DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA IPS MEDICSALUD DE LA CIUDAD DE VALLEDUPAR – CESAR.

RONAL LIÑAN CORDERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2017

DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA IPS MEDICSALUD DE LA CIUDAD DE VALLEDUPAR – CESAR

RONAL LIÑAN CORDERO

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

Directora de proyecto de grado
Ing. ERIKA VILLAMIZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2017

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, 4 de junio de 2017

DEDICATORIA

Primero que todo al Dios todopoderoso por haberme colmado de bendiciones y guiado en el camino para lograr mis objetivos a lo largo de mi formación académica profesional.

A mis padres María Cordero Rodríguez y Hermenegildo Liñan Arriaga, quien has sido una ayuda incondicional en mi vida logrando motivarme para seguir adelante y superarme cada día como personal en ser un gran profesional para contribuir en el bien para la familia y la sociedad. A mi hermanos Albeiro Enrique Liñan Cordero, Endy Rojas Liñan y Jaydith Liñan que también me aconsejaban siempre en lo bueno de crecer como personal y profesional y que han sido fundamentales en mi vida con el objetivo de alcanzar la meta y ser un ejemplo para la familia de esta generación y las siguientes generaciones.

AGRADECIMIENTOS

Agradecemos a Dios en primer lugar por haberme colmado de salud en este proceso de tiempo largo para culminar este gran proyecto, a la directora de proyecto de grado, a los asesores, por su responsabilidad, cuidado, dedicación y diligencia en las retroalimentaciones para que este trabajo se formulara de forma eficiente y adecuada, agradecemos a los tutores que con su trabajo laborioso nos guiaron en esta difícil tarea y por los cuales no nos sentimos trabajando en solitario y por último agradecemos a la administradora del sistema de información de la entidad IPS Medicsalud de Valledupar – Cesar, quien nos dio vía libre para tomar como punto de partida la entidad en la cual se desarrolló la tesis.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

ANEXOS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del centro de estudios.

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

AUDITORÍA: Serie de pasos organizados de una manera lógica, para obtener y analizar evidencia de una manera crítica y objetiva, con el objetivo de dar la dictamen del proceso o gestión evaluado.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CENTRO DE CÓMPUTO: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo Deben cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del ISO 27001. (ISO/IEC727000).

DISPONIBILIDAD: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

EQUIPO DE CÓMPUTO: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

IMPACTO: Cálculo de las consecuencias que pueden ocurrir al concretarse un riesgo o una amenaza.

INCIDENTE DE SEGURIDAD: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

INTEGRIDAD: es la protección de la exactitud y estado completo de los activos.

MAGERIT: Es una metodología de análisis y gestión de riesgos.

PERFILES DE USUARIO: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas.

PLAN: Enmarcado en el contexto de un SGSI, es la fase donde se define cuando, como y donde se realizaran los objetivos de seguridad propuestos, el tiempo que llevara su realización, se define el alcance para la implementación del SGSI.

POLÍTICA: La política del SGSI es un documento, con aprobación de las altas directivas enmarcado en la necesidad de un sistema de gestión para la seguridad de la información, contiene un conjunto de normas y prácticas para lograr los objetivos de seguridad de información de una entidad.

RECURSOS TECNOLÓGICOS: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la entidad MedicSalud.

RIESGO: Riesgo se puede definir como la posibilidad de que ocurra un evento que perturba el cumplimiento de un objetivo.

SALVAGUARDA: Es un mecanismo, política o cualquier otro medio utilizado para minimizar un riesgo.

SEGURIDAD: La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

SISTEMA DE INFORMACIÓN: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SGSI: Sistema de Gestión de Seguridad de la Información

TERCEROS: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos al centro de estudios.

VULNERABILIDAD: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño, según se puede deducir de lo expresado en la información contenida en el Observatorio Tecnológico de España 9

RESUMEN

En la actualidad los sistemas de información son una gran de ayuda para empresas públicas y privadas que permiten agilizar gran cantidad de tareas dentro de un centro de salud para pacientes. Como es el caso de la entidad IPS MedicSalud de Valledupar, el sistema de información tecnológica es fundamental para el desarrollo de labores administrativas ya que permite la comunicación interna y externa de funcionarios asistenciales y administrativos. Lastimosamente este sistema de información no cuenta con las medidas de seguridad y de control físico y lógicos adecuados.

Por lo antes expuesto, el presente proyecto, tiene como propósito mostrar el proceso del diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013, de la IPS MedicSalud de la ciudad de Valledupar- Cesar a través de unas fases estructuradas, partiendo del análisis de riesgos sobre los activos de información relacionados con la investigación a través de la metodología MAGERIT, las políticas de cumplimiento que se aplicaran a la empresa de salud, siguiendo con la identificación de controles implementados teniendo como referencia la ISO/IEC 27002:2013 y terminando con el plan de tratamiento de riesgos para mostrar y mejorar la seguridad del sistema de información brindándole disponibilidad, confidencialidad e integridad en todo momento.

PALABRAS CLAVE: SGSI, Seguridad informática, Análisis y Evaluación de Riesgos, Magerit, Políticas, ISO/IEC 27001:2013, ISO/IEC 27002:2013, Activo de información.

INTRODUCCIÓN

A medida de los años la tecnología ha ido evolucionando comenzando a implementarse en las grandes organizaciones, las actividades que se realizaban no eran tan especificas incluso se realizaban planeación y automatización de los datos.

Los riesgos que se ve enfrentada una empresa van desde la perdida de información de un computador hasta amenazas por internet que produce interrupciones en las operaciones, des configuración en los sistema de cómputo, mala reputación de una empresa.

La seguridad informática se ocupa de proteger los datos informáticos de una empresa entre sus principales funciones están confidencialidad, integridad, disponibilidad y autenticación de los datos, cifrado de la información. Los ataques informáticos son generados para robo, extorsión, terrorismo, vandalismo, espionaje entre otros.

La IPS MEDICSALUD no es ajena al complejo ataque informático tanto de agente externos como de interno, sino que se ve en la necesidad de implementar un SGSI basado en la ISO/IEC 27001 para controlar los ataques informáticos, asegurar el sistema de información y fortalecer el sistema empresarial.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

LA IPS MEDICSALUD es una entidad que presta servicios de salud, a todos los afiliados de la IPS. Para llevar a cabo la administración de los servicios de los afiliados cuenta con un software informático para la gestión de la información.

En la institución prestadora de servicio de salud IPS MEDICSALUD no se le presta atención en cuanto a la seguridad informática por lo que no cuenta con un diseño y una estructura para su sistema de información a la vez no está orientado por metodologías, técnicas y normas estandarizadas lo cual no asegura sus datos para un buen proceso final.

El sistema de información que maneja la IPS se encarga de sistematizar las historias clínicas y la agenda medica de los pacientes pero no cuenta con una política de seguridad informática buena para la integridad, disponibilidad y confidencialidad de la información. Los usuarios que administran el sistema no le presta atención algún evento sospechoso que se presente en el sistema de información debido al poco conocimiento que tiene acerca de la política de seguridad informática solo se limitan a cumplir su labor.

Teniendo en cuenta que uno de los activos más importante en la IPS MEDICSALUD es la información se debe implementar barreras de seguridad que no solo asegure los equipos físicos si no también se apliquen en la seguridad lógica en los programas.

El administrador del sistema informático solo se dedica hacer copia de seguridad periódicamente pero no cuenta con técnicas o procedimiento para evaluar los riesgos que se presente en su sistema de información y tampoco cuenta con herramientas cuando se presente un fraude informático.

Para lograr el aseguramiento de la información se deben implementar medidas de seguridad informática acerca de los procedimientos y normas que trabajen en las estrategias sobre los aspectos de la seguridad. La base de este proceso radica en el análisis profundo de cada riesgo y su clasificación por niveles esto se puede producir a partir del impacto que genera cada uno de ellos en la información de la empresa.

La implementación del SGSI basado en la norma ISO 27001 en la entidad garantiza la disponibilidad, integridad y confidencialidad de la información. La propuesta de esta norma para su posterior aplicación facilitara a la entidad el control seguro de la información para tener un rendimiento óptimo y un porcentaje mínimo de errores.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la IPS MEDICSALUD de Valledupar Cesar puede conocer su estado actual de la seguridad de la información?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar un diagnóstico del estado actual de la seguridad de la información basada en la norma ISO 27001:2013 que le brinde a la IPS MEDICSALUD el contexto de cómo está tratando la seguridad de la información y las mejoras que se pueden implementar en sus procesos.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los procedimientos actuales de la IPS MEDICSALUD para la ejecución de sus actividades.
- Identificar y valorar los activos de información de la IPS MEDICSALUD.
- Identificar los posibles riesgos de los activos de información, sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos.
- Presentar el diagnóstico del estado actual de la seguridad de la información de la IPS MEDICSALUD con sus respectivas recomendaciones de mejora y de implementación basado en la norma ISO 27001:2013.

3. JUSTIFICACIÓN

El diseño de un sistema de información basado en el estándar IEC/ISO 27001 dará las condiciones necesarias para la gobernabilidad, oportunidad y viabilidad para la seguridad de la información con el enfoque para proteger la información de la empresa tanto en la parte financiera, administrativa, operativa de la empresa y con ella asegurar el cumplimiento del objetivo.

El sistema de gestión de la seguridad de la información muestra a la empresa el compromiso que tiene con la seguridad de la información lo que provee los elementos requeridos para administrar los riesgos de forma eficiente que atente contra el sistema de información. Lo cual vemos que las partes interesadas haya mucha confianza y así se fortalezca y se mantenga la entidad.

El sistema de gestión de seguridad de la información ayudara a la entidad a asociar de forma efectiva los riesgo asociados identificando las amenazas que comprometa la confidencialidad, integridad y disponibilidad que se presente en la IPS MEDICSALUD lo cual reduciría el impacto en caso de manifestarse una vulnerabilidad.

La entidad prestadora de servicio de salud MedicSalud requiere de mucho control en el aspecto de la seguridad de los activos informáticos así como de unas políticas bien fijadas en la gestión de información de datos y usuarios que sean precavidas a la hora del acceso en los entornos tecnológicos.

Se realizó una indagación acerca del tema de la seguridad informática que hay en la entidad se determinó que los usuarios tanto en la parte asistencial como administrativa tiene poco conocimiento acerca del tema lo cual genera una afectación tanto económica como organizacional en la entidad de salud debido a una mala gestión de seguridad de los activos informáticos que es la núcleo primordial de la empresa que es la fortaleza y sustento de ella.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

4.1 ALCANCES

El alcance del proyecto abarca el diagnostico de un sistema de gestión de la seguridad de la información para la entidad Medicsalud el cual está orientado a cubrir la infraestructura tecnológica que soporta el sistema, la funcionalidad del mismo y a los usuarios del sistema.

4.2 DELIMITACIÓN

El proyecto se llevará a cabo en la ciudad Valledupar- Cesar para la IPS MEDICSALUD durante el periodo de tiempo del año entre 2016 y 2017, el diagnóstico del SGSI será entregado, dicho sistema está basado en la norma internacional ISO 27001:2013.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

El Sistema de Gestión de Seguridad de la Información (SGSI) es un sistema de gestión, el cual su estructuración se ve basada en seguir los lineamientos de la Norma ISO/27001 Anexo A y apropiarse de las recomendaciones establecidas en la Norma, la Norma ISO/27002 es también parte importante en el establecimiento del SGSI ya que en dicha Norma se describe en un mayor detalle los controles sugeridos en el Anexo A de la Norma ISO/27001. El SGSI permite a través de la implementación de una serie de actividades bien formadas tener un control sobre los activos de información que se han identificado como importantes para las actividades y procesos empresariales, y a partir del control obtenido poder mitigar el riesgo que recae sobre los activos de información.

Según la Organización Internacional de Estandarización – ISO, en Colombia hay 82 compañías certificadas en ISO/IEC 27001.

Igualmente, se puede comparar el comportamiento de Colombia frente a otros países según este número de certificaciones obtenidas, notándose que a nivel suramericano Colombia ha mostrado un adelanto importante en la aplicación de la norma, estando al nivel de Brasil y por encima de países como Argentina y Chile, confirmando así mismo que las grandes economías mundiales apuestan seriamente por la obtención de este tipo de certificaciones, encontrando así los números que se muestran en la tabla número 1.

Tabla 1. Relación de países certificados en ISO/IEC 27001

Número de certificaciones obtenidas en ISO/IEC 27001 a 2013	
País	**Total**
Japón	7084
India	1931
Reino Unido	1923
China	1710
USA	566
Colombia	82
Brasil	82
Argentina	40
Chile	24

Fuente: El autor. Datos obtenidos del modelamiento de procesos basados en el grupo de normas internacionales iso/iec 27000. p 25.

La Compañía UNE EPM Telecomunicaciones es la primera Organización en Colombia y sexta en América Latina en certificarse en ISO/IEC 27001:2005 el 19 de Octubre de 2009.[1]

En la región, algunas organizaciones son conscientes de la necesidad del modelo, sin embargo no es posible determinar con exactitud el número de empresas certificadas en ISO/IEC 27001 en Risaralda por cuanto es difícil encontrar información en entidades certificadoras como ICONTEC la cual no ofrece esta información a través de su página web, así como tampoco el Registro Internacional de organizaciones certificadas en ISO 27001 a nivel mundial al que se accede por la página web www.iso27001certificates.com, ya que se encuentra fuera de servicio.

Actualmente se ha desarrollado estudio e investigaciones y trabajos de grado acerca de la seguridad informática. Los casos que se han desarrollado serian como por ejemplo la Universidad Católica de Pereira cuya política se ha desarrollado a partir de un trabajo de grado, también se encuentran la elaboración de políticas de seguridad para organizaciones como Apostar, de igual manera el CDA de Cartago y en general mucha documentación sobre el tema y sobre los diferentes métodos de detección y ataques a sistemas informáticos.

[1] UNE Telecomunicaciones. Disponible en: http://www.une.com.co/nuestracompania/index.php?option=com_content&task=view&id=444

En el proyecto denominado “SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO presentado por los estudiantes: Yezid Camilo Guerrero Angulo y Robert Marcelo Tabango. En el planteamiento del problema se describe que el manejo de controles de acceso físico aislados y no suficientes para la seguridad de la unidad informática y telecomunicaciones de la universidad de Nariño facilitan el acceso a los recursos que esta concierne, e igualmente se indica que el acceso de usuarios a la red inalámbrica sin ningún tipo de control debido a que no se cuenta con una adecuada configuración de la misma, no favorece el buen desempeño de la misma, por lo cual autores de la propuesta, sugieren un diseño de gestión de la seguridad de la información que permita corregir estas falencias para favorecer el adecuado funcionamiento de esta unidad como de fortalecer la seguridad de la red inalámbrica.

Los autores de este proyecto concluyen que la aplicación de la norma ISO 27001 y 27002 permiten alcanzar un alto grado en la seguridad de la información independientemente del tamaño de la empresa.

En el proyecto de grado presentado por: Fernando Santiago Martínez, que se denomina “APOYO AL PROCESO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA ALCALDÍA DE PASTO BASADO EN LA NORMA ISO 27001:2013 Y BAJO LA DIRECTRIZ DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA VERSIÓN 3.1”. En el planteamiento del problema se indica que la alcaldía de Pasto no cuenta con un SGSI, el cual es un requerimiento del Gobierno Nacional, quien ha implementado la estrategia del gobierno en línea para los organismos y entidades que conforman las ramas del poder público. Describe que la alcaldía no cuenta con un sistema de seguridad definido que permita respaldar con documentación suficiente los procesos que se desarrollan al interior de esta.

Las conclusiones a las que llegó el autor son las siguientes:

- Después de identificar las vulnerabilidades y controles presentes en la Alcaldía de Pasto, se concluye que no cuenta con las normas de seguridad establecidas para salvaguardar los recursos y la información lo cual esta afecta la continuidad de sus labores.

- Es necesario que la documentación de los procesos estén al día y que los controles de seguridad requeridos se pongan en marcha. Igualmente se hace necesaria la concientización del uso de los recursos informáticos al personal que labora en la alcaldía para evitar daños al sistema.

Este proyecto se tiene en cuenta por la caracterización de activos y valoración de activos.

- Diseño de un SGSI para una compañía de seguros.

La Superintendencia de Banca, Seguros y AFP, en el 2009, elaboró la circular G140, que estipula que todas las empresas peruanas que son reguladas por este organismo deben

contar con un plan de seguridad de información. La presente tesis busca diseñar un sistema de gestión de seguridad de información para una compañía de seguros que cubra lo que pide la circular para evitar problemas regulatorios con este organismo.[2]

Cabe resaltar que muchas compañías a nivel mundial, sin importar el nicho del mercado al cual están suscritas deben tener un sistema de gestión de seguridad de la información, para poder salvaguardar el activo más importante con el que trabajan, que es la información.

En esta tesis diseñan un SGSI para poder tener una base que se pueda implementar en cualquier compañía de seguros. Cabe resaltar que se hace bajo estándares y buenas prácticas que indican qué es lo que se debe realizar, pero no especifican cómo se deben implementar los controles. Estos van a depender de la necesidad de la empresa y de la inversión que desee realizar en temas de seguridad, con lo que se puede afirmar que lo expuesto en la tesis es una forma de cómo se puede diseñar un SGSI.

5.2 MARCO CONTEXTUAL

5.2.1 Nombre de la empresa. IPS Medicsalud

5.2.2 Reseña Histórica. En el mes de Enero de 2014, nació la idea de negocio de un ingeniero, impulsado en ese entonces por la gerente de la empresa para la cual laboraba, la cual fue montar una empresa prestadora de servicios de salud, pero únicamente quisieron iniciar con un punto para toma y recolección de muestras clínicas; para lo cual solo dispusieron de una pequeña sala con una camilla, una silla para toma de muestra, algodón, alcohol, jeringas, y tubos para recolectar las muestras.
Al cabo de 4 meses vieron la necesidad de ampliar su punto de toma de muestras y convertirlo en un centro de diagnóstico para los servicios de laboratorio clínico de primer nivel de complejidad y medicina general al servicio de la comunidad de la ciudad de Valledupar.

En el 2015, en vista de las necesidades de nuestros clientes, se determinó ampliar los servicios de salud, incluyendo dentro de estos Salud oral e higiene dental, junto a rehabilitación oral, odontología general, psicología y nutrición.

Para el Año 2016 se decide incursionar en el campo de la salud ocupacional y/o laboral debido a las presentes necesidades de nuestros clientes y a sus requerimientos, se inicia con la prestación de servicios en medicina laboral y del trabajo, proyectando para el 2017

[2] Tesis sobre diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/933/AMPUERO_CHANG_CARLOS_INFORMACION_COMPA%C3%91IA_SEGUROS.pdf?sequence=1&isAllowed=y

la implementación de los mismos con equipos automatizados dentro de las instalaciones de Medicsalud ips s.a.s.

MEDICASALUD IPS SAS, desde su inicio ha sido una entidad de carácter privada que conjuga dentro de todos sus aspectos la sensibilidad y el carácter humano durante los procesos de atención, esto por medio de su gran equipo de trabajo integrado por profesionales quienes garantizan la calidad del servicio y la responsabilidad en el mismo, así como la confiabilidad y confidencialidad de los diagnósticos, mediante un control interno y externo estricto, que permite brindar a la comunidad un servicio seguro.

5.2.3 Misión. Somos una entidad dedicada a la prestación de servicios de salud de primer y segundo nivel, encaminadas a facilitar el acceso de la misma a todas las personas que lo requieran, por lo cual nuestra actividad misional no se encuentra enfocada únicamente en la asistencia de servicios de salud básicos a comunidades específicas, sino a la población en general, por lo que se procura brindar un valor agregado, incluyendo dentro del desarrollo de los procesos de la institución la prevención de las enfermedades por medio de brigadas, campañas y charlas permanentes a los diversos grupos poblacionales; acerca de las primeras causas de morbilidad que aquejan a los habitantes de las todas las localidades.

5.2.4 Visión. Ser la institución colombiana líder en prestación de servicios de salud con calidad, favoreciendo el mayor número de habitantes con oportunidades y actividades que contribuyan al mejoramiento de su calidad de vida, al avance sostenible individual y de su entorno, contribuyendo a la erradicación de la pobreza, el analfabetismo, la desnutrición, y el desempleo, para la máxima satisfacción de las personas y la consecución de la solidez en las familias. Siendo líder en la prestación del servicio al año 2018, a través de innovaciones con alto nivel de excelencia y calidad en el ámbito Municipal y Regional.

5.2.5 Política de seguridad del paciente. Medicsalud ips s.a.s, gestiona permanentemente procesos integrales y articulados, declarando su compromiso con la ATENCIÓN SEGURA para los pacientes a través de acciones de identificación, análisis para manejo del riesgo y del evento adverso; generando procesos seguros en fomento de una cultura organizacional que incentiva y cree en sus colaboradores. el desarrollo de hábitos y practicas seguras, haciendo del aprendizaje organizacional el eje para lograr la excelencia en la prestación de los servicios a nuestros usuarios.

5.2.6 Política de calidad. MEDICSALUD IPS S.A.S, está comprometida en garantizar la calidad de los servicios que presta, así mismo busca centrar todos sus esfuerzos en brindar una atención integral en salud, promoviendo el mejoramiento continuo en cada una de las especialidades que ofrece a la comunidad, con el fin de llenar las expectativas de los diferentes entes interesados tanto los beneficiarios como entidades de vigilancia y control, los proveedores, clientes contratantes, colaboradores, socios, visitantes y población en general; con el propósito de mostrar tanto excelencia operativa y profesional como sentido humanitario, enseñando compromiso ante la responsabilidad social y la satisfacción de las necesidades de los usuarios por lo que garantizamos un servicio de forma eficiente, oportuna, con amabilidad, honestidad y eficiencia.

5.3 MARCO TEÓRICO

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones que demandan un mayor esfuerzo para garantizar la seguridad, a las constantes amenazas que hoy en día atentan contra la seguridad de la información que cada vez son más especializadas, complejas y avanzadas, y a la normatividad vigente que regula y exige una mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros de las personas, la organizaciones deben contar con un modelo o Sistema de Gestión de Seguridad de la Información basado en estándares de seguridad reconocidos a nivel mundial, con el propósito de poder establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, que le permiten gestionar de manera adecuada los riesgos que puedan atentar contra la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio de la seguridad de la información.

La Aplicación de modelos y estándares dentro de lo concerniente a la seguridad de la información se encuentra enmarcada dentro de una norma internacional puntual denominada ISO/IEC 27001 la cuál es un estándar para la seguridad de la información (Information technology - Security techniques – Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos. Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas

de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.[3]

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con 17 orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Para efectos de tener claro los diferentes conceptos que se enuncian en este marco teórico, en el capítulo "5.3. MARCO CONCEPTUAL" se encuentran el glosario de los términos con sus respectivas definiciones, los cuales son utilizados a lo largo del presente trabajo de grado.

5.3.1 Seguridad de la información. La Seguridad de la Información, de acuerdo a la norma ISO 27000:2014, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.[4]

De acuerdo a la Asociación Española para la Calidad, la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada.

5.3.2 Gestión de seguridad de la información. La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática,

[3] Tesis sobre implementación de un sistema de gestión de seguridad informática en la confederación de cámaras de comercio - confecámaras. Disponible en: http://repository.unad.edu.co/bitstream/10596/3653/3/9818019.pdf
[4] ISO/IEC 27000:2014, Tercera Edición, Pág. 4

estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías9.

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

5.3.3 Sistema de gestión de seguridad de la información. Primero se define como SGSI que es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.[5]

El propósito del sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

[5] GUERRERO, Yezid. sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño. Pasto, 2014. p56.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

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

- **Plan (planificar):** establecer el SGSI - es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

- **Do (hacer):** implementar y utilizar el SGSI - es una fase que envuelve la implantación y operación de los controles.

- **Check (verificar):** monitorizar y revisar el SGSI - es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

- **Act (actualizar):** mantener y mejorar el SGSI - en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

La implementación de un Sistema de Gestión de Seguridad de la Información, le provee a las organizaciones un proceso de mejora continua que asegura la debida y continua gestión de los riesgos de seguridad y permite la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de información de la organización.

5.3.4 Serie iso/27000. Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última

edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).[6]

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.[7]

Teniendo en cuenta que en toda organización el propósito fundamental es identificar y satisfacer las necesidades y expectativas de sus clientes empleando normas y estándares que permitan asegurar la información y la calidad de la misma, es importante el empleo de normas y estándares las cuales son un conjunto de mejores prácticas recomendadas para desarrollar, implementar y mantener especificaciones para los diferentes Sistemas de Gestión de la
Seguridad de la Información (SGSI).

Dentro de los beneficios con la utilización de estas normas tenemos:

- ✓ Reducción del impacto de los riesgos, que en caso de materializarse las amenazas, puedan representar pérdidas (de capital, de facturación, de oportunidades de negocio, por reposición de los daños causados, reclamaciones de clientes, sanciones legales, etc), al aumentar la seguridad efectiva de los sistemas de información, con una mejor planificación y gestión de la seguridad.
- ✓ Garantías de continuidad del negocio basándose en un plan de contingencias.
- ✓ Mejora de la imagen de la organización y aumento del valor comercial de la empresa y sus marcas.
- ✓ Incremento de los niveles de confianza de clientes, proveedores, accionistas, entre otros.
- ✓ Mejora del retorno de las inversiones, al tener mejor criterio según los riesgos residuales aceptados y ahorro de tiempo y dinero al reducir o eliminar actividades o inversiones de escasa o nula aplicabilidad a los niveles de riesgo identificados en el negocio.
- ✓ Mejora continua a través de la metodología PDCA (Planificar, Hacer, Verificar y Actuar).
- ✓ Mejorar el conocimiento de los sistemas de información, sus problemas y los medios de protección.
- ✓ Mejorar la disponibilidad, integridad y confidencialidad de los datos que existan en la organización.

