ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001, PARA EL AREA DE HISTORIAS CLÍNICAS EN LA EMPRESA NEUROKIDS HEALT DE LA CIUDAD DE POPAYÁN

JAKELINE ORDOÑEZ SOTELO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYAN
2018

ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001, PARA EL AREA DE HISTORIAS CLÍNICAS EN LA EMPRESA NEUROKIDS HEALT DE LA CIUDAD DE POPAYÁN

JAKELINE ORDOÑEZ SOTELO

Proyecto aplicado para optar al título de:
Especialista en Seguridad Informática

Asesor del proyecto
Jose Hernando Peña
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYAN
2018

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente de jurado

_____

Firma del jurado

_____

Firma del jurado

Popayán, 17 de octubre de 2018

DEDICATORIA

Es maravilloso poder culminar una nueva etapa de mi vida como estudiante, por eso quiero dedicar este trabajo en primer lugar a la fuerza de mi inspiración, a la fé que me hace creer en Dios, que es el que impulsa a lograr todos mis sueños.
A mi amado Esposo Fabinton Sotelo quien ha sido la persona que me ha apoyado en los momentos difíciles y me ha llenado de fuerzas para continuar en la batalla, me ha apoyado a seguir y mirar siempre adelante.

A mis dos hermosas hijas Juliana e Isabela quienes son mis más grandes bendiciones y la fuente de mi inspiración y motivación continua, para poder superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor

Con un aprecio muy especial a mi madre Carmelita, quien de manera incondicional me ha acompañado en este largo camino. A su vez a mi padre Ruribe quien me enseño que con humildad se logra cualquier cosa que me proponga.

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi padre celestial, que me ha permitido culminar esta nueva etapa de mi vida. Gracias Dios por renovar mis fuerzas cada día y enseñarme a tener fé en los momentos difíciles.

Agradezco a mi querido Esposo, quien con su esfuerzo y sacrificio me brindó su apoyo incondicional, gracias por creer en mí y ayudarme a superar cada etapa a lo largo de mi posgrado

De igual manera a mi Director de proyecto de Grado Ing. Hernando José Peña Hidalgo por su dedicación, tiempo y comprensión; quien con sus conocimientos y experiencia ha logrado que pueda terminar mi proyecto.

A la Universidad Nacional Abierta y a Distancia UNAD, por permitirme realizar mis estudios y adquirir conocimientos en el campo de la seguridad informática y de esa manera poder superarme para competir en el campo laboral.

A los funcionarios de la empresa Neurokids Healt, que me abrió sus puertas para que yo pudiera acceder a la información necesaria para llevar a cabo este proyecto.

CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pag.

1. TITULO

Análisis y diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001, para el área de historias clínicas en la empresa Neurokids HEALT a de la ciudad de Popayán

2. INTRODUCCIÓN

Las Tecnologías de la Información y las Comunicaciones (TIC) han protagonizado una transformación en la sociedad en todos sus ámbitos en los últimos años. Son innumerables los avances en los servicios de atención al cliente que emplean y promueven el uso de Sistemas Informáticos, lo que posibilita un aumento en la calidad y eficiencia de dichos servicios

A medida que avanza la tecnología, también aumentan las posibilidades de ataques informáticos a cualquier tipo de usuario, especialmente las empresas que hacen uso de medios informáticos y telemáticos (Aplicaciones web, redes de datos, Internet, base de datos entre otros) para uno o varios procesos, es así, que este tipo de usuarios se convierten en blanco de amenazas los activos de la información. El presente proyecto analiza este tipo de situación en una empresa dedicada a prestar servicios de salud especializados en rehabilitación física y neurológica, Neurokids HEALT, la cual maneja información importante para su funcionamiento. Uno de los servicios informáticos indispensable es el manejo de las historias clínicas de los pacientes; para la cual se requiere diseñar un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 versión 2013, que disminuya la probabilidad de ataques informáticos que alteren la confidencialidad, integridad y disponibilidad de la información

El alcance del proyecto es analizar el riesgo de cada activo informático involucrado en el manejo de las historias clínicas y realizar un estudio de las vulnerabilidades a la que está expuesta esta información, con el propósito de diseñar el SGSI que garantice mantener la información de los pacientes integra.

El proyecto se centra en el análisis y diseño del SGSI, en el área de historias clínicas de la entidad, basado en las experiencias de los empleados, quienes manifiestan la falta de controles de seguridad para el acceso a la información.

Mediante la metodología Magerit se realizará el análisis de los riesgos, amenazas y vulnerabilidades a la que se expone la información día a día, donde se identifiquen las causas que dan lugar a posibles ataques informáticos que puedan causar daño o robo a los activos informáticos.

Con los resultados obtenidos en el análisis de vulnerabilidades y amenazas se procede al diseño del SGSI basado en la norma ISO/IEC 27001 versión 2013 en el área de historias clínicas en Neurokids Healt de la ciudad de Popayán, donde se plantearán las fases de planeación y verificación que permita generar una propuesta para una futura implementación del SGSI por parte de la empresa.

3. DEFINICIÓN DEL PROBLEMA

3.1. ANTECEDENTES DEL PROBLEMA

Neurokids Healt, es una empresa de tipo privado, la cual brinda los servicios de terapias de neurodesarrollo físicas, fotobiología, ocupacional, consultas de pediatría, neuropediatría y psiquiatría infantil, para los niños con deficiencias neurológicas, comportamentales y déficit de atención. Cuenta con tres sedes las cuales están ubicadas en la ciudad de Popayán, Cali y Manizales.

Como en toda empresa el flujo de información es un elemento importante, por cuanto permite conocer el estado de la empresa en sus diferentes áreas. Para este caso. En el área que se gestiona y administra las historias clínicas de pacientes, no existe un control en la manipulación de la información, se carece de controles de seguridad que garanticen la integridad y confidencialidad, dejando la información vulnerable a posibles ataques informáticos desde adentro y fuera de la empresa.

Planteado este contexto, surge la necesidad de diseñar un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 enfocado a garantizar la seguridad de la información de las historias clínicas, para brindar confiabilidad, disponibilidad, integralidad y protección de esta información en la sede de Popayán.

3.2. FORMULACIÓN DEL PROBLEMA

Mediante el uso de las herramientas informáticas y el diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 ¿Cómo se puede mejorar el nivel de seguridad de la información de historias clínicas de la empresa NEUROKIDS HEALT?

3.3. DESCRIPCIÓN DEL PROBLEMA

Cuando se carece de un sistema de gestión de la información, se corre el riesgo de que las historias clínicas de los pacientes sean manipuladas o lo que es peor puedan ser robadas, por lo tanto, es fundamental que exista un sistema el cual proponga un control sobre la manipulación de los datos. Garantizando la integralidad, disponibilidad y confidencialidad de la información que se maneja en Neurokids Healt

4. JUSTIFICACIÓN

La tecnología avanza a pasos agigantados, facilitando así la vida de los seres humanos, son innumerables los avances que han surgido, los cuales han sido importantes para el desarrollo social, económico y cultural, estableciendo una base fundamental para su progreso. A medida que la tecnología avanza, surgen también los problemas de seguridad los cuales impiden garantizar la integridad de la información.

Neurokids Healt maneja información importante y confidencial, como lo es las historias clínicas de los pacientes que atienden en cada una de las áreas. Dicha información carece de un sistema de seguridad que garantice la integridad, confiabilidad y disponibilidad de la información.

Teniendo en cuenta lo anterior, se propone el diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 versión 2013, para el área de historias clínicas, ya que no existe un control de la manipulación de la información que se tiene en la empresa, exponiendo a posibles ataques de ingeniería social, inyección de código, virus, gusanos, entre otros. poniendo en alto riesgo los datos que circulan por la red de la empresa, causando posible pérdida o daño de los datos.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 versión 2013 en el área de historias clínicas para la empresa NEUROKIDS HEALT ubicada en la ciudad de Popayán.

5.2. OBJETIVOS ESPECÍFICOS

- Analizar los activos de información que pertenecen al área de historias clínicas de la empresa de acuerdo con la metodología Magerit.

- Determinar el nivel de seguridad informática existente en la empresa, mediante un análisis de amenazas.

- Diseñar controles para reducir o mitigar el riesgo existente en la empresa basados en la norma ISO/IEC 27001 versión 2013.

6. MARCO REFERENCIAL

6.1. ANTECEDENTES

Con el propósito de identificar los avances y hallazgos en otros proyectos de sistema de gestión de seguridad informática se tomaron los siguientes proyectos:

- ✓ Diseño de un sistema de gestión de seguridad informática para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoria. Trabajo de grado para optar el Titulo de la Especialización de seguridad informática de la Universidad Nacional Abierta y a Distancia UNAD. Esta investigación desarrolla un sistema de gestión de la seguridad informática para empresas del sector textil de las pymes, el diseño se elaboró basado en la norma ISO 27001, la cual provee practicas adecuadas para el desarrollo e implementación de cada uno de sus componentes, estableciendo las fases, documentación y procedimientos requeridos por la norma.

- ✓ Diseño e implementación de un sistema de gestión de seguridad e información en procesos tecnológicos. Tesis para optar el título profesional de Ingeniero de computación y sistemas de la Universidad de San Martin de Porres Lima – Perú. El propósito de este trabajo se centró en la implementación de un sistema de gestión de seguridad de la información, bajo una metodología de análisis y evaluación de riesgos usando la norma ISO 27001:2005 e ISO 17799:2005. Garantizando que

los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados.

- ✓ sistema de gestión de seguridad de información para una institución financiera. Tesis para optar el título de ingeniero informático de la Universidad Pontifica Católica del Perú. El objetivo de esta tesis es realizar una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera

6.2. MARCO CONTEXTUAL

La empresa Neurokids HEALT ha prestado sus servicios de neurodesarrollo y neurorrehabilitación mediante la utilización de diferentes herramientas informáticas tradicionales desde las cuales se ha creado información de historias clínicas, la cual se guarda en diferentes medios de almacenamiento y también de forma escrita, Esta información contiene historias clínicas de los diferentes pacientes.

Neurokids cuenta con tres sedes las cuales están ubicadas en Manizales. Cali y Popayán, es una empresa del sector salud, la cual abre sus puertas a la población infantil, tratando niños con diferentes tipos de incapacidad física y cognitiva. Cuenta con personal especializado entre los cuales están psicólogo, psiquiatra infantil, neuro pediatra, terapeutas físicos, ocupaciones y de lenguaje; quienes son

las personas encargadas de brindar un manejo clínico a los pacientes para su evolución.

✓ **Reseña histórica**: Neurokids Cauca SAS fue fundada el 14 de octubre del año 2012 por un grupo de socios, en la ciudad de Popayán. La empresa de tipo privado ofrecía sus servicios de terapias de neurodesarrollo y programa canguro.

En el año 2013 amplio sus servicios implementando consultas de pediatría, neuroendocrina, psiquiatría infantil y neuro psicopedagogía dirigido a pacientes con problemas neurológicos.

En enero del año 2017 Neurokids Cauca SAS se transforma en Neurokids Healt incursionando en procesos atencionales de alta calidad e integralidad para la población infantil y sobre todo para población en situación de discapacidad. Desde hace varios años nace la inquietud en lograr una coarticulación del área de Salud y Educación, sobre todo para la población con alguna discapacidad (motora, cognitiva, visual, auditiva) que desea ser integrada e incluida en los ámbitos escolares; por ese motivo inicia creando una estrategia de atención para los pacientes que ingresan a la institución y se encuentran escolarizados donde se realiza visitas al colegio y se pretende lograr adaptaciones escolares tanto significativas como no significativas. Posteriormente se trabaja con un proyecto de necesidades educativas especiales en las instituciones educativas del municipio de Popayán.

✓ **Localización**: La entidad se encuentra ubicada en la ciudad blanca de Colombia Popayán Cauca, específicamente en la calle 17N # 11-09 barrio Antonio Nariño.

✓ **Actividad e Infraestructura Computacional**: su actividad básica e la atención a pacientes de la población infantil, ofreciendo el servicio de terapias de Neurodesarrollo y consulta con Especialistas; cuenta con 3 computadores de mesa y dos portátiles, de los cuales 2 se utilizan para fines administrativos y 3 equipos para alimentación de la base de datos de historias clínicas, cuenta con un programa llamado Babyware donde se registran las historias clínicas y las evoluciones diarias de los pacientes en línea, ya que el servidor se encuentra en la ciudad de Cali.

