DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA ISO 27001:2013 PARA INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD – IPS DEL DEPARTAMENTO DEL CHOCÓ

ALEXANDER VALENCIA VALDERRAMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

FACULTAD DE POSGRADOS

ESPECIALIZACION EN SEGURIDAD INFORMATICA

QUIBDÓ

2020

DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA ISO 27001 PARA INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD – IPS DEL DEPARTAMENTO DEL CHOCÓ

ALEXANDER VALENCIA VALDERRAMA

Monografía para obtener el título de:

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director Trabajo de Grado

ESP. YESNIR ANTONIO REDONDO DANIEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

FACULTAD DE POSGRADOS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

QUIBDO

2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Quibdó, octubre de 2020

DEDICATORIA

Dedico esta monografía a mi esposa e hijos
de quienes siempre he recibido apoyo
incondicional, a mis amigos y compañeros
por el acompañamiento y la confianza
gracias por creer que este logro si era posible.

AGRADECIMIENTOS

A Dios por haberme dado el tiempo necesario para cursar la especialización, por las bendiciones que recibo a diario, mis padres por el esfuerzo que hicieron para brindarme un mejor futuro, porque siempre estuvieron brindándome su apoyo incondicional en los momentos más difíciles de mi vida.

A mi esposa e hijos ya que son el motor que me permite avanzar, por su confianza y comprensión, gracias por el tiempo dejado de compartir esto permitió que hoy, pudiéramos ver el resultado de ese sacrificio.

A la Universidad mis más sinceros agradecimientos, a todos los profesionales de quienes recibí el asesoramiento necesario para el desarrollo de la especialización, este logro también es de ellos.

TABLA DE CONTENIDO

Pág.

LISTAS DE TABLAS....10

LISTAS DE FIGURAS....11

GLOSARIO....12

RESUMEN....1

INTRODUCCIÓN....2

DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA ISO 27001 PARA INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD – IPS DEL DEPARTAMENTO DEL CHOCÓ....4

1 PLANTEAMIENTO DEL PROBLEMA....4

2 FORMULACIÓN DEL PROBLEMA....6

3 OBJETIVOS....6

3.1 OBJETIVO GENERAL....6

3.2 OBJETIVOS ESPECIFICOS....6

4 JUSTIFICACION....8

5 ALCANCES Y LIMITACIONES....9

6 MARCO DE REFERENCIA....10

6.1 ANTECEDENTES....10

7 MARCO TEORICO....11

Amenazas:....12

Autenticación:....12

Confidencialidad: 13
Control informático: 13
Disponibilidad: 13
Integridad: 13
Riesgos informáticos: 13
Vulnerabilidad: 14
8 MARCO LEGAL 15
9 UNIDAD DE ANALISIS 20
Muestra: 20
ETAPAS: 20
ETAPA 1: Investigación y levantamiento de información: 21
ETAPA2: Definición de roles y responsabilidades: 21
ETAPA 3. Desarrollo: 21
ETAPA 4. Entrega: 21
10 ETAPA 1 22
10.1 INVESTIGACIÓN Y LEVANTAMIENTO DE INFORMACIÓN 22
10.2 INFORME DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN 23
10.3 IDENTIFICACIÓN DE LOS ACTIVOS 26
ANÁLISIS CUALITATIVO 31
ANÁLISIS CUANTITATIVO: 31
VALORACION DE ACTIVOS: 32
RIESGOS ASOCIADOS AL PERSONAL: 37
RIESGOS OPERATIVOS: 37

RIESGOS NATURALES: 37

MATRIZ DE RIESGOS: 40

REQUERIMIENTOS DE SEGURIDAD DE LA RED Y CONTROLES DE SEGURIDAD: 41

HARDWARE: 41

SOFTWARE: 41

DATOS: 41

PERSONAS: 41

DOCUMENTACIÓN: 42

11 POLITICAS DE SEGURIDAD BASADAS EN LA NORMA ISO 27001 PARA INSTITUCIONES PRESTADORES DE SERVICIOS DE SALUD EN EL DEPARTAMENTO DEL CHOCÓ 46

12 EQUIPOS 48

12.1 De la instalación de equipos de cómputo 48

12.2 Del mantenimiento de los equipos de cómputo 49

12.3 De la actualización de los equipos de cómputo 49

12.4 De la reubicación de los equipos de cómputo 50

13 CONTROL DE ACCESOS 50

13.1 Del Acceso a las áreas críticas 50

13.2 Del control de acceso al equipo de cómputo 51

13.3 Del control de acceso remoto al equipo de cómputo 52

13.4 Del acceso a los sistemas administrativos 52

13.5 Del acceso a internet 53

14 SOFTWARE 54

14.1 De la adquisición del software.....54

14.2 De la instalación del software.....55

14.3 De la actualización del software.....56

14.4 Del software propiedad de las Instituciones Prestadoras de Servicios de Salud –IPS y la propiedad intelectual 56

15 POLITICAS GENERALES 58

16 CONCLUSIONES 59

17 RECOMENDACIONES.....60

18 BIBLIOGRAFÍA.....61

LISTAS DE TABLAS

Pág.

Tabla N° 1 Legislación basada en el manejo de los datos.....16
Tabla N° 2 Activos más relevantes en las IPS del departamento 27
Tabla N° 3 Dimensión de activos según metodología MAGERIT 30
Tabla N° 4 Análisis cuantitativo y cualitativo de activos.....32
Tabla N° 5. Valoración de Activos.....33
Tabla N° 6. Identificación de los riesgos 38
Tabla N° 7 Matriz de riesgo 40
Tabla N° 8 Tabla de controles 43

LISTAS DE FIGURAS

Pág.

Figura N° 1. Unidad de Análisis 20
Figura N° 2. Metodología MAGERIT 25
Figura N° 3. Activos identificados en EAR/PILAR 29
Figura N° 4. Valoración de Activos 36

GLOSARIO

ENCRIPTAR**:** Mecanismo para el tratamiento que permite ocultar la información impidiendo así que alguna persona o sistema a excepción del destinatario pueda leerlos, garantizando la seguridad de la información.

INCIDENTE INFORMATICO**:** Suceso adverso que ocurre con el equipo informático y atenta contra los pilares de la información incluido los recursos tecnológicos.

LAN: Red de Área Local utilizada para interconectar dispositivos en un espacio geográfico determinado

LOGIN: Clave de usuario que se asigna a una persona para identificarlo en una red de datos

MALWARE: Programas cuyo objetivo es causar daños a computadoras, sistemas o redes

MENSAJERÍA INSTANTÁNEA: Sistema de intercambio de mensajes entre personas, escritos en tiempo real a través de red

MIGRACIÓN: Actividad que permite conservar la integridad de los datos al ser transferida por medio de configuraciones distintas de hardware y software

NETWORKING: Este concepto es usado para referirse a las redes de telecomunicaciones en general

POLITICA DE SEGURIDAD DE LA INFORMACIÓN**:** Instrumento de apoyo a la dirección y garantiza los pilares de la información, de acuerdo a los requerimientos de la empresa

PROTOCOLO TCP: Protocolo de transmisión de datos, el cual se compone de tres (3) etapas, establecimiento de conexión, transferencia de datos y fin de la conexión

RIESGO: Probabilidad que una vulnerabilidad se materialice exponiendo la seguridad de la información ocasionando daños o perdidas de la información

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN –SGSI: Conjunto de normas que asegura la confidencialidad, integridad y disponibilidad de la información en una organización.

SISTEMA OPERATIVO: Conjunto de archivos que se ejecutan para entregarle al usuario una interfaz por medio de la cual se gestionan recursos de hardware

VULNERABILIDAD: Responde a las malas prácticas de hardware y software que ponen en riesgo la seguridad y confidencialidad de la información

RESUMEN

La presente Monografía pretende brindar a las Instituciones Prestadoras de Servicios de Salud del departamento del Chocó, un referente con aspectos concernientes al manejo y la seguridad de la información de los estados de salud de los usuarios; identificando y proponiendo los controles, así como las políticas necesarias para garantizar los pilares de la seguridad de la información.

El desarrollo del presente documento se hará por medio del formato de monografía de investigación abordando el conocimiento acerca del diseño de políticas de seguridad informática basadas en la norma ISO27001:2013, teniendo como herramienta las encuestas y entrevistas abiertas, que permitan determinar los riesgos y vulnerabilidades que en materia de informática se encuentra la oficina de Sistemas de Información en Salud de dichas instituciones, garantizando así en un porcentaje muy alto la seguridad de la información.

INTRODUCCIÓN

Con el desarrollo que en materia tecnológica se vive en la actualidad, así mismo prosperan los riesgos y las amenazas, que atentan de forma directa e indirectamente en este campo, por esta razón se deben revisar de forma periódica las medidas, reglas y controles que más convienen para mitigar los riesgos a los que se encuentra expuesta la información de una empresa, en tanto que se realice un correcto tratamiento de los incidentes, ya que los datos deben tratarse y considerarse como el activo más importante y al mismo tiempo el más vulnerable que las compañías hoy en día tienen.

Los profesionales de Tecnología de Información que cada día asumen retos inimaginables para abordar los riesgos y amenazas que en la sociedad actual se presentan y que no evidencian signos de disminución, frente amenazas representativas, que pueden presentarse una y otra vez en ámbitos computacionales y que además pueden causar pérdidas económicas significativas. En tal sentido, es necesario que las empresas de hoy en día sean públicas o privadas deben tener un modelo de políticas de seguridad, que sea lo suficientemente claro, aplicable, conocido y acatado por todos los usuarios en toda la compañía.