[6] Estándar Iso. Disponible en: http://www.iso27000.es/iso27000.html

[7] Estándar Iso. Disponible en: http://www.iso27000.es/iso27000.html

- ✓ Protección del activo más importante para cualquier organización, la información.
- ✓ La aplicación de estándares puede significar la diferenciación y competitividad de la organización ante el mercado nacional e internacional.
- ✓ Reducción de costos en caso de presentarse pérdida de información.

Una adecuada gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y basado en objetivos claros de seguridad, este proceso es el que conforma un Sistema de Gestión de Seguridad de la Información (SGSI).

Actualmente existen una serie de normas que proporcionan un marco de gestión para la seguridad de la información, las cuales pueden ser utilizadas por toda organización a nivel nacional sin importar su naturaleza y propósito. Estas normas son las que componen la serie ISO/IEC 27000 por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), donde se indica como estructurar e implantar un Sistema de Gestión de Seguridad de la Información basada en ISO 27001.

5.3.5 Iso/27001. Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.[8]

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

5.3.6 Activo de la información. Las organizaciones poseen información que deben proteger de amenazas y riesgos, es por ello que todo lo que se considere de valor se considera un activo para la organización y por tanto debe protegerse, tales como;

[8] Estándar Iso. Disponible en: http://www.iso27000.es/iso27000.html

información física y digital, software, hardware, servicios de información, servicios de comunicaciones, servicios de almacenamiento, personas, imagen y reputación.

5.3.7 Identificación de Amenazas y Vulnerabilidades. En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

5.3.8 Las Amenazas. Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.[9] En esta definición, los actores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural. En su libro Information Segurity Risk Analysis (Welter, 2001). Thomas Welter plantea que una amenaza puede significar muchas cosas, dependiendo el texto donde se ubique.

Clasificación de las amenazas. Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. En consecuencia, también difieren los métodos para estimar su posibilidad de ocurrencia:

- Amenazas Naturales
- Amenazas a Instalaciones
- Amenazas Humanas
- Amenazas Tecnológicas
- Amenazas Operacionales
- Amenazas Sociales

5.3.9 Las Vulnerabilidades. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas. Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daños. Simplemente son condiciones que pueden ser una amenaza que afecte a un activo. Las vulnerabilidades se pueden clasificar como:

- Seguridad de los Recursos Humanos
- Control de Acceso
- Seguridad Física y Ambiental

[9] El portal de Iso 27001 en español. Disponible en: http://www.iso27000.es/glosario.html

- Mantenimiento, desarrollo y adquisición de sistemas de información.
- Gestión de operaciones y comunicación

Una vez clasificadas las vulnerabilidades, por cada una de ellas, se deberá evaluar la posibilidad de que sean explotadas por la amenaza. Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para causar incidentes que pueden dañar los activos.

5.3.10 Análisis y gestión de riesgos. En lo relacionado con la tecnología, generalmente el riesgo es planteado solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida. Según la Organización Internacional (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños". En esta definición se identifican varios elementos que deben ser comprendidos adecuadamente para percibir integralmente el concepto de riesgo y los procesos aplicados sobre él. Dentro de estos elementos están la probabilidad, amenazas, vulnerabilidades, activos e impactos.

5.3.11 Análisis de riesgos. El primer paso en la gestión del riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.[10] Existen varias metodologías para evaluar el riesgo, sin embargo el punto de partida nace de la identificación de activos de información, los cuales son todos los recursos involucrados en la gestión de la información. De una adecuada gestión de riesgos depende que una empresa pueda identificar las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, en la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en la información.

El objetivo general del análisis de riesgos, es identificar sus causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para que se pueda tener información suficiente al respecto, optando así por un adecuado diseño e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados, en los diferentes puntos de análisis.

Otros objetivos específicos del proceso de análisis de riesgos son: analizar el tiempo, esfuerzo, recursos disponibles y necesarios para atacar los problemas; llevar a cabo un minucioso análisis de los riesgos y debilidades; identificar, definir y revisar los controles de seguridad; determinar si es necesario incrementar las medidas de seguridad; y la

[10] Gestión de Riesgo en la Seguridad Informática. Disponible en: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

identificación de los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente.

Algunos aspectos que se debe tener en cuenta antes de realizar el análisis de riesgos son los siguientes: las políticas y las necesidades de la organización, los nuevos avances tecnológicos y la astucia de intrusos expertos, los costos vs la efectividad del programa de mecanismos de control a desarrollar, la junta directiva de la organización debe incluir presupuesto, los gastos necesarios para el desarrollo de programas de seguridad. Otro aspecto que se debe tener en cuenta es la sobrecarga adicional que los mecanismos y contramedidas puedan tener sobre el entorno informático, sin olvidar los costos adicionales que se generan por su implementación.

El análisis de riesgos utiliza el método matricial llamado MAPA DE RIESGOS, para identificar la vulnerabilidad de un servicio o negocio a riesgos típicos. El método contiene los siguientes pasos: la localización de los procesos en las dependencias que intervienen en la prestación del servicio y la localización de los riesgos críticos y su efecto en los procesos del Negocio.

5.3.12 Metodología de análisis y gestión de riesgos de los sistemas de información (magerit). Es una metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.[11] Se adoptó como el método formal para analizar los riesgos que soportan los Sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse en la mejora de su control.

Finalidad: el análisis y gestión de los riesgos es uno de los aspectos claves por medio del cual se regula el Esquema Nacional de Seguridad en el ámbito de la administración de la Administración Electrónica en España, que tiene la finalidad de satisfacer el principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT es utilizado por aquellas personas que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

[11] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WA1NduB97IU

5.3.13 Políticas de la seguridad informática. Las políticas de seguridad de la información tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y las personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.

Este dominio articula los objetivos del negocio y la razón social de la pyme, empresa u organización con las necesidades de la seguridad informática, para salvaguardar los datos, registro y demás información confidencial que se desee proteger, por lo tanto el documento debe contemplar todos los niveles y acciones a seguir en determinado caso:

- Clasificación de la información
- Naturaleza del negocio
- Información de uso interno y externo
- Necesidades técnicas y operativas

Las políticas deben surgir a partir del análisis y administración del riesgo, deben ser claras y especificas quien es la autoridad que asuma las medidas disciplinarias y evaluación de la situación, estas deben ser promovidas y dadas a conocer a todos los empleados de la organización.

5.4 MARCO CONCEPTUAL

Activo: Cualquier cosa que tiene valor para la organización.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad: Protección de la información respecto a modificaciones no autorizadas, tanto a la almacenada en los elementos computarizados de la organización como la usada como soporte. Estas modificaciones pueden llevarse a cabo de manera accidental, intencional, o por errores de hardware-software.

Disponibilidad: Propiedad que define que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Autenticidad: Garantía que el usuario autorizado tiene para usar un recurso y que no sea suplantado por otro usuario.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (accountability), no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información: SGSI parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[12]

Control de acceso: Posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización.

Disponibilidad de los recursos y de la información: Protección de los elementos que poseen la información de manera que en cualquier momento, cualquier usuario autorizado pueda acceder a ella, sin importar el problema que ocurra.

Auditoría: Capacidad para determinar todos los movimientos del sistema, como accesos, transferencias, modificaciones, etc., en el momento en que fueron llevados a cabo (fecha y hora).

Vulnerabilidad: Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño del sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.[13]

Amenaza: Será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. De esta manera, el punto más débil.

Mecanismos de seguridad: Todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática.

[12] Sistema Integrado de Gestión SIGUD de la universidad distrital francisco jose de caldas. Disponible en: http://comunidad.udistrital.edu.co/sigud/subsistema-de-seguridad-de-la-informacion-sgsi/

[13] Tesos sobre protocolo de políticas de seguridad informática para las universidades de Risaralda. Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1

Consistencia: Capacidad del sistema de actuar de manera constante y consistente, sin variaciones que alteren el acceso a la información.

Impactos: Son las consecuencias de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financiaras, económicas, tecnológicas, físicas, entre otras.

Probabilidad: Para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada.

Magerit: La metodología magerit, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

5.5 MARCO LEGAL

Las leyes colombianas aplicables a los delitos informáticos ocurridos en Colombia

Ley 1273 del 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.[14]

Actualización agosto 2013

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

Ley 1581 de 2012 (Protección de Datos Personales): Es una ley que complementa la regulación vigente para la protección del derecho fundamental que tiene todas las

[14]Ley 1273 del 2009, El congreso de Colombia. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación.[15]

Ley 1341 del 30 de julio de 2009: Con la que se busca darle a Colombia un marco normativo para el desarrollo del sector de Tecnologías de Información y Comunicaciones (TIC), promueve el acceso y uso de las TIC a través de la masificación, garantiza la libre competencia, el uso eficiente de la infraestructura y el espectro, y en especial, fortalece la protección de los derechos de los usuarios.[16]

Ley Estatutaria 1266 del 31 de diciembre de 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Objeto. tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.[17]

Ley 1273 del 5 de enero de 2009: por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 599 de 2000: Los delitos consagrados en el Código Penal Colombiano, tienen plena aplicación, bajo el entendido en que se cumplan las condiciones establecidas para cada acto criminal, sin importar si se comete en medios tradicionales o electrónicos.[18]

[15] Ley 1581 de 2012 Decreto 1377 de 2013, Colombia Digital, Agosto 29, 2013. Disponible en: http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

[16] Ley1341 del 30 de julio de 2009, Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

[17] Ley Estatutaria 1266 del 31 de diciembre de 2008, El congreso de Colombia. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[18] Ley 599 del 2000, El congreso de Colombia. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

6. MARCO METODOLÓGICO

6.1 METODOLOGÍA DE LA INVESTIGACIÓN

En el desarrollo de este proyecto se utilizara la metodología de investigación de tipo cuantitativa porque se basa en hacer la medición de los análisis y riesgo debido a la confidencialidad, disponibilidad e integridad de la información.

Se analizará paso a paso cuales son las necesidades en el área de informática en cuanto a seguridad física, seguridad interna, seguridad externa, seguridad lógica, seguridad perimetral, elementos de control para la seguridad del hardware y software, alcances, análisis de riesgos, amenazas, posibles ataques y políticas de seguridad.

Este proceso se lo realiza mediante observación directa y encuestas a empleados.

La encuesta aplicada a los empleados de la IPS MedicSalud, pretende medir las buenas prácticas de ellos para el manejo de la información, el conocimiento de los riesgos y el conocimiento sobre la seguridad de la información.

Tanto la observación directa como la aplicación de la encuesta están encaminadas a medir el grado de conocimiento sobre la importancia de seguridad en el manejo de la información y la importancia del seguimiento y aplicación de políticas de seguridad.

Una vez analizada la información se propondrá políticas de seguridad teniendo en cuanta la Norma ISO/IEC 27001 para disminuir los riesgos en cuanto a la seguridad de la información.

6.1.1 Población y muestra. Para la encuesta de los empleados, la población de estudio está conformada por el personal que labora en la IPS MEDICSALUD de Valledupar.

En el presente proyecto abarca la población de estudio conformado por el personal que labora en la IPS MedicSalud quien se verá beneficiada con la prestación de un servicio eficiente y seguro dándoles tranquilidad a los usuarios que la utilicen.

Para el estudio de la referencia se tomó como muestra aquellos empleados ubicados en áreas sensible en desarrollo de las actividades diarias dentro de la IPS (serán escogidos de forma intencional).

6.1.2 Fuentes de recolección de información. La información que se pretende recopilar se obtendrá a través de entrevistas y listas de chequeo para conocer a

profundidad las falencias dentro de la organización estas se aplicaran a los empleados dentro de la muestra.

6.2 TIPO DE INVESTIGACIÓN

La investigación utiliza un método deductivo y analítico y se clasifica como de tipo descriptiva y explicativa.

Es descriptiva porque trata de describir de cómo se lleva a cabo el proceso de análisis y evaluación de los riesgos haciendo uso de la metodología Magerit.

6.3 METODOLOGÍA DE DESARROLLO

Para el desarrollo del proyecto los objetivos se deben cumplir de acuerdo a unas actividades que se deben realizar de acuerdo a cada objetivo que son:

A. Identificar los procedimientos actuales de la IPS MEDICSALUD para la ejecución de sus actividades.

Actividades

- Entrevistar a los empleados con acceso a los activos e información cuestionándoles acerca que procesos o funciones realizan en la entidad de salud de acuerdo con el sistema de información.

B. Identificar y valorar los activos de información de la IPS MEDICSALUD.

Actividades

- Para la determinación de los activos se hace una visita a la IPS y preguntarle al administrador e ingeniero cuales activos maneja la empresa para la gestión del sistema de información
- Para la valoración de los activos se aplicara la metodología Magerit

C. Identificar los posibles riesgos de los activos de información, sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos.

Actividades

- Realizar visita a la IPS para conocer donde están ubicados los empleados que manejan activos de información

- Entrevistar a los empleados con acceso a los activos e información
- Realizar pruebas de vulnerabilidades a los activos informáticos de la empresa.
- La aplicación de la metodología Magerit determino la matriz de riesgos de los activos para ver el impacto y la probabilidad de riesgo para así determinar controles de seguridad

D. Presentar el diagnóstico del estado actual de la seguridad de la información de la IPS MEDICSALUD con sus respectivas recomendaciones de mejora y de implementación basado en la norma ISO 27001:2013.

Actividades

- Revisar el análisis de vulnerabilidades realizado con anterioridad.
- Mediante la implementación de medidas de seguridad permitimos la minimización de riesgos de los activos de información.
- De acuerdo a la metodología Magerit establecemos los controles para prevenir riesgo para tener una buena gestión de riesgos con sus recomendaciones.

7. DESARROLLO DEL PROYECTO

7.1. PROCEDIMIENTOS ACTUALES DE LA IPS MEDICSALUD

Los procedimientos actuales que se desarrollan en la IPS MedicSalud se van a explicar en una tabla de forma detallada y clara como se muestra a continuación:

Tabla 2. Procedimientos de la IPS Medicsalud

Procedimientos	Cargo del responsable	Descripción
Creación de empresas, usuarios profesionales.	Administradora del sistema	• Se encarga de crear las empresas con el que la IPS realiza convenios. • Crear los profesionales que prestan el servicio dentro de su Entidad. • Asignar los datos de usuario y contraseña a los diferentes profesionales relacionándolos con su número de identificación, para que puedan ingresar al software SISCLINIC ya sean (SIAU, médicos, facturación, administrador). • Revisión de los procesos realizados por todos los perfiles (SIAU, médicos, facturación, administrador).
Creación de tarifas para las empresas convenidas	Administradora del sistema	Crea las tarifas para las diferentes empresas convenidas. Relacionando las tarifas para cada área que presta la IPS.
Asignación de agenda médica y admisiones de los pacientes	Secretaria	• Es el encargado de gestionar las citas médicas (Asignar, confirmar, modificar, Información exámenes). • Realiza las admisiones de los diferentes pacientes que pertenezcan para que puedan ser atendidos por los profesionales de la salud. • Impresión de reportes (historias clínicas, formulas medicas).
Gestiones medicas	Administradora del sistema	Este módulo comprende ingresos, consultas y modificaciones de los ingresos de los pacientes a la atención de cada paciente

Procedimientos	Cargo del responsable	Descripción
Sistematización de historias clínicas	Médico general	Es el encargado de recopilar sistemáticamente los detalles de salud de un paciente. O también es una nueva manera de almacenar y organizar la información del paciente. La información almacenada en el formato digital puede incluir los antecedentes médicos de un paciente (entre ellos el estado de las vacunas, resultados de pruebas y registros de crecimiento y desarrollo), información sobre el seguro médico y de facturación y otros datos relacionados con la salud. Como se almacena en formato digital, la información se puede compartir fácilmente entre los distintos proveedores de atención médica dentro de un centro y se puede enviar con rapidez de un centro a otro si un paciente se pasa a otro centro
Facturación	Administradora del sistema	Es el encargado de realizar la facturación de todos los servicios prestados, Generación de Rips e Impresión de reportes (Facturas, historias clínicas, formulas medicas).

Fuente: El autor.

Teniendo en cuenta el ciclo PDCA que permite realizar una serie de pasos y procesos para la construcción de un SGSI, a continuación se procede a realizar cada una de estas etapas:

7.2. SGSI PARA LA IPS MEDICSALUD DE VALLEDUPAR

7.2.1 Metodología de Evaluación del Riesgo. Se elige la metodología Magerit para el análisis y gestión de los de riesgos porque:

- Los pasos para su ejecución están claramente definidos.
- La documentación es clara, amplia y permite realizar una identificación adecuada del entorno donde va a ser aplicada.
- Permite enfocar los esfuerzos al análisis de riesgos críticos para la empresa, por lo tanto se puede trabajar más claramente en las posibles soluciones para dichos riesgos.

- Se puede decir que por estar incluida en los estándares ISO, sirve como como punto de partida para procesos de certificación y mejoramiento del sistema de gestión para la empresa.
- Permite el análisis a riesgos, donde se identifican y valoran los diferentes componentes que pueden tener los riesgos.
- Permite la minimización de riesgos mediante la implementación de medidas de seguridad.
- MAGERIT le permita una empresa saber cuánto valor está en juego y le ayudará a protegerlo.
- Con MAGERIT los resultados de análisis de riesgos se pueden expresar en valores cualitativos y cuantitativos, lo que permite a los directivos tomar decisiones.

Según MAGERIT: El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados estos pasos son:

Paso 1: Inventario de Activos
Paso 2: Valoración de los activos
Paso 3: Amenazas (identificación y valoración)
Paso 4: Salvaguardias
Paso 5: Impacto residual y riesgo residual
Resultados del análisis de riesgos

7.2.2 Metodología MAGERIT para la IPS Medicsalud de Valledupar

7.2.2.1. Inventario de Activos. Las empresas deben proteger la confidencialidad, integridad y disponibilidad de la información para velar por la continuidad del negocio independientemente de su actividad social. Para proteger dicha información de riesgos y amenazas la IPS Medicsalud de Valledupar realiza un inventario de sus activos teniendo en cuenta la metodología Magerit que los clasifica en los siguientes grupos.

[S] Servicios

Para los empleados, de la organización se presta los siguientes servicios:
[SW_WWW] SERVICIO DE HOSTING

[SW] Aplicaciones

Entre las aplicaciones que ostenta la IPS tenemos los siguientes:

- [OFI] OFIMÁTICA
- [ANTI] ANTIVIRUS
- [SO] SISTEMA OPERATIVO
- [SW_SISCLINIC] SISTEMA DE INFORMACIÓN CLINICA
- [OTSW] OTROS SOFTWARE

[HW] Equipos
Dentro de los equipos informáticos que posee la IPS tenemos los siguientes:

- [SERBD] SERVIDORES DE BASE DE DATOS
- [IMP] MEDIOS DE IMPRESIÓN
- [PC] COMPUTADORAS DE ESCRITORIO
- [MOW] MODEM WIFI
-

[COM] Comunicaciones
A través de los siguientes medios de transporte de información tenemos:

- [WIFI] RED WIFI
- [INTR] INTERNET

[MEDIA] Soporte de Información

- [DODISI] DOCUMENTACIÓN DIGITAL DEL SISTEMA DE INFORMACIÓN
- [INDIFI] INFORMES EN DIGITAL Y FÍSICO

[AUX] Equipamiento Auxiliar
La empresa cuenta con los siguientes equipos auxiliares:

- [CABLING_PIB] CABLEADO
- [AUXOTR_PIB] OTROS EQUIPOS AUXILIARES
-

[L] Instalaciones
La infraestructura donde se localiza los sistemas de información y comunicación, está ubicado en dirección - Barrio Cortijos, siendo un propio terreno de una x planta.

- [BUILDING_PIB] EDIFICIO

[P] Personal
El personal involucrado en esta investigación esta los siguientes:

- [GER] GERENTE
- [ADMRA] ADMINISTRADORA
- [SEC] SECRETARIA
- [MED_GRAL] MEDICO GENERAL
- [BACT] BACTERIOLOGA
- [MIC] MICROBIOLOGA
- [ODON] ODONTOLOGA
- [AUX_ENF] AUXILIAR DE ODONTOLOGIA
- [AUX_CONT] AUXILIAR CONTABLE

7.2.2.2 Valorización de los activos

Tabla 3. Criterios de valoración

Nivel	Criterio
10	Alto
9	Alto
8	Alto
7	Alto
6	Alto
5	Medio
4	medio
3	medio
2	Bajo
1	Bajo
0	Depreciable

Fuente: El autor. Datos obtenido del Magerit V3 libro 2 Catalogo de elementos

Dimensiones

- ✓ [D] disponibilidad
- ✓ [I] integridad de los datos
- ✓ [C] confidencialidad de los datos
- ✓ [A] autenticidad de los usuarios y de la información
- ✓ [T] trazabilidad del servicio y de los datos

Tabla 4. Valorización de los activos de acuerdo a las dimensiones de seguridad

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios					
Servicio de hosting	[5]				[5]
Aplicaciones					
Ofimática					[7]
Antivirus					[8]
Sistema operativo					[7]
Sistema de información clínica					[7]
Otros software					[7]
Equipos					
Servidores de base de datos	[9]	[9]	[9]	[9]	[9]
Medios de impresión					[6]

Computadoras de escritorio					[8]
Modem Wifi					[6]
Comunicaciones					
Red Wifi	[8]				[6]
Internet	[8]	[7]			[7]
Soporte de Información					
Documentación digital del sistema de información		[8]	[8]		
Informes en digital y físico		[8]	[8]		
Equipamiento Auxiliar					
Cableado	[7]				
Otros equipos auxiliares	[8]				
Instalaciones					
Edificio			[8]		
Personal					
Gerente			[8]		
Administradora			[8]		
Secretaria			[7]		
Médico general			[7]		
Bacterióloga			[7]		
Microbióloga			[7]		
Odontóloga			[7]		
Auxiliar de odontología			[6]		
Auxiliar contable			[6]		

Fuente: El autor

7.2.2.3. Caracterización de las amenazas. De acuerdo a la metodología Magerit las amenazas están clasificadas en cuatro grupos:

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

“El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, que puede pasar, que consecuencias se derivan y como de probable es que pase. Podemos resumirlo en la expresión “conoce a tu enemigo”.
Esta actividad consta de 2 partes:[19]

- Identificación de las amenazas
- Valoración de la amenazas

[19] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método. Disponible en: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 40

7.2.2.3.1. Identificación de amenazas. Es necesario identificar todos los activos que presenten situaciones de amenazas que podrían suceder y que supondrán un problema de seguridad para la IPS Medicsalud lo cual relaciono a continuación:

Identificar las amenazas relevantes sobre cada activo

Tabla 5. Identificación de las amenazas

Activos	Amenazas	
Servicios		
Servicio de hosting	[E.24]	Caída del sistema por agotamiento de recursos
	[A.5]	Suplantación de la identidad del usuario
	[A.11]	Acceso no autorizado
	[A.24]	Denegación del servicio
Aplicaciones		
Ofimática	[E.1]	Errores de los usuarios
	[E.20]	Vulnerabilidades de los programas (software)
	[E.21]	Errores de mantenimiento / actualización de programas (software)
	[A.8]	Difusión de software dañino
Antivirus	[E.8]	Difusión de software dañino
	[E.20]	Vulnerabilidades de los programas (software)
	[E.21]	Errores de mantenimiento / actualización de programas (software)
Sistema operativo	[I.5]	Avería de origen físico o lógico
	[E.1]	Errores de los usuarios
	[E.8]	Difusión de software dañino
	[E.20]	Vulnerabilidades de los programas (software)
	[E.21]	Errores de mantenimiento / actualización de programas (software)
	[A.7]	Uso no previsto
Sistema de información clínica	[I.5]	Avería de origen físico o lógico
	[E.8]	Difusión de software dañino
	[E.20]	Vulnerabilidades de los programas (Software)
	[E.21]	Errores Mantenimiento / actualización de programas (software)
	[A.5]	Suplantación de identidad
	[A.11]	Acceso no autorizado
Otros software	[E.8]	Difusión de software dañino

	[E.20] [E.21]	Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software)
Equipos		
Servidores de base de datos	[N.1] [N.2] [N.*] [I.3] [I.5] [I.7] [E.2] [E.23] [A.11] [A.23]	Fuego Daños por agua Desastres naturales Contaminación medioambiental Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Errores del administrador del sistema / de la seguridad Errores de mantenimiento / actualización de equipos (hardware) Acceso no autorizado Manipulación del hardware
Medios de impresión	[I.5] [I.7] [E.23] [A.11]	Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Errores de mantenimiento / actualización de equipos (hardware) Acceso no autorizado
Computadoras de escritorio	[N.2] [N.*] [I.*] [I.5] [I.7] [E.23] [E.24] [A.6] [A.7]	Daños por agua Desastres naturales Desastres industriales Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Errores de mantenimiento / actualización de equipos (hardware) Caída del sistema por agotamiento de recursos Abuso de privilegios de acceso Uso no previsto
Modem Wifi	[N.1] [N.2] [N.*] [I.3] [I.5] [I.7] [A.11]	[Fuego Daños por agua Desastres naturales Contaminación medioambiental Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Acceso no autorizado
Comunicaciones		