Se cuenta con una red cableada LAN, la cual se conectan los tres computadores de mesa, los portátiles se conectan por medio de wifi

6.3. MARCO TEÓRICO

6.3.1 Metodología de gestión de riesgo Magerit

Es un método de análisis y gestión de riesgos, elaborado por el consejo superior de administración electrónica, que facilita la implantación y aplicación del esquema de seguridad proporcionando los principios básicos y requisitos mínimos para protección de la información.

Su objetivo fundamental es analizar y evaluar cada activo de información dentro de la empresa, con el fin de corregir errores que provoquen un riesgo, contribuyendo con la mitigación del mismo.

Mediante esta metodología va a ser posible implementar acciones de mejora los cuales van a permitir controles que aporten a la mitigación del riesgo dentro de Neurokids Healt en el área de historia clínicas

Con la metodología Magerit es posible clasificar los activos de información de acuerdo a las características similares y particulares, lo que posibilita establecer el tratamiento del riesgo para contrarrestarlo y asegurar la infraestructura informática.

Paso 1: Inventario y valoración de los activos: Es el proceso mediante el cual se identifican los activos de información tanto hardware como software, y el recurso humano que posee la empresa. Para lograr la valoración es importante contar con el personal encargado del manejo del sistema informático de la organización. Segun Magerit los activos de información se clasifican de la siguiente manera:

Tabla 1 Clasificación de activos según MAGERIT

Tipos de activos	Descripción
Activos esenciales	Información que se maneja, p.e, (bases de datos, contratos, manuales de usuario, políticas, pólizas de seguros etc. Servicios prestados
Servicios internos	Los que estructuran ordenadamente el sistema informático, p.e, (conexión a internet, mantenimiento, apoyo logístico, soporte a usuarios, mejoramiento de procesos, etc.)
Equipamiento informático	Equipos informáticos (hardware)

	Aplicaciones (software) Comunicaciones (dispositivos y elementos de conectividad física o inalámbrica). Soportes de información (discos duros, pendrives, cintas magnéticas, etc.)
Activos del entorno	Equipos para el suministro de energía, sistemas SAI, sistema de climatización, red del acueducto, etc. Mobiliario
Servicios subcontratados a terceros	p Desk, DRP, mantenimiento y soporte de infraestructura de TI, consultoría, capacitación, etc.
Instalaciones físicas	orno físico del CPD, instalaciones eléctricas, arquitectura de la red, y características generales del edificio.
Recurso humano	Personal ejecutivo Personal administrativo Operarios Usuarios, etc.

Fuente: Magerit 3.0, Libro I. P.24

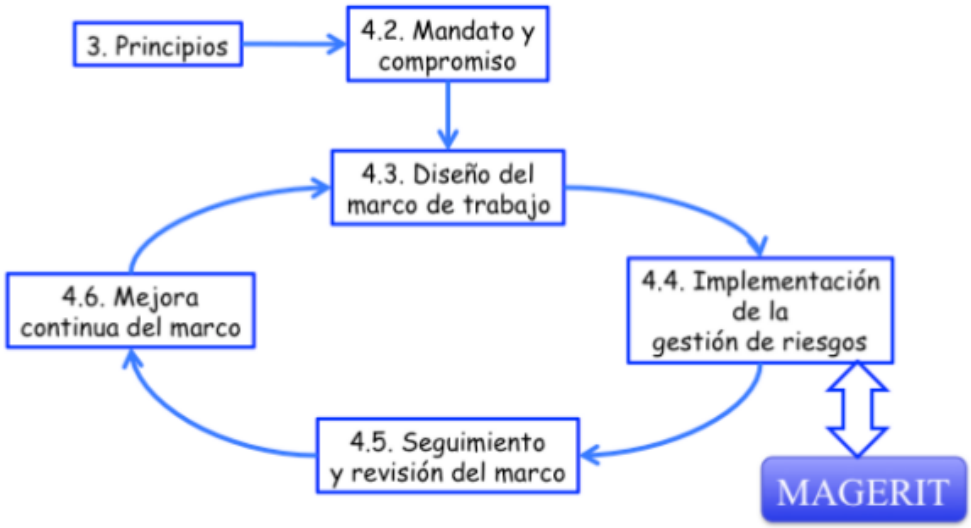
Análisis y el tratamiento de los riesgos: como dice Amutio Gómez[1], para determinar qué tan importante y que valor posee un activo de información, se realiza el análisis del riesgo, según las necesidades y políticas de la empresa, se

1 AMUTIO GOMEZ, Miguel Angel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Madrid, octubre de 2012. p . 10.

diseña un plan de seguridad para implementar y satisfacer los objetivos propuestos para la mitigación de los riesgos.

Para la implementación de las medidas de seguridad se necesita que todo el personal de la empresa que trabaje con el sistema de información participe y se responsabilice de las eventualidades diarias que suceden en general con el sistema, con el fin de determinar si se cumplen los objetivos propuestos.

Figura 1 ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: MAGERIT 3.0 Libro I P.7

Como primer paso se debe hacer una clasificación de los activos de información según Magerit que intervienen en el proceso de tratamiento de riesgos, este tipo de análisis se realiza con la ayuda del personal encargado de cada activo dentro de la Empresa.

Dentro del proceso de valoración de Magerit existen 2 escalas valorativas dentro de las cuales se contemplan la cuantitativa y cualitativa, dentro de la cualitativa permite identificar la importancia relativa de los activos identificados en relación con el impacto que pueda generar una amenaza sobre los mismos. La siguiente tabla se relaciona este tipo de valoración:

Tabla 2 Estimación cualitativa del riesgo

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	**MA**: prácticamente seguro	**MA**: critico
A: alto	**A**: probable	**A**: importante
M: medio	**M**: posible	**M**: apreciable
B: bajo	**B**: poco probable	**B**: bajo
MB: muy bajo	**MB**: muy raro	**MB**: despreciable

Fuente: Magerit 3.0, Libro III. P.7

Valoración cuantitativa: Según Magerit, el valor de un activo se estima mediante valores superiores a cero pesos, teniendo como representación matemática los números reales positivos. La tabla 5 representa un ejemplo de valoración cuantitativa.

Tabla 3 Relación entre escala cualitativa y cuantitativa

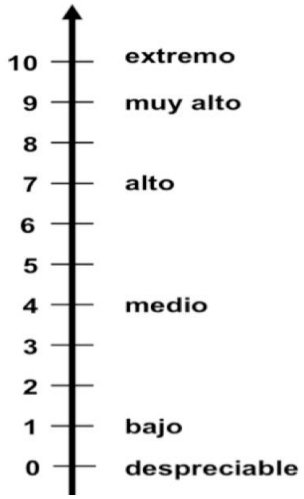
Valoración cualitativa	Escala cuantitativa	Valoración cuantitativa en $
MA: muy alto	5	[2’10.000, 5.000.000]
A: alto	4	[1’010.000, 2’000.000]
M: medio	3	[510.000, 1’000.000]
B: bajo	2	[310.000, 500.000]
MB: muy bajo	1	[0, 200.000]

Fuente: El autor

Criterios de valoración: Para establecer una valoración de activos en cada una de las dimensiones de seguridad, Magerit define unos criterios de valoración que

nos permiten ubicar y posicionar cada activo con relación a cada dimensión. La tabla 6, relaciona unos criterios a tener en cuenta a la hora de valorar activos con respecto al grado de exposición a que una amenaza se materialice sobre los mismos.

Tabla 4 Criterios de valoración de activos de acuerdo al grado de la amenaza



Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit 3.0, Libro II. P.19

En relación a lo anterior, se aplicará la metodología Magerit para el respectivo análisis de riesgos en la Empresa Neurokids Cauca Healt, con el propósito de diseñar un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001 para el área de historias clínicas.

Paso 2: Identificación y valoración de la Amenaza: Todo sistema Informático está expuesto a diferentes amenazas que pueden afectar considerablemente a los procesos de una empresa, de ahí la importancia de analizar de qué manera estas amenazas se producen y se materializan teniendo en cuenta el antes, durante y

después del suceso. Esto ha permitido crear una serie de políticas y mecanizamos dirigidos a la prevención, detección y recuperación de los sistemas de información ante cualquier eventualidad.

Identificación de las amenazas: para realizar este procedimiento, Magerit 3.0, Libro II. p. 25-47, muestra un catálogo de amenazas que pueden dañar un determinado activo, esta clasificación se enumera con las letras N, I, E y A, en donde cada una representa un grupo de amenazas diferentes

Valoración de las amenazas: Una vez identificadas las amenazas el siguiente paso es realizar una valoración para identificar su influencia y en qué medida puede afectar al activo de información

Magerit 3.0, libro I. P. 28, señala que: “Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

degradación: cuán perjudicado resultaría el [valor del] activo

probabilidad: cuán probable o improbable es que se materialice la amenaza[2]

2 AMUTIO GOMEZ, Miguel Angel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Madrid, octubre de 2012. p . 28.

Tabla 5 Probabilidad de ocurrencia de la amenaza

	Valoración cualitativa	Valoración cuantitativa	Rango
MA	Muy alta	100	1 vez al día
A	Alta	70	1 vez cada semana
M	Media	50	1 vez cada mes
B	Baja	10	1 vez cada 6 meses
MB	Muy baja	5	1 vez cada año

Fuente: módulo Gestión de Seguridad Informática

Impacto Potencial: Es la consecuencia de la materialización de una amenaza, que genera impacto a la medida del daño sobre el activo; Conociendo el valor de los activos y la degradación que causan las amenazas, es posible derivar el impacto que estas tendrían sobre el sistema.

Para valorar cuantitativamente las consecuencias del impacto de las amenazas sobre los activos, se tiene en cuenta la siguiente escala porcentual de impactos posibles sobre las dimensiones de seguridad de los activos:

Tabla 6 Impacto de las amenazas sobre las dimensiones de seguridad

Impacto	Valoración cualitativa	Valoración cuantitativa
MA	Muy alto	100%
A	Alto	75%
M	Medio	50%

B	Bajo	10%
MB	Muy bajo	5%

Fuente: módulo Gestión de Seguridad Informática

Paso 3: Análisis de salvaguardas: las salvaguardas son aquellos procedimientos tecnológicos que permiten reducir los riesgos que pueden afectar a los activos informáticos de la empresa.

De acuerdo a Magerit 3.0, Libro I. p. 31 para la selección de salvaguardas; “se debe tener en cuenta los siguientes aspectos:

- Tipo de activo que se debe proteger
- Dimensiones de seguridad que requieren protección
- Amenazas de las que debemos protegernos
- Si existen salvaguardas alternativas[3]

Tipos de salvaguardas: Existen diferentes tipos de protección los cuales se resumen en la tabla 7:

3 Ibíd.; p.31

Tabla 7 Tipos de salvaguardas

Efecto	Tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Magerit 3.0, Libro I. P.34

Paso 4: Impacto Residual: después de aplicar un conjunto de salvaguardas de seguridad, el sistema queda en una situación de posible impacto, el cual se le llama residual, de esta manera el impacto a sido modificado desde un valor potencial a un valor residual.

Paso 5: Riesgo Residual: después de identificar vulnerabilidades y amenazas y aplicar las medidas de protección, el sistema queda en una situación de riesgo, el cual debe superar el riesgo potencial y toda fracción de riesgo que este por debajo de dicho nivel, no se considera como una importante amenaza, y por lo tanto, puede ser aceptado por la organización o reducirse hasta un determinado punto de aceptación.

