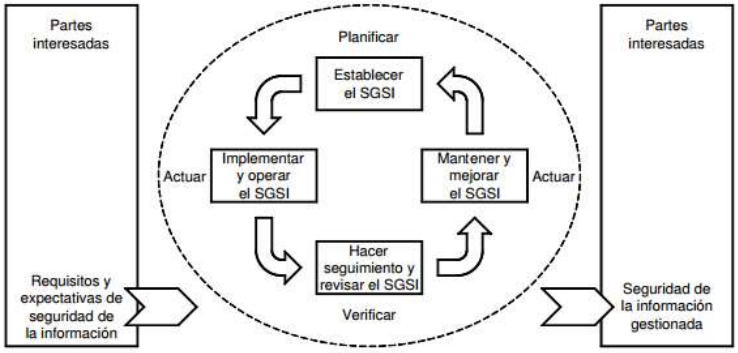
Es un modelo de procesos que permite implementar y gestionar a través del ciclo de mejora continúa (Planear, hacer, verificar, y Actuar) y este se aplica en todos los procesos del SGSI.

---

[6] Archivo General de la Nación – Norma ISO – IEC 27001- Disponible en http://www.archivogeneral.gov.co/normatividad/items/show/34

[7] ICONTEC – Guía Técnica Colombiana GTC – ISO/IEC 27003 Disponible en https://tienda.icontec.org/wp-content/uploads/pdfs/GTC-ISO-IEC27003.pdf

Figura 2 Ciclo PHVA Aplicado en los Procesos SGSI



Fuente http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

4.2.3 Confidencialidad

Propiedad de la seguridad de la información que garantiza que la información no esté disponible ni sea revelada a individuos o entidades no autorizados.[8]

4.2.4 Disponibilidad

Propiedad de la seguridad de la información que determina que la información sea accesible y utilizable por los entes autorizados para accederla[9].

4.2.5 Integridad

Propiedad de la seguridad de la información que determina que la información sea exacta y el estado completo de la misma[10].

4.2.6 Vulnerabilidad

Es un factor de riesgo que representa las falencias o debilidades que presentan los activos lo cual facilita la explotación de una amenaza[11].

[8] ISO 27000.ES – El portal de la ISO 27001en español disponible en http://www.iso27000.es/sgsi.html#seccion1
[9] ISO 27000.ES – El portal de la ISO 27001en español disponible en http://www.iso27000.es/sgsi.html#seccion1
[10] Seguridad informática – Disponible en https://infosegur.wordpress.com/tag/integridad/
[11] Seguridad informática – Disponible en https://infosegur.wordpress.com/tag/integridad/

4.2.7 Seguridad informática

Esta trata de procedimientos, políticas, técnicas así como herramientas de hardware y software que se implementan para salvaguardar los sistemas informáticos así como todo tipo de activo[12].

4.2.8 Sistema de gestión de la información SGSI

Esta es parte del sistema de gestión global, basada en implementar, operar, hacer, seguimiento, revisar, mantener y mejorar la seguridad de la información[13].

4.3 MARCO LEGAL.

4.3.1 Ley 842 de 2003 Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares.14

"ARTÍCULO 29. POSTULADOS ÉTICOS DEL EJERCICIO PROFESIONAL. El ejercicio profesional de la Ingeniería en todas sus ramas, de sus profesiones afines y sus respectivas profesiones auxiliares, debe ser guiado por criterios, conceptos y elevados fines, que propendan a enaltecerlo; por lo tanto, deberá estar ajustado a las disposiciones de las siguientes normas que constituyen su Código de Ética Profesional.

PARÁGRAFO. El Código de Ética Profesional adoptado mediante la presente ley será el marco del comportamiento profesional del ingeniero en general, de sus profesionales afines y de sus profesionales auxiliares y su violación será sancionada mediante el procedimiento establecido en el presente título.

ARTÍCULO 30. Los ingenieros, sus profesionales afines y sus profesionales auxiliares, para todos los efectos del Código de Ética Profesional y su Régimen Disciplinario contemplados en esta ley, se denominarán "Los profesionales"".

---

[12] Seguridad informática – Disponible en https://infosegur.wordpress.com/tag/integridad/

[13] Banco terminológico. Activo de Información. Disponible en: http://banter.archivogeneral.gov.co/vocab/?tema=5
Magerit – Versión 3.0. Metodología de Análisis y Gestión del Riesgos de los Sistemas de Información. – Gobierno de España – Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[14] República de Colombia – Consejo Profesional Nacional de Ingeniería Copnia – Recuperado el 15 de marzo de 2017 – Disponible en https://copnia.gov.co/copnia/normatividad/ley-842-de-2003/

4.3.2 Ley 29 de 1990 Por la cual se dictan disposiciones para el fomento de la investigación científica y el desarrollo tecnológico y se otorgan facultades extraordinarias.[15]

4.3.3 Conpes 3527 De 23 De junio De 2008 Sobre la Política Nacional de Competitividad y Productividad. Según la Política Nacional de Competitividad y Productividad, un país puede aumentar el valor de su producción por 3 vías: produciendo más (productividad), produciendo mejor (aumentando la calidad) o produciendo nuevos productos (transformación productiva). El emprendimiento es fundamental para alcanzar la transformación productiva y de ahí su estrecha relación con la competitividad.[16]

4.3.4 Ley Estatutaria 1266 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.[17]

4.4. MARCO CONTEXTUAL

PC DIGITAL LTDA. Es una Pyme con más de 12 años en el sector informático, que presta servicios de mantenimiento preventivo y correctivo, así como de consultoría y desarrollo de Software, también presta asesoramiento en adquisición de equipos de cómputo a usuario final Help Desk.

4.4.1 Misión

Es una empresa especializada en brindar servicios para la digitalización de archivos, dedicada al desarrollo de soluciones e implementación de servicios integrales para la información, así como la venta, soporte, capacitación, asesoría y mantenimiento de Software y Hardware, que trabaja en proyectos de ingeniería, redes, cableado estructurado, instalación y venta de plantas telefónicas, plantas eléctricas, sistemas de seguridad, computadores, portátiles, y sistemas punto de venta. Atendemos todo el sector empresarial, disponemos de personal calificado, siempre dispuesto a ofrecerle la mejor alternativa y solución para el desarrollo de sus proyectos[18]

---

[15] República de Colombia – Ministerio de Tecnologías de la información y las comunicaciones - Recuperado el 15 de marzo de 2017 – Disponible en http://www.mintic.gov.co/portal/604/w3-article-3669.html

[16] República de Colombia – Consejo Nacional de Política Económica y social - Recuperado el 15 de marzo de 2017 – Disponible en www.colombiacompetitiva.gov.co/sncei/Documents/Conpes-3527-de-2008.pdf

[17] República de Colombia – Congreso de la Republica - Recuperado el 15 de marzo de 2017 – Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[18] Pc Digital - Soluciones Técnicas Disponible en http://pcdigitalcolombia.com/Nosotros.html

4.4.2 Visión

Ser la empresa número 1 en soluciones tecnológicas y desarrollo de software, digitalización de archivos, soporte técnico a equipos de cómputo, venta y mantenimiento de equipos de cómputo y periféricos.

Ser una empresa reconocida, distinguida, renombrada y demandante, en el mundo tecnológico enfocado además en la eficiencia y vanguardia gracias a la buena reputación y distinción adquirida por nuestros productos de gran calidad siempre en contacto con la tendencia y desarrollo, logrando así enfrentar mercados internacionales[19].

4.4.3 Responsabilidad

El compromiso principal de la compañía es con nuestros clientes y sus capacidades tecnológicas, por tal motivo estamos trabajando siempre en una continua búsqueda de conocimiento y aprendizaje de las tecnologías de punta y su aplicabilidad, formulando y desarrollando soluciones que les permitan estar a la vanguardia tecnológica[20].