Red Wifi	[I.8] [E.9]	Fallo de servicios de comunicaciones Errores de [re-]encaminamiento
Internet	[I.8] [E.15]	Fallo de servicios de comunicaciones Alteración de la información
Soporte de Información		
Documentación digital del sistema de información	[E.15] [E.19] [A.15] [A.19]	Alteración de la información Fugas de información Modificación de la información Revelación de información
Informes en digital y físico	[E.15] [E.19] [A.15] [A.19]	Alteración de la información Fugas de información Modificación de la información Revelación de información
Equipamiento Auxiliar		
Cableado	[I.3] [I.7]	Contaminación medioambiental Condiciones inadecuadas de temperatura o humedad
Otros equipos auxiliares	[I.3]	Contaminación medioambiental
Instalaciones		
Edificio	[N.1] [N.2] [N.*.1] [N.*.4] [N.*.11] [I.*] [A.27]	Fuego Daños por agua Tormentas Terremotos Calor extremo Desastres industriales Ocupación enemiga
Personal		
Gerente	[E.28.1] [E.28.2] [A.29] [A.30]	Enfermedad Huelga Extorsión Ingeniería social (picaresca)
Administradora	[E.28.1] [E.28.2] [A.29] [A.30]	Enfermedad Huelga Extorsión Ingeniería social (picaresca)
Secretaria	[E.28.1] [E.28.2] [A.29] [A.30]	Enfermedad Huelga Extorsión Ingeniería social (picaresca)
Médico general	[E.28.1] [E.28.2] [A.29]	Enfermedad Huelga Extorsión
Bacterióloga	[E.28.1] [E.28.2] [A.29]	Enfermedad Huelga Extorsión
Microbióloga	[E.28.1]	Enfermedad

	[E.28.2] [A.29]	Huelga Extorsión
Odontóloga	[E.28.1] [E.28.2] [A.29]	Enfermedad Huelga Extorsión
Auxiliar de odontología	[E.28.1] [E.28.2] [A.29]	Enfermedad Huelga Extorsión
Auxiliar contable	[E.28.1] [E.28.2] [A.29] [A.30]	Enfermedad Huelga Extorsión Ingeniería social (picaresca)

Fuente: El autor

7.2.2.3.2. Valoración de las amenazas. Los objetivos planteados en esta tarea son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

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

Tabla 6. Criterio de la valoración de las amenazas según la degradación del valor y la probabilidad de ocurrencia

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA
0	
CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO POSIBLE
MB	SIGLOS
MR	MUY RARA

Fuente: El autor

Tabla 7. Valorización de las amenazas

Activos	Amenazas		[P]	[D]	[I]	[C]	[A]	[T]
Servicios								
Servicio de hosting	[E.24]	Caída del sistema por agotamiento de recursos	P	M				
	[A.5]	Suplantación de la identidad del usuario	B			PP		
	[A.11]							
	[A.24]	Acceso no autorizado Denegación del servicio		A	MA			
Aplicaciones								
Ofimática	[E.1]	Errores de los usuarios	P	M	M	M		
	[E.20]	Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.21]	Errores de mantenimiento / actualización de programas (software)	P	M	B			
	[A.8]	Difusión de software dañino	PP	B	B	B		
Antivirus	[E.8]	Difusión de software dañino	PP	B	B	B		
	[E.20]	Vulnerabilidades de los programas (software)	P	M	M	M		
	[E.21]	Errores de mantenimiento / actualización de programas (software)	P	M	M			
Sistema operativo	[I.5]	Avería de origen físico o lógico	P	M				
	[E.1]	Errores de los usuarios	PP	M	M	M		
	[E.8]	Difusión de software dañino	PP	B	B	B		
	[E.20]	Vulnerabilidades de los programas (software)	P	B	M	M		
	[E.21]	Errores de mantenimiento / actualización de programas (software)	P	M	B			
	[A.7]	Uso no previsto	P	B	B	B		

Sistema de información clínica	[I.5] [E.8] [E.20] [E.21] [A.5] [A.11]	Avería de origen físico o lógico Difusión de software dañino Vulnerabilidades de los programas (Software) Errores Mantenimiento / actualización de programas (software) Suplantación de identidad Acceso no autorizado	P P PP PP P M	M B B M A	 B B M A	 B B A P		
Otros software	[E.8] [E.20] [E.21]	Difusión de software dañino Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software)	PP PP PP	B B M	B B M	B B		
Equipos								
Servidores de base de datos	[N.1] [N.2] [N.*] [I.3] [I.5] [I.7] [E.2] [E.23] [A.11] [A.23]	Fuego Daños por agua Desastres naturales Contaminación medioambiental Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Errores del administrador del sistema / de la seguridad Errores de mantenimiento / actualización de equipos (hardware) Acceso no autorizado Manipulación del hardware	P P P P P MA P P P P	A A A A A MA M M M A	 M M 	 M M 		
Medios de impresión	[I.5] [I.7]	Avería de origen físico o lógico	P P	M M				

	[E.23] [A.11]	Condiciones inadecuadas de temperatura o humedad Errores de mantenimiento / actualización de equipos (hardware) Acceso no autorizado	P PP	M	 M	 M		
Computadoras de escritorio	[N.2] [N.*] [I.*] [I.5] [I.7] [E.23] [E.24] [A.6] [A.7]	Daños por agua Desastres naturales Desastres industriales Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Errores de mantenimiento / actualización de equipos (hardware) Caída del sistema por agotamiento de recursos Abuso de privilegios de acceso Uso no previsto	PP PP PP P PP P P PP P	M M B M M M M M M				
Modem Wifi	[N.1] [N.2] [N.*] [I.3] [I.5] [I.7] [A.11]	Fuego Daños por agua Desastres naturales Contaminación medioambiental Avería de origen físico o lógico Condiciones inadecuadas de temperatura o humedad Acceso no autorizado	PP PP PP PP P P PP	M M M M M M 				
Comunicaciones								
Red Wifi	[I.8] [E.9]	Fallo de servicios de comunicaciones Errores de [re-]encaminamiento	P P	M 		 B		

Internet	[I.8] [E.15]	Fallo de servicios de comunicaciones Alteración de la información	P P	A M	A M	A M		
Soporte de Información								
Documentación digital del sistema de información	[E.15] [E.19] [A.15] [A.19]	Alteración de la información Fugas de información Modificación de la información Revelación de información	PP PP PP PP		B B 	 B B		
Informes en digital y físico	[E.15] [E.19] [A.15] [A.19]	Alteración de la información Fugas de información Modificación de la información Revelación de información	PP PP PP PP		B B 	 B B		
Equipamiento Auxiliar								
Cableado	[I.3] [I.7]	Contaminación medioambiental Condiciones inadecuadas de temperatura o humedad	PP PP	A M				
Otros equipos auxiliares	[I.3]	Contaminación medioambiental	PP	A				
Instalaciones								
Edificio	[N.1] [N.2] [N.*.1] [N.*.4] [N.*.11] [I.*] [A.27]	Fuego Daños por agua Tormentas Terremotos Calor extremo Desastres industriales Ocupación enemiga	P P P P MA P P	A A A M B B M		 A M		
Personal								
Gerente	[E.28.1] [E.28.2] [A.29] [A.30]	Enfermedad Huelga Extorsión Ingeniería social (picaresca)	P PP PP MA	M B M A	M M A	M M B		
Administradora	[E.28.1] [E.28.2] [A.29]	Enfermedad Huelga Extorsión	P PP PP	M B M	M M	M M		

	[A.30]	Ingeniería social (picaresca)	MA	A	A	B		
Secretaria	[E.28.1]	Enfermedad	PP	M				
	[E.28.2]	Huelga	MR	B				
	[A.29]	Extorsión	PP	M	M	M		
	[A.30]	Ingeniería social (picaresca)	MA	M	M	M		
Médico general	[E.28.1]	Enfermedad	P	M				
	[E.28.2]	Huelga	PP	M	M	M		
	[A.29]	Extorsión	PP	B				
Bacterióloga	[E.28.1]	Enfermedad	PP	M				
	[E.28.2]	Huelga	PP	B				
	[A.29]	Extorsión	PP	M	M	M		
Microbióloga	[E.28.1]	Enfermedad	P	M				
	[E.28.2]	Huelga	PP	M	M	M		
	[A.29]	Extorsión	PP	B				
Odontóloga	[E.28.1]	Enfermedad	P	M				
	[E.28.2]	Huelga	PP	M	M	M		
	[A.29]	Extorsión	PP	B				
Auxiliar de odontología	[E.28.1]	Enfermedad	PP	M				
	[E.28.2]	Huelga	MR	B				
	[A.29]	Extorsión	PP	M	B	M		
Auxiliar contable	[E.28.1]	Enfermedad	MA	M				
	[E.28.2]	Huelga	MR	B				
	[A.29]	Extorsión	PP	M	B	M		
	[A.30]	Ingeniería social (picaresca)	P	M	M	M		

Fuente: El autor

Antes de ver los salvaguardas en el proceso de la metodología Magerit vamos a analizar en este paso las vulnerabilidades observadas en la IPS Medicsalud.

7.2.2.4. Establecimiento de Vulnerabilidades. En este informe se pretende identificar vulnerabilidades que causan daños al sistema, a la IPS Medicsalud y en si comprometer los activos de la misma.

Se toman como referencia primero los servicios que actualmente presta y que forman parte primordial de los objetivos de la empresa y las redes que tienen implementadas, donde es posible la presencia de fallos, robo, o modificación y que pueden comprometer seriamente la integridad de la información.

A continuación se muestran los resultados de la evaluación de los sistemas y dispositivos que forman parte de los activos de la IPS Medicsalud.

Tabla 8. Identificación de las vulnerabilidades

Activos	Vulnerabilidades
Servicio de hosting	La información dentro de la infraestructura y los sistemas pueden ser accesible por usuarios diferentes a los autorizados, Los datos e información dentro de la infraestructura pueden ser alterados, dañados o destruidos y no asegura que cualquier usuario del sistema es quien dice ser y puede haber las posibilidades de suplantación de identidad. La forma de proteger los sistema de información es asegurarse que el servicios que cumplan con la disponibilidad, integridad y confidencialidad de la información y hacer un backup de la información local con periodo cada 3 o 4 días.
Ofimática	Las vulnerabilidades presentes en la suite ofimática de Microsoft, MS Office, son: CVE-2015-1641 y CVE-201554-25. Estas dos vulnerabilidades es para conseguir ganar permisos en el sistema y ejecutar código malicioso con el fin de infectar a sus víctimas con malware, la primera vulnerabilidad puede ser puede ser explotada en ficheros RTF y la segunda es un fallo más específico, pero también más complicado de detectar que el anterior, afectando solo a las versiones desactualizadas de MS Office. La mejor forma de protegerse de estas vulnerabilidades es manteniendo Office actualizado a la última versión disponible, ya que todas ellas cuentan con los correspondientes parches de seguridad. Además, es recomendable evitar la ejecución de documentos

	descargados de Internet o recibidos a través del correo electrónico desde fuentes de dudosa procedencia ya que estas son las principales vías de ataque de los hackers.
Sistemas Operativos	La principal vulnerabilidad que puede tener un sistema operativo es por ataque de virus que tiene por objeto afectar el normal funcionamiento del sistema. Otras es falla del sistema
Sistema de información clínica	Presenta fallas y debilidades en el software con el fácil acceso al mismo y lo hacen menos fiable, cualquier persona se puede autenticar para acceder al sistema, esto lo hace ser vulnerable.
Servidores de base de datos	El gran número de puertos abiertos es una vulnerabilidad para el Servidor, ya que los usuarios del sistema como los atacantes se conectan al sistema por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente. El resto de los puertos deben ser cerrados.
Computadoras de escritorio	El personal de Organización que utiliza el sistema representa la mayor vulnerabilidad del sistema. Toda la seguridad del sistema descansa sobre la persona que cumple la función de administrador del mismo que tiene acceso al Máximo nivel y sin restricciones al mismo.
Red WiFi	La red tiene configurado seguridad WPA2 con contraseñas normales, es decir, sin respetar las reglas de contraseñas seguras o fuertes. Se hizo un hackeo ético con la respectiva autorización a una de las contraseñas débiles, encontramos un resultado positivo donde se pudo descifrar la clave en corto tiempo, utilizando el programa Wifislax. Las recomendaciones son: Crear contraseñas fuertes para WPA2 en cada antena o dispositivo, igualmente desactivar en todos WPS para evitar otros ataques.
Internet	El acceso a internet no se encuentra limitado por algún protocolo de seguridad para los usuarios de la Organización.
Cableado	Las principales vulnerabilidades del cableado son el electromagnetismo, humedad, intervención de personas no autorizadas, mal manejo de temperatura, suspensión del fluido eléctrico, polvo e incendio. Las recomendaciones para el cableado son:

	• Instalar canaletas metálicas para los cables externos. • Restringir el acceso físico a los dispositivos y servidores, controlar el acceso lógico.

Fuente: El autor

7.2.2.5 Caracterización de las Salvaguardas. "Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y por último, está la política de personal.[20]

En esta actividad se identifican las salvaguardas efectivas para la organización junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. Dentro de esta metodología se pueden definir varias etapas de estudio que pueden abarcar lapsos de tiempo corto o largos incluso de un año, pero nuestro caso de estudio tomaremos tres fases:

- Primera etapa llamada POTENCIAL(Potential)
- Segunda etapa llamada SITUACIÓN ACTUAL (Current)
- Tercera etapa llamada OBJETIVO (Target)

Esta actividad consta de dos sub-tareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas

7.2.2.5.1 Identificación de las salvaguardas. Su objetivo principal es:

- Identificar las salvaguardas convenientes para proteger el sistema

La elección de salvaguardas de cada activo para contrarrestar las amenazas identificadas.

Protecciones Generales: A continuación las salvaguardas que fueran escogidas:
Se requiere autorización previa: Pertenece al grupo de Restricción de acceso a la información que a su vez pertenece al Control de Acceso Lógico. La razón se escogió esta salvaguarda ya que cualquier persona puede acceder a los activos inclusive los más importantes. La misma por que hace frente a las amenazas a las que están expuestos los activos. Y esta pueda ser aplicada a estas clases de activos: Datos/ Información, Servicios, Aplicaciones (software), Equipamiento informático (hardware), Redes de comunicaciones y Soportes de información.

[20] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 31

Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad.

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

Se escogió estas salvaguardas por que la empresa no posee ningún de estas medidas de seguridad, las mismas que son pueden ser aplicadas en la capa: Servicios Internos y asegura la dimensión de la Disponibilidad.

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

- Se dispone de normativa sobre el uso autorizado de las aplicaciones
- Se dispone de normativa relativa al cumplimiento de los derechos
- Se controla la instalación de software autorizado y productos con licencia
- Se dispone de procedimientos para realizar copias de seguridad
- Se aplican perfiles de seguridad: esta salvaguarda se encuentra a medias porque solo existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema pero gracias a esta salvaguarda podemos hacer frente a estas amenazas : Errores de los usuarios , Difusión de software dañino, Vulnerabilidad de los programas (software),Errores de mantenimiento/actualización de programas (software) y Uso no previsto
  Se debería tratar de cumplir con lo siguiente:
- Seguridad de los ficheros de datos de la aplicación
- Se protegen los ficheros de configuración
- Seguridad de los mecanismos de comunicación entre procesos

Donde se asegura las dimensiones de seguridad como confidencialidad e integridad

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

Protección de los Equipos Informáticos (HW): A continuación las salvaguardas adecuadas para la protección de los equipos.

- Se dispone de normativa sobre el uso correcto de los equipos
- Se dispone de procedimientos de uso de equipamiento

- Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la empresa minimiza amenazas como son: Errores del administrados del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

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

- Protección física de los equipos: son mecanismos que la empresa no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el Servidor de Web y base de datos
    - Para evitar accesos innecesarios
    - Para evitar acceso no autorizados
- Seguridad del equipamiento de oficina

Después de evaluar las salvaguardas antes mencionadas se debe implantar las siguientes salvaguardas:

- Se evalúa el impacto en la confidencialidad de los datos
- Se evalúa el impacto en la integridad de los datos

Ninguna de estas salvaguardas posee la entidad Medicsalud como son:

- Se priorizan las actuaciones encaminadas corregir riesgos elevados
- Se mantiene en todo momento la regla de “seguridad por defecto”
- Se debe de controlar: Reproducción de documentos

Protección de las comunicaciones: se han escogido las siguientes salvaguardas para minimizar riesgos:

- Se deben de aplicar perfiles de seguridad : para garantizar la comunicación en la empresa y para hacer frente amenazas como: Errores de secuencia, Alteración de la información, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia y Acceso no autorizado, además proteger las dimensiones de seguridad : integridad , confidencialidad y autenticidad.
- La empresa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado
- Ni siquiera de mecanismos como son :
    - Comprobación de origen y destino
    - Mecanismos de control
- No tiene ninguna: Seguridad de los servicios de red

Todas las salvaguardas anteriormente desplegadas hacen frente a la amenaza de Acceso no autorizado

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

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas anti spyware
- Se deshabilitan las “cookies” en los navegadores
- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del trafico
- Se toman medidas frente a la inyección de información espuria
- Se aplica la regla de “seguridad por defecto”
- Se requiere autorización para que medios y dispositivos que tengan acceso a redes y servicios

Protección de los Soportes de Información: para proteger el único activo se han escogido las salvaguardas más apropiadas:

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

Elementos Auxiliares:

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

Protección de las Instalaciones

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

Gestión del Personal: Se deben de crear las siguientes normas de seguridad:

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

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

7.2.2.5.2 Valorización de las salvaguardas. Su objetivo es:

- Determinar la eficacia de las salvaguardas pertinentes

Tabla 9. Niveles de madurez

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Fuente: El autor

Tabla 10. Tarea de Valorización de salvaguardas

Salvaguardas	Target	Current	P
Protección generales	L5	L1	L3-L4
Protección de los servicios (SW)	L5	L0-L1	L2-L3
Protección de las aplicaciones informáticas (SW)	L5	L0-L1	L2-L4
Protección de los equipos informáticos	L5	L0-L1	L2-L4
Protección de las comunicaciones	L5	L1	L2-L5
Protección de los soportes de información	L5	L1	L2-L4
Elementos auxiliares	L5	L1	L2-L3
Protección de las instalaciones	L5	L1	L2-L4
Gestión del personal	L5	L1	L2-L3

Fuente: El autor

7.2.2.6 Estimación del estado de riesgo. En esta tarea se procesa e interpreta los resultados obtenidos de las actividades anteriores para detallar en un informe del estado de riesgo de la empresa.
Y consta de dos tareas:

- Estimación del impacto
- Estimación del riesgo

El objetivo de esta tarea es:

- Disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo)

7.2.2.6.1 Estimación del Impacto. Su objetivo es:

- Establecer el impacto potencial al que está sometido el sistema
- Establecer el impacto residual al que está sometido el sistema

En esta tarea se estima al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesta el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.[21]

La fórmula emplea un sistema de salvaguardas, absolutamente ineficaz (ei=0) deja el impacto donde está, mientras que un sistema de salvaguardas plenamente eficaz (ei=1) reduce el impacto residual a 0

Figura 1. Formula Impacto Residual

$$\text{impacto residual} = \text{impacto potencial} \times (1 - e^i)$$

Fuente: El autor

7.2.2.6.1.1 Impacto Potencial. "Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema.

[21] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 44

Tabla 11. Impacto Potencial sobre cada uno de los activos

Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios					
Servicio de hosting		[8]	[8]		
Aplicaciones					
Ofimática		[6]	[6]		[7]
Antivirus		[6]	[6]		
Sistema operativo		[7]	[7]		
Sistema de información clínica		[8]	[8]		
Otros software		[6]	[6]		
Equipos					
Servidores de base de datos		[8]	[8]		
Medios de impresión		[6]	[6]		
Computadoras de escritorio		[6]	[6]		
Modem Wifi		[3]	[3]		
Comunicaciones					
Red Wifi		[6]	[8]	[6]	
Internet	**[4]**	[6]	[6]		
Soporte de Información					
Documentación digital del sistema de información		[3]	[3]		
Informes en digital y físico		[3]	[3]		
Equipamiento Auxiliar					
Cableado	[6]				
Otros equipos auxiliares	[2]				
Instalaciones					
Edificio			[8]		
Personal					
Gerente			[7]		
Administradora			[6]		
Secretaria			[5]		
Médico general			[5]		
Bacterióloga			[5]		
Microbióloga			[5]		
Odontóloga			[5]		
Auxiliar de odontologia			[6]		
Auxiliar contable			[7]		

Fuente: El autor

Los impactos que se muestran con la siguiente escala de colores según su valor:

[10]: Crítico
[9]: Muy alto
[8]: Muy Alto
[7]: Alto
[6]: Alto
[5]: Medio
[4]: Medio
[3]: Bajo
[2]: Bajo
[1]: Despreciable
[0]: Despreciable

7.2.2.6.1.2 Impacto Residual Acumulado.

Tabla 12. Impacto Residual sobre cada uno de los activos

Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios					
Servicio de hosting		[5]	[5]		
Aplicaciones					
Ofimática		[0]	[0]		
Antivirus		[3]	[3]		
Sistema operativo		[4]	[4]		
Sistema de información clínica		[5]	[5]		
Otros software		[3]	[3]		
Equipos					
Servidores de base de datos		[3]	[4]		
Medios de impresión		[3]	[3]		
Computadoras de escritorio		[3]	[5]		
Modem Wifi		[0]	[0]		
Comunicaciones					
Red Wifi		[3]	[4]	**[3]**	
Internet	[4]	[5]	[5]		
Soporte de Información					
Documentación digital del sistema de información		[3]	[3]		
Informes en digital y físico		[3]	[3]		
Equipamiento Auxiliar					
Cableado	[4]				
Otros equipos auxiliares	[1]				
Instalaciones					
Edificio			**[5]**		

Personal					
Gerente			[2]		
Administradora			[1]		
Secretaria			[0]		
Médico general			[0]		
Bacterióloga			[0]		
Microbióloga			[0]		
Odontóloga			[0]		
Auxiliar de odontología			[1]		
Auxiliar contable			[2]		

Fuente: El autor

7.2.2.6.2 Estimación del Riesgo. Sus objetivos son:

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

En esta tarea se estima el riesgo al o que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El riego residual , al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como eficacia de las salvaguardas actualmente desplegadas.[22]

Emplea la siguiente fórmula:

Figura 2. Formula Riesgo Residual

$$\text{riesgo residual} = \text{impacto residual} \times \text{frecuencia residual}$$

Fuente: El autor

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

[22] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 45

Tabla13. Impacto Residual sobre cada uno de los activos

Activos	[D]	[I]	[C]	[A]	[T]
Servicios					
Servicio de hosting		{6,6}	{6,6}		
Aplicaciones					
Ofimática		{5,4}	{5,4}		
Antivirus		{5,4}	{5,4}		
Sistema operativo		{5,4}	{5,4}		
Sistema de información clínica		{6,6}	{6,6}		
Otros software		{4,5}	{4,5}		
Equipos					
Servidores de base de datos		{6,6}	{6,6}		
Medios de impresión		{3,6}	{3,6}		
Computadoras de escritorio		{4,5}	{4,5}		
Modem Wifi		{1,8}	{1,8}		
Comunicaciones					
Red Wifi		{4,5}	{6,6}	{4,5}	
Internet	{4,2}	{5,4}	{5,4}		
Soporte de Información					
Documentación digital del sistema de información		{1,8}	{1,8}		
Informes en digital y físico		{1,8}	{1,8}		
Equipamiento Auxiliar					
Cableado	{4,5}				
Otros equipos auxiliares	{2,1}				
Instalaciones					
Edificio			{6,6}		
Personal					
Gerente			{4,8}		
Administradora			{6,0}		
Secretaria			{4,8}		
Médico general			{3,0}		
Bacterióloga			{3,0}		
Microbióloga			{3,0}		
Odontóloga			{3,0}		
Auxiliar de odontología			{4,8}		
Auxiliar contable			{5,4}		

Fuente: El autor

[9]: NIVEL 9
[8]: NIVEL 8
[7]: Extremadamente critico
[6]: Muy critico
[5]: Critico
[4]: Muy alto
[3]: Alto
[2]: Medio
[1]: Bajo
[0]: Despreciable

7.2.2.6.2.2 Riesgo Residual.

7.2.2.6.2.2.1 Riesgo Residual Acumulado. La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo. Los valores de la tabla 13 que tienen resultados mayores a 3 son riesgos Altos.