6.3.2 Sistema de gestión de seguridad informática.

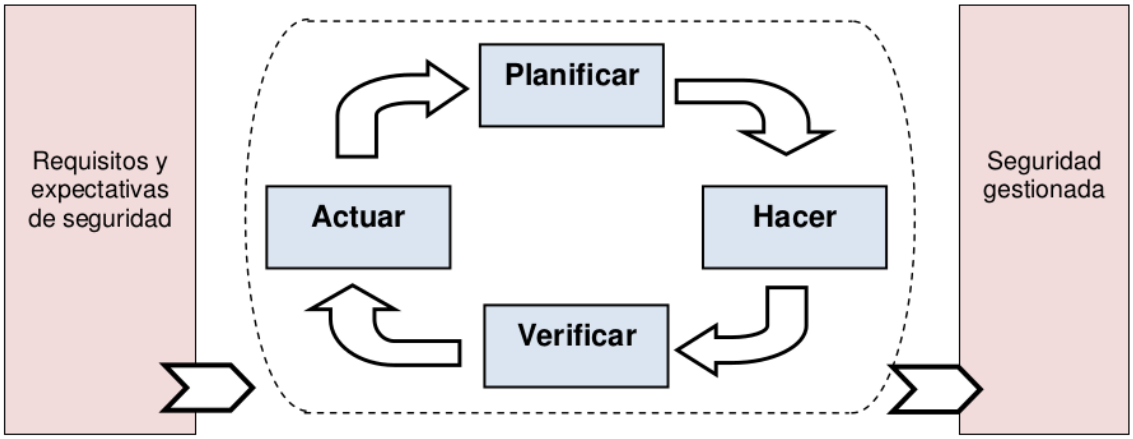
El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados[4].

6.3.3 Procesos de un Sistema de Gestión de la Seguridad Informática.

El SGSI se compone de cuatro procesos básicos:

4 Solarte Solarte Francisco Nicolás Javier, Enriquez Rosero Edgar Rodrigo. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 EN Revista Tecnológica ESPOL. Diciembre, 2015. Vol. 28. No. 5, p. 492-507.

Figura 2 Modelo PHVA aplicado a los procesos del SGSI



Fuente: Oficina de Seguridad para las Redes Informáticas. Metodología Para La Gestión De La Seguridad Informática.

PLANIFICAR: En esta primera etapa se establecen los procesos, objetivos, políticas y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática de la organización.

HACER: Gestionar los controles necesarios, teniendo en cuenta los objetivos propuestos, con el fin de garantizar el correcto funcionamiento de las políticas y procesos diseñados.

VERIFICAR: Verificar que los procesos establecidos tengan un correcto desempeño, para presentar resultados a la dirección de la empresa.

ACTUAR: Proponer acciones preventivas, basados en los resultados que se obtengan en la verificación de los procesos.

6.4 MARCO CONCEPTUAL

Seguridad Informática: la seguridad informática como parte fundamental de este proyecto, se refiere a las condiciones apropiadas para una buena gestión de la información, garantizando la disponibilidad, confidencialidad e -integridad de los datos.

La seguridad significa conocer los riesgos a los que están expuestos los activos informáticos, para clarificarlos y protegerse de los posibles ataques y daños. Cuando se conocen las amenazas y vulnerabilidades, es posible adoptar medidas de protección adecuadas para minimizar los riesgos a la que está expuesta la información y prevenir ataques malintencionados.

La seguridad informática protege todo lo que se considere como un activo dentro de la empresa, como son los recursos financieros, los sistemas de información y los bienes tanto tangibles como intangibles.

En otras palabras, la seguridad informática representa un conjunto de técnicas, las cuales al ser implementadas aseguran la integridad, disponibilidad y confidencialidad de la información.

Pilares de la seguridad informática. Son cuatro los pilares que conllevan a que la información sea resguardada a gran escala:

- ✓ **Confidencialidad**: la información debe ser gestionada solo por las personas que tienen autorización para manipularla. Debe ser protegida y resguardada de manos malintencionadas. “Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados, La confidencialidad es una propiedad de difícil recuperación, pudiendo examinar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos”.[5]
- ✓ **Integridad**: busca mantener los datos libres de modificaciones no autorizadas, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La información que se envía y se recibe debe permanecer integra, garantizando que los datos se mantengan exactos y completos, de tal manera que la información que se remite, sea la que llegue a su destino.

- ✓ **Disponibilidad**: Garantizar que la información se encuentre disponible en el momento que los usuarios lo requieran, conlleva a prevenir ataques de denegación de servicio, para ello es importante contar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos.
- ✓ **Autenticidad**: la información debe permanecer legitima e integra desde su origen hasta su destino. “Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra

5 AMUTIO GOMEZ, Miguel Angel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Madrid, octubre de 2012. p . 9.

la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad".[6]

Amenaza informática: Todo evento que atente contra la seguridad de la información se considera una amenaza, cuando no se cuenta con un manejo de vulnerabilidades en la empresa se genera una amenaza impactando de forma negativa en la entidad colocando en riesgo la integridad de la información.

Vulnerabilidad Informática: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.[7] Representa toda debilidad en cada activo de información, exponiendo a que los datos puedan ser alterados por personas inescrupulosas que buscan afectar a la empresa.

Probabilidad de ocurrencia. Se refiere a la constancia con la cual una amenaza puede darse, cuando se carece de un mecanizo de manejo y control de la información esta probabilidad puede aumentar.

6 AMUTIO GOMEZ, Miguel Angel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Madrid, octubre de 2012. p . 9.

7 gestión De Riesgo En La Seguridad Informática. Definición de Vulnerabilidad Informática. [consultado el 19 de abril de 2018]. Disponible en https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Impacto. En el momento que mediante una vulnerabilidad se genere un ataque informático, resulta una serie de consecuencias que afectan la integridad y confidencialidad de la información.

Riesgo. Es una probabilidad que un suceso relacionado con la amenaza se materialice, afectando los activos como son equipos informáticos, software, información, periféricos, entre otros.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente, es importante conocer las características que tiene cada activo de información y de la misma manera conocer el nivel de peligro que posee cada característica.[8]

Delito Informático: Acciones que implican una actividad ilegal, afectando la integridad, disponibilidad y confidencialidad de la información en los sistemas como redes de datos, equipos de cómputo, software, hardware, entre otros.

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático, se trata de un tipo de amenaza que puede que el software antivirus no sea capaz de bloquear por sí solo.

Hacker: persona que tiene altos conocimientos en tecnología relacionados con programación, redes, sistemas operativos, telecomunicaciones, entre otros, con un

8 AMUTIO GOMEZ, Miguel Angel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Madrid, octubre de 2012. p . 9.

alto gusto por los temas tecnológicos, apasionado por el trabajo con la tecnología y con el deseo de descubrir nuevos espacios tecnológicos

Cracker: considerado como un vandálico virtual, utiliza sus conocimientos para invadir sistemas, descifrar claves, contraseñas de programas y algoritmos de encriptación, ya sea para robar claves, datos personales y otros delitos informáticos.

Virus informático: son programas maliciosos (Malware) que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo, consiste en incrustar su código malicioso en el interior de un archivo.

Norma de seguridad Informática: es un conjunto de reglas de seguridad que se establecen con el fin de controlar toda la información que se maneja dentro de la empresa. De esta manera es posible que los empleados de la empresa conozcan cómo deben cuidar y guardar la información que manejan.

6.5 MARCO LEGAL

Existen diferentes leyes que de una u otra manera complementan el concepto de seguridad, las cuales obligan a diferentes entes a cumplir las normas para que exista regulación y un control sobre este aspecto tan importante como lo es la manipulación de la información.

A continuación, se presentan algunas leyes que el Ministerio Tic ha establecido, las cuales podrán ser aplicadas a esto proyecto con el fin de garantizar un mayor nivel de protección de los datos en Neurokids Cauca Healt:

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

Ley 599 DE 2000: Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

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

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009: Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.

Circular 052 de 2007 (Superintendencia Financiera de Colombia): Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

6.5.1 Normas de Seguridad Informática.

ISO 17799: es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de esta norma es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y reclamaciones de confianza entre las empresas

ISO 27000: Es una familia de estándares de ISO e IEC que proporciona un marco para la gestión de la seguridad de la información. Estas normas especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI.

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

Los objetivos de seguridad, recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva aplicaremos para la gestión del riesgo analizado. El objetivo de la norma es definir los aspectos prácticos y operativos de la implantación del SGSI.

ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO 27007: Consiste en una guía de auditoría de un SGSI.

ISO 27011: Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031: Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032: Consiste en una guía relativa a la ciberseguridad.

ISO 27033: Es una norma consistente en 7 partes:

- gestión de seguridad de redes
- arquitectura de seguridad de redes
- escenarios de redes de referencia
- aseguramiento de las comunicaciones entre redes mediante gateway
- acceso remoto
- aseguramiento de comunicaciones en redes mediante VPNs
- diseño e implementación de seguridad en redes.

ISO 27034: Consiste en una guía de seguridad en aplicaciones.

ISO 27799: Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

6.5.2 norma técnica NTC-ISO-IEC colombiana 27001 – 2013.

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

7. DISEÑO METODOLÓGICO

7.1 METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo del proyecto donde se realizara un diseño de gestión de seguridad informática basado en la norma ISO-IEC 27001 de 2013 en Neurokids Healt, se propone aplicar la **Investigación Explorativa,** ya que permitirá conocer el tema que se va abordar y familiarizarse con algo que se desconoce. Este tipo de investigación aplica al caso en estudio, puesto que en la Empresa no se ha realizado un estudio sobre seguridad de la información, lo que genera la necesidad de diseñar un sistema de gestión que garantice la integridad de la información.

Para el caso específico de diseñar un sistema de gestión de seguridad informática basado en la norma ISO 27001 - 2013 en el área de historias clínicas de Neurokids Healt, el enfoque de i**nvestigación es cuantitativo**, ya que se pretende hacer la medición de amenazas y riesgos en cuanto a la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información.

7.2 METODOLOGÍA DE DESARROLLO

Para el correcto desarrollo del proyecto es necesario realizar tres pasos principales los cuales permitirán realizar un proceso eficiente para el diseño de seguridad informática basado en la norma ISO/IEC 27001 – 2013 en neurokids Healt. Los pasos para la metodología de desarrollo son:

1. Analizar los activos de información que intervengan en el área de historias clínicas de la Empresa, para evaluar los riesgos de acuerdo a la Metodología Magerit: en primer lugar, se debe identificar los activos de información con el objetivo de determinar el nivel de riesgo que cada activo esto permitirá la aplicación de la evaluación del riesgo, lo que traerá como consecuencia la disminución del riesgo informático.

2. Determinar el nivel de seguridad informática existente en la empresa, mediante un análisis de vulnerabilidades. Luego que se haya identificado los activos informáticos, se pasa a determinar en qué nivel de seguridad se encuentra la empresa, por los tanto se realizara una identificación de vulnerabilidades tanto físicas como lógicas.

3. Diseñar controles para reducir o mitigar el riesgo existente en la empresa basados en la norma ISO/IEC 27001 versión 2013. cuando se tenga un estudio completo de los activos informáticos y las vulnerabilidades, se procederá a diseñar controles necesarios para garantizar la integridad, confiabilidad y disponibilidad de la información.

8. DISEÑO DE GESTION DE SEGURIDAD DE LA INFORMACION DE NEUROKIDS HEALT

8.1 IDENTIFICACIÓN Y ANÁLISIS DE ACTIVOS DE INFORMACIÓN

En este capítulo se realiza la identificación de los activos informáticos con los que cuenta la Empresa, los cuales intervienen en el área de historias clínicas, esta clasificación se hace teniendo en cuenta la metodología Magerit.

Después de haber identificado y clasificado los activos, se procede a realizar el análisis de cada uno, mediante la valoración y el nivel de criticidad, determinando a través de un estudio cuantitativo el nivel de impacto que cada activo posee en la institución. Para ello se tiene en cuenta los siguientes pilares de la seguridad informática: confidencialidad, disponibilidad, integralidad, autenticidad y trazabilidad.

8.2 METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

Para la gestión de riesgos del sistema de información de Neurokids, se ha elegido utilizar la metodología MAGERIT, ya que permite identificar las características esenciales que posee cada activo de información, logrando de esta manera identificar las debilidades de cada activo.

8.3 GESTIÓN DE RIESGOS DEL SISTEMA DE INFORMACIÓN DE NEUROKIDS

8.3.1 Inventario de activos.

Para el desarrollo de esta actividad tomamos como modelo el inventario establecido por la metodología magerit 3.0, libro ii. P. 7-13.

De acuerdo a esta clasificación, los activos informáticos disponibles en la Empresa Neurokids Healt, se relacionan en las siguientes tablas.