Debido a esto, en esta monografía se definen los procesos y procedimientos por medio de un Sistema de Gestión de Seguridad de la Información como referencia, al estándar ISO27001:2013, en las Instituciones Prestadoras de Servicios de Salud –IPS del departamento del Chocó, que establezca unas políticas, normas, reglas y

controles que permitan establecer, niveles de acceso y roles en la red de datos de las IPS de modo que se pueda asegurar y salvaguardar la información de los pacientes que consultan diariamente, haciendo un análisis de las posibles amenazas que puede sufrir el sistema informático.

DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA ISO 27001 PARA INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD – IPS DEL DEPARTAMENTO DEL CHOCÓ

1 PLANTEAMIENTO DEL PROBLEMA

En Colombia El sistema General de Seguridad Social en Salud está normalizado por el estado, donde media el Ministerio de Salud y Protección a través de la Ley 100[1], expedida el 23 de diciembre de 1993 y modificada por la ley 1438[2] del 19 de enero de 2011.

Esta ley establece que: "Las Instituciones Prestadoras de Servicios de Salud –IPS sean de carácter público o privada en el Sistema General de Seguridad Social en Salud –SGSSS son los organismos encargados de realizar la atención de los usuarios en los diferentes niveles definidos en la ley, a ellos le corresponde procesar, analizar y almacenar los datos propios de los estados de salud de una persona, grupo familiar, municipio o región."

Los datos que se recopilan con la atención de los pacientes y estos conforman la historia clínica de un paciente, el perfil epidemiológico de una comunidad, municipio o región, en el proceso de análisis y almacenamiento de la información las Instituciones Prestadoras de Servicios de Salud –IPS del departamento del Chocó,

[1] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 100. (23, diciembre, 1993). Por la cual se crea el Sistema de Seguridad Social y se dictan otras disposiciones. En diario oficial. Diciembre, 1993. Nro. 41.148.p.1-168.

[2] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1438. (19, enero, 2011). Por la cual se reforma el Sistema de Seguridad Social y se dictan otras disposiciones. En diario oficial. Enero, 2011. Nro. 47.957.

carecen de procesos, procedimientos y políticas que garanticen los pilares de la información, teniendo en cuenta el grado de confidencialidad de la misma.

Las Instituciones Prestadoras de Servicios de Salud –IPS, analizan, procesan y almacenan la información de los pacientes que reciben servicios de salud, ofrecidos por estas instituciones respecto de su condición de vida y estado de salud, esta información debe ser tratada de acuerdo a los estándares internacionales de seguridad de la información, de los cuales las IPS en el departamento del Chocó no cuentan.

2 FORMULACIÓN DEL PROBLEMA

¿Cómo garantizar la seguridad de la información de los estados de salud de los usuarios que reciben atención en las Instituciones Prestadoras de Servicios de Salud –IPS del departamento del Chocó?

3 OBJETIVOS

OBJETIVO GENERAL

Diseñar políticas de seguridad informática basadas en la norma ISO 27001:2013, para instituciones prestadoras de salud –IPS del departamento del Chocó.

OBJETIVOS ESPECIFICOS

Levantar un informe del estado actual de la seguridad de la Información en algunas instituciones prestadoras de servicios de salud del departamento del Chocó.

Identificar riesgos potenciales a la seguridad de la información en las instituciones prestadoras de servicios de salud–IPS del departamento del Chocó

Determinar los requerimientos de seguridad de la red y los controles que permitan establecer unas políticas basadas en el estándar ISO 27001:2013 para las instituciones prestadoras de servicios de salud.

4 JUSTIFICACION

Teniendo en cuenta que la información que administra y gestionan, las Instituciones Prestadoras de Servicios de Salud–IPS, es de carácter muy confidencial y en ella se expresa la carga de enfermedad, estados de salud, morbilidad, mortalidad y el perfil epidemiológico que sufre una persona o una población, por esta razón se requiere que dicha información sea manejada con base en las normas y criterios de confidencialidad, integridad y disponibilidad por el profesional de la salud que atiende al paciente y por quienes de acuerdo a su perfil laboral en la IPS deban obtener acceso a la misma.

El desarrollo de esta monografía, permite la identificación, propuesta y establecimiento de controles y políticas que permiten garantizar los pilares de la seguridad de la información en las Instituciones Prestadoras de Servicios de Salud que se encuentran ubicadas en el Departamento del Chocó

5 ALCANCES Y LIMITACIONES

El avance de la presente Monografía ofrece un diseño de políticas de seguridad informática para los procesos de sistemas en las instituciones prestadoras de servicios de salud ubicadas en el Departamento del Chocó.

El conocimiento del estado actual, identificación de riesgos potenciales y determinación de requerimientos de seguridad corresponden a los pasos seguidos en el periodo de tiempo en que se desarrolló esta investigación, considerando como referencia la teoría de gestión de riesgo en seguridad informática, las normas ISO27001:2013 para finalmente ofrecer una adaptación de éstas a los requerimientos propios de las instituciones, garantizando la continuidad del servicio y optimizando el tiempo de respuesta de cualquier información que requiera de inmediata atención.

Es importante destacar que el proceso de implementación de las políticas de seguridad en los sistemas de control de las IPS del Departamento del Chocó requiere pasar por pautas administrativas que conllevan a invertir un tiempo mayor de validación y certificación del diseño propuesto. Por ello, en función del tiempo estimado para la realización de la monografía, el alcance quedo limitado exclusivamente al diseño de las políticas de seguridad, respaldo por las actividades mencionadas con anterioridad, más no a la implementación.

6 MARCO DE REFERENCIA

ANTECEDENTES

Según LÓPEZ NEIRA, Agustín y RUIZ SPOHR[3] mencionan que “La primera entidad de normalización a nivel mundial, fue la BSI (*British Standards Institution*), responsable de publicaciones como la BS5750 en 1979 (ahora ISO - 9001) o BS 7750 de 1992 (ahora ISO 1400)”, de tal manera que la norma BS 7799 de BSI da a luz en 1957 y su objetivo fundamental fue difundir un conjunto de buenas prácticas para la gestión de la seguridad de la información. Luego de varios años de modificaciones, adiciones y evolución en el tema, se llega al estándar ISO 27001, que fue aprobado y publicado como estándar internacional en octubre 2005

[3] LÓPEZ, Neira Agustín y RUIZ, Spohr Javier. El portal de ISO 27001 en español: Origen. [en línea]. España, 8 de agosto de 2013 Consultado el 11 de febrero 2020. Disponible en http://iso27000.es/index.html

7 MARCO TEORICO

En este sentido es que se justifica hoy más que nunca asegurar los datos, la información, la infraestructura y las aplicaciones en un mundo donde las amenazas a la seguridad se han convertido cada vez más sofisticadas con la evolución de la tecnología y están más presentes.

Conforme a esta tendencia, las instituciones de salud deben garantizar que la información que producen, procesan, almacenan y reportan, cumplan con los pilares de la seguridad de la información, para ello deben aplicar políticas, controles, procesos y procedimientos que cumplan con unos estándares que permitan desviar de forma proactiva las amenazas y disminuir los riesgos de manera que en caso de ocurrencias el impacto que generen no sean tan significativos.

De acuerdo a los principios sobre la reserva y protección de datos personales establecidos por la Organización de Estados Americanos–OEA[4], la presente monografía pretende amparar los derechos de los usuarios y proteger los de datos personales en lo que respecta a la información contenida en historias clínicas de las Instituciones prestadoras de Servicios de Salud –IPS con presencia en el departamento del Chocó.

[4] COLOMBIA. ORGANIZACIÓN DE ESTADOS AMERICANOS, Propuesta de Declaración de Principios de Privacidad y Protección de Datos en las Américas. 03 de septiembre 2019. Disponible en internet, http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

Las entidades que ofrecen servicios de salud deben reconocer la información como un activo importante para la atención de los pacientes en el desarrollo de sus procesos internos, ya que emplean los datos personales, datos médicos y de historia clínica impresos y archivos electrónicos, generados, procesados y almacenados, por lo tanto deben ocuparse de definir lineamientos que permitan mitigar los posibles riesgos que afecten los pilares de la seguridad de la información[5]
La presente monografía tiene un ámbito de aplicación en las Instituciones Prestadoras de Servicios de Salud de los sectores públicos y privados, en el departamento del Chocó e involucra teoría de seguridad informática, esto permite identificar conceptos muy importantes en el desarrollo de las bases teóricas, algunos conceptos tenidos en cuenta son los siguientes:

AMENAZAS**:** A través del diseño de las políticas de seguridad planteadas por medio de la presente monografía se disminuyen los eventos y amenazas que puede causar daño en la operación de un sistema informático

AUTENTICACIÓN**:** Control implementado en la monografía como garantía que el ingreso es verdadero

[5] COLOMBIA. HOSPITAL GENERAL DE MEDELLIN. Manual https://www.hgm.gov.co Medellín. HOSPITAL GENERAL, Manual de protección y uso de datos personales, 19 junio de 2019 Disponible en internet https://www.hgm.gov.co/documentos/566/manual-de-proteccion-y-uso-de-datos-personales/

CONFIDENCIALIDAD**:** Con la presente monografía garantiza que la información generada de la prestación de servicios de salud en las IPS del departamento del Chocó solo acceda los usuarios autorizados

CONTROL INFORMÁTICO: Proceso administrativo diseñado a través de la monografía cuyo objeto es asegurar la protección de todos los recursos informáticos, mejorando los índices de eficiencia y efectividad de los procesos operativos automatizados

DISPONIBILIDAD: Los controles diseñados por medio de la monografía mantendrán los datos disponibles en todo momento, para ser consultados y descargados por los usuarios.

INTEGRIDAD**:** Las políticas de seguridad diseñadas como objetivo general de la monografía responden a la propiedad de los datos antes de modificaciones no autorizadas, alteraciones y manipulaciones por personas o procesos no autorizadas.