Tabla14. Riesgo Residual sobre cada uno de los activos

Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios					
Servicio de hosting		{4,2}	{4,2}		
Aplicaciones					
Ofimática		{0,83}	{0,83}		
Antivirus		{3,2}	{3,2}		
Sistema operativo		{3,1}	{3,1}		
Sistema de información clínica		{4,2}	{4,2}		
Otros software		{1,7}	{1,7}		
Equipos					
Servidores de base de datos		{2,1}	{3,8}		
Medios de impresión		{0,95}	{0,96}		
Computadoras de escritorio		{1,7}	{3,3}		
Modem Wifi		{0,59}	{0,59}		
Comunicaciones					
Red Wifi		{2,2}	{2,8}	**{2,5}**	
Internet	{4,0}	{4,8}	{4,8}		
Soporte de Información					
Documentación digital del sistema de información		{0,86}	{0,90}		
Informes en digital y físico		{0,86}	{0,90}		

Equipamiento Auxiliar					
Cableado	{3,0}				
Otros equipos auxiliares	{1,8}				
Instalaciones					
Edificio			**{3,5}**		
Personal					
Gerente			{1,9}		
Administradora			{1,3}		
Secretaria			{0,83}		
Médico general			{0,42}		
Bacterióloga			{0,42}		
Microbióloga			{0,42}		
Odontóloga			{0,42}		
Auxiliar de odontologia			{0,92}		
Auxiliar contable			{0,92}		

Fuente: El autor

Como se puede observar de todos los pasos del Análisis de Riesgos ya que se hace fácil saber cuáles son los activos que tiene un nivel alto de riesgos, para mitigarlos en la siguiente fase que es la Gestión de Riesgos

7.2.3 Gestión de Riesgos. Después de haber realizado el Análisis de Riesgos queda a la vista los impactos y los riesgos que están expuesto la empresa.

Lo que ha llegado a una calificación de cada riesgo significativo, determinándose si

- Es crítico en el sentido de que requiere atención urgente
- Es grave en el sentido de que requiere atención
- Es apreciable en el sentido d que pueda ser objeto de estudio para su tratamiento
- Es asumible en el sentido de que no se van a tomar acciones para atajarlo

El resultado del análisis es solo un análisis. A partir de que disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados =, de que lo queremos proteger (amenazas valoradas)) y que hemos por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.[23]

[23] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 45

7.2.3.1 Toma de Decisiones.

7.2.3.1.1 Identificación de Riesgos Críticos. En toda organización los activos están expuestos a riegos, pero lo importante es conocer cuáles de los activos poseen mayor nivel de riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen.

Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, hemos seleccionado los activos que poseen un nivel de riesgo. A continuación se mostramos la siguiente tabla.[24]

Tabla15. Identificación de Riesgos Críticos (current)

Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios					
Servicio de hosting		{4,2}	{4,2}		
Aplicaciones					
Antivirus		{3,2}	{3,2}		
Sistema operativo		{3,1}	{3,1}		
Sistema de información clínica		{4,2}	{4,2}		
Equipos					
Servidores de base de datos		{2,1}	{3,8}		
Computadoras de escritorio		{1,8}	{3,2}		
Comunicaciones					
Red Wifi		{2,5}	{3,5}	**{2,8}**	
Internet	{4,0}	{4,8}	{4,8}		
Equipamiento Auxiliar					
Cableado	{3,0}				
Instalaciones					
Edificio			{3,5}		

Fuente: El autor

[24] Análisis y Gestión de Riegos de los Sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología Magerit, http://dspace.ucuenca.edu.ec/bitstream/123456789/1342/1/tcon640.pdf,78

Los riesgos se muestran con la siguiente escala de colores según su valor:
[9]: NIVEL 9
[8]: NIVEL 8
[7]: Extremadamente critico
[6]: Muy critico
[5]: Critico
[4]: Muy alto
[3]: Alto
[2]: Medio
[1]: Bajo
[0]: Despreciable

7.2.3.1.2 Calificación del Riesgo. A continuación se gestionan los activos con riesgos críticos:

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

La mayor amenaza a la que se enfrenta este activo es la de Suplantación de la identidad del usuario que sufre la integridad y con confidencialidad (4,2).

Esta amenaza nace a partir a que el sistema cuenta con una clave de fácil acceso permitiendo que cualquier trabajador interno o individuo externo, indague en la información perteneciente a la empresa.

Si se llega a materializar esta amenaza podría ser víctimas de robo de información o de generar datos erróneos en la información perjudicando el desempeño de las actividades de la mayoría de los empleados.

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

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

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

La mayor amenaza a la que se enfrenta este activo es la de acceso no autorizado que sufre la integridad y con confidencialidad (4,2).

Si se llega a materializar esta amenaza podría ser víctimas de robo de información perjudicando el desempeño de las actividades de la mayoría de los empleados.

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

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

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

La amenaza a la que está expuesto este activo: Difusión de software dañino que perjudica a las dimensiones con niveles altos de riesgo que son la integridad (3,2) y la confidencialidad (3,2). Una de las principales razones es que la mayoría de veces cuando hacen uso de dispositivos externos como memory flash no la hacen analizar por el antivirus provocando la propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

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

- La medida que se debe tomar es la adquisición de software óptimo para evitar la propagación de virus.
- También es que por lo menos una cuatro veces al mes el antivirus sea actualizado para que pueda contra restar cualquier software dañino.
- que en lo posible de colocar dispositivos externos en las máquinas para así evitar que pueda ser infectadas.

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

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

Errores de los usuarios y Difusión de software dañino, que indisponen a las dimensiones de integridad (3,1) y confidencialidad (3,1). Este tipo de errores se da por el mal del uso de esta aplicación, lo que pueda generar inhabilitado el sistema operativo. Puede disponer de antivirus, pero si este no se actualiza constantemente no puede detectar posibles formas de contagio existentes.

Vulnerabilidades de los programas (software) afecta a la integridad (3,0) y la confidencialidad (3,0). Nunca se podrá garantizar que software es 100% ya que puede aparecer con ciertos errores de fábrica y por tal motivo hay que tomar en cuenta esta amenaza.

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

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

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

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

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

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

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

La amenaza que tiene un nivel de riesgo alto es el uso no previsto que afecta principalmente confiabilidad (3,2) y la integridad (1,8).

Esta es una amenaza muy común ya que algunos empleados pueden instalar programas que no tengan ninguna relación con el trabajo sino que son para su interés personal como juegos, programas personales o almacenamiento de datos personales. Retrasando sus actividades de acuerdo al puesto de trabajo en el que se están desempeñando.

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

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

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

Las amenazas que son: errores de [re]-encaminamiento, que posee un nivel de riesgo alto (3,5) que afecta a la confidencialidad.

Si estas amenazas llegan a materializarse puede causar perdida en la confidencialidad de información. Ya que son víctimas de un atacante que intercepta la información. Existe un mal estado en la red donde se encuentra conectado a equipos de un lugar a otro pero no se ha seguido ninguna norma de seguridad para evitar este tipo de ataques.

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

- Se deberían implementar protecciones criptográficas para la confidencialidad de los datos intercambiados.
- Además de implementar algoritmos para este caso sería mejor :
    - Dispositivos Físicos y emplear servicios certificados.
- Además de realizar mantenimientos regulares del estado de la red Wifi.

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

La amenaza de mayor relevancia que posee es fallo de servicios de comunicaciones que afecta en la disponibilidad (4,0) y en la confidencialidad e integridad (4,8) si se llega a materializar esta amenaza no podrían ejecutar tareas diarias como el envío de emails, la gestión de la página del sistema clínica de la IPS Medicsalud, las otras páginas relacionadas con el software clinic, entre otras.

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

Realizar mantenimientos regulares del estado de la red.

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

La amenaza que es de Contaminación medioambiental que posee un nivel de riesgo alto en la disponibilidad (3,0). Esta amenaza se da por la deplorable instalación del cableado y equipos interrelacionados exponiéndoles a daños físicos por el polvo y suciedad.

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

- Para la protección de cableado se debería tener lo siguiente:
    - Disponer de planos actualizados del cableado.
    - Etiquetar todos los elementos de cableado.
    - Evitar rutas a través de áreas públicas.
    - Controlar todos los accesos al cableado.
    - Separar el cableado de alimentación del de comunicaciones para evitar interferencias.
    - Proteger contra daños o interceptaciones no autorizadas (conductos blindados, cajas o salas cerradas).

Edificio es una de los activos que pertenece a la capa de Instalaciones, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:

Este activo que acoge a todos los activos tiene una amenaza latente que es la Ocupación enemiga que afecta la confidencialidad (3,5) en la entrada no hay guardia por lo que cualquier personas puede entrar sin ser autorizado.

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

- Se deberían de disponer un 1 o más guardias de seguridad

Personal que son todo el personal que se encuentra en la empresa que son: Gerente, administradora, secretaria, médico general, bacterióloga, microbióloga, odontóloga, auxiliar de enfermería, auxiliar de odontología y auxiliar contable.

Las principales amenazas que posee el personal que labora en esta empresa son la ingeniería social y extorción.
La primera amenaza se cumple por que los empleados saben la clave de los demás para acceder a su computador de esta manera se puede sustraer, modificar y destruir la información. Originando a que la segunda amenaza que puede ser utilizada como extorción o como abuso de buena fe para beneficio propio del atacante.

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

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

7.2.4 Mitigar o eliminar los riesgos de la IPS Medicsalud mediante el SGSI. Después de haber realizado el análisis de riesgos de los activos de información de la IPS MEDICSALUD se recomienda a reducir o eliminar estos riesgos bajo planes de acción mediante especificación de políticas y objetivos de la seguridad del área informática a través de la norma ISO/IEC 27002

Con el fin de minimizar los riesgos encontrados en cada dependencia de la IPS MEDICSALUD se define las políticas y objetivos a implementar los cuales son los siguientes:

7.2.4.1 Políticas y objetivos de seguridad del área de informática.

Generalidades: La información es uno de los activos más importantes de una empresa por lo tanto la seguridad de la misma contribuye a cumplir su misión y objetivos. La IPS

Medicsalud se dedica a prestar el servicio de salud a los pacientes de forma eficiente y oportuna.

Objetivo: Definir políticas de seguridad para el área de informática de la IPS Medicsalud, que sirvan como estrategias de apoyo para lograr disminuir riesgos, evitar incidentes, mantener la confidencialidad, brindar un servicio eficiente y de calidad en el servicio de salud a los pacientes, manteniendo permanentemente una excelente imagen empresarial.

Alcance: Esta política se debe aplicar a todos los procesos y dependencias relacionados con el área de informática de la IPS Medicsalud.

Responsables: La responsabilidad de la seguridad de la información está en cabeza del administradora de la IPS, el gerente, seguida por el responsable de la seguridad y el responsable del mantenimiento y todo el equipo de trabajo; es decir todos los empleados que hacen parte de la organización.

Para la aplicación de estas políticas de seguridad la administradora debe designar un responsable de seguridad informática y sistemas de información, un responsable de la seguridad de la información, responsable de recursos humanos, responsable del área legal y administrativa, los cuales conformaran el comité de seguridad.

- **Comité de seguridad de la información:** Tiene las siguientes funciones presentar a la administradora la aprobación de las políticas de seguridad, monitorear riesgos y amenazas, plantear modificaciones en las políticas de seguridad, velar y controlar que sean cumplidas por todos los empleados de la IPS. Este comité debe elegir un coordinador que se encargara de coordinar las acciones de dicho comité y presentar solicitudes de modificaciones y requerimiento para la aprobación de la administradora.

- **Comité de Revisión Interna o Control Interno:** Responsable de practicar auditorias periódicas sobre el manejo de los sistemas de información y la aplicación de las políticas de seguridad, estas deben estar debidamente documentas y son las responsables de encontrar fallas y brindar soluciones para corregir dichas fallas

- **Responsable del Área de Informática y de la seguridad informática:** Cumple la función de documentación, mantenimiento, actualización y gestión de políticas de seguridad para todos los recursos tecnológicos de la organización (Hardware, software, red, servidores etc) y se encarga de supervisar el cumplimiento de las políticas de seguridad.
- **Responsable de la Información y sistemas de información:** Es el encargado de clasificar la información de acuerdo a su grado de confidencialidad y definir los permisos de acceso a los usuarios, además se encargara de controlar, documentar y almacenar toda la información de la empresa, elaborar y almacenar copias de seguridad

- **Responsable de Recursos Humanos:** Es el encargado de divulgar las políticas de seguridad y la obligatoriedad del cumplimiento de las mismas por todos los empleados de la empresa. Si se generan cambios este se encargara de divulgar dichos cambios.

- **Responsable del Área Legal y Administrativa:** Responsable del cumplimiento de todas las políticas de seguridad en todos los contratos laborales.

- **El propietario de la información:** Responsable de conocer y cumplir con todos los requerimientos y políticas de seguridad estipuladas por la empresa y encargado de contribuir con la confidencialidad, disponibilidad e integridad de la información

Política: Esta política define aspectos específicos y pautas sobre la seguridad para el área de informática de la IPS Medicsalud de Valledupar tales como:

- **Organización de la seguridad:** Su objetivo es guiar la administración y dirección de la seguridad para su posterior implementación.

- **Clasificación y Control de Activos:** Su objetivo es clasificar jerárquicamente los activos de la organización y protegerlos de manera apropiada.

- **Control de Acceso:** Su objetivo es controlar y restringir el acceso a la información que es vital para la organización o es catalogada como confidencial.

- **Desarrollo y mantenimiento de los sistemas:** Su objetivo es implementar medidas de seguridad en el desarrollo (confidencialidad, copias de seguridad, acceso restringido), implementación y mantenimiento de los sistemas de información.

- **Administrador de Operaciones:** Su objetivo es contrarrestar las interrupciones en los procesos productivos, solucionar fallas y desastres.

- **Seguridad de los usuarios:** Su objetivo es reducir el riesgo que generan los errores humanos y también velar por la buena utilización de las instalaciones. (Capacitación permanente y adecuada para disminuir errores producidos por un manejo incorrecto o por desinformación)

- **Seguridad Física:** Su objetivo es impedir el acceso no autorizado y evitar daños y robos en la empresa.

- **Cumplimiento:** Su objetivo es hacer cumplir las políticas de seguridad anteriormente establecidas y hacer cumplir las obligaciones establecidas por las leyes, el reglamento, los contratos e imponer sanciones por incumplimiento de las mismas

- **Recursos:** La empresa en cabeza de la administradora cada año debe disponer de un rubro destinado a la seguridad de la información.

7.2.4.2 Organización de la Seguridad de la información.

Generalidades: Establecer la seguridad de la información como una de los objetivos vitales para la IPS.

Objetivo: Organizar, controlar y administrar la información dentro de la organización.

Alcance: Esta política se debe aplicar a todos los procesos de la IPS Medisalud de Valledupar tanto internos como externos.

Responsables: La responsabilidad de la organización de seguridad de la información está en cabeza de la administradora, seguida por director del comité de seguridad de la información y todos sus miembros así:

- **Comité de seguridad de la información:** Es el encargado de desarrollar la implementación de las políticas de seguridad. Se encargara de realizar seguimiento, monitoreo, análisis de riesgo, implementación de controles, velar por la continuidad y hacer conocer de los avances, cambios y dificultades a la dirección general.

- **Responsable del Área de Informática y de la seguridad informática:** Se encargara de dirigir la implementación de políticas de seguridad con la asesoría de profesionales especializados, e implementar medidas de seguridad como la restricción del acceso a la información que sea catalogada como confidencial

- **El comité de revisión Interna o control Interno:** Se encargara de revisar la vigencia y el cumplimiento de las políticas de seguridad.

- **Responsable del área de Administración:** Se encarga de destinar y disponer de recursos necesario para la adquisición de elementos necesarios para el cumplimiento de dichas políticas (Hardware, software, elementos de logística, asesoría especializada)

- **Responsable del Área Legal y Administrativa:** Responsable de informar a proveedores, y equipo de trabajo sobre las modificaciones en las políticas de seguridad.

Política: Infraestructura de la seguridad de la información

- **Organización Interna y coordinación de la seguridad de la información de la IPS Medicsalud de Valledupar:** Crear un comité de seguridad de la información que garantice el apoyo a la implementación de todas las medidas de seguridad.

- **Funciones del comité de seguridad:**
  - ✓ Revisar y proponer políticas de seguridad a la administradora.
  - ✓ Monitorear e identificar cambios que generen riesgos para la organización
  - ✓ Identificar amenazas y posibles vulnerabilidades.
  - ✓ Documentar y monitorear los incidentes concernientes a la seguridad
  - ✓ Evaluar las posibles soluciones y elegir la más adecuada encaminada a contribuir con la seguridad de la información.
  - ✓ Asegurase de que la seguridad haga parte del procesos de planificación de la organización
  - ✓ Determinar y organizar la implementación de controles de seguridad

- **Asignación de responsabilidades para la seguridad de la información:** La administradora asigna las funciones referentes a la seguridad informática al responsable del departamento de seguridad informática quien de ahora en adelante será el directo garante de la seguridad de la información de la empresa y responsable del cumplimiento de lo tratado en la presente política.

Asignación de responsabilidades, que deben quedar debidamente documentadas y aprobadas por el comité de seguridad de la información.

Proceso de autorización para los servicios de procesamiento de información: Los nuevos servicios de procesamiento de información deben ser autorizados previamente por el responsable de la seguridad de la información y deben ser autorizados para el usuario apropiado; de igual manera al implementar hardware y software se debe verificar que sean compatibles con el sistema actual e identificar e implementar controles de seguridad para portátiles y computadores personales nuevos que ingresan a la empresa.

Acuerdos sobre confidencialidad: Identificar y revisar con regularidad los requisitos de confidencialidad (suscribir contratos de confidencialidad y no divulgación para la protección de la información vital para la empresa.), que deben ser encaminados a proteger la información legalmente, para lo cual se debe tener en cuenta la clasificación de la información, en este caso se debe proteger la información confidencial, se debe definir por cuánto tiempo se va a proteger y designar un responsable para hacer buen uso de esta.

Contactos con las autoridades: La organización debe mantener contactos adecuados con las autoridades que especializadas en seguridad y delitos informáticos para comunicarse de manera inmediata en caso de ser necesario. (Saber cuándo y a quién dirigirse en caso de incidentes)
Contactos con grupos de interés especiales: Los responsables de la seguridad deben estar en contacto permanente con foros y empresas especializadas en seguridad ya que estos están a la vanguardia de las nuevas formas de ataque.

Revisión independiente de la seguridad de la información: El comité de revisión interna o control interno se encargara de realizar revisiones independientes para garantizar el cumplimiento de las políticas de seguridad. Este comité debe informar al

administrador de las fallas encontradas y de las mejoras y cambios que son necesarios implementarse. (La revisión la deben realizar profesionales idóneos o expertos en seguridad, de ser necesario se debe contratar personal externo para realizar dicha revisión)

Partes externas y coordinación de la seguridad de la información: Se debe controlar todo acceso a los servicios, comunicación, procesamiento de la información y comunicación que provienen de partes externas así:

- ✓ Se debe definir un convenio con la parte externa para compartir información
- ✓ Se deben identificar los riesgos provenientes de las partes externas e implementar controles adecuados antes de autorizar el acceso.
- ✓ Identificar los servicios de los que va disponer la parte externa.
- ✓ Definir el tipo de acceso que va a tener la parte externa: ya sea acceso físico, acceso lógico, acceso a la red etc.
- ✓ Identificar el valor y la sensibilidad de la información a la que van a tener acceso
- ✓ Implementar controles necesarios para proteger la información de terceros
- ✓ Conocer los controles y medidas que implementara la parte externa para el manejo y uso de la información
- ✓ Definir unos requisitos legales que está obligada a cumplir la parte externa para compartir información y servicios.
- ✓ Establecer y definir posibles medidas de contingencia en caso de fallos, errores, ataques etc.,
- ✓ Todo servicio con terceros se debe hacer mediante contrato y en cada contrato se deben definir claramente las obligaciones, las políticas de seguridad y las implicaciones legales en caso de incumplimiento.

Estas medidas deben ser tomadas para: Proveedores de servicios de red, de internet, de telefonía, de mantenimiento, de soporte, de auditoria, de gestión, de negocios, personal de trabajo temporal, clientes etc.

7.2.4.3 Gestión de Activos.

Generalidades: Una vez realizado el inventario de activos y la evaluación de riesgos se clasifican los activos de acuerdo a su sensibilidad y vulnerabilidad.

Objetivo: Clasificar la información de acuerdo a su grado de confidencialidad, definir niveles de protección y garantizar que los activos de la organización sean protegidos de manera adecuada

Alcance: Esta política se debe aplicar a todos los activos de la organización.
Responsables: La responsabilidad de la seguridad de la información está en manos de:

- **Responsables de la Información:** Son los encargados de clasificar la información de acuerdo a su grado de confidencialidad, mantener actualizada y

documentada la clasificación y de definir los permisos de acceso a los usuarios. Cada dependencia debe supervisar que la clasificación y rotulado de la información sea correcto.

Política

- **Inventario de Activos:** Se realiza un inventario de activos los cuales debe estar debidamente clasificados y ordenados según su importancia, propietario, ubicación e información almacenada, este inventario debe ser actualizado constantemente y conservarse de manera ordenada.

Clasificación de la información: Para clasificar la información de deben tener en cuenta los criterios básicos de seguridad:

Tabla 16: Clasificación de la Información

Categoría	Nivel de Confidencialidad:
0	Información pública: Que puede ser conocida por todo el personal interno y externo.
1	Reservada de uso interno (información que solo puede ser conocida por los miembros de la empresa).
2	Información reservada confidencial (información que solo es conocida por un grupo de la empresa).
3	Reservada secreta (información que solo es conocida por un grupo reducido de la empresa y su divulgación ocasionaría problemas o perdidas).
Categoría	Nivel de Integridad:
0	Si la información, es modificada sin previa autorización esta puede repararse y no afecta a la organización
1	Si la información es modificada sin previa autorización esta puede repararse , pero puede ocasionar perdidas leves
2	Si la información es modificada sin previa autorización esta no puede repararse y ocasiona pérdidas significativas a la organización.
3	Si la información es modificada sin previa autorización esta no puede repararse y ocasiona pérdidas graves a la organización Categoría Nivel
Categoría	Nivel de Disponibilidad:

0	Hace referencia a cuya información en caso de no poderse acceder, no afecta los procesos y servicios de la entidad.
1	Hace referencia a cuya información que en caso de no poderse acceder en un plazo largo como una semana, puede ocasionar pérdidas significativas a la empresa
2	Hace referencia a cuya información que en caso de no poderse acceder en un plazo corto como un día, puede ocasionar pérdidas significativas a la empresa
3	Hace referencia a cuya información que debe estar disponible todo el tiempo y la inaccesibilidad mayor a una hora puede ocasionar pérdidas significativas a la empresa
Criticidad baja: ninguno de los valores asignados superan el Criticidad media: alguno de los valores asignados es 2 Criticidad alta: alguno de los valores asignados es 3	

Fuente: El autor.

Teniendo en cuenta los anteriores criterios el propietario se encarga de clasificarla e identificar los elementos asociados:

- **Rotulado de la información:** Definir procedimientos de rotulado, almacenamiento y físico y electrónico de la información de acuerdo a su Nivel De Criticidad.

7.2.4.4 Seguridad de los recursos humanos.

Generalidades: Es fundamental educar y concienciar al personal sobre la importancia de la aplicación de las políticas de seguridad, desde el primer instante que se ingresa a la empresa y de las sanciones que conlleva el incumplimiento de las mismas. Por lo tanto es importante que el personal este consiente de la importancia, este capacitado y en caso de ocurrir un incidente informar en qué condiciones ocurrió para establecer mecanismos que conduzcan a que dichas fallas o incidentes no vuelvan a ocurrir y establecer los correctivos necesarios.

Objetivo: Minimizar los riesgos ocasionados por errores humanos y promover un uso adecuado de los recursos informáticos así como capacitar y concienciar sobre la importancia de la aplicación de las políticas de seguridad e información oportuna de incidentes para ser corregidos en debida forma.

Alcance: Esta política se debe aplicar a todo el personal de la organización, interno y externo

Responsables:

- El personal de recursos humanos que es el encargado de seleccionar el personal, informara, capacitara y establecerá acuerdos de confidencialidad y de cumplimiento de todas las políticas de seguridad con el personal que ingrese a la empresa.

- Responsable del Área Legal y Administrativa: Es el responsable de establecer términos y condiciones laborales. Mediante cláusulas en los contratos los acuerdos de confidencialidad y cumplimiento de políticas de seguridad con todo el personal y con terceros.

- Responsable de la seguridad informática: Se encargara de capacitar y concienciar al personal con asesoría de profesionales especializados, sobre el uso correcto de los recursos informáticos y el cumplimiento de las políticas de seguridad así como del acuerdo de confidencialidad.

Política

- **Antes de la contratación Laboral:** La organización antes de la contratación laboral debe documentar los roles y responsabilidades que estos van a desempeñar.

  En la selección del personal se debe revisar antecedentes (hoja de vida, experiencia laboral, experiencia crediticia etc.). Se debe seleccionar y clasificar que información va estar disponible para estos tanto para personal como para terceros.

  Términos y condiciones laborales: Tanto para empleados como para terceros estos deben conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad, la confidencialidad y se debe verificar que los contratos estén firmados. (El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento).

- **Durante la Vigencia del contrato:** La dirección debe exigir que los empleados y terceras partes cumplan a cabalidad con las políticas de seguridad establecidas por la empresa. Para esto debe darles a conocer las políticas de seguridad, motivarlos y verificar que estén de acuerdo con los términos y condiciones establecidas en el contrato laboral.

Capacitación y formación: La organización capacitara e informara sobre las políticas de seguridad establecidas en la organización, así mismo capacitara e informara cuando se presenten cambios y modificaciones.

La capacitación al personal y a terceras partes se realizara por personal especializado de la organización que resalte la importancia del cumplimiento de las políticas de seguridad y les enseñe como detectar posibles fallas e incidentes y les explique cómo comunicar estas fallas a la organización.