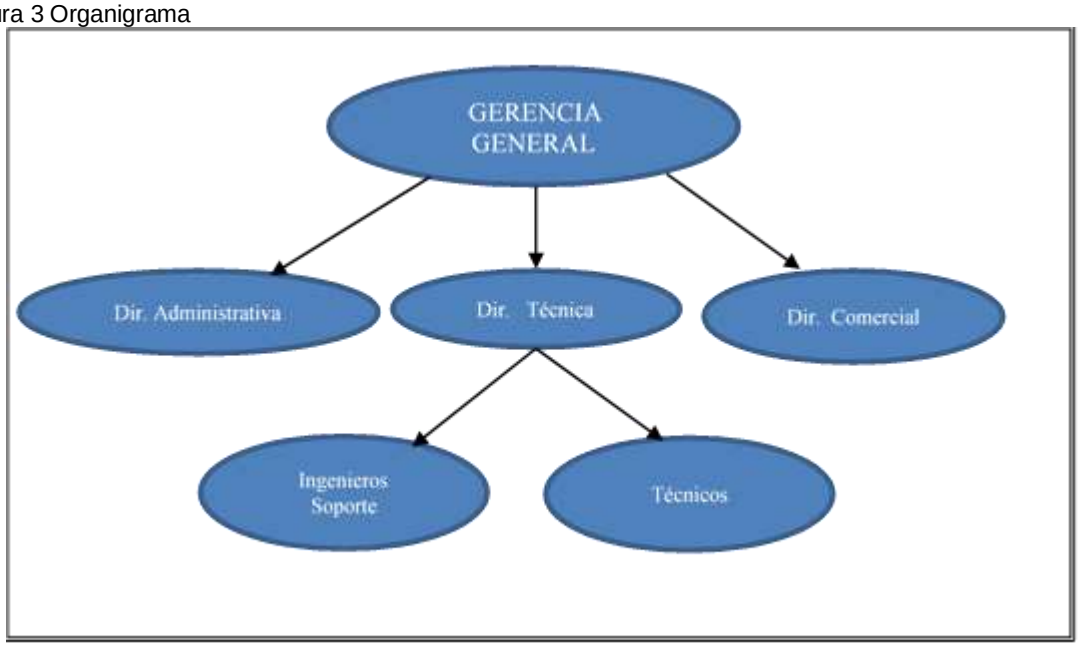
---

[19] Pc Digital - Soluciones Técnicas Disponible en http://pcdigitalcolombia.com/Nosotros.html

[20] Pc Digital - Soluciones Técnicas Disponible en http://pcdigitalcolombia.com/Nosotros.html

4.4.4 Estructura Organizacional PC DIGITAL LTDA

Figura 3 Organigrama



Fuente: El Autor

4.5. ANTECEDENTES

Para el marco de este Diseño de sistema de gestión de seguridad informática en la compañía PC DIGITAL LTDA, no se cuenta con antecedentes de la realización de un diseño o de un sistema de gestión de seguridad informática, o cualquier tipo de políticas, procedimientos que avalen la estructura de seguridad de la información por lo tanto es preciso realizarlo, con el fin de que la compañía PC DIGITAL LTDA obtenga un diseño de sistema de gestión de seguridad de la información bajo la norma técnica ISO 27001.

5. DISEÑO METODOLOGICO

5.1 METODOLOGÍA DE DESARROLLO.

Esta fase del proyecto hace referencia, al cubrimiento y las necesidades de PC DIGITAL LTDA, para con ello determinar los requisitos como el alcance que tendrá el plan estratégico de sistemas de información en la compañía.

Este documento especificara estrategias y proyectos que ejecutara PC DIGITAL LTDA. En el área de Sistemas

Como primera medida se realizará un estudio y análisis de los activos de información con la cual cuenta PC DIGITAL, así mismo se abordará la norma técnica ISO/IEC 27001:2013, para elevar recomendaciones pertinentes con el fin de proteger el activo.

Se determinarán los activos de información y se clasificarán para determinar el estado actual de la seguridad de la información.

Se establecerán amenazas a las que se encuentra expuesta la seguridad de la información tanto en su confidencialidad, integridad y disponibilidad, con el propósito de identificar vulnerabilidades y tomar correctivos.

Por último, paso y de acuerdo a los análisis realizados a los riesgos y amenazas y procesos implementados, serán puestos a consideración en la fase de implementación, acordes a la organización.

6. RESULTADOS Y DISCUCION

6.1 ACTIVOS DE INFORMACIÓN.

Durante el proyecto se identificaron los siguientes activos de información en PC DIGITAL LTDA.

Tabla 1 Activos

TIPO DE ACTIVO	NOMBRE	CARACTERISTICAS
COMUNICACIONES [COM]	Switch	Switch 3COM 24 puertos
	Rack	Servidor Montable en Rack Dell 2850
	Router	Huawei
HARDWARE [HAR]	Impresoras	Ricoh Aficio Sp 4510 Total red 3
	Ups	Symmetra PX 100 de 40 kVA
	Computadores	Lenovo M73E 6 equipos
	Laptop	Dell 2 equipos
INFORMACION FISICA [IF]	Documentos impresos en papel	Toda aquella documentación física de los procesos y servicios que presta PC Digital LTDA, como: Facturas, cotizaciones, contratos, compras, ventas, hojas de vida, garantías, libros y demás.
INFORMACION DIGITAL [ID]	Documentación digital, Word, Excel, pdf	Toda aquella documentación digital de los procesos y servicios que presta PC Digital LTDA, como: Facturas, cotizaciones, contratos, compras, ventas, hojas de vida, garantías, libros y demás.
PERSONAL [P]	Personal Interno (Trabajadores), Externo (Clientes, contratistas)	Personal directivo, ingenieros de soporte, técnicos, secretarias, auxiliares, contratistas
SOFTWARE [SOF]	Sistemas Operativos	Windows 8.1.
	Ofimática	Microsoft Office 2013
	Navegadores Web	Chrome, Explorer, Mozilla
	Antivirus	Eset Nod32

Fuente: el Autor

6.2 DIMENSIONAMIENTO DE ACTIVOS DE INFORMACIÓN.

Ya identificados los activos de la compañía se procede a realizar la valoración para identificar el valor que tiene cada uno de ellos para la compañía PC Digital LTDA, según su importancia, los criterios sobre los cuales son sometidos son los siguientes:

[C] Confidencialidad: El daño que sufre la compañía tanto en imagen, credibilidad, o puede estar abocada en posibles demandas si son divulgados datos o información confidencial.

[I] Integridad: El daño que sufre la compañía tanto en imagen, credibilidad, o puede estar abocada en posibles demandas si el activo es modificado.

[D] Disponibilidad: El daño que sufre la compañía tanto en imagen, credibilidad, o puede estar abocada en posibles demandas si el activo no se encuentra disponible para ser accesado.

[A] Autenticidad: El daño que sufre la compañía tanto en imagen, credibilidad, o puede estar abocada en posibles demandas si el activo no es autenticado o corresponde a su emisor.

[T] Trazabilidad: El daño que sufre la compañía tanto en imagen, credibilidad, o puede estar abocada en posibles demandas si no se tiene claridad de quien accede al activo y que acciones realiza.

Tabla 2 Valoración Confidencialidad de Activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
9 - 10	Muy Alto	Daños Muy Graves Catastróficos
6 - 8	Alto	Daños Graves
3 - 5	Medio	Daño Importante Considerable
1 - 2	Bajo	Daño Menor
0	Despreciable	Irrelevante

Fuente: el Autor

Tabla 3 Valoración integridad de activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
9 – 10	Muy Alto	Daños Muy Graves Catastróficos
6 – 8	Alto	Daños Graves
3 – 5	Medio	Daño Importante Considerable
1 – 2	Bajo	Daño Menor
0	Despreciable	Irrelevante

Fuente: el Autor

Tabla 4 Valoración Disponibilidad de Activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
9 - 10	Muy Alto	Daños Muy Graves Catastróficos
6 - 8	Alto	Daños Graves
3 - 5	Medio	Daño Importante Considerable
1 - 2	Bajo	Daño Menor
0	Despreciable	Irrelevante

Fuente: el Autor

Tabla 5 Valoración Autenticidad de Activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
9 – 10	Muy Alto	Daños Muy Graves Catastróficos
6 – 8	Alto	Daños Graves
3 – 5	Medio	Daño Importante Considerable
1 – 2	Bajo	Daño Menor
0	Despreciable	Irrelevante

Fuente: el Autor

Tabla 6 Valoración Trazabilidad de Activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO
9 – 10	Muy Alto	Daños Muy Graves Catastróficos
6 – 8	Alto	Daños Graves
3 – 5	Medio	Daño Importante Considerable
1 – 2	Bajo	Daño Menor
0	Despreciable	Irrelevante

Fuente: el Autor

6.3 VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

En las siguientes tablas se establecen las valoraciones de cada uno de los activos según su tipo.