RIESGOS INFORMÁTICOS: La presente monografía establece una serie de controles que disminuyen la probabilidad de que un hecho o suceso ocurra afectando la operación en el entorno informático

VULNERABILIDAD: Actualmente la información de los servicios de salud prestados a los usuarios en las IPS del departamento presenta riesgos que afectan los pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad)

8 MARCO LEGAL

Teniendo en cuenta otro aspecto importante que enmarca y direcciona es el marco jurídico que expone la normatividad correspondiente a la protección de datos y la información de los estados y las condiciones de salud de un individuo, comunidad, municipio y departamento contenidas en historias clínicas y software donde se gestionan, procesan y almacenan.

En la siguiente tabla se mencionan las leyes y normas que guardan relación con los datos sensibles de reserva legal, en el manejo de la información de salud de las personas que reciben los servicios de salud ofrecidos por las Instituciones prestadoras de Servicios de Salud en el departamento del Chocó y las políticas que deben cumplir en aras de salvaguardar los datos almacenados en sus sistemas de información.

Tabla 1. Legislación basada en el manejo de los datos

No	NORMATIVIDAD	TEMAS TRATADOS
1	[6]**Decreto 780, Art 2.5.1.7.2**	Este decreto "Otorga a las Entidades Territoriales funciones de modo que puedan realizar un exhaustivo control, inspeccionando, vigilando y realizando el proceso de auditoría para el mejoramiento de la calidad"
2	[7]**Decreto 780, Art 2.5.3.4.1.1**	Le permite a las Administradoras de Recursos del Sistema General de Seguridad Social en Salud como EPS del régimen subsidiado, contributivo y ARL acceder y revisar los datos de la historia clínica y sus soportes, dentro de la labor de auditoria
3	[8]**Resolución 1995 de 1999**	Esta norma establece una serie de parámetros en el manejo de la Historia Clínica"

[6]COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Decreto 780. (16, mayo, 2011). Por medio del cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social. Bogotá: El Ministerio, 2011. P. 168

[7] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Decreto 780. (16, mayo, 2011). Por medio del cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social. Bogotá: El Ministerio, 2011. P. 226

[8] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 1985. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 2011.

Tabla *2.* (Continuación)

No	NORMATIVIDAD	TEMAS TRATADOS
4	**[9]Resolución 1995 de 1999, Literal a) Articulo 1**	Determina que la Historia Clínica es un documento de carácter reservado y obligatorio en el que se debe registrar de forma cronológica las condiciones y estado de salud del paciente, así como las actuaciones médicas
5	**Resolución 1995 de 1999, Capitulo III, Articulo 13[10]**	Instituye que la protección y conservación de la Historia Clínica estará a cargo del prestador de servicios de salud que la generó en el proceso de la atención siempre y cuando éste cumpla los procedimientos de archivos señalados en la presente resolución.
6	**Resolución 1995 de 1999, Capitulo III, Articulo 14[11]**	Establece que el acceso a los datos contenidos en la historia clínica, solo podrán ser entregados en los términos previstos en la Ley a quienes ostenten la calidad de El usuario, El equipo de salud, Las autoridades judiciales y las demás personas determine la ley

[9] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 1985. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 2011. P. 1

[10] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 1985. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 2011. P. 5

[11] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 1985. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 2011. P. 5

Tabla *3.* (Continuación)

No	NORMATIVIDAD	TEMAS TRATADOS
7	[12]**Constitución política de Colombia, Articulo 15**	Determina que a todo ciudadano le asiste el derecho a la intimidad personal y familiar, así mismo al buen nombre y el estado debe garantizar que sean respetados y hacerlos respetar
8	[13]**Ley 1581 de 2012, Ley de Habeas Data**	Por medio de la cual se dictan disposiciones que permiten garantizar la protección de datos personales ,contenidos en archivos, bases de datos y similares

Fuente: Elaboración propia

[12] COLOMBIA. CONGRESO DE LA REPUBLICA. Constitución Política de la Republica de Colombia. (20, julio, 1991). Esta versión corresponde a la segunda edición corregida de la Constitución Política de Colombia, publicada en la Gaceta Constitucional N° 116 de 20 de julio 1991. Julio, 1991.

[13] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1581 de 2012. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En diario oficial. 18 de octubre, 2012. Nro. 48.587

Tabla *4.* (Continuación)

No	NORMATIVIDAD	TEMAS TRATADOS
9	**[14]Ley 1437 de 2011, modificada por la Ley 175 de 2015, Capitulo II, Articulo 24, numeral 3**	Establece que la Información contenida en documentos como hojas de vida, historia laboral y los expedientes pensionales y demás registros de personas que existan en archivos de las instituciones públicas o privadas, así como la historia clínica deben ser de reserva institucional

Fuente: Elaboración propia

[14] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1437 de 2011. (17, enero, 2011). Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. En diario oficial. 18 de enero, 2011. Nro. 47.956

9 UNIDAD DE ANALISIS

La presente investigación sirve de apoyo las Instituciones Prestadoras de Servicios de Salud –IPS en el departamento del Chocó en aspectos concernientes al manejo y la seguridad de la información, que se considera sensible.

MUESTRA: Se toma como muestra los procesos y procedimientos del área de Sistemas de Información en Salud en aquellas Instituciones Prestadoras de Servicios de Salud del departamento del Chocó, que más volumen de atención a pacientes tienen y que en sus procesos de atención a la población existan eventos que puedan generar o materializar los riesgos asociados a la seguridad de la información.

ETAPAS: En el desarrollo de la presente monografía se identifican principalmente cuatro etapas, que se detallan a continuación.

Figura N° 1. Unidad de Análisis

Fuente: Elaboración propia

ETAPA 1: **INVESTIGACIÓN Y LEVANTAMIENTO DE INFORMACIÓN:** Por medio de esta se hará reconocimiento de la información, verificando los procesos y procedimientos del área de sistemas, entendiendo la dinámica, las reglas y todas las particularidades de negocio existentes, en aquellas Instituciones Prestadoras de Servicios de Salud del departamento, teniendo siempre en cuenta la normatividad y las referencias bibliográficas que existe al respecto.

ETAPA2: **DEFINICIÓN DE ROLES Y RESPONSABILIDADES:** Una vez realizada la etapa de levantamiento de la información en la etapa 1. En esta etapa es necesario realizar un análisis de los riesgos, identificando los activos informáticos, sus vulnerabilidades y amenazas a las que están expuestos, para establecer así la probabilidad de ocurrencia y en caso de materialización determinar el impacto que genera en el equipo informático, de manera que se puedan establecer los controles necesarios y adecuados para disminuir, aceptar, transferir o evitar la ocurrencia de los mismos.

ETAPA 3. **DESARROLLO:** a través de esta etapa se establecen los controles y las políticas teniendo en cuenta el estándar ISO27001:2013 para las Instituciones Prestadoras de Servicios de Salud –IPS en el departamento del Chocó.

ETAPA 4. **ENTREGA:** Aprobación de los controles y políticas, promoción y divulgación de las mismas en las Instituciones Prestadoras de Servicios de Salud – IPS del departamento del Chocó

10 ETAPA 1

INVESTIGACIÓN Y LEVANTAMIENTO DE INFORMACIÓN

En esta etapa de la monografía se busca recopilar información de los procesos y procedimientos realizados en la oficina de Sistemas para así conocer cómo opera actualmente y efectuar los cambios necesarios de manera sistemática donde se realiza el procesamiento y almacenamiento de la información para lograr mejorar los niveles de seguridad de la misma.

Para llevar a cabo la investigación y el levantamiento de la información se hace uso la entrevista y la observación directa de los procesos donde se pueda evidenciar de forma general el ritmo de trabajo, el movimiento del personal y documentos en general, las herramientas utilizadas para el procesamiento y almacenamiento de la información, evaluar el grado en el cual estos procedimientos se están llevando a cabo y cuáles son los factores que posiblemente requieran atención especial.

INFORME DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

Entre las debilidades más importantes encontradas en las Instituciones Prestadoras de Servicios de Salud del departamento están las siguientes:

- No poseen un Plan Estratégico de Sistemas de Información –PESI, que sirva de ruta durante un periodo de tiempo
- Carecen de políticas de seguridad informática basadas en la norma ISO 27001
- No cuentan con un plan de mantenimiento preventivo y correctivo de equipos de cómputo e infraestructura tecnológica.
- No existe un Plan de Contingencia donde se deleguen funciones y responsables
- No incluyen la actualización de los procesos y procedimientos administrativos y asistenciales de la entidad.
- No identifican los riesgos asociados a los procesos y procedimientos