La organización lleva a cabo verificaciones del cumplimiento de las obligaciones en los puestos de trabajo.

El empleado debe someterse a: Cumplir con el control y la política de seguridad, formar y cumplir el compromiso de confidencialidad, cumplir los términos y condiciones del contrato, capacitarse, comunicar sobre incidentes y anomalías.

Para el personal y terceras partes que violen o incumplan las políticas de seguridad se llevara a cabo un proceso disciplinario de acuerdo a los estatutos de la empresa.

- **Terminación o Cambio del contrato laboral:** La organización gestiona de manera adecuada la terminación del contrato o cambio de contrato y una vez terminado el contrato verifica la suspensión de los servicios, la devolución de los activos, devolución de documentos, dispositivos (pc, celulares, usb etc), verifica y gestiona el cambio de contraseñas. Los responsables de realizar estos procesos son el responsable de seguridad.

7.2.4.5 Seguridad física y del entorno.

Generalidades: Para la seguridad física se deben tener en cuenta los siguientes aspectos: La protección física de acceso, protección y mantenimiento de equipos de acuerdo a su importancia, los posibles daños e interferencias; El mantenimiento de las instalaciones se debe hacer bajo estrictas normas de seguridad.

Objetivo: Evitar el daño, interferencias y el acceso no autorizado a la información de la entidad de salud.
Alcance: Esta política se debe aplicar las instalaciones de la entidad de salud y todos sus equipos, expedientes, cableados, documentación etc.

Responsables:

- **Responsable de la seguridad informática:** Este se encargara de dirigir las políticas a seguir en el resguardo de los equipos, su mantenimiento y control de acceso etc. También se encargara de clasificar las áreas (Para servidores se creara un área restringida que tendrá un tratamiento especial).

- **El Responsable del Área informática** se encargara de adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.

Política

- **Perímetro de Seguridad Física:** El comité de seguridad con el responsable de seguridad definen un perímetro de seguridad para el área considerada como crítica que si no existen se debe crear (almacena todos los dispositivos considerados vitales como servidores y almacenamiento de información confidencial) y se deben adoptar las siguientes medidas:

  - ✓ Definir claramente el perímetro de seguridad
  - ✓ Establecer barreras de seguridad
  - ✓ Definir el personal autorizado para el acceso al área restringida.

- **Controles de Acceso Físico:** El responsable de la seguridad junto con el responsable del área de informática establecerán controles de acceso al área restringida:

  - ✓ Limitar el acceso al área donde se encuentra almacena la información, llevar un registro solo del personal autorizado.
  - ✓ Verificar que el personal que ingrese porte un documento visible que lo catalogue como personal autorizado.
  - ✓ Revisar periódicamente los registros del personal que accede.
  - ✓ Actualizar constantemente la lista de personal autorizado.

- **Seguridad de Oficinas e instalaciones:** Se debe tener en cuenta las condiciones de iluminación ventilación salubridad, equipamiento antiincendios, medidas que prevengan inundaciones robos etc. Preferiblemente el área de oficinas y atención al público debe estar alejada del área restringida, disponer de guardias de seguridad y de alarmas.
- **Ubicación y protección de copias de seguridad y equipamiento:** El equipamiento se ubicara en un sitio donde se minimice el riesgo, es decir en un lugar aislado y protegido tanto de amenazas naturales ambientales, físicas y humanas, adicional a esta medida se restringirá el acceso. Por lo tanto solo podrá acceder personal autorizado con su credencial y los ingresos y tareas a realizar serán debidamente documentadas por el responsable de la seguridad; las labores de aseo serán verificadas para evitar daños y hurtos.

- **Suministro de Energía:** Periódicamente se deben revisar el buen funcionamiento de las instalaciones eléctricas para evitar incidentes, la organización debe optar por contrarrestar fallas en el suministro de energía tales como la adquisición de una planta eléctrica, la compra de ups para los pc etc.

- **Seguridad en el Cableado:** Proteger el cableado que transporta datos de daños e interceptación cumpliendo con las normas, que el cableado baya por conductos seguros, separa los cables de energía de los cables de comunicación etc.
- **Mantenimiento de Equipos:** Los responsables del área de informática deben someter todos los equipos periódicamente a mantenimiento preventivo, este mantenimiento debe ser registrado y documentado, cada equipo debe tener un inventario de dispositivos para saber qué cambio se hicieron y que dispositivos se retiraron.

- **Seguridad en la reutilización o eliminación de equipos:** Cuando un equipo es cambiado de sitio o eliminado se debe tener total precaución con los dispositivos de almacenamiento como discos duros los cuales deben ser formateados o destruidos de forma segura para evitar incidentes con la información.

7.2.4.6 Gestión de operaciones y comunicaciones.

Generalidades: La IPS Medicsalud debe crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de comunicación.

Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la proliferación y expansión de software malicioso que son catalogadas como amenazas en potencia, garantizar el adecuado funcionamiento de los sistemas de información y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques

Alcance: Esta política se debe aplicar a todo el sistema informático (red, servidores, comunicaciones y equipos) etc.

Responsables:

- **El responsable de la seguridad informática:** Sera el encargado de definir procedimientos para el control actualización y modificación de los sistemas operativos tanto de servidores como pcs.

    - ✓ Toda actualización, modificación y mantenimiento debe estar debidamente documentada
    - ✓ Definir mecanismos para el reporte y manejo de incidentes
    - ✓ Definir políticas de control para el uso de correo electrónico, consulta de páginas, navegación en internet y uso de redes sociales.
    - ✓ Adquirir antivirus licenciado y verificar que las actualizaciones se estén realizando periódicamente.
    - ✓ Establecer y verificar políticas de control de usuarios mediante contraseñas y gestión de privilegios.
    - ✓ Controlar la realización de copias de seguridad

- ✓ Solicitar recursos para actualizaciones (Software) para cubrir necesidades a futuro en materia de seguridad.
- ✓ Adquirir herramientas de monitoreo de sistemas y verificar que estén siendo utilizadas para tal fin
- ✓ Establecer protocolos para la destrucción de herramientas de almacenamiento, como discos duros, cintas, usb (en el caso de ya no ser necesarias)
- ✓ Todo procedimiento debe ser debidamente documentado.

- **El Responsable del Área informática** se encargara de adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.

- **El responsable del área legal,** junto con el responsable de la seguridad y el responsable de área informática se encargaran de verificar y hacer cumplir a cabalidad los contratos y acuerdos.

Política

- **Procedimientos y responsabilidades operativas**

  - ✓ Documentación de los procedimientos operativos: Los S.O. se actualizarán permanentemente y toda actualización y modificación de los S.O. será autorizada por el responsable de seguridad y debidamente documentada y realizada por el área de informática.
  - ✓ Control de Cambios en las Operaciones: Todo cambio debe ser evaluado y aprobado previamente y se tendrán en cuenta los siguientes aspectos: Evaluación del cambio y posible impacto, planificación, prueba, e identificación de responsabilidades en caso de que el cambio sea fallido.
  - ✓ Procedimientos de Manejo de incidentes: El responsable de la seguridad junto con el jefe del área de informática establecerán protocolo para el manejo de incidentes tales como: Definir los posibles tipos de incidentes (Fallas operativas, código malicioso, intrusiones, fraude informático, error humano, desastres naturales). En caso de presentarse incidentes comunicarlos a la dirección y seguir el plan de contingencia, implementar controles de acceso a los sistemas y medidas de recuperación.

- **Planificación y Aprobación de sistemas**

  - ✓ **Planificación de la Capacidad:** El responsable del área de seguridad informática es el encargado de evaluar constantemente las necesidades a futuro de los S.O. para evitar posibles fallas.
  - ✓ **Aprobación del sistema:** El responsable de la seguridad y el responsable del área informática sugieren a la dirección las posibles especificaciones necesarias para actualizar los sistemas Operativos.

- **Protección Contra software malicioso:** El responsable de la seguridad y el responsable del área de informática definen los siguientes criterios de seguridad y el cumplimiento de los mismos:

  - ✓ Prohibir las instalaciones y descargas en los pc de la empresa.
  - ✓ Verificar constantemente el contenido del software
  - ✓ Escanear constantemente el software
  - ✓ Monitorear constantemente el software de los servidores
  - ✓ Antes de realizar instalaciones o cambios verificar que toda información entrante esté libre de virus
  - ✓ Concientizar al personal de la importancia de la protección en el manejo de la información.

- **Mantenimiento**

  - ✓ **Resguardo de la información:** Los responsables de la información definirán un esquema de protección de la información entre ellas: Copias de seguridad y prueba de restauración, definir un esquema de rotulado de copias, almacenar copias de seguridad en una ubicación remota, el almacenamiento de copias de seguridad debe estar físicamente protegida con un esquema de seguridad especial.

  - ✓ **Registro de actividades del personal operativo:** El responsable de seguridad debe llevar un registro del uso de los sistemas como: Tiempo de inicio, cierre, errores del sistema, intentos de acceso al sistema, medidas tomada etc

  - ✓ **Registro de fallas:** El responsable de seguridad debe llevar un registro fallas en los sistemas, como fueron resueltas, medidas correctivas etc (documentar todas las fallas de los sistemas)

- **Administración de la Red:** El responsable de la seguridad define y toma las medidas necesarias para proteger la red de datos para evitar posibles daños, interferencias etc.

  - ✓ Establece procedimiento de administración y delega un responsable que debe documentar todos los procedimientos realizados en la red
  - ✓ Establecer controles para asegurar la disponibilidad, la confidencialidad y la integridad de la información.
  - ✓ Garantizar mediante actividades de supervisión que los controles se apliquen.

- **Administración de medios de almacenamiento:** El responsable de la seguridad y el responsable del área de informática establecerán y verificaran el cumplimiento del correcto almacenamiento de respaldos de seguridad y eliminación de información de cintas magnéticas, discos duros para evitar incidentes con el manejo de la información.

- ✓ **Eliminación de medios de información:** El responsable de la seguridad y el responsable del área de informática deben verificar la correcta eliminación de información desde dispositivos de almacenamiento.

- ✓ **Procedimientos de manejo de información:** Para almacenar la información los empleados deben seguir el siguiente procedimientos tales como: Proteger documentos, redes y dispositivos informáticos, restringir el acceso a personal no autorizado, conservar los dispositivos de almacenamiento en medios seguros.

- ✓ **Seguridad de la documentación del sistema:** La documentación del sistema debe estar almacenada en un lugar seguro y el acceso a esta debe ser restringido

- **Intercambios de Información y de Software:** Se debe utilizar medios de mensajería confiable, se deben de tener en cuenta las siguientes recomendaciones: Uso adecuado por de la mensajería electrónica por parte del personal, no abrir mensajes de remitentes desconocidos, toda información que llega debe ser escaneada, se debe conocer los posibles riesgos de seguridad a los que se enfrenta un usuario al utilizar mensajería electrónica (interceptación, robo, engaños, bombas lógicas etc.) y transferir por este medio información confidencial.

7.2.4.7 Control de Acceso.

Generalidades: La política de control debe ser documentada, revisada y actualizada constantemente con el fin de evitar el acceso a los sistemas de información, bases de datos y documentos por personal no autorizado que pongan en peligro la información de la empresa.

Objetivo: Controlar el acceso a la información

Alcance: Esta política se aplica a todas los procesos o formas de acceso a los sistemas de información, bases de datos o servicios de información de la empresa.

Responsables:

- **Responsable de la seguridad informática:** Es el encargado de definir normas, pautas y procedimientos para los accesos a los sistemas, bases de datos y servicios de información (acceso a los pc, acceso a la red, acceso a los servidores, acceso a internet, acceso a claves de seguridad, acceso a transacciones etc.). También debe realizar un control de los privilegios de los usuarios y concientizar a los usuarios de la importancia de la no divulgación de las contraseñas

- **El Responsable del Área informática** Se encarga de dirigir normas y procedimientos para implementar Sistemas operativos, Gateway, firewall, servicios de red etc., debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión. Además debe promover y realizar la gestión de contraseñas y privilegios, capacitar y concientizar a los usuarios de la utilización de las medidas de control de acceso.

Política

- **Política de Control de acceso:** El responsable del área de informática cumplirá con las siguientes funciones:

  - ✓ Implementar métodos de autenticación y control de acceso
  - ✓ Segmentar la red
  - ✓ Implementar el control de puertos y ruteo de red
  - ✓ Efectuar un control de los registros de auditoria.
  - ✓ Definir perfiles de acceso
  - ✓ Controlar los cambios en los accesos

- **Administración de accesos de usuarios**

  ✓ **Registración de usuarios:** Definir un registro formal de usuarios para otorgar y revocar accesos, utilizar identificadores de usuarios únicos.

  ✓ **Administración de Privilegios:** Identificar los privilegios, asignar los privilegios de acuerdo a las necesidades del trabajo, mantener un registro actualizado de los privilegios.

  ✓ **Administración de contraseñas de usuario:** Los usuarios deben comprometerse a utilizar y mantener en secreto sus contraseñas esto debe estar estipulado en el contrato laboral, cambiar periódicamente las contraseñas, las contraseñas deben cumplir con todos los criterios de seguridad.

  ✓ **Administración de contraseñas críticas:** Para realizar configuraciones, asignaciones y cambios en los servidores etc., se utilizara contraseñas con un nivel de complejidad más alto

- **Responsabilidad de los usuarios:** Los usuarios deben usar contraseñas, deben mantener la contraseña en secreto, pedir cambio de contraseña en caso de riesgo, usar contraseñas de calidad etc. El usuario está obligado a proteger los equipos asignados, no debe dejar los equipos abandonados o desatendidos, una vez

terminado un servicio debe cerrar cesión, cerrar cesión después de utilizar correos electrónicos, apagar el equipo en forma correcta.

- **Control de acceso a la red:** El responsable de la seguridad informática es el encargado de otorgar los permisos para el acceso a la red y sus recursos, realizar normas y procedimientos de autorización, establecer controles y procedimientos de control de acceso, para autenticación de usuarios para conexiones externas debe de escogerse un método de autenticación, un protocolo de autenticación, a autenticar las conexiones a sistemas informáticos remotos, protección de puertos para evitar accesos no autorizados, en lo posible subdividir o segmentar la red para realizar procesos separados con el fin de que si se presenta un incidente no se contamine toda la red o si un espía ingresa a esta no tenga acceso a toda la información, por otra parte se debe controlar el acceso lógico a los servicios, configurar los servicios de manera segura etc. El acceso a internet solo será autorizado por el jefe del área de informática.

Se debe restringir algunos servicios como: Utilización de correo electrónico, transferencias de archivos, acceso interactivo y acceso a red fuera del horario laborar.

- **Control de Acceso al sistema operativo:** Los responsables de la seguridad y el jefe del área de informática deben definir los procedimientos para realizar la protección de los sistemas operativos, el acceso a los servicios de información solo se realizara a través de un proceso de conexión seguro, limitar el tiempo para el procesos de conexión, limitar el número de intentos de conexión; todos los usuarios utilizaran contraseñas seguras.

- **Control de Acceso a las aplicaciones:** Controlar los derechos los acceso de los usuarios, restringir la información, controlar el acceso a las funciones de los sistemas, revisar las salidas de información es decir que solo se envié la información solicitada.

- **Monitoreo de acceso y uso de los sistemas:** Revisar y monitorear que los usuarios solo estén realizando actividades que hayan sido autorizadas previamente, se debe monitorear, el acceso, la identificación de usuarios, fecha y hora de eventos, archivos accedidos, se debe supervisar el inicio y cierre del sistema, las operaciones con privilegios, cambios de configuración del sistema, intentos de acceso no autorizado, alertas fallas del sistema etc.

7.2.4.8 Adquisición, desarrollo y mantenimiento de sistemas de información.

Generalidades: Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

Objetivo: Adoptar medidas de seguridad en la implementación de los sistemas de información.

Alcance: Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la entidad.

Responsables:

- **Responsable de la seguridad informática, el propietario de la información** se encargaran de definir e implementar controles en el desarrollo y mantenimiento de sistemas de información.

- **El Responsable del Área informática** se encargara de definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.

- **El responsable del área legal y administrativa,** se encargara del licenciamiento del software adquirido y en el caso del software desarrollado por la organización de establecer las políticas de derechos de autor y fijar las condiciones de los contratos y de entrega.

Política

- **Requerimientos de seguridad de los sistemas:**

  - ✓ **Análisis y especificaciones de los requerimientos de seguridad:** Identificar y definir los requerimientos y controles necesarios en materia seguridad desde las etapas de análisis y diseño del sistema ya que implementar medidas de seguridad desde estas etapas sale menos costoso que hacerlo después.

  - ✓ **Seguridad en los sistemas de aplicaciones:** Se debe establecer controles de los registro de auditoria para evitar la pérdida de los datos de los sistemas de información (validación y autenticación de los datos de entrada y de salida)

  - ✓ **Validación de datos de entrada:** Se debe establecer un control de validación de los datos de entrada como: Revisión periódica de contenidos e campos claves, se debe establecer como se realizara y con qué método, además se definirá las responsabilidades del personal.

  - ✓ **Controles de procedimientos interno:** El responsable de la seguridad junto con el jefe del área de sistemas deben establecer controles para la etapa del diseño, se deben implementar procedimientos que permitan identificar el uso y localización en los aplicativos, controles y verificaciones, revisión periódica de los registros, controles de integridad de los registros y de los archivos,

controles que verifique la consecución y orden en la ejecución de los aplicativos.

- ✓ También se deben implementar controles para la autenticación de mensajes y para la validación de datos de salida.

- **Controles criptográficos**

  - ✓ **Política controles criptográficos:** Se debe utilizar controles criptográficos para los siguientes casos: Protección de claves de acceso a sistemas, datos y servicios, transmisión de información clasificada, resguardo de información. El responsable de la seguridad se encargara de definir la política de controles criptográficos, el método y el responsable de administración de claves (Uso de algoritmo de cifrado y firma digital, servicios de no repudio)

  - ✓ **Administración de claves:** El responsable de administrar las claves debe aplicar las políticas de protección de las claves implementando un sistema de administración de claves criptográficas que permitan usar técnicas de clave secreta, estas claves serán protegidas contra copia, destrucción, divulgación, modificación etc.

- **Seguridad de los procesos de soporte**

  - ✓ **Procedimiento de control de cambios:** Verificar que los cambios sean propuestos por personal autorizado, mantener un registro del nivel de autorización, identificar todos los elementos que requieren modificaciones, obtener aprobación por parte del responsable del área de informática para cumplir con los requerimientos del software.

  - ✓ **Revisión técnica de los cambios en el sistema operativo:** Antes de realizar cambios en el sistema operativo se debe revisar y verificar que los cambios son necesarios, que impacto genera, informar al área involucrada y verificar la continuidad del negocio.

  - ✓ **Restricción del cambio de paquetes de software:** Se debe evaluar la necesidad, los costos, la parte legal (licencias) y el impacto del cambio que este genera en la organización

  - ✓ **Canales ocultos y código malicioso:** Se debe adquirir software a personal confiable y conocido, examinar códigos fuentes que estén libres de virus, llevar un control de acceso al software y las modificaciones instaladas, utilizar antivirus y software de monitoreo y escaneo.

  - ✓ **Adquisición de software:** Para la adquisición de software a terceros se deben establecer condiciones puntuales rigurosas tales como: acuerdos de licencias,

procedimientos certificación de calidad, calidad en el software, verificación del cumplimiento de las condiciones de seguridad.

7.2.4.9 Gestión de los incidentes de seguridad de la información.

Generalidades: Todos los empleados de la IPS Medicsalud deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata.

Alcance: Esta política la deben cumplir todos los empleados de la Entidad de salud.

Responsables:

- **Responsable de la seguridad informática:** El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos empleados para conozcan cual es el procesos a seguir en caso de presentarse una falla. Es decir cómo y a quien reportarlo para que se tomen los correctivos necesarios.

- **El Responsable del Área informática:** debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

Política

- **Reportes sobre los eventos de seguridad de la información:** Se debe establecer un punto de contacto que siempre esté disponible y brinde respuesta oportuna y adecuada a los incidentes. Todos los empleados deben estar informados sobre la obligatoriedad de reportar e informar sobre incidentes, fallas, vulnerabilidades y debilidades observadas en el sistema (los empleados para reportar los incidentes deben diligencian un formato).

- **Gestión de incidentes y las mejoras en la seguridad de la información:** La organización en cabeza del responsable de la seguridad establece procedimientos para el manejo de eventos y debilidades de la seguridad. Se debe evaluar y gestionar todos los incidentes de seguridad de la información así:
  - ✓ **Responsabilidades y procedimientos:** Establecer procedimientos para manejar eventos como: Fallas en el sistema, virus, negación del servicio, violación de confidencialidad, integridad y disponibilidad, uso inadecuado de los sistemas informáticos, código malicioso; identificar la causa, implementar acciones correctivas y reportar todo el procesos realizado al responsable de la seguridad.

- ✓ **Aprendizaje debido a los incidentes de seguridad informática:** El responsable del área de informática, debe llevar un registro de los incidentes presentados, de cómo se han manejado, las posibles causas y cuanto le cuestan a la empresa resolverlos, para en un futuro no cometer los mismos errores.

- ✓ **Recolección de Evidencia:** En el caso de llevar a cabo una acción disciplinaria, se debe recolectar la evidencia siguiendo las siguientes pautas: No se debe manipular la evidencia, se debe crear una copia intacta de la evidencia y esta debe ser resguarda a través de una cadena de custodia.

7.2.4.10 Gestión de la continuidad del negocio.

Generalidades: Es indispensable que toda empresa disponga de un procesos de gestión de continuidad del negocio en caso de llegarse a presentar una eventualidad como un desastre natural, robo, daños en los servidores etc.

Objetivo: Asegurar el funcionamiento continuo de la organización

Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de la empresa.

Responsables:

- **El comité de seguridad junto con el responsable de la seguridad informática** debe identificar las amenazas, evaluar los riesgos identificar controles preventivos, desarrollar un plan estratégico y un plan de contingencia.
- **El Responsable del Área informática** participara en la elaboración y documentación del plan de contingencia.

Política

- **Proceso de la administración de la continuidad de la empresa:** El comité de la seguridad será el encargado de identificar los procesos críticos, asegurarse de que todos los empleados de la empresa comprendan y conozcan los riesgos, elaborar y documentar una estrategia de continuidad del negocio y proponer la adquisición de pólizas y seguros
- **Continuidad de las actividades y análisis de los impactos:** Antes de elaborar el plan de contingencia el comité de seguridad debe identificar los eventos o amenazas, evaluar los riesgos e identificar controles preventivos. Todo esto debe estar debidamente documentado.

- **Elaboración e implantación de los planes de continuidad de las actividades de la empresa:** El comité de seguridad junto con el responsable de la seguridad debe elaborar el plan de contingencia que debe contemplar los siguientes aspectos: Responsables de los procedimientos de emergencia, definir acciones y

correctivos, implementar procedimientos de emergencia, documentar estos procedimientos e instruir al personal; actualizar constantemente el plan de contingencia.

- **Marco para la planificación de la continuidad de las actividades de la empresa:** Se debe especificar claramente los requisitos y condiciones para su puesta en marcha, los responsables y los requerimientos etc. Adicionalmente debe prever las condiciones de implementación, definir los procedimientos de emergencia, y las acciones a realizarse, describir los procedimientos de recuperación, definir un cronograma de mantenimiento y documentar las responsabilidades y funciones de las personas. (elaborar un documento muy completo del plan de contingencia.)

- **Ensayo, mantenimiento y reevaluación de los planes de continuidad de la empresa:** El comité de seguridad establecerá un cronograma de pruebas, el cronograma señalara quienes son los responsables, efectuara pruebas, realizara simulaciones y pruebas completas en las instalaciones, involucrando procesos y con todo el personal.

7.2.4.11 Cumplimiento.

Generalidades: Todas las empresas deben cumplir con las obligaciones estipuladas por la ley.

Objetivo: Cumplir con todas las obligaciones estipuladas por la ley

Alcance: Esta política se debe aplicar a todo el personal de la empresa.

Responsables:

- **Responsable de la seguridad informática:** Este se encargara de definir procedimientos encaminados a cumplir con todas las normas y restricciones legales, se encargara de realizar revisiones periódicas a la empresa para verificar el cumplimiento de las políticas de seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.
- **Todos los empleados y directivos** están obligados a conocer y dar a conocer a cumplir y hacer cumplir la presente política y la normativa vigente.

Política

- **Cumplimiento de requisitos legales:**

  - ✓ **Identificación de la legislación aplicable:** Se definirán claramente los requisitos normativos contractuales.

- ✓ **Derechos de propiedad intelectual:** Solo se podrá utilizar material autorizado, respetando la propiedad intelectual.

- ✓ **Derecho de propiedad intelectual del software:** El responsable de la seguridad junto con el responsable del área de informática implementar controles y procedimientos para el manejo de licencias.

- ✓ **Protección de los registros de la empresa:** Los registros críticos serán debidamente protegidos contra pérdida, falsificación o robo. Para el almacenamiento y protección de los registros contables, base de datos y otros de estos se debe realizar un inventario, implementar controles, y establecer procedimientos de almacenamiento, divulgación, manipulación o eliminación.

- ✓ **Protección de datos:** Todos los empleados están obligados a cumplir un compromiso de confidencialidad es decir a utilizar la información solo para bien de la IPS Medicsalud.