Es importante resaltar que la valoración de cada uno de los activos no requiere que se clasifiquen en las cinco dimensiones, solo depende si estas aplican o no.

Nota: Las valoraciones fueron tomadas por medio de entrevista al responsable de cada uno de los activos.

6.3.1 Valoración de Activos tipo Comunicaciones [COM]

Tabla 7 Valoración Comunicaciones

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Switch	10	10	10	9	
Rack	10	10	10	9	
Router	10	10	10	9	

Fuente: el Autor

6.3.2 Valoración de Activos tipo Hardware [HAR]

Tabla 8 Valoración Hardware

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Impresoras	5	5	5	3	5
Ups	7	7	7	3	8
Computadores	7	9	9	9	8
Laptop	7	9	9	9	8

Fuente: el Autor

6.3.3 Valoración de Activos tipo Información Física [IF]

Tabla 9 Valoración Información Física

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Documentación física de la empresa	10	10	10	9	9

Fuente: el Autor

6.3.4 Valoración de Activos tipo Información Digital [ID]

Tabla 10 Valoración Información Digital

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Documentación Digital de la empresa	10	10	10	9	9

Fuente: el Autor

6.3.5 Valoración de Activos tipo Información Personal [P]

Tabla 11 Valoración Información Personal

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Gerente	10	10	10	10	10
Director Administrativo	9	9	9	9	9
Director Comercial	9	9	9	9	9
Director Tecnología	10	10	10	10	10
Ingenieros Soporte	9	9	9	9	9
Técnicos	8	8	8	7	7
Secretarias	8	8	8	7	7

Fuente: el Autor

6.3.6 Valoración de Activos tipo Información Software [SOF]

Tabla 12 Valoración Información Software

ACTIVO	DIMENSIONES				
	D	I	C	A	T
Sistemas Operativos	10	10	10	10	10
Ofimática	10	10	10	10	10
Navegadores Web	9	9	9	9	9
Antivirus	10	10	10	10	10

Fuente: el Autor

6.4 IDENTIFICACIÓN Y FRECUENCIA DE AMENAZAS.

Luego de valorar todos los activos de información, se procede a la identificación y valoración de las amenazas por cada uno de los activos de la información.

Se toma como base la metodología que se estableció “MAGERIT” de la siguiente manera:

- [N] Desastres Naturales (Inundaciones, tormentas eléctricas, terremotos, variaciones en los picos de electricidad)
- [I] De Origen Industrial (Errores en los dispositivos, daño en equipos)
- [E] Errores y Fallos no Intencionados (Mala manipulación, desconocimiento, olvidos)
- [A] Ataques Intencionados (Robos, Intrusiones, Sabotaje, Ingeniería Social, Malware, Virus, Troyanos)

En cuanto a la probabilidad de la ocurrencia o materialización de una amenaza se tomará como referencia los siguientes niveles de probabilidad.

Tabla 13 Niveles Probabilidad Amenaza

Nivel	Descripción
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: el Autor

A su vez cada una de las amenazas se identifica con un código según la metodología "MAGERIT"[21] de la siguiente forma:

Tabla 14 Amenaza Impacto

Cod	AMENAZA	IMPACTO
[N] Desastres Naturales		
[N.1]	Fuego	[D]
[N.2]	Daño por agua	[D]
[N.*]	Otros desastres	[D]
[I] De origen industrial		
[I.1]	Fuego	[D]
[I.2]	Daños por agua	[D]
[I.*]	Desastres industriales	[D]
[I.3]	Contaminación mecánica	[D]
[I.4]	Contaminación electromagnética	[D]
[I.5]	Avería de origen físico o lógico	[D]
[I.6]	Corte del suministro eléctrico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.8]	Fallo de servicios de comunicación	[D]

[21] Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2-Catalogo de Elementos Pág. 25 – 47 Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Tabla 14. (Continuación)

[I.9]	Interrupción de otros servicios o suministros esenciales	[D]
I.10]	Degradación de los soportes de almacenamiento	[D]
[I.11]	Emanaciones electromagnéticas	[C]
[E] Errores y fallos no intencionados		
[E.1]	Errores de los usuarios	[D][I][C]
[E.2]	Errores del administrador	[D][I][C]
[E.3]	Errores de monitorización	[I]
[E.4]	Errores de configuración	[I]
[E.7]	Deficiencias en la organización	[D]
[E.8]	Difusión de software dañino	[D][I][C]
[E.9]	Errores de re-encaminamiento	[C]
[E.10]	Errores de secuencia	[I]
[E.14]	Escapes de información	[C]
[E.15]	Alteración accidental de la información	[I]
[E.18]	Destrucción de la información	[D]
[E.19]	Fugas de información	[C]
[E.20]	Vulnerabilidades de los programas (software)	[D][I][C]
[E.21]	Errores de mantenimiento o actualización (software)	[D][I]
[E.23]	Errores de mantenimiento o actualización (hardware)	[D]
[E.24]	Caiga del sistema por agotamiento de recursos	[D]
[E.25]	Perdida de equipos	[D][C]
[E.28]	Indisponibilidad del personal	[D]
[A] Ataques intencionados		
[A.3]	Manipulación de los registros de actividad	[I]
[A.4]	Manipulación de la configuración	[D][I][C]
[A.5]	Suplantación de la identidad del usuario	[C][A][I]
[A.6]	Abuso de privilegios de acceso	[D][I][C]
[A.7]	Uso no previsto	[D][I][C]
[A.8]	Difusión de software dañino	[D][I][C]
[A.9]	Re-encaminamiento de mensajes	[C]
[A.10]	Alteración de secuencia	[I]
[A.11]	Acceso no autorizado	[C][I]
[A.12]	Análisis de tráfico	[C]
[A.13]	Repudio	[I]
[A.14]	Interceptación de información	[C]
[A.15]	Modificación deliberada de la información	[I]
[A.18]	Destrucción de la información	[D]
[A.19]	Divulgación de información	[C]
[A.22]	Manipulación de programas	[D][I][C]
[A.23]	Manipulación de los equipos	[C][D]
[A.24]	Denegación de servicio	[D]
[A.25]	Robo	[C][D]

Tabla 14. (Continuación)

[A.26]	Ataque destructivo	[D]
[A.27]	Ocupación enemiga	[D][C]
[A.28]	Indisponibilidad del personal	[D]
[A.29]	Extorsión	[D][I][C]
[A.30]	Ingeniería social	[D][I][C]

Fuente: el Autor

Tabla 15 Escala Rango Frecuencia Amenazas

Valoración	Vulnerabilidad	Rango	Valor
MA	Frecuencia Muy Alta	1 vez al día	100
A	Frecuencia alta	1 vez cada semana	10
M	Frecuencia Media	1 vez cada 2 meses	1
B	Frecuencia Baja	1 vez cada 6 meses	1/10
MB	Frecuencia muy Baja	1 vez al año	1/100

Fuente: el Autor

Tabla 16 Amenazas Comunicaciones

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
SWITCH	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/10
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10

Tabla 16. (Continuación)

	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/100
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1/10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1/10
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/100
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100

Tabla 16. (Continuación)

RACK	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/10
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/100
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1/10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1/10
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100

Tabla 16. (Continuación)

	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/100
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
ROUTER	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/10
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100

Tabla 16. (Continuación)

	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/100
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1/10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1/10
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/100
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100

Tabla 16. (Continuación)

	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100

Fuente: el Autor

Tabla 17 Amenazas Hardware

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
IMPRESORAS	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/10
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/100
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100

Tabla 17. (Continuación)