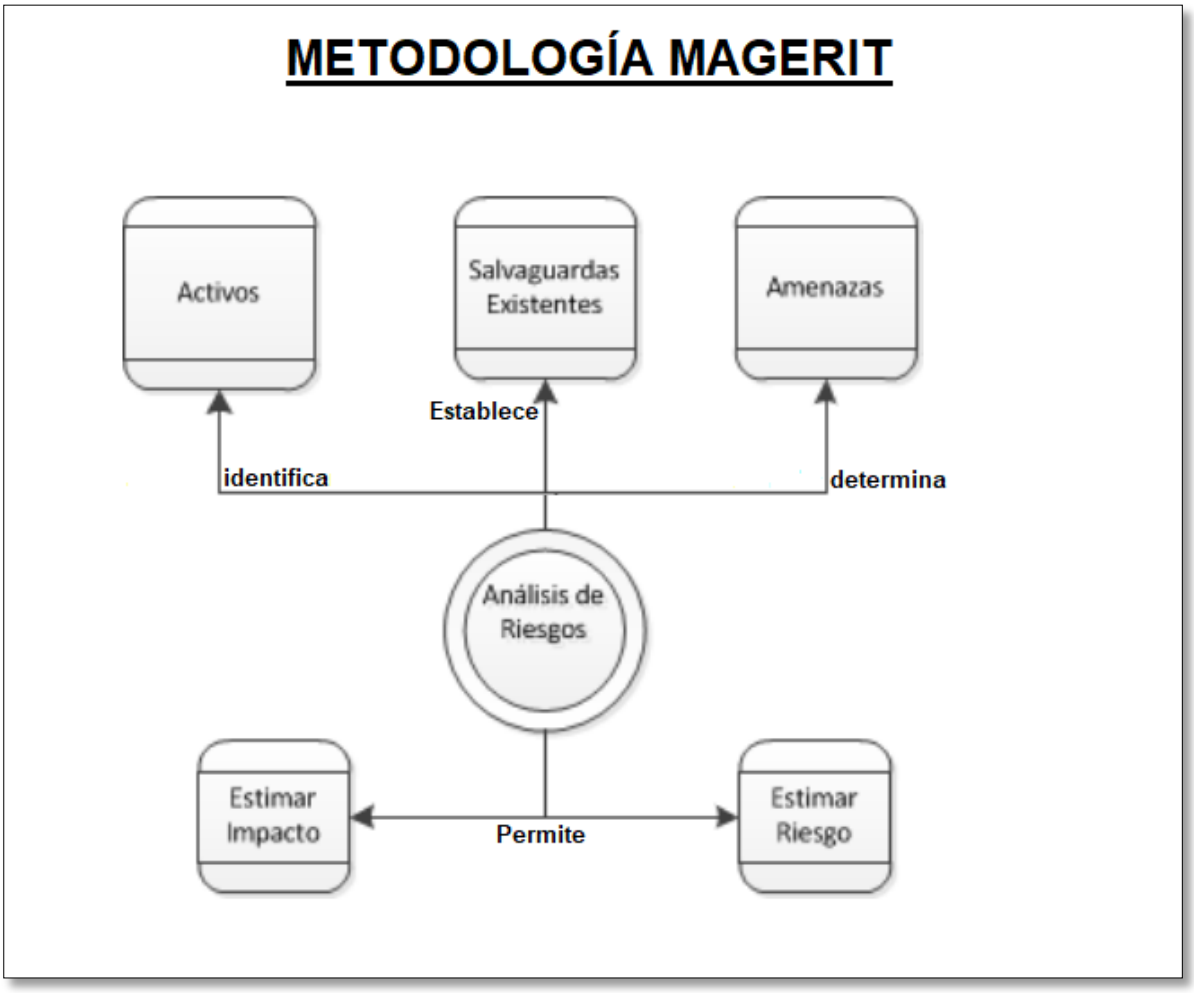
En el desarrollo de la presente monografía es necesario hacer uso de la metodología MAGERIT[15] la cual permite analizar y gestionar riesgos mediante el

[15] ESPAÑA, UNIVERSIDAD DE MURCIA, Metodología De Análisis y Gestión De Riesgos de los Sistemas de Información (MAGERIT Versión 3). Metodología que permite analizar y gestionar los riesgos asociados a la operación de los sistemas de información 30 de Octubre de 2019

método sistemático que analiza los conflictos derivados del uso de tecnologías de información y comunicación, permitiendo así proponer medidas de control a las debilidades encontradas.

La metodología MAGERIT, establece una serie de pasos, que inicia con la identificación de los activos y la interrelación entre estos dentro de la compañía, luego se debe determinar a qué amenazas se encuentran expuestos los activos antes identificados, así mismo establecer y disponer medidas preventivas que permitan minimizar el impacto que generaría la materialización del riesgo, así mismo realizar la medición del impacto ponderado contra la probabilidad de materialización de la amenaza.

Figura 2. Metodología MAGERIT



Fuente: Elaboración propia

IDENTIFICACIÓN DE LOS ACTIVOS

La identificación de los activos según la Metodología MAGERIT, fue importante apoyar este proceso en el libro 2 de la metodología denominado “Catalogo de elementos” (Ver ANEXO A: libros de metodología MAGERIT)

En general las Instituciones Prestadores de Servicios de Salud del departamento del Chocó tienen una infraestructura tecnológica un poco reducida, debido al poco personal y recursos tecnológicos, que no superan los 100 empleados, lo que redunda en pocos activos informáticos, de acuerdo a la siguiente tabla:

Tabla N° 5. Activos más relevantes en las IPS del departamento

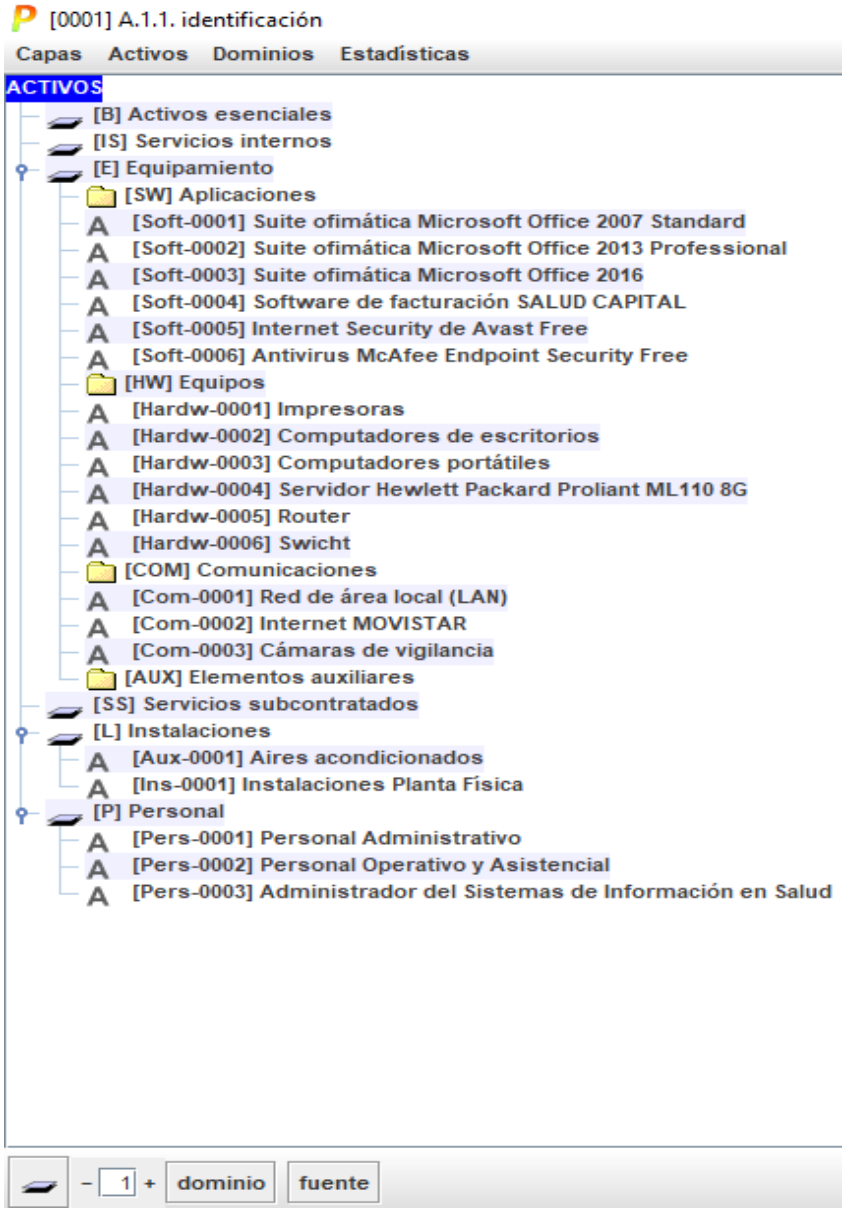
TIPO ACTIVO	COD-ACTIVO	DESCRIPCION	CANTIDAD	CRITICO
SOFTWARE	Soft-0001	Suite ofimática Microsoft Office 2007 Standard	9	SI
	Soft-0002	Suite ofimática Microsoft Office 2013 Professional	17	SI
	Soft-0003	Suite ofimática Microsoft Office 2016	5	SI
	Soft-0004	Software de facturación SALUD CAPITAL	1	NO
	Soft-0005	Internet Security de Avast Free	22	SI
	Soft-0006	Antivirus McAfee Endpoint Security Free	9	SI

Tabla N° 6. (Continuación)

TIPO ACTIVO	COD-ACTIVO	DESCRIPCION	CANTIDAD	CRITICO
HARDWARE	Hardw-0001	Impresoras	6	NO
	Hardw-0002	Computadores de escritorios	22	SI
	Hardw-0003	Computadores portátiles	9	SI
	Hardw-0004	Server Hewlett Packard Proli ML110 8G	1	SI
	Hardw-0005	Router	2	NO
	Hardw-0006	Swicht	4	NO
COMUNICACIONES	Com-0001	Red de área local (LAN)	1	SI
	Com-0002	Internet MOVISTAR	1	NO
	Com-0003	Cámaras de vigilancia	6	NO
INSTALACIONES	Aux-0001	Aires acondicionados	9	NO
	Ent-0001	Instalaciones Planta Física	1	SI
PERSONAL	Pers-0001	Personal Administrativo	22	SI
	Pers-0002	Personal Operativo y Asistencial	17	SI
	Pers-0003	Administrador del Sistemas de Información en Salud	2	NO

Fuente: Elaboración propia

Figura 3. Activos identificados en EAR/PILAR



Fuente: Elaboración propia

De acuerdo a los activos identificados es necesario realizar una valoración de forma que se pueda proteger según la necesidad que se tiene de dicho activo, pues cuanto más valioso es un activo, mayor debe ser el nivel de protección que se requiere.