- ✓ **Prevención del uso inadecuado de los recursos de procesamiento de información:** Cuando un empleado utilice la información o los recursos de la organización sin ser autorizado será considerado como uso indebido y esto va en contra de las normas de la empresa y puede estar sujeto a sanciones.

- ✓ **Regulación de controles para el uso de criptografía:** Para hacer usos de herramientas criptográficas el responsable del área legal junto con el responsable del área de seguridad deben cumplir con las leyes de firma digital y encriptación vigentes en el país, una vez conozcan las normas de uso, se implementan los controles y se dan a conocer al encargado.

- ✓ **Recolección de Evidencia:** Cuando una acción indebida o inapropiada involucre la aplicación de la ley, la evidencia presentada debe cumplir con lo establecido en las leyes que rigen a nuestro país.

  Para la recolección de la evidencia se debe cumplir con las siguientes condiciones: Realizar una copia de seguridad para que la evidencia original no sea modificada, guardar la evidencia en un sitio seguro.

- **Revisión de las políticas de seguridad y la compatibilidad técnica**

  - ✓ Cumplimiento de las políticas de seguridad: El responsable del área de informática realizara revisiones del cumplimiento de las políticas de seguridad en la empresa.

  - ✓ Verificación de la compatibilidad técnica: El responsable de la seguridad revisara que los controles para el hardware y el software sean implementados correctamente.

- **Auditorías de sistemas**

  - ✓ Controles de auditoria de sistemas: Cuando se realicen auditorías a los sistemas, el responsable de la seguridad debe definir el área a auditar, controlar el alcance de las comprobaciones, limitar la auditoria para evitar modificaciones.

  - ✓ Protección de los elementos utilizados por la auditoria de sistemas: El responsable de la seguridad debe definir instrucciones y procedimientos para el acceso archivos, datos o software.

- **Sanciones previstas por incumplimiento:** El incumplimiento o violación de las políticas de seguridad implica sanciones, de acuerdo a los contratos suscritos con la empresa y en caso de acciones legales se procederá de acuerdo a la ley.

7.2.5. Identificación y análisis de los requerimientos de seguridad según la norma ISO 27001:2013.

7.2.5.1 Declaración de aplicabilidad. Se recomienda contar un documento de declaración de aplicabilidad (Dda) porque con este documento se puede determinar con mayor claridad el tratamiento a seguir para cada uno de los activos, se verifica el cumplimiento de cada uno de los controles establecidos por la norma ISO/IEC 27002:2013 a través del método de observación directa y entrevistas al personal.

El método de observación directa consto de varias visitas guiadas y supervisión de todas salas y oficinas pertenecientes a la IPS MedicSalud. Esto se complementó con revisión documental de los manuales de funciones y procedimientos, formatos, etc.

Para la declaración de aplicabilidad de la IPS Medicsalud, se ha tenido en cuenta los siguientes documentos: Los 133 controles sugeridos en el Anexo A de la norma ISO 27001, las política de Seguridad de la Información, la evaluación y tratamiento de riesgos y el Informe de evaluación y tratamiento de riesgos. Una vez identificados los riesgos la declaración de aplicabilidad permite identificar los controles necesarios documentando si cada uno de estos controles es aplicable o no o si ya está implementado o no.

La declaración de aplicabilidad se realizó sobre el análisis de riesgos teniendo en cuenta los siguientes parámetros:

- Dominio: Que indica el número del control de acuerdo al anexo A de la Norma ISO/IEC 27001.
- Controles según la ISO/IEC 27001: Se identifica el nombre del control
- Aplicabilidad: Se identifica si es o no es aplicable a la IPS MedicSalud.
- Justificación: Explica porque es o no es aplicable dicho control.
- Estado del control.

- Objetivo del Control
- Recomendaciones de actividades para la implementación de los controles

El estado del control se lo identifica y clasifica con la siguiente tabla teniendo en cuenta la abreviatura y el color

Tabla 17. Estado de los Controles

Estado	Abreviatura
Planificado [No implementado]	(P)
Parcialmente implementado	(PI)
Totalmente implementado	(TI)

Fuente: Basado en Magerit

7.2.5.2 Aplicabilidad de los Controles.

Tabla 18. Lista de controles

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
5	Políticas de seguridad							
5.1	Políticas de seguridad de la información.							
5.1.1	Documentos de políticas de seguridad de la información	Si	La implementación de las políticas de seguridad debe estar debidamente documentada y para que sirva como guía en la implementación del SGI			X	Garantizar que los procedimientos para el manejo de la información sean conocidos por los miembros de la IPS MedicSalud.	Debe documentar todos los procesos a desarrollarse para la implementación de la seguridad
5.1.2	Revisión de las políticas de seguridad de la información	Si	Es necesario revisar seguidamente las políticas de seguridad para verificar el cumplimiento de las mismas			X	Garantizar que las políticas de seguridad de la información se mantengan actualizadas.	Se recomienda que las políticas se revisen a menos una vez al año.
6	Aspectos organizativos de la seguridad de la información.							
6.1	Organización interna							
6.1.1	Compromiso de la dirección con la seguridad de la información	Si	Cada trabajador debe conocer cuáles son sus responsabilidades frente al manejo de la información en la IPS MedicSalud para asumirlas de manera adecuada, además conocer el rol que desempeña.			X	Garantizar que sólo personas dentro de cierta jerarquía dentro de la empresa tengan acceso a la información.	Establecer las políticas para la gestión de privilegios.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
6.1.2	Coordinación de la seguridad de la información	Si	Es importante que cada empleado que labora en la IPS MedicSalud conozca su límite en el manejo de la información		X		Garantizar que sólo personas idóneas tengan acceso a la información.	Fijar políticas de seguridad para el interior de la empresa acerca de la gestión de la información
6.1.3	Asignación de las responsabilidades relativas a la seguridad de la información	Si	Los empleados de la IPS MedicSalud que tiene acceso a la información deben contribuir de manera exhaustiva al mejoramiento de la seguridad dentro de la empresa			X	Garantizar que las políticas de seguridad de la información estén acordes con los requerimientos y exigencias del entorno.	Proponer planes de capacitación para la gestión de la información a cargo del personal.
6.1.4	Procesos de autorización de recursos para el tratamiento de la información	Si	Los empleados de la IPS MedicSalud que tiene acceso a la información deben contribuir de manera exhaustiva al mejoramiento de la seguridad dentro de la empresa			X	Garantizar que las políticas de seguridad de la información estén acordes con los requerimientos y exigencias del entorno.	Proponer planes de capacitación para la gestión de la información a cargo del personal.
6.1.5	Acuerdos de confidencialidad	Si	Se deben definir acuerdos de confidencialidad para el manejo de la información que deben quedar establecidos en el contrato laboral o en los contratos de prestación de servicios		X		Garantizar el adecuado manejo de la información en todos los niveles de acceso a la misma.	Fijar acuerdo de confidencialidad para el personal de la empresa
6.1.6	Contacto con las autoridades	Si	La información debe ser manejada de acuerdo a las políticas de seguridad y a través de canales de comunicación seguros para evitar incidentes.		X		Evitar fallas en los canales de comunicación para el manejo de la información.	Se debe definir canales seguros para la gestión de la información

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
6.1.7	Contacto con los grupos de especial interés	Si	Para el cumplimiento de los objetivos y alcances del SGSI se deben definir políticas internas para la protección de la información que deben ser conocidas por todos los empleados de la IPS MedicSalud.			X	Estandarizar el manejo de la información a nivel interno.	Se debe establecer políticas para el manejo de la información dentro de la organización.
6.1.8	Revisión independiente de la seguridad de la información	Si	Se debe definir de qué manera serán adoptadas y modificadas las políticas de seguridad cuando se presenten cambios en los activos de la empresa (nuevos programas, nuevos servicios etc.)			X	Dinamizar las políticas de seguridad para que se ajusten a los nuevos activos que entran a formar parte de la empresa.	Establecer reglas pensadas en futuros activos que formaran parte de la empresa
6.2	Terceros							
6.2.1	Identificación de los riesgos derivado del acceso a terceros	No	Es necesario identificar los posibles riesgos asociados a los accesos otorgados a la información entidades externas o a terceros, considerando el uso de aplicaciones web y portales electrónicos.(cuando se dé la conectividad con planeación y se haga uso de un servidor web)				Identificar los riesgos asociados al acceso a la información y sistemas de información por parte de terceros.	Se debe definir controles de acceso a la información redundantes
6.2.2	Tratamiento de la seguridad en la relación con los clientes	No	Es necesario que los terceros que necesiten acceder a la información conozcan bajo qué condiciones pueden tener acceso a la información.				Brindar lineamientos a la hora de que un clienta requiera tener acceso a la información.	Se debe definir controles de seguridad para clientes externos.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
6.2.3	Tratamiento de la seguridad en contratos con terceros	No	Cualquier convenio o acuerdo realizado con otra entidad como planeación que implique la relación con los activos internos (información) de la entidad deben garantizar el cumplimiento de requisitos de seguridad.				Establecer controles de seguridad para el acceso a activos internos de la empresa por parte de terceros.	Se debe establecer reglas o políticas para el manejo de acuerdos que implique con información interna de la empresa.
7	Gestión de Activos							
7.1	Responsabilidades sobre los activos							
7.1.1	Inventario de activos	Si	Es importante identificar los activos de acuerdo a su grado de importancia dentro de la Entidad, en la que se deja claro que el activo más relevante es la base de datos donde se registran los datos clínicos.			X	Jerarquizar la importancia de los activos al interior de la empresa.	Se debe clasificar los activos y establecerlos del nivel de importancia de los mismos.
7.1.2	Propietario de activos	Si	Cada activo dentro de la Entidad debe tener relacionado un responsable de la seguridad.		X		Tener responsables de los activos que forman parte de la empresa.	Se debe atribuir responsabilidades para los activos de información a través del área de gestión, como para activos físicos que formas parte de los SI.
7.1.3	Uso aceptable de los activos	Si	Las políticas sobre manejo de la información deben permitir tener claridad acerca del manejo adecuado de activos.		X		Definir políticas para el manejo de activos.	Determinar reglas de gestión de activos.
7.2	Clasificación de la información							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
7.2.1	Directrices de clasificación	Si	La información debe ser clasificada de acuerdo a su grado de importancia para establecer los controles adecuados para el manejo de la misma.		X		Identificar el nivel de importancia de los activos de información al interior de la empresa.	Se recomienda establecer prioridades en el manejo de la información
7.2.2	Etiquetado y manipulado de la información	Si	Cada tipo de información debe ser identificado para que cada persona conociendo su naturaleza respete su nivel de confidencialidad		X		Identificar el nivel de confidencialidad y acceso a la información.	Se debe fijar políticas para el acceso de la información.
8	Seguridad en los recursos Humanos							
8.1	Seguridad antes del empleo							
8.1.1	Funciones y responsabilidades	Si	Antes de contratar personal es necesario definir claramente el perfil y responsabilidades del cargo.			X	Contratar personal idóneo para ocupar un cargo determinado.	Se recomienda tener claridad en las políticas de contratación.
8.1.2	Investigación de antecedentes.	Si	Para contratar al personal se deben evaluar las cualidades profesionales, el nivel de ética y compromiso con la empresa.	X			Garantizar en los nuevos empleados tanto cualidades profesionales específicas como principios éticos.	Se recomienda tener claridad en las políticas de contratación.
8.1.3	Términos y condiciones de contratación.	Si	Es necesario que los nuevos empleados conozcan las políticas en cuanto a sus funciones y manejo del SI.			X	Establecer las reglas que debe seguir quien desee formar parte de la empresa.	Se recomienda tener claridad en las políticas de contratación.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
8.2	Seguridad en el desempeño de las funciones al interior de la empresa							
8.2.1	Responsabilidades de la dirección	Si	Se debe asegurar que las políticas diseñadas para el manejo de la información sean cumplidas por los empleados de la IPS MedicSalud		X		Garantizar que los empleados usen las políticas definidas por la empresa.	Se debe definir reglas acerca del manejo de la información acompañada de planes de capacitación.
8.2.2	Concienciación, formación y capacitación en seguridad de la información	Si	Todas las políticas de seguridad de la información deben ser conocidas al interior de la Entidad.			X	Dar a conocer las políticas de seguridad de la información.	Se recomienda planes de capacitación en política de seguridad de la información semestral
8.2.3	Proceso disciplinario.	Si	Las posibles sanciones por incumplimiento de las políticas de seguridad o el mal manejo de la información que pongan en riesgo la seguridad de la información deben ser conocidas por todos los empleados de la Empresa.			X	Dar a conocer las sanciones que acarrea el mal manejo de la información.	Se recomienda planes de capacitación en política de seguridad de la información semestral
8.3	Finalización o cambio de empleo							
8.3.1	Responsabilidad del cese o cambio	Si	Es necesario garantizar que después de la finalización de un contrato interno, la información que maneja esta persona no se vea afectada o divulgada.			X	Evitar impacto negativo en la información tras la salida de un empleado que tenga conocimiento sobre la misma.	Se debe implementar políticas de manejo de privilegios de la información.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para implementación de los controles
8.3.2	Devolución de activos	Si	Se deben tener protocolos que garanticen que un empleado haga entrega de los activos que tiene a su cargo.	X			Garantizar que los activos no se vean afectados tras la salida de un empleado de la empresa.	Se debe implementar mecanismo para la devolución de activos
8.3.3	Retirada de los derechos de acceso	Si	Se debe contar con procedimientos para revocar privilegios a personal que no requiera de los mimos.		X		Evitar niveles de acceso a la información inadecuados, que pongan en riesgo la seguridad de la misma.	Se debe implementar políticas de manejo de privilegios de la información.
9	Seguridad física y del ambiente							
9.1	Áreas Seguras							
9.1.1	Perímetro de seguridad física.	Si	Se debe garantizar la seguridad de las zonas que manejan información sensible (archivo físico, ubicación de servidores, equipos, almacenamiento copias de seguridad etc).			X	Asegurar las áreas que contengan información sensible	Implementar políticas de control de acceso físico a áreas que contiene información sensible.
9.1.2	Controles físicos de entrada.	Si	Sólo personal autorizado debe acceder a áreas que contengan activos sensibles. (Archivo histórico físico, almacenamiento de copias de seguridad, uso de servidor).		X		Restringir el acceso a áreas que contengan información sensible.	Implementar políticas de control de acceso físico a áreas que contiene información sensible.
9.1.3	Seguridad de oficinas, despachos e instalaciones.	Si	En oficinas al interior de la IPS MedicSalud se puede tener acceso a información sensible por lo cual se debe aplicar controles de seguridad		X		Garantizar la seguridad en oficinas y despachos.	Implementar políticas de control de acceso físico.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
9.1.4	Protección contra las amenazas externas y de origen ambiental.	Si	Se debe garantizar que ninguna amenaza ambiental externa pueda generar daño sobre la información.			X	Garantizar la protección contra amenazas ambientales externas.	Se recomienda protección contra factores atmosféricos como temperatura, humedad, etc.
9.1.5	Trabajo en áreas seguras.	Si	Las áreas sobre las que se desarrollan las actividades deben cumplir estándares de seguridad lo cual es muy importante tanto para equipos como para el personal.			X	Garantizar el desarrollo de las actividades sobre áreas seguras.	Se recomienda verificar el nivel de seguridad de las áreas de trabajo.
9.1.6	Áreas de acceso público y de carga y descarga.	Si	Las áreas como archivo histórico y ubicación de servidores se denominan áreas sensibles por la información que maneja, por tanto se debe evitar que terceros puedan llegar a tener acceso a esta.		X		Garantizar que el acceso a áreas sensibles dentro de la empresa tenga mecanismos de control.	Se debe tener control de acceso físico a determinadas áreas de la empresa.
9.2	Seguridad en equipos							
9.2.1	Emplazamiento y protección de equipos.	Si	Es necesario tener protecciones contra daños ambientales, especialmente para los servidores que se maneja al interior de la empresa.		X		Garantizar la integridad de los equipos al interior de la empresa.	Se debe establecer controles para el control de factores ambientales como humedad, polvo, etc.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
9.2.2	Instalaciones de suministro.	Si	La integridad de los equipos depende de los controles para la protección antes fallas eléctricas, ya un fallo de energía puede dejar inutilizable un equipo, dañar su disco duro etc.		X		Garantizar que fallos eléctricos no afecten la integridad de los equipos que forman parte del sistema de información.	Se debe implementar UPS.
9.2.3	Seguridad del cableado.	Si	Se debe garantizar que las redes de datos no vean afectada su integridad y confidencialidad de los datos que transportan.		X		Garantizar que las redes de datos no sean alteradas físicamente y no puedan ser interceptados los datos que se transportan a través de estas.	Se recomienda auditar e implementar los sistema de cableado existentes cada año.
9.2.4	Mantenimiento de los equipos.	Si	Se debe realizar mantenimiento periódico de los equipos como política interna de la empresa.		X		Garantizar la integridad y disponibilidad de los equipos.	Desarrollar e implementar planes de mantenimiento de equipos dentro de la empresa cada 6 meses.
9.2.5	Seguridad de los equipos fuera de las instalaciones.	No	Todo equipo que trabaje fuera de la empresa pero tenga injerencia interna debe tener reglas y restricciones de acceso.				Garantizar la seguridad al interior de la empresa al permitir acceso a equipos que trabajen fuera.	Aplicar controles de acceso a equipos externos que tengan que ver directamente con la actividad de la empresa (Acceso remoto derivado del teletrabajo)
9.2.6	Reutilización o retirada segura de equipos.	Si	Al dar de baja un equipo puede quedar almacenada información que puede comprometer la confidencialidad de la empresa.	X			Garantizar que ningún dato sensible o licencia sean expuestos a terceros tras un proceso de baja de equipos.	Establecer reglas para el proceso de retirada de equipos.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
9.2.7	Retirada de materiales propiedad de la empresa.	Si	Tanto las aplicaciones propias como de terceros que la empresa utiliza deben ser protegidas para evitar que puedan ser sacadas de la empresa.	X			Garantizar que ningún tipo de aplicación salga de la empresa.	Se debe fijar políticas sobre el manejo de aplicaciones y licencias al interior de la entidad.
10	Administración de comunicaciones y operaciones							
10.1	Procedimientos y responsabilidades operacionales							
10.1.1 1	Documentación de los procedimientos de operación.	Si	Para garantizar la continuidad de procesos se debe contar con bitácoras que permitan conocer los procedimientos operacionales especialmente los que tengan que ver con activos esenciales.			X	Garantizar la documentación de procesos operacionales.	Fijar políticas para documentación de procesos.
10.1.2 2	Gestión de cambios.	Si	Se debe tener claridad de quienes serán los encargados de realizar el proceso de administración de la información.			X	Gestionar los cambios de roles encargados de la administración de la información.	Implementar políticas de gestión de privilegios sobre la información.
10.1.3 3	Segregación de tareas.	Si	Sólo el personal autorizado debe tener acceso a la información.		X		Garantizar que un número reducido de personas tengan acceso a la información.	Implementar políticas de gestión de privilegios sobre la información.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.1.4 4	Separación de los recursos de desarrollo, prueba y operación.	Si	Cada área dentro de la empresa debe ser separada de acuerdo a sus funciones y competencias.	X			Reducir los riesgos de Acceso no autorizado a la información.	Establecer controles para el acceso de áreas seguros
10.2	Supervisión de los servicios prestados por terceros							
10.2.1	Provisión de servicios	No	Cualquier servicio subcontratado debe contar con políticas de seguridad de la información.				Garantizar que los servicios prestados por terceros cumplan con requerimientos mínimos de seguridad.	Se recomienda fijar políticas para la integración y control de sistemas de terceros dentro de la entidad.
10.2.2	Supervisión y revisión de los servicios prestados por terceros.	No	Cualquier servicio prestado por terceros debe ser controlado internamente mediantes procesos de autoridad.				Garantizar la calidad en la prestación de servicios ofrecidos por tercero.	Se recomienda fijar políticas para la integración y control de sistemas de terceros dentro de la entidad.
10.2.3	Gestión del cambio en los servicios prestados por terceros.	No	Cualquier cambio en los servicios prestados por terceros debe ser monitoreado constantemente.				Garantizar que los cambios en la prestación de servicio sean acordes con las necesidades y requerimientos de la empresa.	Se recomienda fijar políticas para la integración y control de sistemas de terceros dentro de la entidad.
10.3	Planificación y aceptación del sistema							
10.3.1	Gestión de capacidades.	Si	Es importante que dentro de las políticas sea planificado el crecimiento de la empresa para que los recursos sean acordes con el mismo.	X			Garantizar que los recursos con los que cuenta sean acordes con los requerimientos de la misma.	Se debe planificar recursos relacionado con las necesidades y proyecciones de crecimiento de la entidad de salud.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.3.2	Aceptación del sistema.	Si	Se debe definir la capacidad de integración de nuevos elementos al sistema, ya sea por actualización, renovación o totalmente nuevos.			X	Garantizar la compatibilidad de nuevos elementos en cuanto a sus dimensiones físicas y lógicas que garanticen la seguridad de la información.	Se debe fijar políticas para la integración de nuevos componentes al SI.
10.4	Protección contra software malicioso y código móvil.							
10.4.1	Controles contra el código malicioso.	Si	Se deben tener controles que garanticen que códigos maliciosos no terminen afectando el sistema.			X	Garantizar la seguridad en contra de amenazas lógicas al sistema de información.	Implementar métodos de seguridad para asegurar el control lógico del SI interno de la entidad de salud.
10.4.2	Controles contra el código descargado en el cliente.	No	Por seguridad no se autoriza el uso de código móvil.				NA	NA
10.5	Gestión interna de soportes y recuperación							
10.5.1	Copias de seguridad de la información.	Si	Respaldar la información garantiza que ante cualquier problema de seguridad se tendrá una fácil recuperación de la información. bases de datos, archivo de licencias, archivo de contabilidad, archivo de manejo técnico, ingenieros, documentos auxiliares, normativa), de acuerdo con la política de recuperación	X			Garantizar políticas de respaldo para el manejo de la información.	Se debe realizar copias de seguridad de la información cada 3, 4, 5 días o semanal.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.6	Gestión de redes							
10.6.1	Controles de red.	Si	Es necesaria que la red inalámbrica que maneja la empresa sea controlada.		X		Garantizar la protección de las redes contra ataques informáticos.	Se recomienda definir políticas de administración y uso de redes.
10.6.2	Seguridad de los servicios de red.	Si	Deben existir políticas que permitan la definición de acuerdos sobre el manejo de las redes.		X		Garantizar el uso adecuado de los recursos de red en cada nivel del servicio.	Se recomienda definir políticas de administración y uso de redes.
10.7	Utilización y seguridad de los soportes de información							
10.7.1	Gestión de soportes extraíbles.	Si	No se permite el uso de medios informáticos removibles para evitar fugas y amenazas que puedan contener información.		X		Garantizar que la información no sea extraída por los trabajadores de la empresa	Establecer reglas para que la información no sea extraída.
10.7.2	Retirada de soportes.	Si	Se debe contar con políticas que permitan eliminar de forma segura los soportes de información de la empresa. (Destrucción segura de elementos desde papel hasta discos duros.)		X		Evitar que información almacenada en medios que van a ser eliminados pueda quedar expuesta a terceros.	Establecer reglas para el manejo y destrucción de medios de almacenamiento.
10.7.3	Procedimientos de manipulación de la información.	Si	Se debe garantizar que la información en cualquier nivel sea manipulada y almacenada de forma segura.	X			Evitar que malas manipulaciones puedan dejar expuesta la información.	Establecer políticas para la manipulación y almacenamiento de la información.
10.7.4	Seguridad de la documentación del sistema.	Si	La documentación de los sistemas (información de proyectos y bases de datos) deben ser protegidos.		X		Garantizas la protección del activo más importante al interior de la empresa.	Fijar políticas relacionado al sistema de protección para la documentación del sistema informático.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.8	Intercambio de información y software							
10.8.1	Políticas y procedimientos de intercambio de información.	Si	Se debe garantizar que la información se encuentre segura al ser transportada haciendo uso de diferentes servicios de comunicación.	X			Garantizas la seguridad de la información al ser enviada por diferentes medios de comunicación.	Se debe desarrollar políticas y controles para el intercambio seguro de la información.
10.8.2	Acuerdos de intercambio.	Si	Se debe tener claridad de la forma como se puede compartir información al interior de la empresa.	X			Garantizar el intercambio seguro de información.	Se debe desarrollar políticas y controles para el intercambio seguro de la información.
10.8.3	Soportes físicos en tránsito.	Si	Se debe proteger la información durante el transporte de la misma			X	Garantizar la protección de la información al ser transportada.	Se debe llevar a cabo mecanismo de protección de la información como por ejemplo encriptación.
10.8.4	Mensajería electrónica.	Si	Se debe proteger la información contenida en correos electrónicos.	X			Garantizar que la información de mensajería electrónica se encuentre totalmente protegida.	Fijar modelos de protección para evitar acceso no autorizado a los servicios de mensajería.
10.8.5	Sistemas de información empresariales.	Si	Todos los sistemas de información tanto internos como externos deben estar conectados de forma segura.	X			Garantizar la conexión segura entre los sistemas de información.	Se debe definir políticas para el acceso a la información tanto a nivel interno como externo.
10.9	Servicios de comercio electrónico							
10.9.1	Comercio electrónico	Si	Se debe garantizar que la información involucrada en comercio sea protegida, por la naturaleza de la empresa esto se puede garantizar.				Proteger la información que es usada en comercio electrónico.	Definir mecanismo para la protección de la información involucrada en comercio electrónico.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.9.2	Transacciones en línea	Si	La información involucrada en procesos de transacciones electrónicas que maneja la empresa por su actividad económica deber ser protegida para evitar problemas de seguridad.			X	Garantizar la seguridad de la información involucrada en transacciones en línea.	Se recomiendas mecanismo de seguridad implementados para garantizar la seguridad de la información usada en transacciones en línea.
10.9.3	Información públicamente disponible	Si	La información que se maneja por aplicaciones de acceso público debe ser protegida.				Garantizar la integridad de la información disponible en sistemas de acceso público.	Se debe fijar políticas para la verificación de integridad de sistemas de información de acceso público.
10.10	Monitorización							
10.10.1	Registros de Auditoria	Si	Se deben tener registros de auditorías que permitan facilitar investigaciones futuras en caso de detectarse algún incidente de seguridad.			X	Contar con soportes de actividades para procesos de investigación asociados a los mismos.	Se recomienda implementar control de registro de actividad.
10.10.2	Supervisión del usos del sistema	Si	Se debe realizar monitoreo de cualquier cambio en los sistemas de información, revisando sus resultados. Revisar las actividades de monitoreo			X	Verificar la instalación de sistemas de información.	Se recomienda implementar control de registro de actividad.
10.10.3	Protección de la información de los registros	Si	Se debe tener control sobre los registros de actividad para que no puedan ser alterados (intentos forzosos o no autorizados)			X	Proteger los registros de actividad contra acciones de modificación de los mismos.	Se recomienda implementar control de registro de actividad.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
10.10.4	Registros de administración y operación.	Si	Es muy importante que la actividad de quienes tengan mayores privilegios sean monitoreados.			X	Garantizar que las acciones de tipo administrativo se realicen de forma adecuada.	Se recomienda implementar control de registro de actividad.
10.10.5	Registro de fallos.	Si	Se debe controlar cualquier avería que se presente en el sistema de información.			X	Garantizar la trazabilidad de averías en el sistema.	Definir reglas de control y gestión de fallas en el sistema.
10.10.6	Sincronización del reloj.	Si	Es muy importante que todos los sistemas estén sincronizados para que cualquier registro coincida en tiempos y se pueda hacer la trazabilidad del mismo.			X	Garantizar que todo el sistema esté sincronizado.	Definir políticas de implementación y control de registros de actividad.
11	Control de acceso							
11.1	Requisitos de negocio para control de accesos							
11.1.1	Política de control de acceso.	Si	Basado en los servicios que presta la entidad de salud que es las historias clínicas, se deben establecer políticas de control de acceso.		X		Controlar el acceso de acuerdo a las actividades que desarrolla la empresa.	Se recomienda definir políticas para el control de acceso teniendo en cuenta áreas críticas.
11.2	Gestión de acceso de usuario							
11.2.1	Registro de usuario.	Si	Es importante gestionar los usuarios para que sean asignados y dados de alta en el sistema sin generar problemas de seguridad.			X	Brindar o quitar acceso a usuarios basado en procedimientos propios de la empresa.	Se debe definir políticas para el ingreso o eliminación de usuarios del sistema.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
11.2.2	Gestión de privilegios.	Si	Se debe garantizar que cada usuario tenga acceso al sistema de información basado en privilegios.			X	Controlar los privilegios de acceso.	Se recomienda establecer políticas para el manejo de privilegios.
11.2.3	Gestión de contraseñas de usuario.	Si	Debe existir un procedimiento para la asignación de contraseñas al interior de la empresa.			X	Asignar contraseñas de forma segura.	Se debe definir políticas para asignar contraseñas.
11.2.4	Revisión de los derechos de acceso de usuario.	Si	Se debe verificar que los usuarios puedan acceder sólo a los sistemas que tienen permiso.			X	Verificar el acceso a sistemas de información.	Se debe fijar políticas para la verificación regular del acceso a sistemas de información.
11.3	Responsabilidades del usuario							
11.3.1	Uso de contraseñas.	Si	Se debe definir y verificar el uso de contraseñas seguras.		X		Controlar el uso de contraseñas seguras.	Se debe definir políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.
11.3.2	Equipo de usuario desatendido.	Si	Es importante que los servidores de los clientes tengan mecanismos de protección para los sistemas de la empresa que alojan en los mismos.		X		Garantizar la seguridad de las aplicaciones entregadas a los clientes.	Se debe definir políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.
11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	Si	Se debe evitar que por alguna razón quede expuesta información a la vista de terceros. Políticas para escritorios y monitores limpios de información			X	Garantizar que la información no sea expuesta a la vista de terceras personas.	Se debe definir políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
11.4	Control de acceso en red							
11.4.1	Política de uso de los servicios en red.	Si	Los clientes de los servicios de la empresa sólo podrán tener acceso a los servicios autorizados.			X	Garantizar el acceso a servicios autorizados.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.
11.4.2	Autenticación de usuario para conexiones externas.	NO	Tanto para clientes externos de servicios alojados en la empresa como para empleados con acceso remoto deben existir políticas de acceso adecuadas.				Garantizar el acceso remoto seguro.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.
11.4.3	Identificación de los equipos en las redes.	Si	Se debe garantizar conocer la procedencia de cualquier petición de servicio.			X	Garantizar que todas las conexiones establecidas sean seguras.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.
11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Si	El entorno de diagnóstico de la empresa debe estar protegido.			X	Proteger el sistema de diagnóstico de los sistemas de información.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.
11.4.5	Segregación de las redes.	Si	Se debe tener claramente definido el papel de cada usuario dentro de la red, asignándolo a un grupo determinado.		X		Garantizar la identificación de los usuarios en un grupo determinado.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.
11.4.6	Control de la conexión a la red.	Si	El acceso a los sistemas internos de la empresa debe estar limitado para que no se puedan usar servicios que pongan en juego la seguridad.		X		Restringir el acceso a servicios de red desde ubicaciones externas.	Se recomienda establecer políticas de acceso a servicios ofrecidos por la entidad.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
11.4.7	Control de encaminamiento (routing) de red.	Si	Se debe controlar el enrutamiento de información.			X	Garantizar que la información de la empresa no use rutas que pongan en peligro su integridad.	Se debe definir políticas de enrutamiento de la información.
11.5	Control de acceso al sistema operativo							
11.5.1	Procedimientos seguros de inicio de sesión.	Si	Se debe controlar el acceso a los sistemas operativos con los procedimientos adecuados.			X	Controlar el acceso al SO con procedimientos seguros.	Se debe definir políticas de acceso a los S.O.
11.5.2	Identificación y autenticación de usuario.	Si	Deben existir mecanismos de identificación únicos para los usuarios.			X	Garantizar que los usuarios tengan credenciales únicas de acceso.	Se debe definir políticas de gestión de credenciales de usuarios.
11.5.3	Sistema de gestión de contraseñas.	Si	Se debe garantizar que los sistemas de gestión de contraseñas sean eficientes.			X	Garantizar la eficiencia y seguridad en los sistemas de gestión de contraseñas.	Se debe definir políticas de gestión de credenciales de usuarios.
11.5.4	Uso de los recursos del sistema.	Si	Se debe controlar el uso de aplicaciones administrativas seguras que pueden ser usadas para generar algún tipo de daño al sistema.			X	Realizar control sobre el uso de aplicaciones administrativas.	Se debe fijar políticas de uso de aplicaciones de carácter administrativo propias del sistema.
11.5.5	Desconexión automática de sesión.	Si	Se debe controlar el tiempo de inactividad del equipo.			X	Garantizar el bloqueo de equipos tras cierto tiempo de inactividad.	Se debe definir políticas de acceso a los S.O.
11.5.6	Limitación del tiempo de conexión.	Si	Se debe controlar el tiempo de conexión al SO basado en el uso de aplicaciones.			X	Controlar el uso del sistema operativo	Se debe definir políticas de acceso a los S.O.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
11.6	Control de acceso a las Aplicaciones							
11.6.1	Restricción del acceso a la información.	Si	Se debe restringir el acceso a los sistemas en especial al programa que maneja la base de datos, genera licencia, reportes, notificaciones, citaciones y estado de cada proyecto.		X		Generar restricciones a la gestión de aplicaciones.	Fijar políticas acerca de controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan entornos diferentes.
11.6.2	Aislamiento de sistemas sensibles.	Si	Los sistemas sensibles como copias de seguridad, archivo físico y servidores deben estar aislados		X		Garantizar que los sistemas sensibles de la empresa tengan un entorno informático propio.	Fijar políticas acerca de controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan entornos diferentes.
11.7	Informática móvil y tele trabajo							
11.7.1	Ordenadores portátiles y comunicaciones móviles.	Si	La conexión a través de red inalámbrica hace necesario la definición de políticas de protección en cuenta a recursos móviles.				Brindar protección contra riesgos derivados del uso de recursos móviles.	Se debe diseñar políticas para el manejo de riesgos derivados de la informática móvil.
11.7.2	Teletrabajo.	NO	Ya que se considera el teletrabajo al interior de la empresa es necesario considerar políticas y procedimientos tanto para acceso como para cumplimiento de funciones.				Garantizar el desempeño seguro y eficiente de actividades de teletrabajo.	Se debe diseñar políticas para la gestión del teletrabajo en la entidad MedicSalud.
12	Adquisición, desarrollo y mantenimiento de SI							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
12.1	Requisitos de seguridad de los sistemas							
12.1.1	Análisis y especificación de los requisitos de seguridad	Si	Es importante que todo nuevo sistema de seguridad especifique los controles necesarios para su implementación.			X	Garantizar que todo nuevo sistema incluya controles de seguridad.	Definir políticas de seguridad para la integración de sistema de información.
12.2	Seguridad de las aplicaciones del sistema	Si	Las aplicaciones del sistema deben brindar seguridad.			X	Garantizar seguridad en las aplicaciones del sistema.	Definir políticas de seguridad para las aplicaciones.
12.2.1	Validación de los datos de entrada.	Si	Cualquier acceso debe ser validado para garantizar que se esté haciendo desde una aplicación confiable.			X	Garantizar la seguridad del acceso a las aplicaciones.	Definir políticas de seguridad para las aplicaciones.
12.2.2	Control del procesamiento interno.	Si	Se deben verificar las aplicaciones para detectar alteraciones en la información.			X	Garantizar que la información no haya sido modificada durante el procesamiento o de forma deliberada.	Definir políticas de seguridad para las aplicaciones.
12.2.3	Integridad de los mensajes.	Si	Se debe asegurar la autenticidad de la información en los mensajes en las aplicaciones.			X	Garantizar que los mensajes en las aplicaciones no sean modificados.	Definir políticas de seguridad para las aplicaciones.
12.2.4	Validación de los datos de salida.	Si	Se debe garantizar la correcta funcionalidad de la aplicación al arrojar los datos esperados.			X	Garantizar la integridad de la información de salida de la aplicación.	Definir políticas de seguridad para las aplicaciones.
12.3	Controles criptográficos							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
12.3.1	Política de uso de los controles criptográficos.	No	Es necesario contar con políticas de protección de la información al ser entregada al usuario.				Garantizar la confidencialidad de la información	Se recomienda definir políticas de protección de la información.
12.3..2	Gestión de claves.	No	Se debe gestionar adecuadamente las claves como por ejemplo haciendo uso de un PKI.				Garantizar la gestión adecuada de claves al interior de la empresa.	Se recomienda definir políticas de protección de la información.
12.4	Seguridad de los ficheros del sistema							
12.4.11	Control del software en explotación.	No	Es necesario controlar la instalación de software de tal manera que responda a las necesidades de la empresa.				Controlar la instalación de software.	Se recomienda definir políticas para la instalación de software y modificación de ficheros del sistema.
12.4.22	Protección de los datos de prueba del sistema.	No	Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.				Proteger la información empleada en el entorno de pruebas.	Se recomienda definir políticas para la protección de códigos fuente y archivos del sistema.
12.4.33	Control de acceso al código fuente de los programas.	No	Se debería restringir el acceso al código fuente de los programas				Garantizar la protección del código fuente de aplicaciones desarrolladas por la empresa.	Se recomienda definir políticas para la protección de códigos fuente y archivos del sistema.
12.5	Seguridad en los procesos de desarrollo y soporte							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
12.5.1 1	Procedimientos de control de cambios.	Si	Se debe tener control de versiones de aplicaciones para que los cambios sean realizados conforme a necesidades reales de la empresa.			X	Garantizar que los cambios respondan a procedimientos formales dentro de la empresa.	Definir políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.
12.5.2 2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Si	Se debe revisar la funcionalidad de las aplicaciones tras realizar cambios en el Sistema Operativo para no crear conflictos		X		Garantizar que un cambio en el SO no afecte el funcionamiento de las aplicaciones.	Definir políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.
12.5.3 3	Restricciones s a los cambios en los paquetes de software.	Si	Se debe tener control de cualquier modificación en el software de la empresa.	X			Garantizar el adecuado funcionamiento de las aplicaciones.	Definir políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.
12.5.4	Fugas de información.	Si	Se debe garantizar la confidencialidad de la información referente a aplicaciones como programa licenciador, base de datos, licencias etc.		X		Garantizar la confidencialidad de la información.	Definir políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.
12.5.5	Externalización del desarrollo de software.	No	Si se contrata desarrollo de software a la medida es importante realizar monitorización para evitar incidentes en el manejo.				NA	NA
12.6	Gestión de las vulnerabilidades técnicas							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
12.6.1	Control de Vulnerabilidades técnicas	Si	Se debe estar verificando constantemente las vulnerabilidades que puedan presentar los sistemas o tecnologías usadas dentro de la IPS MedicSalud.			X	Garantizar la protección contra vulnerabilidades de los sistemas empleados en la empresa.	Se debe definir políticas para la gestión de vulnerabilidad es de aplicaciones o sistemas usados por la empresa.
13	Gestión de incidentes de seguridad de la información							
13.1	Comunicación de eventos y debilidades en la seguridad de la información							
13.1.1	Notificación de los eventos de seguridad de la información.	Si	Se deben disponer canales que permitan dar a conocer eventos de seguridad que afecten la seguridad de la empresa.		X		Garantizar la pronta solución a eventos de seguridad presentes en la empresa.	Se debe establecer políticas para la gestión de incidentes en la seguridad de la información.
13.1.2	Notificación de puntos débiles de seguridad.	SI	Se deben definir mecanismos para que todas las personas que tengan que ver con el sistema de información puedan reportar incidentes de seguridad.		X		Garantizar la rápida solución de incidentes informáticos.	Se debe establecer políticas para la gestión de incidentes en la seguridad de la información.
13.2	Gestión de incidentes y mejoras en la seguridad de la información							