	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1
	[E.23]	Errores de mantenimiento o actualización (hardware)	1
	[E.24]	Caiga del sistema por agotamiento de recursos	1/10
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/100
	[A.7]	Uso no previsto	1
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
UPS	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10

Tabla 17. (Continuación)

	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/10
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/100
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1/10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1/10
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/100
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100

Tabla 17. (Continuación)

	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
COMPUTADORES	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1

Tabla 17. (Continuación)

	[E.15]	Alteración accidental de la información	1
	[E.18]	Destrucción de la información	1
	[E.19]	Fugas de información	1
	[E.20]	Vulnerabilidades de los programas (software)	1
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	10
	[A.6]	Abuso de privilegios de acceso	10
	[A.7]	Uso no previsto	10
	[A.8]	Difusión de software dañino	10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1
LAPTOP	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10

Tabla 17. (Continuación)

	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1
	[E.15]	Alteración accidental de la información	1
	[E.18]	Destrucción de la información	1
	[E.19]	Fugas de información	1
	[E.20]	Vulnerabilidades de los programas (software)	1
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	10
	[A.6]	Abuso de privilegios de acceso	10
	[A.7]	Uso no previsto	10

Tabla 17. (Continuación)

	[A.8]	Difusión de software dañino	10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1

Fuente: el Autor

Tabla 18 Amenazas Información Física

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
DOCUMENTACIÓN EMPRESA	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/100
	[I.2]	Daños por agua	1/100
	[I.*]	Desastres industriales	1/100
	[I.3]	Contaminación mecánica	1/100
	[I.4]	Contaminación electromagnética	1/100
	[I.5]	Avería de origen físico o lógico	1/100
	[I.6]	Corte del suministro eléctrico	1/100
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1/100
	[I.9]	Interrupción de otros servicios o suministros esenciales	1/100
	I.10]	Degradación de los soportes de almacenamiento	1/100

Tabla 18. (Continuación)

	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/100
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1/100
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1
	[E.15]	Alteración accidental de la información	1
	[E.18]	Destrucción de la información	1
	[E.19]	Fugas de información	1
	[E.20]	Vulnerabilidades de los programas (software)	1/100
	[E.21]	Errores de mantenimiento o actualización (software)	1/100
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/100
	[E.24]	Caiga del sistema por agotamiento de recursos	1/100
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	10
	[A.6]	Abuso de privilegios de acceso	10
	[A.7]	Uso no previsto	10
	[A.8]	Difusión de software dañino	1/100
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	10
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	10
	[A.14]	Interceptación de información	10
	[A.15]	Modificación deliberada de la información	10
	[A.18]	Destrucción de la información	10
	[A.19]	Divulgación de información	10
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100

Tabla 18. (Continuación)

	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	10
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	10
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100

Fuente: el Autor

Tabla 19 Amenazas Información Digital

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
DOCUMENTACION DIGITAL DE LA EMPRESA	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/10
	[I.2]	Daños por agua	1/10
	[I.*]	Desastres industriales	1/10
	[I.3]	Contaminación mecánica	1/10
	[I.4]	Contaminación electromagnética	1/10
	[I.5]	Avería de origen físico o lógico	1/10
	[I.6]	Corte del suministro eléctrico	1
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/10
	[I.8]	Fallo de servicios de comunicación	1
	[I.9]	Interrupción de otros servicios o suministros esenciales	1
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1
	[E.2]	Errores del administrador	1/10
	[E.3]	Errores de monitorización	1/10
	[E.4]	Errores de configuración	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.8]	Difusión de software dañino	1
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1
	[E.15]	Alteración accidental de la información	1
	[E.18]	Destrucción de la información	1

Tabla 19. (Continuación)

	[E.19]	Fugas de información	1
	[E.20]	Vulnerabilidades de los programas (software)	1
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/10
	[E.24]	Caiga del sistema por agotamiento de recursos	1
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/100
	[A.5]	Suplantación de la identidad del usuario	10
	[A.6]	Abuso de privilegios de acceso	10
	[A.7]	Uso no previsto	10
	[A.8]	Difusión de software dañino	10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/100
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1

Fuente: el Autor

Tabla 20 Amenazas Personal

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
GERENTE	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
DIRECTOR ADMINISTRATIVO	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10
	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/10
	[A.30]	Ingeniería social	1/10
DIRECTOR COMERCIAL	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10

Tabla 20. (Continuación)

	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10
	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/10
	[A.30]	Ingeniería social	1/10
DIRECTOR TECNOLOGICO	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10
	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/10
	[A.30]	Ingeniería social	1/10
INGENIEROS SOPORTE	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10

Tabla 20. (Continuación)

	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/10
TECNICOS	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10
	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/10
SECRETARIAS	[E.1]	Errores de los usuarios	1/10
	[E.2]	Errores del administrador	1/10
	[E.7]	Deficiencias en la organización	1/10
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/10
	[E.18]	Destrucción de la información	1/10
	[E.19]	Fugas de información	1/10
	[E.28]	Indisponibilidad del personal	1/10
	[A.5]	Suplantación de la identidad del usuario	1/10
	[A.13]	Repudio	1/10
	[A.14]	Interceptación de información	1/10
	[A.15]	Modificación deliberada de la información	1/10
	[A.18]	Destrucción de la información	1/10
	[A.19]	Divulgación de información	1/10
	[A.28]	Indisponibilidad del personal	1/10
	[A.29]	Extorsión	1/10
	[A.30]	Ingeniería social	1/10

Fuente: el Autor

Tabla 21 Amenazas Software

ACTIVO	AMENAZAS		FRECUENCIA
	ID	AMENAZA	
SISTEMAS OPERATIVOS	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/100
	[I.2]	Daños por agua	1/100
	[I.*]	Desastres industriales	1/100
	[I.3]	Contaminación mecánica	1/100
	[I.4]	Contaminación electromagnética	1/100
	[I.5]	Avería de origen físico o lógico	1/100
	[I.6]	Corte del suministro eléctrico	1/100
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/100
	[I.8]	Fallo de servicios de comunicación	1/100
	[I.9]	Interrupción de otros servicios o suministros esenciales	1/100
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/100
	[E.2]	Errores del administrador	1/100
	[E.3]	Errores de monitorización	1/100
	[E.4]	Errores de configuración	1/100
	[E.7]	Deficiencias en la organización	1/100
	[E.8]	Difusión de software dañino	1/10
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	10
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/100
	[E.24]	Caiga del sistema por agotamiento de recursos	1/100
	[E.25]	Perdida de equipos	1/100

Tabla 21. (Continuación)

	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/10
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/10
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/10
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
OFIMATICA	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/100
	[I.2]	Daños por agua	1/100
	[I.*]	Desastres industriales	1/100
	[I.3]	Contaminación mecánica	1/100
	[I.4]	Contaminación electromagnética	1/100
	[I.5]	Avería de origen físico o lógico	1/100
	[I.6]	Corte del suministro eléctrico	1/100
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/100
	[I.8]	Fallo de servicios de comunicación	1/100
	[I.9]	Interrupción de otros servicios o suministros esenciales	1/100

Tabla 21. (Continuación)

	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/100
	[E.2]	Errores del administrador	1/100
	[E.3]	Errores de monitorización	1/100
	[E.4]	Errores de configuración	1/100
	[E.7]	Deficiencias en la organización	1/100
	[E.8]	Difusión de software dañino	1/10
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	10
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/100
	[E.24]	Caiga del sistema por agotamiento de recursos	1/100
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/10
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/10
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/10
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100

Tabla 21. (Continuación)

	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
NAVEGADORES WEB	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/100
	[I.2]	Daños por agua	1/100
	[I.*]	Desastres industriales	1/100
	[I.3]	Contaminación mecánica	1/100
	[I.4]	Contaminación electromagnética	1/100
	[I.5]	Avería de origen físico o lógico	1/100
	[I.6]	Corte del suministro eléctrico	1/100
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/100
	[I.8]	Fallo de servicios de comunicación	1/100
	[I.9]	Interrupción de otros servicios o suministros esenciales	1/100
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/100
	[E.2]	Errores del administrador	1/100
	[E.3]	Errores de monitorización	1/100
	[E.4]	Errores de configuración	1/100
	[E.7]	Deficiencias en la organización	1/100
	[E.8]	Difusión de software dañino	1/10
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	10