En la valoración de los activos es necesario considerar la dimensión del mismo para ese efecto se toma el libro 2 de la metodología MAGERIT, en la que se describen las 5 dimensiones en las que el activo debe ser valorado, esta valoración se hará en la herramienta EAR/PILAR

Tabla 7. Dimensión de activos según metodología MAGERIT

DIMENSIONES	
[D]	**DISPONIBILIDAD:** Esta dimensión hace referencia a los perjuicios que le causa a la Institución Prestadora de Servicios de Salud –IPS no poder usarlo, porque el activo no se encuentra disponible en un determinado momento
[I]	**INTEGRIDAD:** Hace referencia a los prejuicios que causa si el activo se encuentra corrupto, debido a que los datos hayan sido alterados de forma voluntaria o involuntaria
[C]	**CONFIDENCIALIDAD:** Afecta a la compañía si alguien no autorizado conoce o tiene acceso al activo
[A]	**AUTENTICIDAD:** Causa afectación si se desconoce los sujetos que realizan las acciones desarrolladas sobre el activo,

Tabla 8. (Continuación)

DIMENSIONES	
[T]	**TRAZABILIDAD:** Son aquellos perjuicios que se causan cuando se desconoce las acciones llevadas a cabo sobre un activo y adicionalmente no queda constancia del uso del mismo

Fuente: Elaboración propia

Conforme las anteriores definiciones, se debe constituir una escala de valores que permita la evaluación y su correspondiente análisis cualitativo o cuantitativo del determinado activo, de la siguiente forma:

ANÁLISIS CUALITATIVO**:** La valoración se hará por niveles de importancia así: Muy alto, Alto, Medio, Bajo y Despreciable.

ANÁLISIS CUANTITATIVO: La valoración de los activos mediante este tipo de análisis se hará por medio de escala numérica con valores de 0 a 10 donde el cero se considera despreciable y el número 10 se considera como la calificación más alta e importante a considerar dentro de los activos de la Institución Prestadora de Servicios de salud –IPS, este proceso se hará en la herramienta EAR/PILAR

Tabla 9. Análisis cuantitativo y cualitativo de activos

VALOR		CRITERIO	DIMENSIONES
10	EXTREMO	Daño extremadamente grave	DICAT
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: Elaboración propia

VALORACION DE ACTIVOS: La valoración de los activos de Instituciones Prestadoras de Servicios de Salud –IPS en el departamento del Chocó a razón de las dimensiones previamente establecidas de Integridad, Confidencialidad, Disponibilidad, Autenticidad y Trazabilidad y bajo los criterios establecidos del análisis cualitativo y cuantitativo se demuestran en la siguiente tabla:

Tabla 10. Valoración de Activos

CODIGO	DESCRIPCION	DIMENSIONES					ANÁLISIS	
		[D]	[I]	[C]	[A]	[T]	Cuantitativa	Cualitativa
Soft-0001	Suite ofimática Microsoft Office 2007 Standard	9	10	9	10	9	9	Alto
Soft-0002	Suite ofimática Microsoft Office 2013 Professional	9	10	9	10	9	9	Alto
Soft-0003	Suite ofimática Microsoft Office 2016	9	10	9	10	9	9	Alto
Soft-0004	Software de facturación SALUD CAPITAL	10	10	10	10	10	10	Alto

Tabla 11 (Continuación)

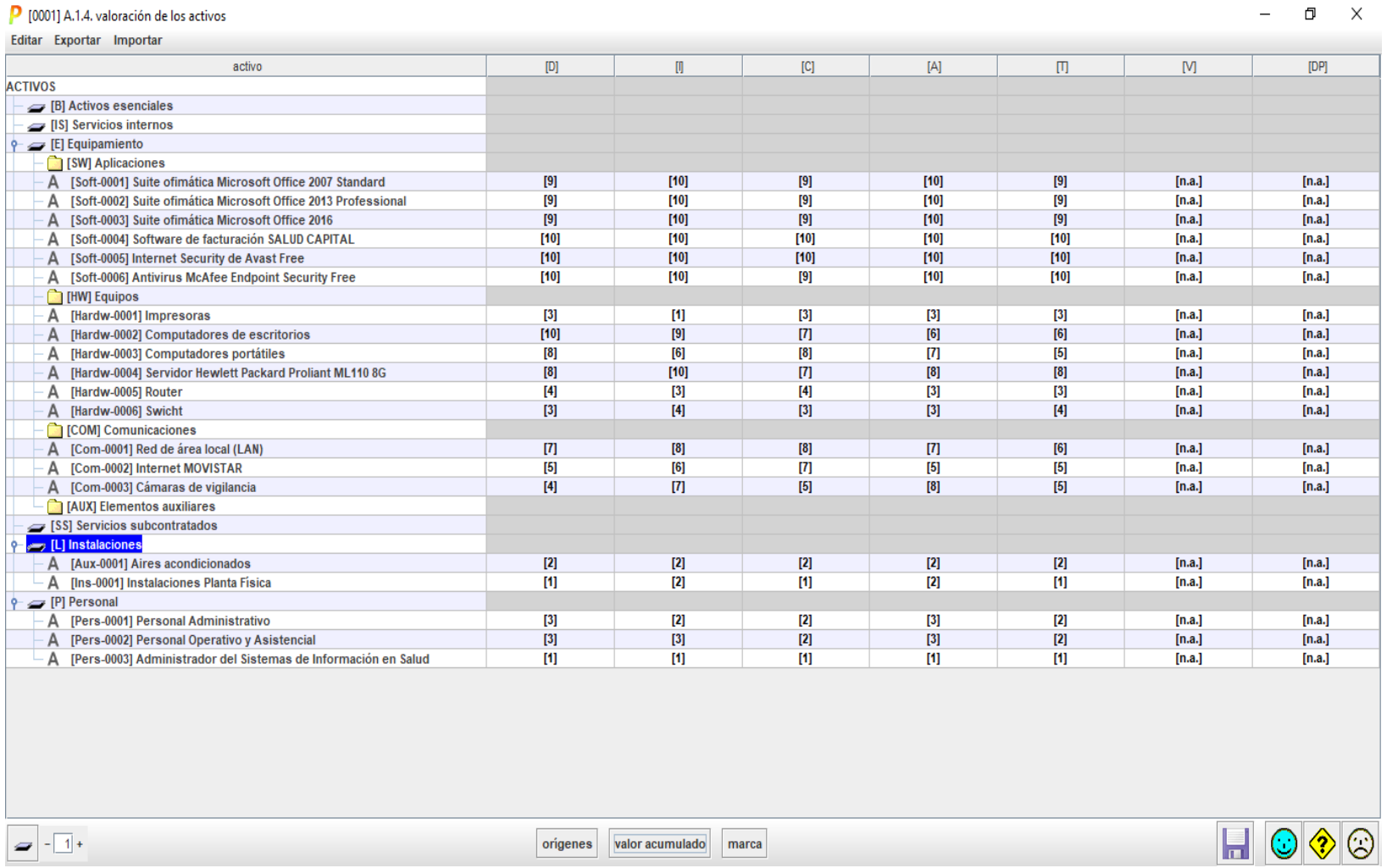
CODIGO	DESCRIPCION	DIMENSIONES					ANÁLISIS	
		[D]	[I]	[C]	[A]	[T]	Cuantitativa	Cualitativa
Soft-0005	Internet Security de Avast Free	10	10	10	10	10	10	Muy Alto
Soft-0006	Antivirus McAfee Endpoint Security Free	10	10	9	10	10	10	Muy Alto
Hardw-0001	Impresoras	3	1	3	3	3	3	Bajo
Hardw-0002	Computadores de escritorios	10	9	7	6	6	8	Alto
Hardw-0003	Computadores portátiles	8	6	8	7	5	7	Alto
Hardw-0004	Servidor Hewlett Packard Proliant ML110 8G	8	10	7	8	8	8	Alto
Hardw-0005	Router	4	3	4	3	3	3	Bajo
Hardw-0006	Swicht	3	4	3	3	4	3	Bajo
Com-0001	Red de área local (LAN)	7	8	8	7	6	7	Alto

Tabla 12 (Continuación)

CODIGO	DESCRIPCION	DIMENSIONES					ANÁLISIS	
		[D]	[I]	[C]	[A]	[T]	Cuantitativa	Cualitativa
Com-0002	Internet MOVISTAR	5	6	7	5	5	6	Alto
Com-0003	Cámaras de vigilancia	4	7	5	8	5	6	Alto
Aux-0001	Aires acondicionados	2	2	2	2	2	2	Bajo
Ent-0001	Instalaciones Planta Física	1	2	1	2	1	1	Bajo
Pers-0001	Personal Administrativo	3	2	2	3	2	2	Bajo
Pers-0002	Personal Operativo y Asistencial	3	3	2	3	2	3	Bajo
Pers-0003	Administrador del Sistemas de Información en Salud	1	1	1	1	1	1	Bajo