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
13.2.1	Responsabilidades y procedimientos.	Si	Se debe establecer quién es el responsable de manejar determinado tipo de incidente para que sea mucha más rápida la respuesta.		X		Definir responsables para la gestión de eventos de seguridad.	Se debe establecer políticas para la gestión de incidentes en la seguridad de la información.
13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Si	Se debe poder establecer el costo de un evento de seguridad de la información.		X		Determinar el costo de un evento de seguridad informática.	Se debe establecer políticas para la gestión de incidentes en la seguridad de la información.
13.2.3	Recopilación de evidencias.	Si	Se deben tener mecanismos para determinar la forma como se debe actuar contra personas que se les compruebe la generación de eventos de seguridad informática.			X	Definir medidas en contra de quienes generen eventos de seguridad informática.	Se debe establecer políticas para la gestión de incidentes en la seguridad de la información.
14	Gestión de continuidad del negocio							
14.1	Aspectos de la gestión de continuidad del negocio							
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Si	Es necesario contar con procesos de seguridad de la información que aseguren la continuidad del negocio al interior de la empresa.		X		Contar con procedimientos de seguridad de la información que garanticen la continuidad del negocio.	Se recomienda establecer políticas de seguridad de la información que garanticen la continuidad del negocio.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
14.1.2	Continuidad del negocio y evaluación de riesgos.	Si	Es necesario tener claridad de los eventos que pueden afectar el negocio y el impacto de los mismos.			X	Tener claridad del grado de afectación sobre el negocio de un evento determinado.	Se recomienda establecer políticas de seguridad de la información que garanticen la continuidad del negocio.
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la Información.	Si	Es muy importante contar con planes de contingencia que permitan la recuperación del negocio ante cualquier evento que ponga en riesgo la información.			X	Tener planes de contingencia ante eventos informáticos.	Se recomienda establecer políticas de seguridad de la información que garanticen la continuidad del negocio.
14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	Si	Es ideal tener estandarizado el esquema del plan de continuidad para garantizar su fácil aplicabilidad en la empresa.			X	Contar con un plan de continuidad estandarizado.	Se recomienda establecer políticas de seguridad de la información que garanticen la continuidad del negocio.
14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Si	Se deben evaluar los planes de continuidad garantizando que evoluciones con los requerimientos del negocio.			X	Garantizar que los planes de continuidad evolucionen en concordancia con los requerimientos del negocio.	Se recomienda establecer políticas de seguridad de la información que garanticen la continuidad del negocio.
15	Conformidad							
15.1	Conformidad con los requisitos legales							
15.1.1	Identificación de la legislación aplicable.	Si	Es muy importante que la empresa sea consciente de sus obligaciones legales para garantizar el cumplimiento de esta.			X	Alinear los sistemas de información con los requerimientos legales.	Se debe establecer políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
15.1.22	Derechos de propiedad intelectual (DPI).	Si	Se debe garantizar el uso de cualquier material u software de acuerdo a las licencias definidas para los mismos.		X		Garantizar el uso de software debidamente licenciado y contenidos respetando los derechos de autor.	Se debe establecer políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.
15.1.3	Protección de los documentos de la organización	Si	Se debe garantizar la integridad de los registros importantes para evitar cualquier pérdida de información.		X		Definir mecanismos para garantizar la integridad de los registros importantes de carácter legal.	Se debe establecer políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.
15.1.4	Protección de datos y privacidad de la información de carácter personal.	Si	Debe garantizar la protección de los datos en concordancia con requerimientos de carácter legal y que mucha de la información que maneja tiene esta característica.		X		Brindar protección de los datos de acuerdo a requerimientos de carácter legal.	Se debe fijar políticas de protección de información alineadas con requerimientos de carácter legal.
15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.	Si	Se debe garantizar que los recursos empleados para el tratamiento de la información sean dedicados sólo a este fin.		X		Garantizar el uso exclusivo de los sistemas de tratamiento de la información para este propósito.	Fijar políticas para la gestión de los sistemas de información.
15.1.6	Regulación de los controles criptográficos.	No	Los controles empleados deben estar cifrados para asegurar su concordancia con la legislación vigente teniendo en cuenta el tipo de información que se maneja.				Garantizar la confidencialidad de los controles de seguridad y su concordancia con la legislación.	Fijar políticas para la gestión de los sistemas de información.

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/No)	Justificación de elección/ no elección	TI	PI	P	Objetivos del control	Recomendaciones de actividades para la implementación de los controles
15.2	Revisiones de la política de seguridad y de la conformidad técnica							
15.2.1	Cumplimiento de las políticas y normas de seguridad.	Si	Cada director de área debe asegurarse de que los procedimientos de seguridad se realicen adecuadamente.			X	Garantizar la adecuada realización de los procedimientos de seguridad en cada área de la empresa.	Se recomienda revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.
15.2.2	Comprobación del cumplimiento o técnico.	Si	Es importante que los procedimientos de seguridad estén en concordancia con los estándares definidos para los mismos.			X	Garantizar la alineación entre procedimientos de seguridad y estándares.	Se recomienda revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.
15.3	Consideraciones sobre la auditoría de sistemas							
15.3.1	Controles de auditoria de los sistemas de información	Si	Es muy importante tener control sobre los procedimientos de auditoría desarrollados al interior de la empresa sobre sistemas en funcionamiento.			X	Evitar que procedimientos de auditoría terminen sacando de funcionamiento algún sistema importante dentro de la empresa.	Se debe definir políticas para el desarrollo de procesos de auditoria.
15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Si	Se deben tener control sobre el acceso a herramientas de auditoría ya que muchas pueden comprometer la seguridad al interior de la empresa.			X	Establecer políticas para el desarrollo de procesos de auditoria.	Se debe definir políticas para el desarrollo de procesos de auditoria.

Fuentes: ISO/MEC/IEC 27001, Anexo A y complementado.

7.2.5.3 Plan del tratamiento de riesgo.

El objetivo primordial es el de establecer responsabilidades sobre la aplicación de la declaración de aplicabilidad del SGSI, definiendo además las medidas necesarias para mitigar o minimizar el riesgo.

7.2.5.3.1 Roles y responsabilidades relacionados con seguridad de la información.

La seguridad de la información es un área amplia que afecta a toda la institución prestadora de salud, por esta razón se hace necesario describir los roles y responsabilidades que se relacionan a continuación:

Tabla 19. Definición de roles y responsabilidades

Rol	Responsabilidad
Administradora y gerente	• Establece la política del SGSI. • Se asegura que se establezcan los objetivos y planes del SGSI. • Establece funciones y responsabilidades de seguridad de la información. • Asegura la integración de los requisitos del SGSI en los procesos de la organización. • Asegurar que el SGSI logre los resultados previstos. • Dirige y apoya a las personas, para contribuir a la eficacia del SGSI. • Apoya otros roles para demostrar liderazgo aplicado a sus áreas de responsabilidad. • Establece y mantiene un compromiso con el proceso de medición. • Comunica la importancia de cumplir los objetivos de seguridad de la información de conformidad con la política, responsabilidades de ley y mejora continua. • Responsable de la visión, toma de decisiones estratégicas y coordinación de las actividades

	para dirigir y controlar la organización. • Aprueba la política de gestión de incidentes de seguridad de la información. • Provee los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI. • Decidir sobre los criterios de aceptación y niveles de riesgos. • Asegurarse que se efectúan auditorías internas de SGSI. • Garantiza que la seguridad de la información se aborde adecuadamente en toda la organización. • Compromiso con el esquema de gestión de incidentes de seguridad de la información. • Efectuar revisión por la dirección del SGSI.
Jefe de seguridad de la información (Actual jefe de sistemas)	• Responsabilidad y gobierno de la seguridad de la información, que asegura el manejo correcto de los activos de información. • Asesora al equipo de la alta dirección, proporciona soporte especializado al personal de la organización y asegura que los límites del estado de seguridad de la información estén disponibles. • Asegura el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. • Asegura que la información recibe un nivel apropiado de protección, de acuerdo
Parte involucrada	• La parte involucrada se define aquí principalmente como las personas por fuera de las operaciones normales, tales como la parte administrativa, usuarios, entidades de salud relacionadas con la salud en Colombia.

Seguridad física (Celadores)	• Responsable de la seguridad física e instalaciones. • Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la entidad de salud.

Fuente: El autor

7.2.5.3.2 Listado de procedimientos preventivos.

Con el fin de buscar reducir el riesgo, se hacen algunas recomendaciones para la IPS Medicsalud.

- Se debe garantizar una temperatura adecuada para el buen funcionamiento del equipo.

- La temperatura será especificada de acuerdo al dispositivo e indicada en el manual del respectivo elemento.

- La ubicación de los equipos debe ser preferiblemente en lugares donde existan paredes de concreto.

- No se deben ubicar papeleras de basura en los recintos destinados como cuartos de telecomunicaciones, ya que se pueden convertir en yesca de un posible incendio.

- El personal que tiene a cargo la administración de la red, debe tener claro los tipos de incendio que se pueden presentar y diseñar los controles tanto preventivo como correctivo para cada caso.

- Se deben tener extintores de polvo químico seco y de bióxido de carbono en lugares visibles y cercanos a donde se encuentran ubicados los equipos.

- Se debe capacitar al personal sobre el manejo de los diferentes extintores con que se cuenta.

- Dar el adecuado uso a los diferentes elementos evitando siempre prácticas inseguras.

- No fumar en lugares donde se concentra los equipos como centro de cómputos, cuarto de comunicaciones.

- Nunca consumir alimentos ni ingerir bebidas cerca de los equipos.

- No manipule equipos en estado de embriaguez ni bajo efecto de sustancias alucinógenas.

- Controlar el acceso de paquetes al centro de cómputo y cuarto de comunicaciones.

- Tener una excelente distribución eléctrica, evitando conectar los equipos a una misma fuente.

- Evitar extensiones y cables sueltos cerca a los equipos.

- Instalar alarmas de activación manual o automáticas en caso de presentarse incendio, inundación, sobrecalentamiento de equipos.

- Evitar la acumulación de la energía estática referenciando todos los equipos a una misma tierra.

- Todos los equipos deben tener protección contra cortocircuitos y sobre voltaje ya sea interna o externa.

- Tener pólizas de seguros vigentes de los elementos que conforman la red corporativa.

- No ubicar aparatos eléctricos dentro del centro de cómputo y cuarto de comunicaciones tales como grabadoras, hornos microondas, licuadoras, televisores y demás.

- Verificar diariamente el correcto funcionamiento de las lámparas y tomacorrientes ubicados en el centro de cómputo.

- Colocar los equipos en un cuarto de telecomunicaciones o centro de cómputo, donde se concentre la mayoría de equipos de comunicaciones.

- La ubicación debe ser en un sitio interior, de alta seguridad, no tener ventanales y no existir tuberías alrededor.