Tabla 21. (Continuación)

	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/100
	[E.24]	Caiga del sistema por agotamiento de recursos	1/100
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/10
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/10
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/10
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100
	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100
ANTIVIRUS	[N.1]	Fuego	1/100
	[N.2]	Daño por agua	1/100
	[N.*]	Otros desastres	1/100
	[I.1]	Fuego	1/100
	[I.2]	Daños por agua	1/100
	[I.*]	Desastres industriales	1/100
	[I.3]	Contaminación mecánica	1/100
	[I.4]	Contaminación electromagnética	1/100
	[I.5]	Avería de origen físico o lógico	1/100

Tabla 21. (Continuación)

	[I.6]	Corte del suministro eléctrico	1/100
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1/100
	[I.8]	Fallo de servicios de comunicación	1/100
	[I.9]	Interrupción de otros servicios o suministros esenciales	1/100
	I.10]	Degradación de los soportes de almacenamiento	1/100
	[I.11]	Emanaciones electromagnéticas	1/100
	[E.1]	Errores de los usuarios	1/100
	[E.2]	Errores del administrador	1/100
	[E.3]	Errores de monitorización	1/100
	[E.4]	Errores de configuración	1/100
	[E.7]	Deficiencias en la organización	1/100
	[E.8]	Difusión de software dañino	1/10
	[E.9]	Errores de re-encaminamiento	1/100
	[E.10]	Errores de secuencia	1/100
	[E.14]	Escapes de información	1/10
	[E.15]	Alteración accidental de la información	1/100
	[E.18]	Destrucción de la información	1/100
	[E.19]	Fugas de información	1/100
	[E.20]	Vulnerabilidades de los programas (software)	10
	[E.21]	Errores de mantenimiento o actualización (software)	10
	[E.23]	Errores de mantenimiento o actualización (hardware)	1/100
	[E.24]	Caiga del sistema por agotamiento de recursos	1/100
	[E.25]	Perdida de equipos	1/100
	[E.28]	Indisponibilidad del personal	1/100
	[A.3]	Manipulación de los registros de actividad	1/100
	[A.4]	Manipulación de la configuración	1/10
	[A.5]	Suplantación de la identidad del usuario	1/100
	[A.6]	Abuso de privilegios de acceso	1/10
	[A.7]	Uso no previsto	1/100
	[A.8]	Difusión de software dañino	1/10
	[A.9]	Re-encaminamiento de mensajes	1/100
	[A.10]	Alteración de secuencia	1/100
	[A.11]	Acceso no autorizado	1/10
	[A.12]	Análisis de tráfico	1/100
	[A.13]	Repudio	1/100

Tabla 21. (Continuación)

	[A.14]	Interceptación de información	1/100
	[A.15]	Modificación deliberada de la información	1/100
	[A.18]	Destrucción de la información	1/100
	[A.19]	Divulgación de información	1/100
	[A.22]	Manipulación de programas	1/100
	[A.23]	Manipulación de los equipos	1/100
	[A.24]	Denegación de servicio	1/100
	[A.25]	Robo	1/100
	[A.26]	Ataque destructivo	1/100
	[A.27]	Ocupación enemiga	1/100
	[A.28]	Indisponibilidad del personal	1/100
	[A.29]	Extorsión	1/100
	[A.30]	Ingeniería social	1/100

Fuente: el Autor

6.5 VALOR DEL IMPACTO.

Este se valora por el daño causado cuando se materializa una amenaza sobre el activo de información se calcula según la siguiente formula.

Impacto = Valor del Activo X Degradación

6.6 VALORACION DE RIESGOS.

Este se valora por la probabilidad de que ocurra la amenaza por el impacto causado el daño causado cuando se materializa una amenaza sobre el activo de información se calcula según la siguiente formula:

Riesgo = Impacto X Probabilidad

6.7 NIVEL DE RIESGOS.

Tabla 22 Nivel Riesgos

NIVEL DE RIESGOS		
NOMBRE	**VALOR**	**IDENTIFICACION**
BAJO	< 0 Y <= 100	
MEDIO	101 Y <= 200	
ALTO	201 Y <= 300	
MUY ALTO	301 Y <= 400	
CRITICO	401 Y <= 500	

Fuente: el Autor

Según la valoración anterior de riesgos y las tablas anteriormente descritas los niveles de riesgo se estiman de la siguiente manera:

Tabla 23 Niveles Riesgos

COMUNICACIONES						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Switch	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
Rack	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[I.1] Fuego					
	[I.2] Daños por agua					
	[I.*] Desastres industriales					
	[I.3] Contaminación mecánica					
	[I.4] Contaminación electromagnética					

Tabla 23. (Continuación)

	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
Router	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					

Tabla 23. (Continuación)

	[E.24] Caiga del sistema por agotamiento de recursos					
HARDWARE						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Impresoras	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
Ups	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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					

Tabla 23. (Continuación)

	[I.6] Corte del suministro eléctrico					
	[I.7] Condiciones inadecuadas de temperatura o humedad					
	[I.8] Fallo de servicios de comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
Computadores	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					

Tabla 23. (Continuación)

Laptop	[N.1] Fuego					
	[N.2] Daño por agua					
	[N.*] Otros desastres					
	[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 comunicación					
	[I.9] Interrupción de otros servicios o suministros esenciales					
	I.10] Degradación de los soportes de almacenamiento					
	[I.11] Emanaciones electromagnéticas					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
HARDWARE						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Documentación física de la empresa	[E.1] Errores de los usuarios					
	[E.2] Errores del administrador					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.11] Acceso no autorizado					

Tabla 23. (Continuación)

	[A.15] Modificación deliberada de la información					
	[A.18] Destrucción de la información					
	[A.19] Divulgación de información					
	[A.25] Robo					
	[A.26] Ataque destructivo					
DOCUMENTACIÓN DIGITAL DE LA EMPRESA						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Documentación digital de la empresa	[E.1] Errores de los usuarios					
	[E.2] Errores del administrador					
	[E.7] Deficiencias en la organización					
	[E.8] Difusión de software dañino					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.20] Vulnerabilidades de los programas (software)					
	[E.21] Errores de mantenimiento o actualización (software)					
	[E.23] Errores de mantenimiento o actualización (hardware)					
	[E.24] Caiga del sistema por agotamiento de recursos					
	[E.25] Perdida de equipos					
	[E.28] Indisponibilidad del personal					
	[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.11] Acceso no autorizado					
	[A.14] Interceptación de información					

Tabla 23. (Continuación)

	[A.15] Modificación deliberada de la información					
	[A.18] Destrucción de la información					
	[A.19] Divulgación de información					
	[A.23] Manipulación de los equipos					
	[A.24] Denegación de servicio					
	[A.25] Robo					
	[A.26] Ataque destructivo					
PERSONAL						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Gerente	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					
Director Administrativo	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					

Tabla 23. (Continuación)

Director Tecnología	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					
Ingenieros de Soporte	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					
Técnicos	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					

Tabla 23. (Continuación)

Secretarias	[E.1] Errores de los usuarios					
	[E.14] Escapes de información					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.19] Fugas de información					
	[E.28] Indisponibilidad del personal					
	[A.28] Indisponibilidad del personal					
	[A.29] Extorsión					
	[A.30] Ingeniería social					
SOFTWARE						
Nom Activo	**Amenaza**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Critico**
Sistemas Operativos	[I.5] Avería de origen físico o lógico					
	[E.2] Errores del administrador					
	[E.4] Errores de configuración					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.20] Vulnerabilidades de los programas (software)					
	[E.21] Errores de mantenimiento o actualización (software)					
	[A.4] Manipulación de la configuración					
	[A.8] Difusión de software dañino					
	[A.11] Acceso no autorizado					
	[A.14] Interceptación de información					
	[A.24] Denegación de servicio					
	[A.26] Ataque destructivo					
Ofimática	[I.5] Avería de origen físico o lógico					
	[E.2] Errores del administrador					
	[E.4] Errores de configuración					