Tabla 8 Activos Esenciales

[ESSENTIAL] ACTIVOS ESENCIALES			
Nombre grupo de activo MAGERIT	**Código grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
[info] Información	[vr] datos vitales (registros de la organización)	D_admon	Hojas de vida de funcionarios. Estatutos. Convenios interinstitucionales. Resoluciones. Licencias. Licitaciones vigentes Actas. Informes. Memorias. Autorizaciones protocolos de atención

		D_políticas	comite de salud ocupacional. Política interna. Deberes y derechos de los pacientes
		D_Contratos	Documentos de contratación privada. Contratos de arrendamiento.
		D_Financieros	Cuentas de ahorro. Estados financieros. Acciones financieras. Flujos de caja menor Nomina Recibos de caja menor. Comprobantes de recaudo. Comprobantes de pago Cuentas de cobro facturas Inventario de activos fijos.
		D_Inversion	
		D_Polizas	Pólizas de seguros
	[Per] datos de carácter personal.	D_Historias clínicas.	Historias clínicas de los pacientes Evoluciones

	[Per] datos de carácter personal.	O_Financieras	Pagares Aceptaciones bancarias.
	[classified] datos clasificados	D_Historicos	Documentos históricos institucionales.
[Services] servicios	[ext] a usuarios externos	S_Terapias	Terapias de neurodesarrollo (física, fonoaudiologia, ocupacional)
		S_ Consultas	Consultas de pediatria, Neuropediatria, psiquiatra Infantil

Fuente: el autor

Tabla 9 Archivos de datos

[D] DATOS/INFORMACIÓN

Nombre grupo de activo MAGERIT	Código grupo según MAGERIT	Código grupo según NEUROKIDS	Nombre grupo según NEUROKIDS
Datos	[files] ficheros	Arch_gadmva	Archivos de gestión administrativa
		Arch_politicas	Archivos de las políticas de la institución
		Arch_Contratos	Archivos de contratación
		Arch_hisnt	Archivos históricos institucionales
		Arch_audit	Archivos de auditorias
		Arch_inv	Archivos de inventarios
[int]	Datos de gestión interna	Dtos_ginst	Información de la gestión estratégica institucional
[password]	Credenciales	Contraseñas_us	Contraseñas de acceso de los usuarios al sistema

Fuente: el autor

Tabla 10 Servicios

[S] SERVICIOS			
Código grupo de activo MAGERITT	**Nombre grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
[pub]	al público en general (sin relación contractual)	S_pacientes	Servicios ofrecidos a los pacientes (Terapias, consultas, asesorías)
[int]	a usuarios de la organización	S_funcionarios	Servicios ofrecidos a todo el personal de funcionarios para el buen desempeño de sus funciones.
[email]	Correo electrónico	S_email	Servicio de correo electrónico institucional

Fuente: el autor

Tabla 11 Aplicaciones (software)

[SW] APLICACIONES (SOFTWARE)			
Código grupo de activo MAGERITT	Nombre grupo según MAGERIT	Código grupo según NEUROKIDS	Nombre grupo según NEUROKIDS
		sw_historias clinicas	BABYWARE Aplicación donde se manejan todas las

			historias clinicas y las evoluciones de los pacientes
[office]	Ofimática	A_OF	OFFICE 2007
[os]	Sistema operativo	A_SO	Windows 7, windows 10, windws 8
[av]	Antivirus	Antivirus	AVAST

Fuente: el autor

Tabla 12 Equipos informáticos

[HW] EQUIPOS INFORMÁTICOS (HARDWARE)			
Código grupo de activo MAGERITT	**Nombre grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
[pc]	Informática personal	E_Trabajo	Computadores de escritorio
[mobile]	Informática móvil	E_portatiles	Portátiles
[print]	Medios de impresión	E_Impresion	Impresoras
[router]	Encaminadores	Routers	Routers
[pabx]	Centralita telefónica	C_tel	Central telefónica administrada externamente por claro

Fuente: el autor

Tabla 13 Redes de comunicaciones

[COM] REDES DE COMUNICACIONES			
Código grupo de activo MAGERITT	**Nombre grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
[wifi]	red inalámbrica	Red_wifi	Red de acceso inalámbrico de la entidad.
[LAN]	Red local	Red_LAN	Red de área local encargada de

			gestionar todas las comunicaciones internas de la entidad.
[internet]	Internet	Internet	Servicio de interconexión nacional.

Fuente: el autor

Tabla 14 Equipamiento auxiliar

[AUX] EQUIPAMIENTO AUXILIAR			
Código grupo de activo MAGERITT	**Nombre grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
		Sist_cincendios	Sistema de extintores clase A, B y C
[cabling]	[wire] cable eléctrico	Cable eléctrico	Cable que conforma el sistema eléctrico del edificio
		UTP cat.6	Elemento físico que conforma la red horizontal de telecomunicacione

Fuente: el autor

Tabla 15 Instalaciones

[L] INSTALACIONES			
Código grupo de	**Nombre grupo**	**Código grupo**	**Nombre grupo**

activo MAGERITT	según MAGERIT	según NEUROKIDS	según NEUROKIDS
[building]	edificio	edificio	Calle 17N # 11-03 B/ Antonio Nariño ciudad de Popayán - Cauca

Fuente: el autor

Tabla 16 Personal

[P] Personal			
Código grupo de activo MAGERITT	**Nombre grupo según MAGERIT**	**Código grupo según NEUROKIDS**	**Nombre grupo según NEUROKIDS**
[ue]	Usuarios externos	pac	pacientes
[ui]	Funcionarios	Funcionarios	Personal encargado de las diferentes tareas administrativas de la entidad.

Fuente: el autor

8.3.2 valoración de los activos.

Teniendo en cuenta la tabla 3, donde se relacionan una serie de criterios de valoración cuantitativa y cualitativa según lo establece Magerit, se toma la valoración cuantitativa con el propósito de obtener resultados más precisos, mediante los cuales será posible tener una mayor precisión sobre los resultados obtenidos por cada activo informático.

Para valorar el nivel de criticidad de cada activo, utilizaremos la tabla 17, teniendo en cuenta su valor promedio de acuerdo a los valores de las dimensiones de seguridad.

Tabla 17 Criterios de valoración del nivel de criticidad de los activos

criterios de valoración de los activos	valor relacional	valor cualitativo de criticidad
El activo gestionado es altamente potente para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad.	**>=4**	**Alto**
El activo gestionado es medianamente potente para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad	**>2 y <4**	**Medio**
El activo gestionado tiene un bajo potencial para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad.	**>0 y <2**	**Bajo**
El activo gestionado es irrelevante como para impactar de forma significativa, el cumplimiento de objetivos organizacionales en base a su rendimiento y dimensiones de seguridad	**= 0**	**N/A**

Fuente: El autor

En la tabla que se presenta a continuación se realiza la valoración de cada activo informático que hay en la empresa, se evaluá mediante los cinco pilares de la seguridad informática, determinando de esa manera el grado de importancia que cada uno posee:

Tabla 18 Valoración de activos y nivel de criticidad

ACTIVOS		VALORACION DE ACTIVOS Y NIVEL DE CRITICIDAD						
grupo según magerit	grupo según NK COOPS	Confidencialidad	Disponibilidad	Integridad	Autenticidad	Trazabilidad	Promedio total	Nivel de criticidad
[vr]	D_admon	5	4	5	4	3	4,2	Alto
	D_politicas	3	3	4	4	2	3,2	Medio
	D_Contratos	4	3	3	4	3	3,4	Medio
	D_Financieros	5	4	5	5	5	4,8	Alto
	D_Inversiones	4	5	4	5	4	4,4	Alto
	D_Polizas	3	3	4	4	3	3,4	Medio
[Per]	O_Financieras	4	4	5	4	4	4,2	Alto
[Per]	D_Historias Clinicas	5	5	5	5	5	5	Alto
[classified]	D_Historicos	2	2	2	1	1	1,6	Bajo
[Services]	S_Terapias	4	5	4	3	4	4	Alto
	S_Consultas	5	4	5	5	4	4,6	Alto
[files]	Arch_gadmva	4	4	5	4	3	4	Alto
	Arch_politicas	3	3	4	3	2	3	Medio
	Arch_contratos	4	3	3	4	2	3,2	Medio
	Arch_audit	4	4	4	3	3	3,6	Medio
	Arch_inv	4	4	4	3	3	4,5	Alto
	Arch_hisnt	3	2	3	2	2	2,4	Bajo
[int]	Dtos_ginst	4	4	5	5	4	4,4	Alto
[password]	Contraseñas_us	5	5	5	5	4	4,8	Alto

[pub]	S_pacientes	4	4	5	4	4	4,2	Alto
[int]	S-funcionarios	4	3	3	3	2	3	Medio
[email]	e-mail	3	3	2	1	1	2	Bajo
	sw_historias clinicas	5	4	5	5	5	4,8	Alto
[office]	A_OF	3	3	2	3	2	2,4	Bajo
[os]	A_SO	4	5	4	4	4	4,2	Alto
[av]	Antivirus	3	4	3	3	2	3	Medio
[pc]	E_Trabajo	3	3	2	2	2	2,4	Bajo
[mobile]	E_portatiles	3	4	3	3	3	3,2	Medio
[print]	E_Impresion	3	2	2	2	1	2	Bajo
[router]	Routers	4	4	4	4	4	4	Alto
[wifi]	Red_wifi	4	3	4	3	4	3,6	Medio
[LAN]	Red_LAN	3	4	4	4	3	3,6	Medio
[Internet]	Internet	5	3	4	4	4	4	Alto
[wire]	Cable electrico	4	4	3	3	3	3,4	Medio
	UTP cat.4	3	3	3	3	2	2,8	Bajo
[building]	Edificio	4	3	4	1	1	2,8	Bajo
[ue]	pac	3	3	2	2	1	2,2	Bajo
[ui]	Funcionarios	4	4	4	4	3	3,8	Medio

Fuente: El Autor

9. VALORACIÓN DEL RIESGO INFORMÁTICO IDENTIFICADO

Luego de obtener una identificación y análisis de los activos informáticos, el siguiente paso es realizar la valoración del riesgo, teniendo en cuenta una serie de amenazas que según Magerit podrían afectar el buen funcionamiento de la empresa.

9.1 IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS.

Con el fin de realizar este proceso se debe tener en cuenta los siguientes aspectos:

- Impacto de las amenazas sobre las dimensiones de seguridad (tabla 6)
- Catálogo de amenazas posibles sobre los activos de Magerit 3.0, libro II. P. 25-47
- Tablas 19,20,21

En los anteriores elementos se establecen una serie de parámetros que se deben tener en cuenta para la identificación y valoración de riesgos.

Tabla 19 Probabilidad de ocurrencia de la amenaza

Valoración cualitativa	Frecuencia	Valoración cuantitativa
Muy baja	Una vez por año	1
Baja	Dos veces por año	2

Media	Una vez trimestral	3
Media Alta	Una vez al mes	4
Alta	semanalmente	5

Fuente: El Autor

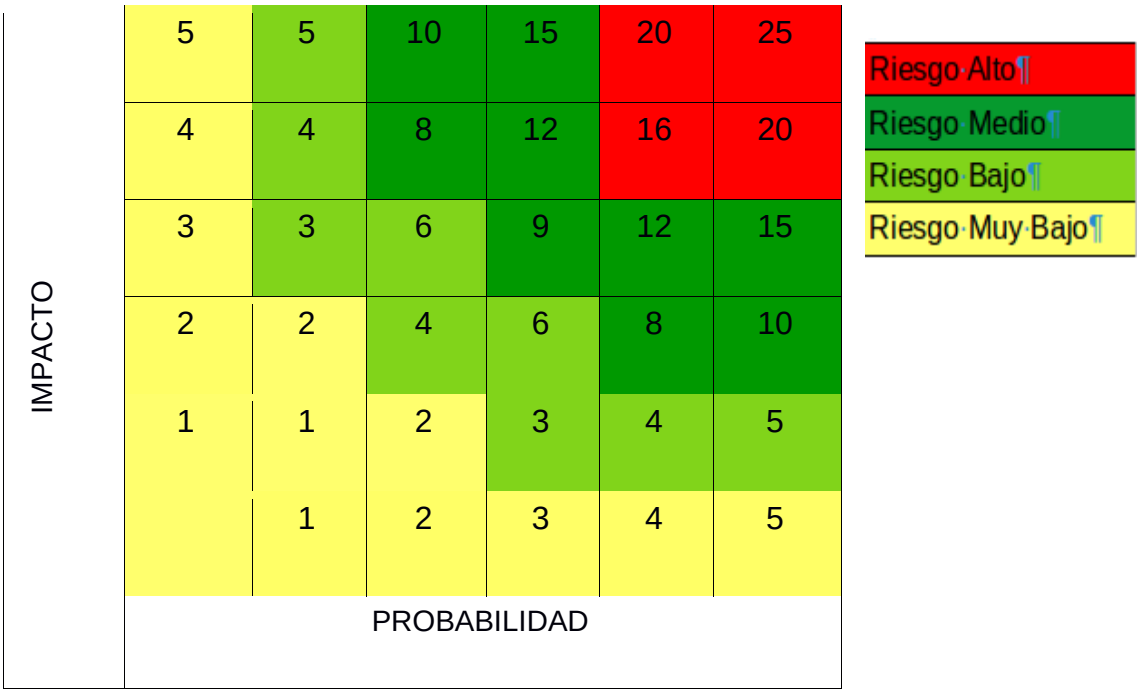
Tabla 20 Dimensiones de seguridad según MAGERIT

Dimensión	**Código**
Confidencialidad	C
Disponibilidad	D
Integralidad	I
Autenticidad	A
Trazabilidad	T

Fuente: El Autor

Teniendo en cuenta las cinco dimensiones de valoración del riesgo, establecidas por Magerit, se muestra a continuación una tabla, la cual permite determinar la valoración del riesgo en cada uno de los activos.