Fuente: Elaboración propia

Figura 4. Valoración de Activos



[0001] A.1.4. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[Soft-0001] Suite ofimática Microsoft Office 2007 Standard	[9]	[10]	[9]	[10]	[9]	[n.a.]	[n.a.]
[Soft-0002] Suite ofimática Microsoft Office 2013 Professional	[9]	[10]	[9]	[10]	[9]	[n.a.]	[n.a.]
[Soft-0003] Suite ofimática Microsoft Office 2016	[9]	[10]	[9]	[10]	[9]	[n.a.]	[n.a.]
[Soft-0004] Software de facturación SALUD CAPITAL	[10]	[10]	[10]	[10]	[10]	[n.a.]	[n.a.]
[Soft-0005] Internet Security de Avast Free	[10]	[10]	[10]	[10]	[10]	[n.a.]	[n.a.]
[Soft-0006] Antivirus McAfee Endpoint Security Free	[10]	[10]	[9]	[10]	[10]	[n.a.]	[n.a.]
[HW] Equipos							
[Hardw-0001] Impresoras	[3]	[1]	[3]	[3]	[3]	[n.a.]	[n.a.]
[Hardw-0002] Computadores de escritorios	[10]	[9]	[7]	[6]	[6]	[n.a.]	[n.a.]
[Hardw-0003] Computadores portátiles	[8]	[6]	[8]	[7]	[5]	[n.a.]	[n.a.]
[Hardw-0004] Servidor Hewlett Packard Proliant ML110 8G	[8]	[10]	[7]	[8]	[8]	[n.a.]	[n.a.]
[Hardw-0005] Router	[4]	[3]	[4]	[3]	[3]	[n.a.]	[n.a.]
[Hardw-0006] Swicht	[3]	[4]	[3]	[3]	[4]	[n.a.]	[n.a.]
[COM] Comunicaciones							
[Com-0001] Red de área local (LAN)	[7]	[8]	[8]	[7]	[6]	[n.a.]	[n.a.]
[Com-0002] Internet MOVISTAR	[5]	[6]	[7]	[5]	[5]	[n.a.]	[n.a.]
[Com-0003] Cámaras de vigilancia	[4]	[7]	[5]	[8]	[5]	[n.a.]	[n.a.]
[AUX] Elementos auxiliares							
[SS] Servicios subcontratados							
[L] Instalaciones							
[Aux-0001] Aires acondicionados	[2]	[2]	[2]	[2]	[2]	[n.a.]	[n.a.]
[Ins-0001] Instalaciones Planta Física	[1]	[2]	[1]	[2]	[1]	[n.a.]	[n.a.]
[P] Personal							
[Pers-0001] Personal Administrativo	[3]	[2]	[2]	[3]	[2]	[n.a.]	[n.a.]
[Pers-0002] Personal Operativo y Asistencial	[3]	[3]	[2]	[3]	[2]	[n.a.]	[n.a.]
[Pers-0003] Administrador del Sistemas de Información en Salud	[1]	[1]	[1]	[1]	[1]	[n.a.]	[n.a.]

Fuente: Elaboración propia

Una vez realizada la identificación de los activos y la valoración de los mismo se debe realizar la identificación de los riesgos los cuales se pueden categorizar en 3 grandes grupos. RIESGOS ASOCIADOS AL PERSONAL, RIESGOS OPERATIVOS, RIESGOS NATURALES.

RIESGOS ASOCIADOS AL PERSONAL: En ésta categoría se encuentran todas aquellos que pueden generarse por los usuarios internos o externos del sistema y pueden ocurrir de forma voluntaria o involuntaria debido a acciones no autorizadas, daño físico, fallas técnicas y desconocimiento

RIESGOS OPERATIVOS: Este tipo de riesgos se presentan en la operación del sistema informático y pueden materializarse debido a los errores, fallas, en la gestión y operación de procesos internos tanto en el hardware o el software.

RIESGOS NATURALES: Estos pueden materializarse como consecuencia de desastres naturales, truenos, inundaciones, tormentas e incendios.

Teniendo en cuenta esta clasificación de riesgos, en la siguiente matriz podemos determinar la probabilidad de ocurrencia y el impacto que genera la materialización de estos riesgos.

Tabla 13. Identificación de los riesgos

IDENTIFICACION DE RIESGOS EN INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD			
CATEGORIA	**RIESGO**	**PROBABILIDAD**	**IMPACTO**
RIESGOS FACTORES HUMANOS	Falta políticas y normas	Frecuente	Peligroso
	Fraude y robo de información y hardware	Frecuente	Peligroso
	Falta de formación y concienciación en seguridad informática	Frecuente	Peligroso
	Publicación de información confidencial	Probable	Peligroso
RIESGOS OPERATIVOS	Antivirus y software sin licencias	Frecuente	Peligroso
	Control de accesos a la red	Probable	Peligroso
	Falta de backups y copias de respaldos	Frecuente	Catastrófico
	Falta de seguridad física	Frecuente	Peligroso
	Inadecuada y poco inversión en tecnología	Frecuente	Moderado
	Falta de Bitácoras de eventos	Frecuente	Moderado
	Fugas de información	Probable	Peligroso

Tabla 6 (Continuación)

IDENTIFICACION DE RIESGOS EN INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD			
CATEGORIA	**RIESGO**	**PROBABILIDAD**	**IMPACTO**
RIESGOS NATURALES	Tormentas	Probable	Catastrófico
	Fallas en el fluido eléctrico	Frecuente	Peligroso
	Incendios	Frecuente	Moderado
	Sismos	Probable	Moderado

Fuente: Elaboración propia

MATRIZ DE RIESGOS: La presente monografía hace uso de este instrumento para realizar un diagnóstico objetivo de las Instituciones Prestadoras de Servicios de Salud -IPS evaluando la efectividad de la gestión de los riesgos asociados factores humanos, operativos o desastres naturales

Tabla 14. Matriz de riesgo

MATRIZ DE RIESGO					
IMPACTO	PROBABILIDAD				
	IMPROBABLE	POSIBLE	OCASIONAL	PROBABLE	FRECUENTE
INSIGNIFICANTE					
MENOR					
MODERANO					
PELIGROSO					
CATASTROFICO					

Fuente: Elaboración propia

REQUERIMIENTOS DE SEGURIDAD DE LA RED Y CONTROLES DE SEGURIDAD: La identificación de los riesgos y la determinación de la matriz de riesgos indicando la probabilidad y el impacto que genera la materialización de los riesgos tipificados en la presente monografía, permite realizar una valoración de los requerimientos necesarios basadas en el estándar ISO27001:2013.

Para establecer los requerimientos de seguridad y los controles es posible realizar una agrupación por categorías de forma que se pueda identificar los bienes informáticos a proteger así:

HARDWARE: Son considerados como bienes informáticos la red de datos, computadoras personales, computadores portátiles, líneas de comunicaciones, módems, routers, swicht.

SOFTWARE: En esta categoría se encuentran los programas fuentes de propósito misional, sistemas operativos, programas utilitarios, software de comunicaciones.

DATOS: Almacenados en discos, almacenados en bases de datos, en tránsito durante la operación.

PERSONAS: Usuarios internos y externos, operadores y personal de mantenimiento.

DOCUMENTACIÓN: Licencias de uso de sistemas operativos, de office, de antivirus, de software de propósito misional etc.

Esto permite establecer en qué medida uno es más importante que otro y así mismo su grado de importancia de acuerdo a la función que realiza, su costo y las consecuencias que genera la perdida, los costos y tiempos al tener que recuperarla, así mismo como la preservación de la confidencialidad, integridad y la disponibilidad de la información. La determinación de la importancia de cada bien informático puede ser realizada de forma descriptiva o de forma numérica

La siguiente tabla relaciona los requerimientos y controles de seguridad teniendo en cuenta el estándar ISO 27002[16] por medio del cual se establecen "Directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en las Instituciones Prestadoras de Servicios de Salud –IPS"

[16] ORGANIZACIÓN INTERNACIONAL DE ESTANDARES , http://www.iso27000.es/ Madrid. Estándar internacional que permite establecer una serie de controles organizados con base en los 14 dominios, 35 objetivos de control y 114 controles del estándar [Consultado 30 de Octubre de 2019] Disponible en: http://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

Tabla 15. Tabla de controles

DOMINIO	OBJETIVO DE CONTROL	CONTROL	DESCRIPCION
Política de Seguridad	Directrices de la Dirección en seguridad de la información	Conjunto de políticas para la seguridad de la información	A través de esta política se establecen los controles de acceso, físico y lógico, clasificación de la información entre otros
Aspectos organizativos de la seguridad de la información	Organización interna	Asignación de responsabilidades para la seguridad de la información	En este control se definen las restricciones a la instalación de software y el uso, copias de seguridad, protección contra el malware
Seguridad ligada al recurso humano	Durante la contratación	Concienciación, educación y capacitación en seguridad de la información	A través de este control se pretende capacitar al usuario nombrado y contratista de la IPS en Seguridad Informática

Tabla 8 (Continuación)

DOMINIO	OBJETIVO DE CONTROL	CONTROL	DESCRIPCION
Seguridad ligada al recurso humano	Durante la contratación	Concienciación, educación y capacitación en seguridad de la información	A través de este control se pretende capacitar al usuario nombrado y contratista de la IPS en Seguridad Informática
Gestión de activos	Responsabilidad sobre los activos	Inventario de activos	Se establece la realización periódica de inventario de hardware y software
Control de accesos	Requisitos de negocios para el control de accesos	Control de acceso a las redes y servicios asociados	En este control se permite establecer el ingreso a la red de datos y todos los demás servicios asociados a ella
	Control de acceso a sistemas y aplicaciones	Procedimientos seguros de inicio de sesión	Control que establece los usuarios de las diferentes aplicaciones
Seguridad operativa	Copias de seguridad	Copias de seguridad de la información	Implanta el procedimiento de copias de seguridad de la información
	Gestión de la vulnerabilidad técnica	Restricciones en la instalación de software	Controla la instalación de sistemas, aplicaciones en equipos de las Instituciones de salud del departamento

Tabla 8 (Continuación)

DOMINIO	OBJETIVO DE CONTROL	CONTROL	DESCRIPCION
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Continuidad de la seguridad de la información	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Este control determina y establece los procedimientos y responsabilidades del plan de continencia
Cumplimiento	Cumplimiento de los requisitos legales y contractuales	Protección de datos y privacidad de la información personal	Controla y garantiza que los datos personales de usuarios sean de reserva de la institución y solo sean accedidos por personal autorizado

Fuente: Elaboración propia

11 POLITICAS DE SEGURIDAD BASADAS EN LA NORMA ISO 27001 PARA INSTITUCIONES PRESTADORES DE SERVICIOS DE SALUD EN EL DEPARTAMENTO DEL CHOCÓ

La propuesta de políticas de seguridad informática basadas en la norma ISO 27001, tiene como propósito fundamental proteger los activos de información frentes a las amenazas que las Instituciones Prestadoras de Servicios de Salud –IPS, se encuentra expuestas, estableciendo controles y mecanismos que permitan mitigar o minimizar el impacto que pueda generar la materialización de los riesgos anteriormente identificados.