Tabla 23. (Continuación)

	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.20] Vulnerabilidades de los programas (software)					
	[E.21] Errores de mantenimiento o actualización (software)					
	[A.4] Manipulación de la configuración					
	[A.8] Difusión de software dañino					
	[A.11] Acceso no autorizado					
	[A.14] Interceptación de información					
	[A.24] Denegación de servicio					
	[A.26] Ataque destructivo					
Navegadores Web	[I.5] Avería de origen físico o lógico					
	[E.2] Errores del administrador					
	[E.4] Errores de configuración					
	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.20] Vulnerabilidades de los programas (software)					
	[E.21] Errores de mantenimiento o actualización (software)					
	[A.4] Manipulación de la configuración					
	[A.8] Difusión de software dañino					
	[A.11] Acceso no autorizado					
	[A.14] Interceptación de información					
	[A.24] Denegación de servicio					
	[A.26] Ataque destructivo					
Antivirus	[I.5] Avería de origen físico o lógico					
	[E.2] Errores del administrador					
	[E.4] Errores de configuración					

Tabla 23. (Continuación)

	[E.15] Alteración accidental de la información					
	[E.18] Destrucción de la información					
	[E.20] Vulnerabilidades de los programas (software)					
	[E.21] Errores de mantenimiento o actualización (software)					
	[A.4] Manipulación de la configuración					
	[A.8] Difusión de software dañino					
	[A.11] Acceso no autorizado					
	[A.14] Interceptación de información					
	[A.24] Denegación de servicio					
	[A.26] Ataque destructivo					

Fuente: el Autor

6.8 TRATAMIENTO DE LOS RIESGOS.

El tratamiento de los riesgos a la luz de la norma técnica tiene cuatro formas de atacarlos como son[22]:

- Mitigar el riesgo: Se considera mitigar el riesgo a la implementación de controles que permitan reducir este a un nivel aceptable.

- Transferir el Riesgo: Se trata de la utilización de un tercero llámese este proveedor o asegurador con el fin de que este mitigue el riesgo.

- Aceptar el Riesgo: Se trata de aceptar el riesgo, por ser inherente al desempeño del oficio.

- Evitar el Riesgo: Aunque es sumamente difícil evitar cualquier tipo de riesgo, lo que se busca es cesar la actividad que genera el riesgo.

De acuerdo a ello se tomaron como datos los riesgos con mayor incidencia y se da un tratamiento a ellos, como se muestra a continuación.

[22] ISO 27000. ES- El Portal de la ISO 27001 en español disponible en http://www.iso27000.es/sgsi_implantar.html

Tabla 24 Tratamiento Riesgo

Categoría	Amenaza	Impacto	Tratamiento del Riesgo
Comunicaciones	Condiciones inadecuadas de temperatura o humedad	Medio	Mitigación: Controles: La Alta gerencia dispondrá de un sistema de enfriamiento y control de temperatura y humedad, en el lugar donde se encuentran los dispositivos de comunicación.
	Interrupción de otros servicios o suministros esenciales	Medio	Mitigación: Controles: La Alta gerencia dispondrá de un sistema de Ups con mayor capacidad para evitar interrupciones
	Degradación de los soportes de almacenamiento	Medio	Mitigación: Controles: La Alta gerencia dispondrá de un sistema de enfriamiento y control de temperatura y humedad, en el lugar donde se encuentran los dispositivos de comunicación.
Hardware	Condiciones inadecuadas de temperatura o humedad	Medio	Mitigación: Controles: La Alta gerencia dispondrá de un sistema de enfriamiento y control de temperatura y humedad, en el lugar donde se encuentran los dispositivos de Hardware.
	Interrupción de otros servicios o suministros esenciales	Medio	Mitigación: Controles: La Alta gerencia dispondrá de un sistema de Ups con mayor capacidad para evitar interrupciones
	Errores de mantenimiento o actualización (hardware)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.
	Caiga del sistema por agotamiento de recursos	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.

Tabla 24. (Continuación)

Documentación física de la empresa	Errores de los usuarios	Medio	Mitigación: Controles: Se debe tener presente el mínimo de conocimiento para el manejo de la información, así como contratar periódicamente sensibilización o capacitaciones para el manejo del activo documental
	Escapes de información	Medio	Mitigación: Controles: Se debe contar con archivadores con sistema de seguridad y la documentación sensible debe almacenarse en algún tipo de caja fuerte o con una seguridad más robusta
	Alteración accidental de la información	Medio	Mitigación: Controles: Se debe tener presente el mínimo de conocimiento para el manejo de la información, así como contratar periódicamente sensibilización o capacitaciones para el manejo del activo documental
	Acceso no autorizado	Medio	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Modificación deliberada de la información	Medio	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Destrucción de la información	Alto	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Divulgación de información	Alto	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Robo	Alto	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Ataque destructivo	Alto	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía

Tabla 24. (Continuación)

Documentación digital de la empresa	Errores de los usuarios	Alto	Mitigación: Controles: Se debe tener presente el mínimo de conocimiento para el manejo de la información, así como contratar periódicamente sensibilización o capacitaciones para el manejo del activo digital
	Deficiencias en la organización	Medio	Mitigación: Controles: se debe contar con sensibilizaciones, capacitaciones y charlas informativas con el fin de socializar las políticas se seguridad de la información
	Difusión de software dañino	Medio	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Fugas de información	Medio	Mitigación: Controles: Se debe contar con socialización del uso responsable de las contraseñas de seguridad, así como implementar el vencimiento de estas, para que periódicamente sean cambiadas, también solicita más robustez en estas.
	Vulnerabilidades de los programas (software)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.
	Errores de mantenimiento o actualización (software)	Alto	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.

Tabla 24. (Continuación)

	Errores de mantenimiento o actualización (hardware)	Alto	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.
	Caiga del sistema por agotamiento de recursos	Alto	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos.
	Perdida de equipos	Alto	Mitigación: Controles: Contar con restricción para ingreso de personal no autorizado a zonas sensibles donde repose información física de la compañía
	Indisponibilidad del personal	Alto	Mitigación: Controles: Contar con campañas de promoción y prevención en cuanto a enfermedades laborales que aumenten la deserción laboral
	Suplantación de la identidad del usuario	Alto	Mitigación: Controles: Se debe contar con socialización del uso responsable de las contraseñas de seguridad, así como implementar el vencimiento de estas, para que periódicamente sean cambiadas, también solicita más robustez en estas.
	Abuso de privilegios de acceso	Alto	Mitigación: Controles: Se debe contar con socialización del uso responsable de las contraseñas de seguridad, así como implementar el vencimiento de estas, para que periódicamente sean cambiadas, también solicita más robustez de las mismas, también contar, el encargado del proceso técnico debe monitorear la red y el tráfico de la misma .

Tabla 24. (Continuación)

	Uso no previsto	Alto	Mitigación: Controles: Se debe contar con socialización del uso responsable de las contraseñas de seguridad, así como implementar el vencimiento de estas, para que periódicamente sean cambiadas, también solicita más robustez de las mismas, también contar, el encargado del proceso técnico debe monitorear la red y el tráfico de la misma.
	Difusión de software dañino	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Acceso no autorizado	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Interceptación de información	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Modificación deliberada de la información	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Destrucción de la información	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.