Tabla 21 Guía de valoración del riesgo



Fuente: El Autor

Tabla 22 Riesgo por activo informático Neurokids Healt

RIESGO POR ACTIVO INFORMÁTICO NEUROKIDS HEALT												
Amenaza	**Activo**	**Frecuencia**	**Valoración Impacto Potencial**					**Valoración riesgo potencial**				
			C	**D**	**I**	**A**	**T**	**C**	**D**	**I**	**A**	**T**
[N.1] Fuego	Computadores de escritorio, portátiles, impresora.	1	_	4	4	_	4	_	4	4	_	4
	Router	1	_	4	4	_	4	_	4	4	_	4
	Cable eléctrico, cableado de telecomunicaciones	1	_	5	4	_	4	_	5	4	_	4
	edificio	1	_	4	4	_	4	_	4	4	_	4

[N.2] Daños por agua	Computadores de escritorio, portátiles, impresora.	1	_	4	4	_	4	_	4	4	_	4
	Router	1	_	4	4	_	4	_	4	4	_	4
	Cable eléctrico, cableado de telecomunicaciones	1	_	5	4	_	4	_	5	4	_	4
	edificio	1	_	4	3	_	4	_	4	3	_	4
[I.4] Contaminación electromagnética	Computadores de escritorio, portátiles, impresora.	1	_	3	3	_	3	_	3	3	_	3
	Cable eléctrico, cableado de telecomunicaciones	1	_	3	3	_	3	_	3	3	_	3
[I.5] Avería de origen físico o	software administrativo, historias clinicas,	2	_	5	5	_	4	_	10	10	_	8

lógico	antivirus											
	Computadores de escritorio, portátiles, impresora.	2	_	4	4	_	4	_	8	8	_	8
	Cable eléctrico, cableado de telecomunicaciones	1	_	4	4	_	4	_	4	4	_	4
[I.6] Corte del suministro eléctrico	Computadores de escritorio, portátiles, impresora.	3	_	5	4	_	4	_	15	12	_	12
	Router	3	_	5	4	_	4	_	15	12	_	12
	Cable eléctrico, cableado de telecomunicaciones	3	_	5	4	_	4	_	15	12	_	12
[I.7] Condiciones inadecuadas de	Computadores de escritorio, portátiles,	1	_	4	4	_	3	_	4	4	_	3

temperatura o humedad	impresora.											
	Router	1	_	4	4	_	3	_	4	4	_	3
	Cable eléctrico, cableado de telecomunicaciones	1	_	4	4	_	3	_	4	4	_	3
[I.8] Fallo de servicios de comunicaciones	Router, cable UTP.	2	_	5	4	_	4	_	10	8	_	8
[E.1] Errores de los usuarios	Datos/Información	2	4	4	4	_	3	8	8	8	_	6
	servicios	2	4	4	4	_	3	8	8	8	_	6
	software de sistemas, aplicaciones administrativas	2	4	4	4	_	3	8	8	8	_	6
[E.2] Errores del administrador	Datos/Información	2	4	4	4	_	3	8	8	8	_	6
	servicios	2	4	4	4	_	3	8	8	8	_	6

	software de sistemas, aplicaciones administrativas	2	4	4	4	_	3	8	8	8	_	6
	Computadores de escritorio, portátiles, impresora.	2	4	4	4	_	3	8	8	8	_	6
	redes de comunicaciones	2	3	4	4	_	3	6	8	8	_	6
[E.4] Errores de configuración	Computadores de escritorio, portátiles, impresora.	2	4	4	4	_	3	8	8	8	_	6
[E.7] Deficiencias en la organización	Personal Administrativo	1	3	3		_	_	3	3	_	_	_
[E.8] Difusión de software dañino	Software de sistemas y administrativo	2	5	4	5	_	2	10	8	10	_	4
[E.9] Errores de	redes de	1	4			_	_	4	_	_	_	_

[re-]encaminamiento	comunicaciones											
	servicios	1	4			_	_	4	_	_	_	_
	software de sistemas, aplicaciones administrativas	1	4			_	_	4	_	_	_	_
[E.15] Alteración accidental de la información	Datos/Información	1	5	5	5	_	4	5	5	5	_	4
	servicios	1	4	4	4	_	3	4	4	4	_	3
	software de sistemas, aplicaciones administrativas	1	4	4	4	_	3	4	4	4	_	4
	Contraseñas	1	5	5	5	_	4	5	5	5	_	4
	Comunicación via red	1	4	4	4	_	3	4	4	4	_	3
[E.18] Destrucción de información	Datos/Información	1	_	5	5	_	4	_	5	5	_	4
	servicios	1	_	4	4	_	4	_	4	4	_	4

	Aplicaciones	1	_	4	4	_	4	_	4	4	_	4
	Contraseñas	1	_	5	4	_	3	_	5	4	_	3
	Comunicación en transito	1	_	4	4	_	3	_	4	4	_	4
[E.19] Fugas de información	Datos/Información	1	4		4	_	3	4	_	4	_	3
	servicios	1	4		5	_	3	4	_	5	_	3
	software de sistemas, aplicaciones administrativas	1	4		4	_	4	4	_	4	_	4
	Contraseñas	1	4		5	_	3	4	_	5	_	3
	Comunicación en transito	1	4		5	_	4	4	_	5	_	4
	Personal (revelación)	2	4		4	_	4	8	_	8	_	8
	Soportes de	2	5		5	_	4	10	_	10	_	8

	información											
[E.20] Vulnerabilidades de los programas (software)	software de sistemas, aplicaciones administrativas	2	5	5	4	_	4	10	10	8	_	8
[E.21] Errores de mantenimiento / actualización de programas (software)	software de sistemas, aplicaciones administrativas	2	_	4	4	_	4	_	8	8	_	8
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Computadores de escritorio, portátiles, impresora.	2	_	4	4	_	4	_	8	8	_	8
	Router	2	_	4	4	_	4	_	8	8	_	8
	Cable eléctrico, cableado de telecomunicaciones	1	_	3	3	_	3	_	3	3	_	3

[E.24] Caída del sistema por agotamiento de recursos	Computadores de escritorio, portátiles, impresora.	3	_	5		_		_	15		_	_
	redes de comunicaciones	1	_	5		_		_	5		_	_
	Servicios	2	_	5		_		_	10		_	_
[E.25] Pérdida de equipos	Computadores de escritorio, portátiles, impresora.	1	5	5	5	_	5	5	5	5	_	5
	Soportes de información	2	5	5	5	_	5	10	10	10	_	10
	Cable eléctrico, cableado de telecomunicaciones	1	4	4	4	_	3	4	4	4	_	3
[E.28] Indisponibilidad	Personal interno	2	_	4		_	_	_	8		_	_

del personal												
[A.4] Manipulación de la configuración	software de sistemas, aplicaciones administrativas	1	5	5	5	5	5	5	5	5	5	5
	Computadores de escritorio, portátiles, impresora.	1	5	5	5	5	5	5	5	5	5	5
	Router	1	5	5	5	5	5	5	5	5	5	5
[A.5] Suplantación de la identidad del usuario	Datos/Información	1	5	4	5	5	3	5	4	5	5	3
	servicios	1	5	4	5	5	4	5	4	5	5	4
	software de sistemas, aplicaciones administrativas	1	5	4	5	4	3	5	4	5	4	3
	Contraseñas	1	5	3	4	4	3	5	3	4	4	3

	redes de comunicaciones	1	5	4	4	4	3	5	4	4	4	3
[A.6] Abuso de privilegios de acceso	Datos/Información	2	5	4	5	4	3	10	8	10	8	6
	servicios	2	4	4	4	3	3	8	8	8	6	6
	software de sistemas, aplicaciones administrativas	2	4	4	4	3	3	8	8	8	6	6
	Contraseñas	2	5	4	5	5	4	10	8	10	10	8
	redes de comunicaciones	2	4	3	4	3	3	8	6	8	6	6
	Computadores de escritorio, portátiles, router	2	5	5	5	5	5	10	10	10	10	10
[A.7] Uso no previsto	servicios	2	3	4	3	–	3	6	8	6	–	6
	software de sistemas,	3	4	5	5	–	4	12	15	15	–	12

	aplicaciones administrativas											
	Soportes de información	2	4	3	3	_	3	8	6	6	_	6
	redes de comunicaciones	1	4	4	4	_	4	4	4	4	_	4
	Computadores de escritorio, portátiles, router	2	4	4	4	_	3	8	8	8	_	6
[A.8] Difusión de software dañino	software de sistemas, aplicaciones administrativas	3	_	5	5	_	5	_	15	15	_	15
	Datos/Información	2		4	5	_	4	_	8	10	_	8
[A.9] [Re-]encaminamiento de mensajes	servicios	2	5		5	_	_	10	_	10	_	_
	software de sistemas, aplicaciones	2	5		5	_	_	10	_	10	_	_

	administrativas											
	redes de comunicaciones	2	4		4	–		8	–	8	–	–
[A.11] Acceso no autorizado	Datos/Información	2	5	4	5	4	3	10	8	10	8	6
	servicios	2	4	4	4	3	2	8	8	8	6	4
	software de sistemas, aplicaciones administrativas	2	5	3	5	3	3	10	6	10	6	6
	Soportes de información	2	5	4	5	4	3	10	8	10	8	6
	redes de comunicaciones	2	4	4	3	3	2	8	8	6	6	4
	Computadores de escritorio, portátiles, router	2	5	5	5	4	3	10	10	10	8	6

	Contraseñas	2	5		5	5	3	10	_	10	10	6
	Equipamiento auxiliar	1	4		4	4		4	_	4	4	_
	Instalaciones	1	5		4	4		5	_	4	4	_
[A.12] Análisis de tráfico	redes de comunicaciones	1	5	4		_	4	5	4	_	_	4
[A.13] Repudio	servicios	1	_	4	4	_	3	_	4	4	_	3
[A.14] Interceptación de información (escucha)	redes de comunicaciones	1	4		5	4	4	4	_	5	4	4
[A.15] Modificación deliberada de la información	Datos/Información	1	4	5	5	5	3	4	5	5	5	3
	servicios	1	4	4	5	3	3	4	4	5	3	3
	Soportes de información	1	4	4	5	5	3	4	4	5	5	3