Estas políticas están encauzadas a convertirse en una cultura empresarial donde se involucre a todo el personal, funcionarios, contratistas, visitantes, usuarios y terceros que prestan sus servicios y gocen de algún tipo de correlación con las IPS en el departamento del Chocó.

Debe ser además la orientación de estas políticas el cumplimiento de toda la normatividad legal y las buenas prácticas de seguridad informática establecidas en el estándar ISO 27001, adicionalmente el cumplimiento del modelo seguridad y privacidad de la información de Gobierno Digital determinadas por el Ministerio de Tecnologías de Información y las Comunicaciones de Colombia –MinTic.

Es fundamental que esta política sea adoptada en el área de Gestión Humana las Instituciones Prestadoras de Servicios de Salud -IPS, como requisito para la contratación y al mismo tiempo se pueda realizar capacitaciones al personal y terceros que presten algún tipo de servicios, esto permitirá que sean difundidas,

conocidas y aplicadas en el entorno, con el objeto de proteger uno de los activos más importantes de la institución (la Información)

De acuerdo a las consultas realizadas a las IPS en su organigrama de forma general se encontró que la oficina de SISTEMAS DE INFORMACIÓN, estas dependencias están conformadas por lo general por dos (2) máximo tres (3) funcionarios que cumplen funciones de soporte y mantenimiento de la plataforma tecnológica, desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de la red de datos, administración del banco de datos, estadística, archivo y correspondencia entre otras, por tal razón existe la necesidad imperiosa de establecer políticas particulares para el mejor manejo de todos los recursos informáticos llámense hardware o software, la presente Monografía agrupa las políticas de seguridad informática en las IPS del departamento así:

12 EQUIPOS

DE LA INSTALACIÓN DE EQUIPOS DE CÓMPUTO

- ✓ La protección física de los equipos de cómputo es responsabilidad de quien le haya sido asignado y deberá notificar al área de sistemas de Información el movimiento y el tiempo que será movido el mismo

- ✓ Todo equipo de cómputo o estación de trabajo que sea conectado a la red de datos que sea propiedad o no de la IPS debe ajustarse a las normas y procedimientos establecidas en las políticas de seguridad informática de la entidad

- ✓ La oficina de Gestión Administrativa n de Recursos Tecnológicos y Documentales en coordinación con la Subgerencia Administrativa y Financiera convendrán un registro, inventario de todos los equipos de cómputo propiedad de la IPS

- ✓ Los equipos de cómputo que sean de propósito específico y su misión sea critica deben ubicarse en un área que cumpla con los requisitos de seguridad física, las condiciones ambientales y los controles de acceso necesarios para operación

[redacted]DEL MANTENIMIENTO DE LOS EQUIPOS DE CÓMPUTO

- ✓ Es responsabilidad de la oficina de Sistemas de Información programar y ejecutar el mantenimiento preventivo y correctivo de los equipos de cómputo con una periodicidad anual de manera que garanticen la conservación de los mismos

- ✓ En caso de que el mantenimiento preventivo y correctivo de los equipos de cómputo sea atendido por terceros oficina de Sistemas de Información deberá coordinar y velar por el cuidado y conservación del mismo.

- ✓ Ninguna dependencia de las IPS podrá realizar mantenimiento preventivo o correctivo a los equipos de cómputo.

[redacted] DE LA ACTUALIZACIÓN DE LOS EQUIPOS DE CÓMPUTO

- ✓ Es responsabilidad de la oficina de Sistemas de Información programar actualizaciones software de los equipos de cómputo que sean de propósito específico (Ofimática, Antivirus, Sistemas operativos etc.)

- ✓ Es responsabilidad de cada usuario realizar la actualización de antivirus del equipo de cómputo bajo su responsabilidad

[redacted] DE LA REUBICACIÓN DE LOS EQUIPOS DE CÓMPUTO

- ✓ La reubicación de los equipos de cómputo se hará siempre satisfaciendo las normas y procedimientos establecidos por la oficina de Sistemas de Información.

- ✓ La reubicación del equipo de cómputo se hará con la autorización de la oficina de Sistemas de Información, siempre y cuando en el lugar de reubicación existan los medios necesarios para la instalación del equipo.

13 CONTROL DE ACCESOS

[redacted]DEL ACCESO A LAS ÁREAS CRÍTICAS

- ✓ El acceso de personal a las áreas críticas se realizará de acuerdo a las normas y procedimientos establecidas por la oficina de Sistemas de Información, debido a la naturaleza de estos sitios se llevará un registro permanente del tráfico de personal, sin excepción alguna.

- ✓ La oficina de Sistemas de Información, deberá proveer la infraestructura de seguridad requerida con base en los requerimientos especifico de cada área.

- ✓ Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio critico estará sujeto a las que especifiquen las autoridades superiores a las IPS.

DEL CONTROL DE ACCESO AL EQUIPO DE CÓMPUTO

- ✓ Es competencia del usuario responsable de equipo de cómputo hacer buen uso de los equipos asignados.

- ✓ Cada usuario deberá acceder a los equipos de cómputo utilizando una cuenta de usuario y una clave

- ✓ Toda acción realizada usando claves de acceso es responsabilidad directa del usuario al que se le asignó la clave

- ✓ Toda clave o contraseña debe cumplir con el siguiente estándar o cumplir con los siguientes requisitos
- ✓ Debe tener al menos un carácter mayúscula
- ✓ Debe tener al menos un carácter minúscula
- ✓ Debe tener al menos un digito (0 a 9)
- ✓ Debe tener caracteres no alfabéticos (#$&*[{%)

DEL CONTROL DE ACCESO REMOTO AL EQUIPO DE CÓMPUTO

- ✓ Es competencia y responsabilidad de la oficina de Sistemas de Información proporcionar el servicio de acceso remoto.

- ✓ Para el caso especial de acceso a los servidores a terceros deberán ser autorizados por la oficina de Sistemas de Información.
- ✓ El acceso remoto que realicen las personas ajenas a las IPS deberán cumplir las normas que emite la oficina de Sistemas de Información.

DEL ACCESO A LOS SISTEMAS ADMINISTRATIVOS

- ✓ Tendrá acceso a los sistemas administrativos solo el personal de las IPS que por su cargo y funciones estén autorizados para ello y este acceso deberá hacerse cumpliendo todas las consideraciones establecidas en esta política

- ✓ El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad

- ✓ Los servidores donde se encuentran almacenada la información (Bases de datos) es prohibido el acceso excepto para la oficina de Sistemas de Información.

- ✓ El control de acceso a cada sistema de información será determinado por la unidad responsable de generar y procesar los datos involucrados

[redacted]DEL ACCESO A INTERNET

- ✓ De acuerdo con la Ley 1273 de 2009 y en concordancia con las políticas de seguridad informática la oficina de Sistemas de Información es la responsable de autorizar el acceso a páginas de carácter oficial.

- ✓ Se prohíbe el acceso a páginas de internet de contenido de redes sociales como Facebook, Twitter, Instagram, YouTube etc.

- ✓ De acuerdo a la libertad de investigación que tienen todos los usuarios de las Instituciones Prestadoras de Servicios de Salud –IPS, el material de investigación y consulta que se haga a través de los medios que las IPS deberá respetar la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección)

- ✓ La oficina de Sistemas de Información tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información y conservar información de tráfico

14 SOFTWARE

DE LA ADQUISICIÓN DEL SOFTWARE

- ✓ La oficina de Sistemas de Información es la responsable de verificar las condiciones y recursos que requiera el software, a adquirir, siempre que cumpla con las licencias y los requerimientos necesarios de desarrollo de sistemas de información a la medida.

- ✓ La oficina de Sistemas de Información de las Instituciones Prestadoras de Servicios de Salud propiciará la adquisición de licencias de sitio, licencias flotantes y licencias por empleado en cantidad para obtener ventajas significativas, así mismo le corresponde a esta oficina establecer las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

- ✓ La oficina de Sistemas de Información promoverá y respaldará que la consecución de software de dominio público provenga de sitios oficiales y seguros

DE LA INSTALACIÓN DEL SOFTWARE

- ✓ Inicialmente la protección lógica de los sistemas le corresponde a los usuarios responsables a quienes se les asigne usuario y contraseña y estos deben notificar a la oficina de Sistemas de Información, los periodos de vacaciones, licencias o finalización de contratos.

- ✓ Le corresponde a la oficina de Sistemas de Información permitir la instalación y supervisión de software básico con licenciamiento apropiado y acorde con la propiedad intelectual, para los equipos de cómputo, de telecomunicaciones, y cualquier dispositivo de las Instituciones Prestadoras de Servicios de Salud –IPS.

- ✓ La instalación de software que desde el punto de vista de la oficina de Sistemas de Información, pudiera poner en riesgo los recursos de las IPS no está permitida

- ✓ Para proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos los equipos que hacen parte de los activos de las IPS involucrados en los procesos dispongan de software de seguridad (antivirus, malware, antispam, firewall etc)

DE LA ACTUALIZACIÓN DEL SOFTWARE

- ✓ Toda actualización de software de equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario propuesto por la oficina de Sistemas de Información.

- ✓ Las actualizaciones de aplicaciones y software de uso común y/o más generalizados se llevarán a cabo de acuerdo a los planes desarrollados por la oficina de Sistemas de Información.