- Los equipos sólo debe ser manipulados por el personal que tenga los suficientes conocimientos acerca de ellos.

- Permitir solo el acceso de personas que realicen labores de operación y mantenimiento de los equipos.

- Mantener información en archivos e impresa de los proveedores y garantías vigentes de todos los equipos utilizados en la red.

- Tener información actualizada de las diferentes empresas que prestan servicios de soporte y mantenimiento de los equipos.

- Realizar un contrato y mantenerlo vigente con una empresa prestadora del servicio de soporte y mantenimiento en redes de datos.

- Comprar seguros a los equipos de la red, que cubran daños, actos mal intencionados, hurto.

- Guardar en un archivo tanto dentro como fuera de la IPS Medicsalud la información sobre la configuración inicial de todos los equipos.

- Destinar un sitio seguro y de acceso restringido para guardar manuales, software de instalación (Cds, Diskettes), documentación de los equipos, ejerciendo un estricto control sobre su uso.

- Tener copia de cada uno de los manuales y software, evitando al máximo el uso de originales.

- No se debe tener más del 20% del tráfico sostenido por segmento, este número podría disminuir de acuerdo al tipo de aplicaciones que se manejen en el segmento.

- Capacitar continuamente al personal de sistemas en temas de relacionados con tecnología de punta.

- Tener un sistema de energía regulada alterno que entre a operar en el momento que falle el suministro actual.

- Cualquier falla en el hardware o software llamar inmediatamente al proveedor o a la empresa.

8. PRODUCTO A ENTREGAR

El Producto Final entregado será la implementación de un manual SGSI para minimizar los riesgos que se ve expuestos la información y establecer controles necesarios para la prevención de riesgos y vulnerabilidades que afecten al sistema de información de la IPS Medicsalud. También vemos que habrá cambio rotundos en el proceso administrativo de la IPS Medicsalud de acuerdo con lo establecido por la norma SGSI todo con la finalidad para tener una gestión en el sistema de información integral, confiable y segura.

9. RECURSOS NECESARIOS PARA EL DESARROLLO

Los recursos necesarios para llevar a cabo la investigación son:

9.1 RECURSOS HUMANOS

- Ingeniero de sistemas
- Tutor del proyecto
- Personal administrativo y asistencial

9.2 RECURSOS FISICO

- El proyecto se desarrollara en la IPS Medicsalud de la ciudad Valledupar – cesar.

9.3 RECURSOS TECNOLÓGICOS

- Portátil
- Memoria USB
- Internet
- Software

9.4 RECURSOS FINANCIERO

Tabla 20. Recursos Financieros del Proyecto

Rubros	Valor Mensual	Valor Total (por 6 meses)
Internet	$41000	$246000
Servicio de Luz	$35000	$210000
Equipo		$1400000
Materiales	$10000	$60000
Transporte	$30000	$180000
Imprevistos (en caso de necesitar adquisición de material complementario)		$40000
Total		$2136000

Fuente: El autor.

10. CRONOGRAMA DE ACTIVIDADES

Figura 3. Cronograma propuesto para el SGSI

No.	Actividades	Mes	Septiembre				Octubre				Noviembre				Diciembre			
		Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
		Duración (Semanas)																
1	Realizar un análisis del estado actual de seguridad de la información de la IPS Medicsalud de Valledupar.	2																
2	Identificar los activos dentro de los límites de alcance del SGSI	2																
3	Determinar las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos de información del área de sistemas.	3																
4	Evaluar los riesgos a los que se ve expuesto el sistema de información, generando planes de acción que permitan mitigar o eliminar estos, bajo el SGSI	2																
6	Diseñar un manual del Sistema de Gestión de la Seguridad Informática con los controles para la gestión de riesgo implementados en las políticas institucionales y los procedimientos de trabajo en el área informática.	3																
7	Entrega del proyecto y en espera de correcciones	2																
8	Entrega del trabajo final para sustentar	2																

Fuente: El autor

11. CONCLUSIÓN

En algunas Instituciones Prestadoras de Servicios en Salud no se están rigiendo por ninguna norma de estandarización o modelo como lo son la norma ISO 27001 y la norma ISO 17000 que brindan una guía para el establecimiento e implementación adecuada de la seguridad informática.

Paralelamente se pudo observar que en las IPS donde hay políticas de seguridad establecidas no se ha realizado socializaciones o difusión de una forma adecuada ni, en la parte asistencial ni en la administrativa lo que acarrea desconocimiento y malas prácticas en la utilización de los sistemas informáticos.

Por otra parte se detectó que los usuarios tanto administrativos como asistenciales en la IPS MedicSalud no tienen claro el concepto de seguridad informática, por consiguiente no lo aplican. Lo anterior conlleva a que no dimensionen la importancia del tema y los problemas que pueden ocasionar su mal uso de los entornos tecnológicos.

12. RESULTADOS E IMPACTOS

12.1 RESULTADOS OBTENIDOS DURANTE EL DESARROLLO DEL PROYECTO:

- Los objetivos, el alcance y la política del sistema de gestión de seguridad de la información.
- Los roles y responsabilidad en cuanto a la seguridad de la información.
- La relación del SGSI se hizo con el análisis de las partes interesadas y las necesidades de la entidad.
- La realización de la metodología para el análisis y valorización de riesgo y clasificación de los activos de información.
- Inventarios de los activos informático por medio de la metodología de clasificación y valorización de los activos.
- Informe del análisis de riesgos del sistema de información por medio de la aplicación de la metodología del análisis y evaluación de riesgos.
- El plan de tratamiento de riesgos el cual tiene las acciones requeridas para la gestión de riesgos del proceso de gestión informática y tecnológica.
- Diagnóstico del cumplimento de los controles establecidos por la norma ISO/IEC 27001:2013 y las acciones para cerrar las brechas de seguridad para la gestión tecnológica de la entidad.
- El manual de las políticas del SI.
- Procedimientos para la gestión de incidentes de seguridad de la información en la empresa.

12.2 IMPACTOS

El sistemas de información de la entidad IPS MedicSalud lo que se quiere hacer es diseñar y establecer las norma ISO/IEC 27001:2013 para que la seguridad de la información soportada en la empresa apoye los objetivos estratégicos de calidad.

En este proyecto los objetivos fijados para el establecimiento de un sistema de seguridad adecuado para la entidad de salud están orientados para obtener los siguientes beneficios que son:

- Garantizar su misión y alcanzar su visión: El diseño y establecimiento de un SGSI en la entidad proveerá los mecanismos necesarios para el aseguramiento óptimo de la información. Lo cual proveerá efectivamente las gestiones administrativa, financiera, operativa y técnica de la entidad de salud para garantizar su misión y alcanzar su visión.

- Mejora la imagen de la entidad: un sistema de gestión de seguridad de la información le proveerá a la entidad de salud la metodología de gestión de riesgo adecuada lo cual mejora la imagen de las partes interesadas que identifica clasifica, valora y trata los riesgos que presenta la entidad por lo tanto genera confianza entre las partes para la seguridad de la información de la empresa.

- Disminuir costos: un SGSI puede generar un impacto positivo en la gestión financiera de la empresa debido a que los colaboradores puede gestionar los riesgos eficientemente en los activos fundamentales que provee el sistema informático de la entidad y así evitar inversiones innecesarias en seguridad y tecnologías a la entidad si no estar concentrado en una sola parte donde es más débil y amenazado los activos donde está alojado y concentrado el sistema base de la empresa.

- Cumplimiento normativo: sistema de información de seguridad de información de la entidad permite observar la seguridad real del sistema de información empresarial, ver las amenazas que afectan a la entidad para aplicar las acciones efectivas para mitigarlas, darle seguridad a la información personal de sus clientes para dar cumplimiento a la normatividad vigente relacionada con la seguridad del sistema de información.

13. BIBLIOGRAFÍA

DALTABUIT GODÁS, Enrique, HERNÁNDEZ AUDELO, Leobardo, MALLÉN FULLERTON, Guillermo y VÁZQUEZ GÓMEZ, José de Jesús. (2007) La seguridad de la información. México. Limusa.

Empresas colombianas no están preparadas antes Riesgos Informáticos {En línea} {22 de Abril de 2016} Disponible en: www.colombiadigital.net/actualidad/noticias/item/8168-organizaciones-colombianas-no-estan-preparadas-ante-riesgos-informaticos.html

GARCÍA, Alfonso. Hurtado Cervigón. Alegre Ramos, María del Pilar. (2011) Seguridad informática. Madrid – España: Paraninfo SA.

Gestión de proyecto de software {En línea} {22 de Abril de 2016} Disponible en: http://ocw.unican.es/ensenanzas-tecnicas/gestion-de-proyectos-software/otros-recursos-1/GP-t5-magerit.pdf

ISO 27001: El método MAGERIT {En línea} {22 de Abril de 2016} Disponible en: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

La norma ISO/27001 para las empresas municipales de Cali, EMCALI E.I.C.E-ESP {En línea} {25 de Abril de 2016} Disponible en: http://bdigital.uao.edu.co/bitstream/10614/5327/1/TIS01678.pdf

Metodología de Implantación de un SGSI en un grupo empresarial jerárquico {En línea} {25 de Abril de 2016} Disponible en: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Modelo PDCA, Instituto Nacional de Tecnologías de la Comunicación, España {En línea} {25 de Abril de 2016} Disponible en:

http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Modelos_PDCA_SGSI/#modelo

Modelo PDCA ISO 27000, Instituto Uruguayo de normas técnicas, 2012 {En línea} {25 de Abril de 2016} Disponible en: http://www.unit.org.uy/iso27000/iso27000.php?&imprimir=1

REGUEIRO, Arturo. (2009). Autoridades de Certificación y Confianza Digital. Consultado el 4 de mayo de 2012 {En línea} {28 de Abril de 2016} Disponible en: http://www.fundaciondike.org.ar/seguridad/firmadigital-autoridades.html

Sistema de Administración de controles de seguridad informática basado en ISO/IEC 27002. {En línea} {28 de Abril de 2016} Disponible en: http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

SUMMERS, Rita C. (1996). Seguridad informática: Amenazas y Salvaguardias. México: McGraw-Hill Companies.

Tesis sobre Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana Sede Guayaquil {En línea} {28 de Abril de 2016} Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

Tesis acerca de implementación de un sistema de gestión de seguridad informática en la confederación de cámara de comercio – CONFECAMARAS {En línea} {03 de Mayo de 2016} Disponible en: http://repository.unad.edu.co/handle/10596/3653

Tesis sobre diseño de un sistema de gestión de la información mediante la aplicación de la norma ISO/IEC 27001:2013 en la oficina de sistema de información y telecomunicaciones de la universidad de córdoba {En línea} {03 de Mayo de 2016} Disponible en: http://repository.unad.edu.co/handle/10596/3649

ANEXOS

ANEXO A

ENCUESTA PARA EL PERSONAL DE LA PARTE ADMINISTRATIVA Y ASISTENCIAL DE LA IPS MEDISALUD DE LA CIUDAD DE VALLEDUPAR

Como contratista de la IPS MedicSalud, le solicitamos responder esta sencilla encuesta con el fin de mejorar los procesos y mitigar los riesgos de la Seguridad de la Información.

La encuesta tiene duración de 17 minutos.

Como personal administrativo o asistencial de la IPS MedicSalud y en su experiencia marque con una X su respuesta en la letra correspondiente:

1. ¿A la pregunta si conoce o ha escuchado sobre Seguridad Informática?

SI_____ NO_____

2. ¿A la pregunta Qué tan importante les parece la seguridad informática?

a) Alto

b) Medio

c) Bajo

d) No importante

3. ¿Con que frecuencia se cambian las contraseñas del equipo de cómputo a su cargo?

a) Cada mes

b) Entre 2 y 6 meses

c) Dos veces al año

d) Nunca

4. Usted como personal administrativo o asistencial de la IPS Medisalud califique las siguientes afirmaciones:

Dónde: 1) Malo 2) Aceptable 3) Bueno 4) Excelente

	1	2	3	4
a) Actualización de software permanente	_____	_____	_____	_____
b) Respaldo de Backups	_____	_____	_____	_____
c) Conocimiento sobre las responsabilidades para el manejo de información.	_____	_____	_____	___
d) La ubicación de los servidores se encuentran aislados y seguros	_____	_____	_____	_____
e) Cambio de contraseñas periódicamente	_____	_____	_____	_____

5. Usted tiene claras las políticas de seguridad en cuanto el correo electrónico (Eliminar usuario, crear, cambio de contraseñas)

SI_____ NO_____

6. ¿Usted tiene conocimientos sobre las políticas de seguridad de la información y de esta forma mitigar riesgos de la misma?

SI_____ NO_____

7. ¿Las dificultades que usted ha encontrado en su equipo de cómputo influyen en el tiempo utilizado y en la calidad de su trabajo?

SI_____ NO_____

8. Las incidencias o requerimientos que se presentan en el equipo de cómputo que tiene a su cargo son:

Dónde: 1) Siempre 2) Alguna Vez 3) Nunca

	1	2	3
a) El equipo de cómputo se bloquea con frecuencia	___	___	___
b) El equipo de cómputo no se conecta a la red	___	___	___
c) El equipo de cómputo es lento	___	___	___

9. ¿Con que frecuencia utiliza Internet?

a) Una vez al día

b) Varias veces al día

c) Todo el tiempo

10. ¿Usted considera que las dificultades presentadas en el equipo de cómputo influyen en la atención al cliente?

SI_____ NO_____

11. ¿Usted ha tenido problemas en el momento de utilizar el equipo de cómputo?

SI_____ NO_____

12. ¿A la pregunta sobre si conocen las políticas de seguridad implementadas por las universidades?

SI_____ NO_____

Observaciones:_____
_____
_____
_____
_____
_____

ANEXO B

RESUMEN ANALÍTICO EDUCATIVO (RAE)

Título de la Investigación
DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA IPS MEDICSALUD DE LA CIUDAD DE VALLEDUPAR – CESAR
Autor
Ronal Liñan Cordero
Publicación Lugar y Año de Publicación y Edición
Lugar: Valledupar, Colombia Año: 2017
Unidad Patrocinante
Universidad Nacional Abierta y a Distancia - UNAD
Descripción de la investigación:
Tesis de Grado
Palabras Clave o descriptores
SGSI, Metodología Magerit, Políticas, Controles, Riesgos, Amenazas, Vulnerabilidades, MedicSalud.
Problema que aborda la investigación:
Carencia de un diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 para el sistema de información en la IPS MedicSalud Valledupar – cesar, donde se pueda gestionar los riesgos por medio de una serie de controles y políticas establecidos para la empresa.
Objetivos de la investigación:
Objetivo General Realizar un diagnóstico del estado actual de la seguridad de la información basada en la norma ISO 27001:2013 que le brinde a la IPS MEDICSALUD el contexto de cómo está tratando la seguridad de la información y las mejoras que se pueden implementar en sus procesos. Objetivos específicos: • Identificar los procedimientos actuales de la IPS MEDICSALUD para la ejecución de sus actividades. • Identificar y valorar los activos de información de la IPS MEDICSALUD. • Identificar los posibles riesgos de los activos de información, sus vulnerabilidades y amenazas, así como su probabilidad de ocurrencia y el impacto de los mismos. • Presentar el diagnóstico del estado actual de la seguridad de la información de la IPS MEDICSALUD con sus respectivas recomendaciones de mejora y de implementación basado en la norma ISO 27001:2013.

Duración investigación:
Desarrollo el proyecto de tesis en mención, tomo aproximadamente doce (12) meses.
Hipótesis planteada por la investigación:
Contenidos:
El diagnostico de un sistema de información basado en el estándar IEC/ISO 27001 dará las condiciones necesarias para la gobernabilidad, oportunidad y viabilidad para la seguridad de la información con el enfoque para proteger la información de la empresa tanto en la parte financiera, administrativa, operativa de la empresa y con ella asegurar el cumplimiento del objetivo. La diagnosticación del SGSI basado en la norma ISO 27001 en la entidad garantiza la disponibilidad, integridad y confidencialidad de la información. La propuesta de esta norma para su posterior aplicación facilitara a la entidad el control seguro de la información para tener un rendimiento óptimo y un porcentaje mínimo de errores. La IPS MedicSalud de Valledupar pretende que la información manejada por la entidad referente al estudio, tramite, y archivo sobre la información clínica del paciente; esté debidamente protegida con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información. La gerente es el responsable de la implementación de los requerimientos de seguridad con el fin de proteger la información por lo tanto en su organización se debe elaborar un análisis y evaluación del riesgo para gestionarlos adecuadamente y disminuir eventos indeseados. La metodología de evaluación del riesgo que se elige es la metodología Magerit para el análisis y gestión de los de riesgos porque: • Los pasos para su ejecución están claramente definidos. • La documentación es clara, amplia y permite realizar una identificación adecuada del entorno donde va a ser aplicada. • Permite enfocar los esfuerzos al análisis de riesgos críticos para la empresa, por lo tanto se puede trabajar más claramente en las posibles soluciones para dichos riesgos. • Se puede decir que por estar incluida en los estándares ISO, sirve como como punto de partida para procesos de certificación y mejoramiento del sistema de gestión para la empresa. • Permite el análisis a riesgos, donde se identifican y valoran los diferentes componentes que pueden tener los riesgos. • Permite la minimización de riesgos mediante la implementación de medidas de seguridad. • MAGERIT le permita una empresa saber cuánto valor está en juego y le ayudará a protegerlo.

Contenidos:

- Con MAGERIT los resultados de análisis de riesgos se pueden expresar en valores cualitativos y cuantitativos, lo que permite a los directivos tomar decisiones.

Según MAGERIT: El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados estos pasos son:
Paso 1: Inventario de Activos
Paso 2: Valoración de los activos
Paso 3: Amenazas (identificación y valoración)
Paso 4: Salvaguardias
Paso 5: Impacto residual y riesgo residual
Resultados del análisis de riesgos

Después de haber realizado el análisis de riesgos de los activos de información de la IPS MEDICSALUD se procederá a reducir o eliminar estos riesgos bajo planes de acción mediante especificación de políticas y objetivos de la seguridad del área informática a través de la norma ISO/IEC 27002

Con el fin de minimizar los riesgos encontrados en cada dependencia de la IPS MEDICSALUD se define las políticas y objetivos establecidos para brindar la seguridad de información de manera eficaz y óptima.

Por último se aplica la declaración de aplicabilidad para la IPS MedicSalud donde se ha tenido en cuenta los siguientes documentos: Los 133 controles sugeridos en el Anexo A de la norma ISO 27001, las política de Seguridad de la Información, la evaluación y tratamiento de riesgos y el Informe de evaluación y tratamiento de riesgos. Una vez identificados los riesgos la declaración de aplicabilidad permite identificar los controles necesarios documentando si cada uno de estos controles es aplicable o no o si ya está implementado o no.
La declaración de aplicabilidad se realizó sobre el análisis de riesgos teniendo en cuenta los siguientes parámetros:

- Dominio: Que indica el número del control de acuerdo al anexo A de la Norma ISO/IEC 27001.
- Controles según la ISO/IEC 27001: Se identifica el nombre del control
- Aplicabilidad: Se identifica si es o no es aplicable a la IPS MedicSalud.
- Justificación: Explica porque es o no es aplicable dicho control.
- Estado del control.
- Objetivo del Control
- Recomendaciones de actividades para la implementación del control

Tipo de Investigación

El proyecto es una Tesis, un documento escrito y extenso, donde se presentan los temas objeto de estudio abordados en el desarrollo del proyecto del SGSI de acuerdo a la metodología Magerit y el estudio de políticas y controles a aplicar; también se presentan herramientas de medición y el análisis del resultado obtenido al aplicar encuestas y entrevistas.

Población y muestra
Ciudad: IPS MedicSalud de Valledupar País: Colombia Población: Funcionarios de la IPS MedicSalud
Técnicas de Investigación
Obtención, revisión y análisis de Documentos, Entrevistas y Encuestas.
Instrumentos de investigación
Consultas en la web, artículos, metadatos, libros, encuestas, entrevistas, análisis documental.
Metodología y estrategias seguidas por la investigación:
Metodología MAGERIT: se basa en un ciclo de 5 pasos: inventario de activos, valoración de los activos, amenazas (identificación y valoración), salvaguardias, impacto residual y riesgo residual, Resultados del análisis de riesgos. Es normalmente utilizada en la implementación de sistemas de gestión de la calidad lo cual es la mayor probabilidad exitosa para el sistema de información.
Argumentos expuestos por el autor:
• La empresa debe establecer directrices o actos administrativos que permitan reglamentar la gestión de la Información que se encuentra al interior de la IPS MedicSalud de Valledupar. • Diseñar dentro del SGSI el Plan de continuidad del negocio. • Desarrollar una Declaración de Aplicabilidad (SoA), con el propósito de que de acuerdo al riesgo identificado y analizado que permitan mitigar, transferir, compartir y aceptar el riesgo; en este documento se deben registrar los controles de seguridad que son aplicables (necesarios), los cuales deben ser verificados para comprobar si se encuentran operando o no. • La IPS MedicSalud debe realizar campañas de sensibilización y estrategias de comunicación interna sobre Seguridad, tratamiento y niveles de confidencialidad de la Información para el sistema de información de la empresa lo cual ayudara a mitigar y prevenir posibles robo de información a los que actualmente se encuentra expuesta la entidad.
Conclusiones de la investigación:
• En algunas Instituciones Prestadoras de Servicios en Salud no se están rigiendo por ninguna norma de estandarización o modelo como lo son la norma ISO 27001 y la norma ISO 17000 que brindan una guía para el establecimiento e implementación adecuada de la seguridad informática. • Paralelamente se pudo observar que en las IPS donde hay políticas de seguridad establecidas no se ha realizado socializaciones o difusión de una forma adecuada ni, en la parte asistencial ni en la administrativa lo que acarrea desconocimiento y malas prácticas en la utilización de los sistemas informáticos. • Por otra parte se detectó que los usuarios tanto administrativos como asistenciales en la IPS MedicSalud no tienen claro el concepto de seguridad informática, por consiguiente no lo aplican. Lo anterior conlleva a que no dimensionen la importancia del tema y los problemas que pueden ocasionar su mal uso de los entornos tecnológicos.

Bibliografía:

DALTABUIT GODÁS, Enrique, HERNÁNDEZ AUDELO, Leobardo, MALLÉN FULLERTON, Guillermo y VÁZQUEZ GÓMEZ, José de Jesús. (2007) La seguridad de la información. México. Limusa.

Empresas colombianas no están preparadas antes Riesgos Informáticos {En línea} {22 de Abril de 2016} Disponible en: www.colombiadigital.net/actualidad/noticias/item/8168-organizaciones-colombianas-no-estan-preparadas-ante-riesgos-informaticos.html

GARCÍA, Alfonso. Hurtado Cervigón. Alegre Ramos, María del Pilar. (2011) Seguridad informática. Madrid – España: Paraninfo SA.

Gestión de proyecto de software {En línea} {22 de Abril de 2016} Disponible en: http://ocw.unican.es/ensenanzas-tecnicas/gestion-de-proyectos-software/otros-recursos-1/GP-t5-magerit.pdf

ISO 27001: El método MAGERIT {En línea} {22 de Abril de 2016} Disponible en: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

La norma ISO/27001 para las empresas municipales de Cali, EMCALI E.I.C.E-ESP {En línea} {25 de Abril de 2016} Disponible en: http://bdigital.uao.edu.co/bitstream/10614/5327/1/TIS01678.pdf

Metodología de Implantación de un SGSI en un grupo empresarial jerárquico {En línea} {25 de Abril de 2016} Disponible en: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Modelo PDCA, Instituto Nacional de Tecnologías de la Comunicación, España {En línea} {25 de Abril de 2016} Disponible en: http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Modelos_PDCA_SGSI/#modelo

Modelo PDCA ISO 27000, Instituto Uruguayo de normas técnicas, 2012 {En línea} {25 de Abril de 2016} Disponible en: http://www.unit.org.uy/iso27000/iso27000.php?&imprimir=1

REGUEIRO, Arturo. (2009). Autoridades de Certificación y Confianza Digital. Consultado el 4 de mayo de 2012 {En línea} {28 de Abril de 2016} Disponible en: http://www.fundaciondike.org.ar/seguridad/firmadigital-autoridades.html

Sistema de Administración de controles de seguridad informática basado en ISO/IEC 27002. {En línea} {28 de Abril de 2016} Disponible en: http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

SUMMERS, Rita C. (1996). Seguridad informática: Amenazas y Salvaguardias. México: McGraw-Hill Companies.

Tesis sobre Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana Sede Guayaquil {En línea} {28 de Abril de 2016} Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

Tesis acerca de implementación de un sistema de gestión de seguridad informática en la confederación de cámara de comercio – CONFECAMARAS {En línea} {03 de Mayo de 2016} Disponible en: http://repository.unad.edu.co/handle/10596/3653

Tesis sobre diseño de un sistema de gestión de la información mediante la aplicación de la norma ISO/IEC 27001:2013 en la oficina de sistema de información y telecomunicaciones de la universidad de córdoba {En línea} {03 de Mayo de 2016} Disponible en: http://repository.unad.edu.co/handle/10596/3649

Preparado por:

RONAL LIÑAN CORDERO

Teléfono - Email

Teléfono: 3016793862

E-mail: Ronald_0731@hotmail.com

Analista del RAE:

RONAL LIÑAN CORDERO

Fecha de diligenciamiento

Valledupar, Diciembre 02 de 2016