	Contraseñas	1	4	3	4	5	4	4	3	4	5	4
	Comunicación en transito	1	4	4	5	4	3	4	4	5	4	3
	Aplicaciones	1	4	4	3	3	3	4	4	3	3	3
	Instalaciones	1	4	4	4	4	2	4	4	4	4	2
[A.18] Destrucción de información	Datos/Información	1	4	5	4	_	4	4	5	4	_	4
	servicios	1	4	5	4	_	3	4	5	4	_	3
	Soportes de información	1	4	5	4	_	4	4	5	4	_	4
	Contraseñas	1	4	4	4	_	4	4	4	4	_	4
	Aplicaciones	1	4	5	4	_	4	4	5	4	_	4
	Instalaciones	1	4	4	4	_	3	4	4	4	_	3
[A.19] Divulgación	Datos/Información	2	4		5	4	3	8	_	10	8	6

de información	servicios	1	4		4	4	3	4	_	4	4	3
	Soportes de información	2	4		5	4	4	8	_	10	8	8
	Contraseñas	1	4		4	4	4	4	_	4	4	4
	Aplicaciones	1	3		4	4	3	3	_	4	4	3
	Instalaciones	1	3		4	3	3	3	_	4	3	3
	Comunicación en transito	1	4		4	4	4	4	_	4	4	4
[A.22] Manipulación de programas	Aplicaciones, software	1	4	5	4	4	3	4	5	4	4	3
[A.23] Manipulación de los equipos	Computadores de escritorio, portátiles, impresora.	1	4	5	4	_	3	4	5	4	_	3
	Soportes de	1	4	4	5	_	4	4	4	5	_	4

	información											
[A.24] Denegación de servicio	servicios	2	_	5	4	_	4	_	10	8	_	8
	equipos informáticos	2	_	5	4	_	4	_	10	8	_	8
	redes de comunicaciones	2	_	5	4	_	4	_	10	8	_	8
[A.25] Robo	equipos informáticos Hardware	1	4	5	4	_	4	4	5	4	_	4
	Soportes de información	1	4	5	5	_	4	4	5	5	_	4
	Router	1	4	5	4	_	3	4	5	4	_	3
[A.26] Ataque destructivo	equipos informáticos Hardware	1	_	5	4	_	3	_	5	4	_	3
	Soportes de información	1	_	5	5	_	3	_	5	5	_	3

	Equipamiento auxiliar	1	_	4	3	_	_	_	4	3	_	_
	Instalaciones	1	_	4	3	_	_	_	4	3	_	_
[A.29] Extorsión	Personal interno	1	_	4	4	_	_	_	4	4	_	_
[A.30] Ingeniería social (picaresca)	Gerente	2	5	4	5	_	_	10	8	10	_	_
	Subgerente	2	5	4	5	_	_	10	8	10	_	_
	Secretaria	2	5	4	5	_	_	10	8	10	_	_
	Contador	2	5	4	5	_	_	10	8	10	_	_

10. DISEÑO DE POLÍTICAS Y CONTROLES DE SEGURIDAD INFORMÁTICA

En la tabla 23 que se ilustra a continuación se establece la efectividad cualitativa y cuantitativa de los controles de la norma ISO 27001 – 2013, indicados a establecer para cada uno de los riesgos que se han identificado con el fin de mitigarlo, reducirlo o eliminarlo.

Tabla 23 Eficacia de controles

Eficacia del control	
Muy eficiente	4
Eficiente	3
Poco eficiente	2
Ineficiente	1

Fuente: El Autor

Una vez propuestos los controles por cada uno de los riesgos presentes en la empresa, se realiza un análisis cuantitativo donde se determina el valor del riesgo residual, los cuales Neurokids asumirá según la siguiente tabla:

Tabla 24 Valoración del riesgo residual

VALORACIÓN DEL RIESGO RESIDUAL

Nivel del riesgo residual	Calificación
Inaceptable	>=15
Importante	8 a 15
Moderado	3 a 8
Aceptable	<3

Fuente: El Autor

Para calcular el riesgo residual se tiene en cuenta la siguiente formula:

$$Riesgoresidual = \frac{Valordelriesgoinherente}{Valoreficaciadelcontrol}$$

Teniendo en cuenta lo anterior, a continuación, se relaciona la matriz de valoración del riesgo por cada activo informático de Nurokids Healt

Tabla 25 Valoración del riesgo por activo informático Neurokids Healt

RIESGO POR ACTIVO INFORMÁTICO NEUROKIDS HEALT																		
Amenaza	**Activo**	**Frecuencia**	**Valoración Impacto Potencial**					**Valoración riesgo potencial**					**Controles ISO/IEC 27001:2013**	**Eficacia del control**	**Valoración del riesgo residual**				
			C	**D**	**I**	**A**	**T**	**C**	**D**	**I**	**A**	**T**			**C**	**D**	**I**	**A**	**T**
[N.1] Fuego	Computadores de escritorio, portátiles, impresora.	1	_	4	4	_	4	_	4	4	_	4	11.1.4 Protección contra amenazas externas y Ambientales	3	_	1,3	1,3	_	1,3
	Router	1	_	4	4	_	4	_	4	4	_	4		3	_	1,3	1,3	_	1,3
	Cable eléctrico, cableado de telecomunicaciones	1	_	5	4	_	4	_	5	4	_	4		3	_	1,6	1,3	_	1,3
	edificio	1	_	4	4	_	4	_	4	4	_	4		3	_	1,3	1,3	_	1,3

[N.2] Daños por agua	Computadores de escritorio, portátiles, impresora.	1	_	4	4	_	4	_	4	4	_	4	11.1.4 Protección contra amenazas externas y Ambientales	3	_	1,3	1,3	_	1,3
	Router	1	_	4	4	_	4	_	4	4	_	4		3	_	1,3	1,3	_	1,3
	Cable eléctrico, cableado de telecomunicaciones	1	_	5	4	_	4	_	5	4	_	4		3	_	1,6	1,3	_	1,3
	edificio	1	_	4	3	_	4	_	4	3	_	4		3	_	1,3	1	_	1,3
[I.4] Contaminación electromagnética	Computadores de escritorio, portátiles, impresora.	1	_	3	3	_	3	_	3	3	_	3	11.1.4 Protección contra amenazas externas y Ambientales	3	_	1	1	_	1
	Cable eléctrico, cableado de telecomunicaciones	1	_	3	3	_	3	_	3	3	_	3		3	_	1	1	_	1
[I.5] Avería de origen físico o	software administrativo, historias clinicas,	2	_	5	5	_	4	_	10	10	_	8	A.11.2.4 Mantenimiento de	4	_	2,5	2,5	_	2

lógico	antivirus											equipos							
	Computadores de escritorio, portátiles, impresora.	2	_	4	4	_	4	_	8	8	_	8		4	_	2	2	_	2
	Cable eléctrico, cableado de telecomunicaciones	1	_	4	4	_	4	_	4	4	_	4		4	_	2	2	_	1
[I.6] Corte del suministro eléctrico	Computadores de escritorio, portátiles, impresora.	3	_	5	4	_	4	_	15	12	_	12	12.6.1 Gestión de las vulnerabilidades técnicas	4	_	3,8	3	_	3
	Router	3	_	5	4	_	4	_	15	12	_	12		4	_	3,8	3	_	3
	Cable eléctrico, cableado de telecomunicaciones	3	_	5	4	_	4	_	15	12	_	12		4	_	3,8	3	_	3
[I.7] Condiciones inadecuadas de	Computadores de escritorio, portátiles,	1	_	4	4	_	3	_	4	4	_	3	11.1.4 Protección contra amenazas	3	_	1,3	1,3	_	1

temperatura o humedad	impresora.												externas y Ambientales						
	Router	1	_	4	4	_	3	_	4	4	_	3		3	_	1,3	1,3	_	1
	Cable eléctrico, cableado de telecomunicaciones	1	_	4	4	_	3	_	4	4	_	3		3	_	1,3	1,3	_	1
[I.8] Fallo de servicios de comunicaciones	Router, cable UTP.	2	_	5	4	_	4	_	10	8	_	8	12.6.1 Gestión de las vulnerabilidades técnicas	3	_	3,3	2,6	_	2,6
[E.1] Errores de los usuarios	Datos/Información	2	4	4	4	_	3	8	8	8	_	6	7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	3	2,6	2,6	2,6	_	2
	servicios	2	4	4	4	_	3	8	8	8	_	6		3	2,6	2,6	2,6	_	2
	software de sistemas, aplicaciones administrativas	2	4	4	4	_	3	8	8	8	_	6		3	2,6	2,6	2,6	_	2
[E.2] Errores del	Datos/Información	2	4	4	4	_	3	8	8	8	_	6	7.2.2 Toma de	3	2,6	2,6	2,6	_	2

administrador	servicios	2	4	4	4	_	3	8	8	8	_	6	conciencia, educación y formación en la seguridad de la información	3	2,6	2,6	2,6	_	2
	software de sistemas, aplicaciones administrativas	2	4	4	4	_	3	8	8	8	_	6		3	2,6	2,6	2,6	_	2
	Computadores de escritorio, portátiles, impresora.	2	4	4	4	_	3	8	8	8	_	6		3	2,6	2,6	2,6	_	2
	redes de comunicaciones	2	3	4	4	_	3	6	8	8	_	6		3	2	2,6	2,6	_	2
[E.4] Errores de configuración	Computadores de escritorio, portátiles, impresora.	2	4	4	4	_	3	8	8	8	_	6	A.14.2.5 Principios de construcción de los sistemas seguros	3	2,6	2,6	2,6	_	2

[E.7] Deficiencias en la organización	Personal Administrativo	1	3	3		_	_	3	3	_	_	_	A.6.1.1 Roles y responsabilidades para la seguridad de la Información	3	1	1	_	_	_
[E.8] Difusión de software dañino	Software de sistemas y administrativo	2	5	4	5	_	2	10	8	10	_	4	A.12.2.1 Controles contra Códigos maliciosos	4	2,5	2	2,5	_	1
[E.9] Errores de [re-]encaminamiento	redes de comunicaciones	1	4			_	_	4	_	_	_	_	A.13.2.1 Políticas y procedimientos de transferencia de Información	4	1	_	_	_	_
	servicios	1	4			_	_	4	_	_	_	_		4	1	_	_	_	_
	software de sistemas, aplicaciones administrativas	1	4			_	_	4	_	_	_	_		4	1	_	_	_	_
[E.15] Alteración	Datos/Información	1	5	5	5	_	4	5	5	5	_	4	A.9.4.1	3	1,7	1,7	1,7	_	1,3

accidental de la información	servicios	1	4	4	4	_	3	4	4	4	_	3	Restricción de acceso a la información	3	1,3	1,3	1,3	_	1
	software de sistemas, aplicaciones administrativas	1	4	4	4	_	3	4	4	4	_	4		3	1,3	1,3	1,3	_	1,3
	Contraseñas	1	5	5	5	_	4	5	5	5	_	4	A.9.4.2 Procedimiento de ingreso seguro	4	1,2	1,2	1,2	_	1
	Comunicación via red	1	4	4	4	_	3	4	4	4	_	3	A.13.2.1 Políticas y procedimientos de transferencia de Información	3	1,3	1,3	1,3	_	1
[E.18] Destrucción de información	Datos/Información	1	_	5	5	_	4	_	5	5	_	4	A.12.3.1 Respaldo de la información	4	_	1,2	1,2	_	1
	servicios	1	_	4	4	_	4	_	4	4	_	4		4	_	1	1	_	1
	Aplicaciones	1	_	4	4	_	4	_	4	4	_	4		4	_	1	1	_	1
	Contraseñas	1	_	5	4	_	3	_	5	4	_	3		4	_	1,2	1	_	1

	Comunicación en transito	1	_	4	4	_	3	_	4	4	_	4		4	_	1	1	_	1
[E.19] Fugas de información	Datos/Información	1	4		4	_	3	4	_	4	_	3	A.13.2.4 Acuerdos de confidencialidad o de no Divulgación	3	1,3	_	1,3	_	1
	servicios	1	4		5	_	3	4	_	5	_	3		3	1,3	_	1,7	_	1
	software de sistemas, aplicaciones administrativas	1	4		4	_	4	4	_	4	_	4		3	1,3	_	1,3	_	1,3
	Contraseñas	1	4		5	_	3	4	_	5	_	3		3	1,3	_	1,7	_	1
	Comunicación en transito	1	4		5	_	4	4	_	5	_	4	A.13.1.2 Seguridad de los servicios de red	3	1,3	_	1,7	_	1,3
	Personal (revelación)	2	4		4	_	4	8	_	8	_	8	A.13.2.4 Acuerdos de confidencialidad o de no Divulgación	3	2,7	_	2,7	_	2,7
	Soportes de información	2	5		5	_	4	10	_	10	_	8		3	3,3	_	3,3	_	2,7