Tabla 24. (Continuación)

	Divulgación de información	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Manipulación de los equipos	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Denegación de servicio	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Robo	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
	Ataque destructivo	Alto	Mitigación: Controles: El encargado del proceso técnico debe velar por que los controles de antivirus se encuentren actualizados y operando, así mismo se debe contar por parte de la alta gerencia, el aprovisionamiento de un firewall.
Personal	Errores de los usuarios	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización de en el manejo de equipos de cómputo así mismo como con socialización de políticas de seguridad y prevención de riesgos
	Escapes de información	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización de en el manejo de equipos de cómputo así mismo como con socialización de políticas de seguridad y prevención de riesgos

Tabla 24. (Continuación)

	Alteración accidental de la información	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización de en el manejo de equipos de cómputo así mismo como con socialización de políticas de seguridad y prevención de riesgos
	Destrucción de la información	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización de en el manejo de equipos de cómputo así mismo como con socialización de políticas de seguridad y prevención de riesgos
	Fugas de información	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización de en el manejo de equipos de cómputo así mismo como con socialización de políticas de seguridad y prevención de riesgos
	Ingeniería social	Medio	Mitigación: Controles: Contar con capacitaciones y sensibilización con grupos de interés como el Csirt de la Policía Nacional, Ministerio de las Tic´s, Colcert
Software	Errores de configuración	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Alteración accidental de la información	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave

Tabla 24. (Continuación)

	Vulnerabilidades de los programas (software)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Errores de mantenimiento o actualización (software)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Manipulación de la configuración	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Difusión de software dañino	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave

Tabla 24. (Continuación)

	Acceso no autorizado	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Interceptación de información	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Denegación de servicio	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Ataque destructivo	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave

Tabla 24. (Continuación)

	] Vulnerabilidades de los programas (software)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Errores de mantenimiento o actualización (software)	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Manipulación de la configuración	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Difusión de software dañino	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave

Tabla 24. (Continuación)

	Acceso no autorizado	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Interceptación de información	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Denegación de servicio	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave
	Ataque destructivo	Medio	Mitigación: Controles: El encargado de la administración de los equipos de cómputo debe tener presente que los equipos cuenten con hoja de vida así contar con un cronograma de mantenimientos preventivos y correctivos. Así como una clave de administrador que debe ser cambiada periódicamente y guardada bajo llave

Fuente: el Autor

7. DIVULGACION

7.1 POLÍTICA PC DIGITAL LTDA.

PC DIGITAL LTDA adopto la siguiente política para su sistema de gestión de seguridad de la información SGSI:

La información es el principal activo en PC Digital por ello debe ser protegida adecuadamente, frente a posibles amenazas internas o externas que la puedan poner en riesgo.

Para proteger la información de una manera acertada y eficaz se implementará un sistema de gestión de información, basado y sustentado en la Norma ISO/IEC 27001:2013. En donde se establecerá los controles de seguridad de acuerdo a las necesidades.

La Política de seguridad de la información de PC Digital Ltda. Contemplara, la seguridad de la información, así como la seguridad informática. Siempre manteniendo los estándares de confiabilidad, integridad y disponibilidad, para lo cual se contará con los recursos necesarios para que se garantice el correcto desarrollo planteado por la gerencia.

La gerencia de PC Digital Ltda., implementará y mantendrá actualizado el Sistema con el fin de preservar su activo más valioso.

La política garantizara que existan responsables y responsabilidades que se asignen claramente, así como áreas seguras para la gestión, almacenamiento y procesamiento de la información, en donde se debe contar con protección física y ambiental para el activo que se proteja.

7.2 POLÍTICAS.

El manual de políticas de seguridad de la información se basa en el anexo A de la norma ISO/IEC 27001:2013 y por ello se sugieren las siguientes políticas[23]

[23] NORMA TECNICA COLOMBIANA NTC – ISO/IEC 207001- Anexo A Pagina 15 a 32 – Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

7.3 ACCESO A LA INFORMACIÓN.

Todos los funcionarios de PC DIGITAL LTDA, incluyendo personal de contrato sea cual sea su modalidad, visitantes, contratistas, y proveedores, tendrá solo acceso a la información necesaria para el desarrollo de la actividad, para la que se encuentre contratado.

Si un funcionario debe tener acceso a información que no está contemplada en su manejo, el acceso a esta debe ser autorizado por su superior jerárquico, asumiendo este cualquier tipo de problema o afectación en que se vea envuelta la información proporcionada.

Los privilegios para el uso de la información solo serán concedidos en el tiempo que sea necesario o mientras se encuentre en la actividad, una vez concluya todos los privilegios deben ser suspendidos. Entiéndase esto también en caso de terminación de contrato o cancelación del mismo.

7.4 ADMINISTRACIÓN DE HARDWARE Y SOFTWARE.

Todos los cambios en el Hardware y software de la compañía PC DIGITAL LTDA, deben ser solicitados a la Dirección Técnica, y avalados por ella, en ningún caso podrá ser instalado en software no licenciado en los equipos de PC DIGITAL.

Bajo ninguna circunstancia personal ajeno a la Dirección técnica podrá instalar, modificar, actualizar hardware o software en PC DIGITAL.

Cualquier cambio de características de tipo hardware o software deberá quedar registrado para llevar su seguimiento, así mismo el manejo de documentación de este debe ser enviado con oficio a la dirección administrativa para que esta salvaguarde la documentación, llámese garantías o manuales de instalación.

7.5 SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS.

Todos los funcionarios utilizaran el recurso informático de acuerdo a su labor específica, en ningún caso se autorizará el uso de este para fines personales.

La propiedad intelectual que se desarrolle o sea concebida dentro de las instalaciones de PC DIGITAL, será propiedad exclusiva de PC DIGITAL, esta política incluye patentes, derechos de reproducción, derechos de propiedad intelectual, códigos fuente, documentación y otros materiales.

La dirección Técnica podrá monitorear o tomar control total de algún equipo que infrinja esta política y comunicará automáticamente a la Dirección Administrativa con el fin de realizar las acciones competentes.

Si algún funcionario sospecha de la infección por un virus, troyano o malware, o cualquier tipo de infección en su equipo de cómputo deberá elevar un reporte automáticamente a la Dirección Técnica, con copia a la Dirección administrativa.

7.6 SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.

Todos los servicios deben tener las siguientes características

Administrador: Es el Director de tecnología o su delegado para administrar la red, quien establecerá patrones en las contraseñas y vigencia de las mismas.

Rol de usuario: Este será dado por el Director de Tecnología o su delegado previa autorización por la Gerencia, indicando los privilegios que tendrá cada uno de ellos.

Las contraseñas serán personales e intransferibles, dado que cada usuario tendrá un rol específico y acceso especifico, cualquier funcionario que sea sorprendido ingresando con credenciales diferentes a las suyas, será bloqueado y se procederá a las sanciones a que den a lugar.

Toda la información de bases de datos e información sensible debe ser sujeta a backups, ya sean estos diarios, semanales, mensuales y anuales, según determine el director de tecnología.

Antes de que un nuevo sistema informático sea puesto en producción, se deberá contar con una socialización y capacitación para evitar trastornos en la compañía.

7.7 COPIAS DE RESPALDO O BACKUPS.

Todo proceso de respaldo debe ser documentado y archivado por la dirección administrativa.

El proceso de respaldo o copias de seguridad estará en manos de la Dirección Técnica la periodicidad de estas será dada y avalada por la Gerencia.

Todos los respaldos deben reposar en gavetas de seguridad, con control de acceso, así mismo deberán reposar en forma lógica debidamente asegurados.

La Gerencia General deberá abastecer de un segundo lugar para salvaguardar la información en sitio alterno en caso de presentarse daños catastróficos en la compañía.

7.8 AUDITORIAS.

La Gerencia General proporcionara de auditorías periódicamente con el fin de revisar los procesos y procedimientos que se llevan a cabo en PC DIGITAL, con el fin de contribuir al mejoramiento continuo del proceso de calidad de la compañía.

8. CONCLUSIONES

La importancia de la información para cualquier tipo de organización, siendo esta el activo más valioso con que cuenta una compañía, por tanto, se debe garantizar la conservación de este activo, analizando, diseñando e implementando todo tipo de acciones que propendan a salvaguardar la información.

La utilización una metodología como Magerit para identificación de riesgos, valoración y control hace que el planear del ciclo de vida PHVA, sea mucho más fácil ordenado.

Se identificaron los activos de información de PC DIGITAL LTDA, así como riesgos Su valoración y su análisis, y se creó la política de seguridad de la Información para PC DIGITAL LTDA.

Se debe tener una gran visión de lo que representa ser un especialista en seguridad de la información, sabiendo que la responsabilidad de implementar procesos y procedimientos van de la mano con la sensibilización y capacitación del usuario sea este la alta dirección o un usuario básico.