DEL SOFTWARE PROPIEDAD DE LAS INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD –IPS Y LA PROPIEDAD INTELECTUAL

- ✓ Todo sistema de información, software de propósito general, de propósito específico, software a la medida adquirido por la IPS sea por compra, donación o sesión será propiedad del mismo y mantendrá los derechos que la ley de propiedad intelectual le confiera

- ✓ Toda la información generada y procesada por el personal y los recursos informáticos de las IPS deberán ser resguardadas ya que se consideran como un activo.

- ✓ La oficina de Sistemas de Información, deberá promover y difundir los mecanismos de backup y respaldos de los datos almacenados en servidores y equipos de propósito general y específico.

- ✓ La oficina de Sistemas de Información, administrará y almacenará las diferentes licencias de software y vigilará las vigencias de las mismas.

15 POLITICAS GENERALES

- ✓ En la oficina de Sistemas de Información está totalmente prohibido fumar, consumir alimentos o bebidas, portar armas de fuego o corto punzantes, cambiar o desconectar equipos de cómputo sin previa autorización
- ✓ Es prohibido además modificar o alterar la configuración del equipo o del software instalado en los equipos de cómputo sin previa autorización
- ✓ Cada uno de los procesos deberá emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
- ✓ Todo el personal de la oficina de Sistemas de Información deberá comprometerse y comportase de acuerdo a los códigos de ética profesional, normas y procedimientos establecidos en la normatividad vigente en el país.
- ✓ Cualquier vulneración o violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la entidad y las normas.
- ✓ Todas las acciones en las que se comprometa la seguridad de la red de datos de las Instituciones Prestadoras de Servicios de Salud –IPS y que no estén previstas en esta política, deberán ser revisadas por la oficina de Gestión Humana.
- ✓ Los daños a la infraestructura tecnológica, red de telecomunicaciones, suplantación de sitios web, interceptación ilegitima de datos, acceso abusivo o cualquier otra forma de delito informático será sancionado conforme la Ley 1273 de 2009

16 CONCLUSIONES

El desarrollo de la presente monografía permitió examinar de forma detallada los diferentes riesgos y amenazas presentes en las Instituciones Prestadoras de Servicios de Salud en el departamento del Chocó, instituciones que ofrecen servicios de salud que en el desarrollo de su misión deben registrar, procesar y almacenar grandes volúmenes de información confidencial, producto de las atenciones médicas realizadas a los pacientes que diariamente consultan, gracias a la metodología MAGERIT y la herramienta EAR/PILAR que combinadas componen un instrumento eficaz en el análisis de riesgos informáticos presentes en ellas.

Este estudio permitió determinar e identificar las vulnerabilidades y amenazas que ocurren en muchos casos por la falta de conocimientos sobre los riesgos, la falta de políticas y controles informáticos que protegen de una manera eficiente los recursos informáticos con que cuentan las instituciones de salud, en ese sentido es necesario preparar y capacitar a todo el personal en aspectos relacionados con la seguridad informática y así mismo prepara a los usuarios en el cómo responder a los diferentes eventos que se puedan presentar en el desarrollo de la misión.

17 RECOMENDACIONES

El desarrollo del presente estudio contempla además recomendaciones a las Instituciones Prestadoras de Servicios –IPS las cuales ayudan a disminuir los riesgos y amenazas identificados.

- ✓ Se recomienda implementar las políticas de seguridad de la información basadas en la norma ISO 27001

- ✓ Se exhorta hacer revisiones periódicas de las políticas y controles de seguridad y comprobar el cumplimiento por parte de los usuarios internos

- ✓ Se recomienda hacer capacitaciones periódicas respecto la seguridad de la información a los empleados nuevos de la Institución

- ✓ Promocionar y divulgar esta política y los controles de manera que se convierta en una cultura por parte de los funcionarios de la institución.

.

.

.

18 BIBLIOGRAFÍA

AGUIRRE CARDONA, Juan David y Aristizábal Betancourt, Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda. [en línea]. Tesis profesional. Universidad tecnológica de Pereira, 2013. [Consultado: 12 mayo 2019]. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. [sitio web]. [Consultado: 12 junio 2019]. entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. Disponible en: http://www.cybsec.com

BUENAÑO QUINTANA, Jose Luis; GRANDES LUCES, Marcelo Alfonso, Planeación y Diseño de un SGSI Basado en la Norma ISO/IEC 27001 – 27002. Tesis de Titulo como Ingeniero de Sistemas. Quito – Ecuador: Universidad Politécnica Salesiana. 2009.

COLOMBIA. *MINISTERIO* DE *TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES*. Políticas de Seguridad de la Información. Bogotá: MINTIC, 05 noviembre [En línea], 2017. [Consultado: 10 de septiembre 2019]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009). Por la cual se modifica el código penal, se crea un bien jurídico tutelado-denominado “De la protección de la información y de los datos” y se preservan integralmente los sistemas los sistemas que utilicen las las tecnologías de información y las comunicaciones entre otras disposiciones. Bogotá: El Congreso, 2009.

ERB, Markus. Amenazas y Vulnerabilidades en Seguridad Informáticos. [sitio web]. [Consultado: 15 junio 2019]. 3ª edición. Madrid – España. Creative Commons Atribución-No Comercial-Compartir Obras Derivadas 2012. Julio, 2015. Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

FERNADEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A.. España. 1988. Página 105.

GARCÍA, Alfonso, CERVIGÓN Hurtado, María del Pilar, (2011). Seguridad Informática. España – Madrid. (Pág. 19 - 20).

Hilarion Novoa, Francisco Javier. Auditoría a la seguridad informática de los servicios de tecnologías de la información en la E.S.E Hospital San Francisco de Gachetá. [En línea] Tesis profesional. Universidad Nacional Abierta y a Distancia – UNAD, 2017. [Consultado: 25 de julio 2019]. Disponible en internet https://repository.unad.edu.co/handle/10596/12796

ICONTEC, Certificación del Sistema de Gestión de Seguridad de la Información con ISO/EIC 27001. [Sitio web], 2013. [Consultado: 2 de julio 2019]. Disponible en: https://www.icontec.org/

ISO 27001. [Sitio web]. 1a ed. Madrid – España. 2012. [18/Julio/2015]. [Consultado: 2 de septiembre 2019]. Disponible en: http://www.iso27000.es/sgsi.html

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software*, *6*(3), 25-34. [En línea], 2010. [Consultado: 26 de mayo 2019]. Disponible en: https://www.redalyc.org/pdf/922/92218768002.pdf

Metodología MAGERIT. [Sitio web]. 1a ed. Madrid – España. 2012. [18/Julio/2015]. [Consultado: 2 de septiembre 2019]. Disponible en: https://seguridadinformaticaufps.wikispaces.com/MAGERIT

PADILLA UBAQUE, Mario Andrés. Diseño del sistema de gestión de seguridad de la información para el instituto tolimense de formación técnica profesional- ITFIP para el departamento de sistemas, bajo la norma ISO 27001:2013 en la empresa Institución de Educación Superior – ITFIP del Espinal, Tolima. [En línea] Tesis de especialista. Universidad Nacional Abierta y a Distancia – UNAD, 2019. [Consultado: 10 de abril 2019]. Disponible en: https://repository.unad.edu.co/handle/10596/35860

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5). [En línea], 2015. [Consultado: 26 de mayo 2019]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Valencia-Duque, F. J., & Orozco-Alzate, M. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI-Revista Ibérica de Sistemas e Tecnologías de Información*, (22), 73-88. [En línea], 2017. [Consultado: 20 de mayo 2019]. Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006

ZAQUE GONZÁLEZ, Oscar Javier. Proyección Financiera y Tecnologíca requerida para la implementación del Sistema de Gestión de la Seguridad de la Información SGSI, norma ISO/IEC 27001:2013 en la empresa INDAIRE ingeniería SAS. [En línea] Tesis de especialista, Universidad Nacional Abierta y a Distancia – UNAD, 2016. [Consultado: 10 de marzo 2019]. Disponible en: https://repository.unad.edu.co/handle/10596/8595

ANEXOS

ANEXO A

FORMATO DE ENTREVISTA

ENTREVISTA

Fecha: _____

Nombre de la empresa: _____

Nombre del entrevistado: _____

Cargo: _____

OBJETIVO:

Conocer el funcionamiento de la oficina de Sistemas de Información en Salud de las Instituciones Prestadoras de Servicios de Salud del departamento del Chocó

1. ¿Cómo reciben la información médica de los pacientes atendidos diariamente?

   _____

   _____

   _____

   _____

2. ¿Dónde se registra los datos médicos de los pacientes que atienden?

_____

_____

_____

3. ¿Existe algún sistema de información donde se registran los datos de la historia clínica?

_____

_____

_____

4. ¿Cuántos computadores tiene la oficina de Sistemas de Información en Salud?

_____

_____

_____

5. ¿Los computadores de la oficina están en red?

_____

_____

_____

6. ¿Los computadores tienen contraseña para el ingreso?

_____

_____

_____

7. ¿Quiénes tienen acceso a los computadores de la oficina de Sistemas de Información en Salud?

   _____

   _____

   _____

8. ¿Según usted cuales son las deficiencias que actualmente existen en el manejo de las historias clínicas?

   _____

   _____

   _____

9. ¿Cuáles son los procesos que se llevan a cabo para el control de la información almacenada en las historias clínicas?

   _____

   _____

   _____

10. ¿Quiénes tienen acceso a las historias clínicas?

    _____

    _____

    _____

11. ¿Las historias clínicas son entregadas a los usuarios?

_____

_____

_____

12. ¿Qué criterios se utilizan para la entrega de las historias clínicas?

_____

_____

_____

13. ¿Cómo se garantiza el acceso en tiempo y forma oportuna al paciente y al médico?

_____

_____

_____

Fuente: Elaboración propia