[E.20] Vulnerabilidades de los programas (software)	software de sistemas, aplicaciones administrativas	2	5	5	4	_	4	10	10	8	_	8	A.14.2.5 Principios de construcción de los sistemas seguros	3	3,3	3,3	2,7	_	2,7
[E.21] Errores de mantenimiento / actualización de programas (softwa re)	software de sistemas, aplicaciones administrativas	2	_	4	4	_	4	_	8	8	_	8	A.14.2.5 Principios de construcción de los sistemas seguros	3	_	2,7	2,7	_	2,7
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Computadores de escritorio, portátiles, impresora.	2	_	4	4	_	4	_	8	8	_	8	A.14.2.2 Procedimientos de control de cambios en sistemas	3	_	2,7	2,7	_	2,7
	Router	2	_	4	4	_	4	_	8	8	_	8		3	_	2,7	2,7	_	2,7
	Cable eléctrico, cableado de telecomunicaciones	1	_	3	3	_	3	_	3	3	_	3		3	_	1	1	_	1

[E.24] Caída del sistema por agotamiento de recursos	Computadores de escritorio, portátiles, impresora.	3	_	5		_		_	15		_	_	A.11.2.4 Mantenimiento de equipos	3	_	5	_	_	_
	redes de comunicaciones	1	_	5		_		_	5		_	_		3	_	1,7	_	_	_
	Servicios	2	_	5		_		_	10		_	_		3	_	3,3	_	_	_
[E.25] Pérdida de equipos	Computadores de escritorio, portátiles, impresora.	1	5	5	5	_	5	5	5	5	_	5	A.8.1.1 Inventario de activos	4	1,2	1,2	1,2	_	1,2
	Soportes de información	2	5	5	5	_	5	10	10	10	_	10		4	2,5	2,5	2,5	_	2,5
	Cable eléctrico, cableado de telecomunicaciones	1	4	4	4	_	3	4	4	4	_	3		4	1	1	1	_	1,3

[E.28] Indisponibilidad del personal	Personal interno	2	–	4		–	–	–	8		–	–	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	3	–	2,6	–	–	–
[A.4] Manipulación de la configuración	software de sistemas, aplicaciones administrativas	1	5	5	5	5	5	5	5	5	5	5	A.9.2.5 Revisión de los derechos de acceso de usuarios	3	1,6	1,6	1,6	1,6	1,6
	Computadores de escritorio, portátiles, impresora.	1	5	5	5	5	5	5	5	5	5	5		3	1,6	1,6	1,6	1,6	1,6
	Router	1	5	5	5	5	5	5	5	5	5	5		3	1,6	1,6	1,6	1,6	1,6
[A.5] Suplantación de la identidad del	Datos/Información	1	5	4	5	5	3	5	4	5	5	3	A.9.3.1 Uso de información de autenticación	3	1,6	1,3	1,6	1,6	1
	servicios	1	5	4	5	5	4	5	4	5	5	4		3	1,6	1,3	1,6	1,6	1,6

usuario	software de sistemas, aplicaciones administrativas	1	5	4	5	4	3	5	4	5	4	3	secreta	3	1,6	1,3	1,6	1,3	1
	Contraseñas	1	5	3	4	4	3	5	3	4	4	3		3	1,6	1	1,3	1,3	1
	redes de comunicaciones	1	5	4	4	4	3	5	4	4	4	3		3	1,6	1,3	1,3	1,3	1
[A.6] Abuso de privilegios de acceso	Datos/Información	2	5	4	5	4	3	10	8	10	8	6	A.9.2.5 Revisión de los derechos de acceso de usuarios	3	3,3	2,6	3,3	2,6	2
	servicios	2	4	4	4	3	3	8	8	8	6	6		3	2,6	2,6	2,6	2	2
	software de sistemas, aplicaciones administrativas	2	4	4	4	3	3	8	8	8	6	6		3	2,6	2,6	2,6	2	2
	Contraseñas	2	5	4	5	5	4	10	8	10	10	8		3	3,3	2,6	3,3	3,3	2,6
	redes de comunicaciones	2	4	3	4	3	3	8	6	8	6	6		3	2,6	2	2,6	2	2

	Computadores de escritorio, portátiles, router	2	5	5	5	5	5	10	10	10	10	10		3	3,3	3,3	3,3	3,3	3,3
[A.7] Uso no previsto	servicios	2	3	4	3	_	3	6	8	6	_	6	A.8.1.3 Uso aceptable de los activos	3	2	2,6	2	_	2
	software de sistemas, aplicaciones administrativas	3	4	5	5	_	4	12	15	15	_	12		3	4	5	5	_	4
	Soportes de información	2	4	3	3	_	3	8	6	6	_	6		3	2,6	2	2	_	2
	redes de comunicaciones	1	4	4	4	_	4	4	4	4	_	4		3	1,3	1,3	1,3	_	1,3
	Computadores de escritorio, portátiles, router	2	4	4	4	_	3	8	8	8	_	6		3	2,6	2,6	2,6	_	2
[A.8] Difusión de	software de sistemas,	3	_	5	5	_	5	_	15	15	_	15	A.12.2.1 Controles contra	4	_	3,8	3,8	_	3,8

software dañino	aplicaciones administrativas												códigos Maliciosos						
	Datos/Información	2		4	5	_	4	_	8	10	_	8		4	_	2	2,5	_	2
[A.9] [Re-]encaminamiento de mensajes	servicios	2	5		5	_	_	10	_	10	_	_	A.13.2.1 Políticas y procedimientos de transferencia de Información	3	3,3	_	3,3	_	_
	software de sistemas, aplicaciones administrativas	2	5		5	_	_	10	_	10	_	_		3	3,3	_	3,3	_	_
	redes de comunicaciones	2	4		4	_		8	_	8	_	_		3	2,6	_	2,6	_	_
[A.11] Acceso no autorizado	Datos/Información	2	5	4	5	4	3	10	8	10	8	6	A.9.1.1 Política de control de Acceso	4	2,5	2	2,5	2	1,5
	servicios	2	4	4	4	3	2	8	8	8	6	4		4	2	2	2	1,5	1
	software de sistemas, aplicaciones administrativas	2	5	3	5	3	3	10	6	10	6	6		4	2,5	1,5	2,5	1,5	1,5

	Soportes de información	2	5	4	5	4	3	10	8	10	8	6		4	2,5	2	2,5	2	1,5
	redes de comunicaciones	2	4	4	3	3	2	8	8	6	6	4		4	2	2	1,5	1,5	1
	Computadores de escritorio, portátiles, router	2	5	5	5	4	3	10	10	10	8	6		4	2,5	2,5	2,5	2	1,5
	Contraseñas	2	5		5	5	3	10	_	10	10	6		4	2,5	_	2,5	2,5	1,5
	Equipamiento auxiliar	1	4		4	4		4	_	4	4	_		4	1	_	1	1	_
	Instalaciones	1	5		4	4		5	_	4	4	_		4	1,2	_	1	1	_
[A.12] Análisis de tráfico	redes de comunicaciones	1	5	4		_	4	5	4	_	_	4	A.13.1.1 Controles de redes	3	1,6	1,3	_	_	1,3

[A.13] Repudio	servicios	1	_	4	4	_	3	_	4	4	_	3	A.9.2.4 Gestión de información de autenticación secreta de usuarios	3	_	1,3	1,3	_	1
[A.14] Interceptación de información (escucha)	redes de comunicaciones	1	4		5	4	4	4	_	5	4	4	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	3	1,3	_	1,6	1,3	1,3
[A.15] Modificación deliberada de la información	Datos/Información	1	4	5	5	5	3	4	5	5	5	3	A.9.4.1 Restricción de acceso a la información	4	1	1,2	1,2	1,2	0,8
	servicios	1	4	4	5	3	3	4	4	5	3	3		4	1	1	1,2	0,8	0,8
	Soportes de información	1	4	4	5	5	3	4	4	5	5	3		4	1	1	1,2	1,2	0,8
	Contraseñas	1	4	3	4	5	4	4	3	4	5	4		4	1	0,8	1	1,2	1

	Comunicación en transito	1	4	4	5	4	3	4	4	5	4	3		4	1	1	1,2	1	0,8
	Aplicaciones	1	4	4	3	3	3	4	4	3	3	3		4	1	1	0,8	0,8	0,8
	Instalaciones	1	4	4	4	4	2	4	4	4	4	2		4	1	1	1	1	0,5
[A.18] Destrucción de información	Datos/Información	1	4	5	4	_	4	4	5	4	_	4	A.12.3.1 Respaldo de la información	4	1	1,2	1	_	1
	servicios	1	4	5	4	_	3	4	5	4	_	3		4	1	1,2	1	_	0,8
	Soportes de información	1	4	5	4	_	4	4	5	4	_	4		4	1	1,2	1	_	1
	Contraseñas	1	4	4	4	_	4	4	4	4	_	4		4	1	1	1	_	1
	Aplicaciones	1	4	5	4	_	4	4	5	4	_	4		4	1	1,2	1	_	1
	Instalaciones	1	4	4	4	_	3	4	4	4	_	3		4	1	1,2	1	_	0,8
[A.19] Divulgación de	Datos/Información	2	4		5	4	3	8	_	10	8	6	A.13.2.4 Acuerdos de confidencialidad o	3	2,6	_	3,3	2,6	2
	servicios	1	4		4	4	3	4	_	4	4	3		3	1,3	_	1,3	1,3	1

información	Soportes de información	2	4		5	4	4	8	_	10	8	8	de no Divulgación	3	2,6	_	3,3	2,6	2,6
	Contraseñas	1	4		4	4	4	4	_	4	4	4		3	1,3	_	1,3	1,3	1,3
	Aplicaciones	1	3		4	4	3	3	_	4	4	3		3	1	_	1,3	1,3	1
	Instalaciones	1	3		4	3	3	3	_	4	3	3		3	1	_	1,3	1	1
	Comunicación en transito	1	4		4	4	4	4	_	4	4	4		3	1,3	_	1,3	1,3	1,3
[A.22] Manipulación de programas	Aplicaciones, software	1	4	5	4	4	3	4	5	4	4	3	A.9.4.4 Uso de programas utilitarios privilegiados	4	1	1,2	1	1	0,8
[A.23] Manipulación de los equipos	Computadores de escritorio, portátiles, impresora.	1	4	5	4	_	3	4	5	4	_	3	A.8.1.3 Uso aceptable de los activos	3	1,3	1,6	1,3	_	1
	Soportes de información	1	4	4	5	_	4	4	4	5	_	4		3	1,3	1,3	1,6	_	1,3

[A.24] Denegación de servicio	servicios	2	_	5	4	_	4	_	10	8	_	8	A.13.1.2 Seguridad de los servicios de red	3	_	3,3	2,6	_	2,6
	equipos informáticos	2	_	5	4	_	4	_	10	8	_	8		3	_	3,3	2,6	_	2,6
	redes de comunicaciones	2	_	5	4	_	4	_	10	8	_	8		3	_	3,3	2,6	_	2,6
[A.25] Robo	equipos informáticos Hardware	1	4	5	4	_	4	4	5	4	_	4	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	4	1	1,2	1	_	1
	Soportes de información	1	4	5	5	_	4	4	5	5	_	4		4	1	1,2	1,2	_	1
	Router	1	4	5	4	_	3	4	5	4	_	3		4	1	1,2	1	_	0,8
[A.26] Ataque destructivo	equipos informáticos Hardware	1	_	5	4	_	3	_	5	4	_	3	A.12.3.1 Respaldo de la información	4	_	1,2	1	_	0,8
	Soportes de información	1	_	5	5	_	3	_	5	5	_	3		4	_	1,2	1,2	_	0,8
	Equipamiento auxiliar	1	_	4	3	_	_	_	4	3	_	_		4	_	1	0,8	_	_

	Instalaciones	1	_	4	3	_	_	_	4	3	_	_		4	_	1	0,8	_	_
[A.29] Extorsión	Personal interno	1	_	4	4	_	_	_	4	4	_	_	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	3	_	1,3	1,3	_	_
[A.30] Ingeniería social (picaresca)	Gerente	2	5	4	5	_	_	10	8	10	_	_	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	3	3,3	2,6	3,3	_	_
	Subgerente	2	5	4	5	_	_	10	8	10	_	_		3	3,3	2,6	3,3	_	_
	Secretaria	2	5	4	5	_	_	10	8	10	_	_		3	3,3	2,6	3,3	_	_
	Contador	2	5	4	5	_	_	10	8	10	_	_		3	3,3	2,6	3,3	_	_

10.1 POLITICAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA NEUROKIDS HEALT

En la matriz anterior se establecieron algunos controles **ISO/IEC 27001:2013**, los cuales van a permitir mitigar la materialización de la amenaza, obteniendo como resultado una cifra cuantitativa del riesgo residual, para el cual es pertinente proponer algunas políticas de seguridad que van a permitir controlar con más el riesgo existente.