El apoyo de la alta dirección en proceso de optar por la realización de SGSI, es básica y relevante, puesto que sin el apoyo y disposición de esta el resultado no sería el esperado, con este proyecto se espera que PC DIGITAL LTDA, implemente el SGSI y ponga en marcha sus fases.

9. RECOMENDACIONES

Es indispensable que la Alta Dirección en cabeza de la gerencia, se apropie de encaminar a la compañía en implementar el modelo de seguridad de la información.

Las políticas de seguridad de la información definidas en este Diseño son de obligatoriedad por parte de todos los implicados ya sean estos empleados, contratistas y/o visitantes que se encuentren dentro de PC Digital, laboren o presten sus servicios para esta empresa.

La Alta dirección en cabeza de la gerencia, deberá propender por realizar sensibilizaciones, capacitaciones, foros, a todos los empleados de PC Digital en los temas de seguridad de la información, con fin de mitigar los riesgos y posibles fugas de información.

BIBLIOGRAFIA

WIBU SYSTEMS. Protección del Software. {En línea}. {15 de marzo de 2017}. Disponible en http://www.wibu.com/es/proteccion-software.html

GANTTPROJECT. Gantt Project 2.6.6. {En línea}. {15 de marzo de 2017}. Disponible en http://www.ganttproject.biz/brno

CYNERTIA CONSULTING.PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN. {En línea}. {15 de marzo de 2017}. Disponible en http://www.cynertiaconsulting.com/sites/default/files/PDF/Cynertia_Planificacion_estrategica_sistemas_resumen.pdf

REPÚBLICA DE COLOMBIA COPNIA. Código de ética profesional. {En línea}. {15 de marzo de 2017}. Disponible en https://copnia.gov.co/codigo-de-etica-profesional/

REPÚBLICA DE COLOMBIA MPRENDE. MARCO LEGAL PARA LA POLÍTICA NACIONAL DE EMPRENDIMIENTO. {En línea}. {15 de marzo de 2017}. Disponible en http://mprende.co/emprendimiento/marco-legal-para-la-pol%C3%ADtica-nacional-de-emprendimiento

REPÚBLICA DE COLOMBIA LEY 1266 DE 2008 NIVEL NACIONAL. {En línea}. {15 de marzo de 2017}. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

REPÚBLICA DE COLOMBIA UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD. Capítulo 1 Seguridad Informática. {En línea}. {15 de marzo de 2017}. Disponible en http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_1_seguridad_informatica.html

ISO 27001 LOS CONTROLES. {En línea}. {18 de marzo de 2017}. Disponible en http://www.iso27000.es/download/iso-27001_los-controles_parte_i.pdf

NORMA TECNICA COLOMBIANA NTC ISO/IEC COLOMBIANA 27001 {En línea}. {18 de marzo de 2017}. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

PROCESO DESARROLLO OPEN UP /OAS. Sub Proceso Gestión del Riesgo Capitulo 5. {En línea}. {18 de marzo de 2017}. Disponible en http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

CN. CERT CENTRO CRIPTOLOGICO NACIONAL. DEFENSA FRENTE A LAS CIBERAMENAZAS. {En línea}. {18 de marzo de 2017}. Disponible en https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/metodologia.html

Banco terminológico. Activo de Información. {En línea}. {18 de marzo de 2017}. Disponible en: http://banter.archivogeneral.gov.co/vocab/?tema=5
Magerit – Versión 3.0. Metodología de Análisis y Gestión del Riesgos de los Sistemas de Información. – Gobierno de España – Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Archivo General de la Nación. Norma ISO – IEC 27001 {En línea}. {18 de marzo de 2017}. Disponible en http://www.archivogeneral.gov.co/normatividad/items/show/34

ICONTEC. Guía Técnica Colombiana GTC. ISO/IEC 27003. {En línea}. {18 de marzo de 2017}. Disponible en https://tienda.icontec.org/wp-content/uploads/pdfs/GTC-ISO-IEC27003.pdf

República de Colombia. Consejo Profesional Nacional de Ingeniería Copnia. {En línea}. {18 de marzo de 2017}. Disponible en https://copnia.gov.co/copnia/normatividad/ley-842-de-2003/

República de Colombia. Ministerio de Tecnologías de la información y las comunicaciones. {En línea}. {18 de marzo de 2017}. Disponible en http://www.mintic.gov.co/portal/604/w3-article-3669.html

República de Colombia. Consejo Nacional de Política Económica y social. {En línea}. {18 de marzo de 2017}. Disponible en www.colombiacompetitiva.gov.co/sncei/Documents/Conpes-3527-de-2008.pdf

República de Colombia. Congreso de la Republica. {En línea}. {18 de marzo de 2017}. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2- Catalogo de Elementos Pág. 25 – 47. {En línea}. {18 de marzo de 2017}. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Pc Digital. Soluciones Técnicas. {En línea}. {18 de marzo de 2017}. Disponible en http://pcdigitalcolombia.com/Nosotros.html

ANEXOS

RESUMEN ANALÍTICO ESPECIALIZADO	
1. Título.	Diseño de un Sistema de Gestión de Seguridad Informática para la Empresa PC Digital Ltda. Usando ISO/IEC 27001:2013
2. Autor:	Ruiz Rodríguez, Khaanko Norberto
3. Edición	Universidad Nacional Abierta y a distancia UNAD especialización en seguridad de la información
4. Fecha	28 de mayo de 2017
5. Palabras Claves,	Seguridad de la información, metodología, Magerit, riesgos, activos, políticas, ciclo PHVA.
6. Descripción.	El documento se basa en el diseño de un sistema de gestión de seguridad informática para una pequeña empresa ubicada en la ciudad de Bogotá, que se dedica a la venta y soporte de servicios informáticos y tecnología.
7. Fuentes.	Se basaron en la metodología Magerit, al igual que las experiencias profesionales, entrevistas con el gerente de la compañía y sus subalternos así como las recomendaciones de la norma ISO/IEC 27001:2013
8. Contenidos.	El documento se basa en el diseño de un SGSI, cumpliendo con el ciclo de planear de PHVA, en donde se revisan los activos de la información, se valoran, se revisan los riesgos y se dan recomendaciones para el tratamiento de los mismos. El diseño de un Sistema de gestión de seguridad de la información permite identificar amenazas y vulnerabilidades y los riesgos a que están expuestos los activos de una organización, permitiendo establecer normas y controles adecuados para proteger el activo más valioso en cualquier compañía, y de este modo garantizar la continuidad de todos los procesos de la compañía
9. Metodología.	Se realiza un estudio y análisis de los activos de información con la cual cuenta PC DIGITAL, así mismo se abordará la norma técnica ISO/IEC 27001:2013, para elevar recomendaciones pertinentes con el fin de proteger el activo. Se determinarán los activos de información y se

	clasificarán para determinar el estado actual de la seguridad de la información. Se establecerán amenazas a las que se encuentra expuesta la seguridad de la información tanto en su confidencialidad, integridad y disponibilidad, con el propósito de identificar vulnerabilidades y tomar correctivos. Por último, paso y de acuerdo a los análisis realizados a los riesgos y amenazas y procesos implementados, serán puestos a consideración en la fase de implementación, acordes a la organización.
10. Conclusiones.	La importancia de la información para cualquier tipo de organización, siendo esta el activo más valioso con que cuenta una compañía, por tanto, se debe garantizar la conservación de este activo, analizando, diseñando e implementando todo tipo de acciones que propendan a salvaguardar la información. La utilización una metodología como Magerit para identificación de riesgos, valoración y control hace que el planear del ciclo de vida PHVA, sea mucho más fácil ordenado. Se identificaron los activos de información de PC DIGITAL LTDA, así como riesgos Su valoración y su análisis, y se creó la política de seguridad de la Información para PC DIGITAL LTDA. Se debe tener una gran visión de lo que representa ser un especialista en seguridad de la información, sabiendo que la responsabilidad de implementar procesos y procedimientos van de la mano con la sensibilización y capacitación del usuario sea este la alta dirección o un usuario básico.
11. Autor del RAE.	Khaanko Norberto Ruiz Rodríguez