En la siguiente tabla se proponen algunas políticas de seguridad, que en relación con los controles ISO 27001:2013, van a permitir mantener un buen nivel de seguridad informática.

Tabla 26 Políticas de seguridad Informática

Controles ISO/IEC 27001:2013	**Políticas de seguridad Informática**	**Responsable**
1. Protección contra amenazas externas y ambientales 2. Seguridad de oficinas, recintos e instalaciones	• La dirección debe garantizar la seguridad estructural de los lugares donde están instalados los activos informáticos • Adquirir un seguro contra amenazas externas y ambientales • realizar un mantenimiento periódico de las instalaciones. • Los funcionarios del área administrativa y de historias clínicas deberán bloquear sus equipos al momento de levantarse de su puesto de trabajo para evitar alteraciones a la integridad de los activos de información necesarios para el cumplimiento de sus funciones	• Gerente • Subgerente • Terapeutas • Médicos Especialistas
1. Mantenimiento de equipos 2. Procedimientos de control de cambios en	• Se debe programar mantenimiento preventivo y correctivo cada 6 meses, para garantizar el buen funcionamiento de los equipos	• Gerencia

sistemas	de computo, redes y telecomunicaciones	
Toma de conciencia, educación y formación en la seguridad de la información	• La dirección debe brindar a todo el personal de la empresa capacitación sobre la importancia de la seguridad informática y las diferentes recomendaciones que se deben tener en cuenta en el momento de manipular la información. • Establecer un periodo de tiempo para el manejo de claves de acceso.	• Gerencia
Principios de construcción de los sistemas seguros	• Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	• Subgerente
Roles y responsabilidades para la seguridad de la Información	• Se debe capacitar y controlar que los funcionarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un	• Gerencia

	usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos	
Controles contra Códigos maliciosos	• Mediante herramientas libres de seguridad informática como **volafox**, se debe mantener controlados ataques por código malicioso.	• Subgerente
1. Políticas y procedimientos de transferencia de Información 2. Acuerdos de confidencialidad o de no divulgación	• Es responsabilidad de la dirección capacitar a todo el personal sobre los procedimientos que se debe realizar cuando se va a transferir información. • Concientizar a los funcionarios de Neurokids para que no divulguen información confidencial. • Realizar un estudio de los canales de comunicación que se utilizan para la transferencia de información.	• Gerencia • Terapeutas • Secretaria
1. Restricción de acceso a la información	• Es responsabilidad de la dirección proveer a los funcionarios las claves para el acceso a los servicios de red y	• Gerente • Subgerente

2. Procedimiento de ingreso seguro 3. Revisión de los derechos de acceso de usuarios 4. Uso de información de autenticación secreta 5. Política de control de Acceso	sistemas de información, estas claves son de uso personal y ningún funcionario deberá revelar su clave de acceso. • La dirección deberá asignar a cada funcionario los privilegios de acceso a la información que se maneja en neurokids, según funciones realizadas dentro de la empresa. • Es obligación de la dirección capacitar y controlar al personal para que tengan buenas prácticas de seguridad en el uso y protección de contraseñas, las cuales permite a los usuarios validar y establecer el derecho de acceso a las instalaciones, equipos y servicios informáticos	• Secretaria • Terapeutas • Médicos Especialistas
Respaldo de la información	• La dirección debe programar cada 3 meses la realización de las copias de seguridad de la información (backup).	• Subgerencia
Inventario de activos	• Es responsabilidad de la dirección realizar el inventario de todos los activos informáticos, con el fin de mantener	• Secretaria

	controlado cada activo y evitar la pérdida de un bien informático que pueda afectar el buen funcionamiento de la empresa.	
Uso aceptable de los activos	• La dirección deberá diseñar e implementar reglas y procedimientos para el uso de los activos de información, especificando privilegios de acceso y manipulación de cada activo.	• Gerencia
Controles de redes	• Todo el personal de neurokids tiene prohibido el ingreso a sitios web con propositos deferentes a los visionales y misionales dentro de la entidad como: pornografía, terrorismo, hacktivismo, redes sociales u otras fuentes definidas por la organización. • La descarga de archivos de internet que realicen los funcionarios debe responder a propósitos laborales y esto debe hacerse de forma razonable para no afectar el servicio de Internet. • La dirección debe garantizar la	• Gerente • Subgerente • Secretaria • Terapeutas • Médicos Especialistas

	seguridad física para el acceso a los equipos de cómputo y de red.	
Uso de programas utilitarios privilegiados	• Se debe realizar una revisión continua de los programas y aplicaciones que se tiene instalados en los equipos de cómputo con el fin de determinar que programas afectan el buen funcionamiento de los sistemas de información.	• Gerente • Subgerente
Seguridad de los servicios de red	• Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente	• Gerente • Subgerente

11. CONCLUSIONES

Con la culminación del presente trabajo enfocado a contribuir a la seguridad informática de una empresa del área de salud en la ciudad de Popayán, se concluye lo siguiente:

Mediante el diseño de un SGSI, es posible gestionar la seguridad de los sistemas tecnológicos que maneja la empresa, de una forma organizada y eficiente, considerando activos informáticos, amenazas y vulnerabilidades.

Con el estudio realizado en Neurokids Healt, se identificó los activos informáticos que presentan un tipo de riesgo, mediante una valoración cuantitativa y teniendo en cuenta los pilares de la seguridad informática, obteniendo como resultado el grado de importancia que cada uno posee para la organización.

Mediante la aplicación de la metodología Magerit, fué posible valorar e identificar el riesgo informático por cada activo, de igual manera las amenazas a las que puede estar expuesta la información del área de historias clínicas de la empresa.

Después de realizar un análisis potencial de los riesgos, se propone implementar controles teniendo en cuenta la norma ISO 27001 - 2013

Para controlar, mitigar o eliminar el riesgo que existe en la empresa, se sugiere implementar una serie de políticas de seguridad informática, las cuales se diseñaron teniendo en cuenta los controles propuestos.

12. TRABAJOS FUTUROS

Con la realización del presente trabajo se deja una documentación con bases ingenieriles y de seguridad informática para la cual la empresa objeto de este estudio debe implementar y colocar en práctica para mitigar cada riesgo identificado.

El presente trabajo se puede utilizar como referente a otras empresas de la ciudad y especialmente aquellas que se desempeñen en el área de salud.

13. BIBLIOGRAFÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela De Ciencias Básicas, Tecnología E Ingeniería Modulo curso: Riesgos y control informático

KASPERSKY LAB. ¿Qué es un código malicioso? [Consultado 13 de Septiembre de 2015]. Disponible en Internet:http://latam.kaspersky.com/mx/internet-security-center/definitions/malicious-code

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela De Ciencias Básicas, Tecnología E Ingeniería Modulo curso: Modelos y estándares de seguridad informática

TECNOLOGIA Y MUCHO MAS. Definición de cracker. [consultado el 15 de febrero de 2018]. Disponible en https://tecnologia-informatica.com/que-es-un-cracker/

COLOMBIA. MINISTERIO TIC. Ley 527 de 1999, Ley 599 DE 2000, Ley 1273 de 2009. Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. Bogotá, D.C., 2011. 1-43.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC) tecnología de la información. técnicas de seguridad. sistemas de gestión de seguridad de la información. NTC-ISO-IEC 27001. Bogotá D.C.: 2013. 33 pag.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT. Madrid, octubre de 2012. Disponible en el Portal de Administración Electrónica (Pae): http://administracionelectronica.gob.es/

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001:2013, Bogotá, D.C. Primera actualización Editada 2013-12-20, Disponible en https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

AMIÓ AGUIRRE, Jorge. Libro Electrónico de Seguridad Informática y Criptografía. Introducción a la seguridad informática. {En línea}. 01 marzo 2006. {Consultado en junio de 2018}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001a.htm

INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION. Guía avanzada de gestión de riesgos. {En línea}. {Consultado en agosto de 2018}. Disponible en: http://www.ficad.org/lecturas/adicional_uno_tercera_unidad_soma.pdf

Anexo 1 Formato RAE

Fecha de Realización: 20/11/2018
Título: ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001, PARA EL AREA DE HISTORIAS CLÍNICAS EN LA EMPRESA NEUROKIDS HEALT DE LA CIUDAD DE POPAYÁN
Autor: Ordoñez Sotelo, Jakeline
Palabras Claves: riesgo, amenaza, vulnerabilidad, tecnología, seguridad informática, magerit, confidencialidad, disponibilidad, integralidad, Autenticidad.
Descripción: El proyecto presentado trata sobre el análisis y diseño de un sistema de gestión de seguridad informática en el area de hostorias clinicas para la empresa Neurokids Healt, donde se realizó un análisis de riesgos de cada activo informático de la dependencia en estudio, obteniendo como resultado un riesgo residual el cual se propone mitigar con algunos controles ISO/IEC 27001-2013 y políticas de seguridad informática.
Fuentes: - UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela De Ciencias Básicas, Tecnología E Ingeniería Modulo curso: Riesgos y control informático - UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela De Ciencias Básicas, Tecnología E Ingeniería Modulo curso: Modelos y estándares de seguridad informática - MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT. Madrid, octubre de 2012. Disponible en el Portal de Administración Electrónica (Pae):

http://administracionelectronica.gob.es/

- Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001:2013, Bogotá, D.C. Primera actualización Editada 2013-12-20, Disponible en https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

Contenido del documento:

Marco referencial

Marco conceptual

Marco Teórico

Marco legal

Diseño metodológico

Diseño de gestión de seguridad de la información de Neurokids Healt

Valoración del riesgo informático identificado

Diseño de políticas y controles de seguridad informática

Metodología:

Para el desarrollo del proyecto donde se realizara un diseño de gestión de seguridad informática basado en la norma ISO-IEC 27001 de 2013 en Neurokids Healt, se propone aplicar la **Investigación Explorativa,** ya que permitirá conocer el tema que se va abordar y familiarizarse con algo que se desconoce. Para este caso específico, el enfoque de i**nvestigación es cuantitativo**, ya que se pretende hacer la medición de amenazas y riesgos en cuanto a la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información.

Para la gestión de riesgos del sistema de información de Neurokids, se ha

elegido utilizar la metodología **MAGERIT**, ya que permite identificar las características esenciales que posee cada activo de información, logrando de esta manera identificar las debilidades de cada activo.

Conceptos nuevos: Gestión del riesgo, metodología Magerit, Riesgo residual, controles de seguridad informática, investigación explorativa.

Conclusiones: Mediante el diseño de un SGSI, es posible gestionar la seguridad de los sistemas tecnológicos que maneja la empresa, de una forma organizada y eficiente, considerando activos informáticos, amenazas y vulnerabilidades.

Con el estudio realizado en Neurokids Healt, se identificó los activos informáticos que presentan un tipo de riesgo, mediante una valoración cuantitativa y teniendo en cuenta los pilares de la seguridad informática, obteniendo como resultado el grado de importancia que cada uno posee para la organización.

Mediante la aplicación de la metodología Magerit, fué posible valorar e identificar el riesgo informático por cada activo, de igual manera las amenazas a las que puede estar expuesta la información del área de historias clínicas de la empresa.

Después de realizar un análisis potencial de los riesgos, se propone implementar controles teniendo en cuenta la norma ISO 27001 - 2013

Para controlar, mitigar o eliminar el riesgo que existe en la empresa, se sugiere implementar una serie de políticas de seguridad informática, las cuales se diseñaron teniendo en cuenta los controles propuestos.

AUTOR: JAKELINE ORDOÑEZ SOTELO